FACULTAD DE POSGRADOS

# PROPUESTA DE UN MODELO DE GOBIERNO DE TECNOLOGÍA DE LA INFORMACIÓN PARA HOSPITALES PÚBLICOS. CASO: HOSPITAL GENERAL DOCENTE DE CALDERÓN.

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Magister en Gerencia de Sistemas y Tecnologías de la Información.


Profesor Guía

MSc. Robert Arturo Enríquez Reyes

Autor

Darwin Marcelo Pillo Guanoluisa


Año

2017

## DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los trabajos de titulación”.

…….....

Robert Arturo Enríquez Reyes

Magister en Gestión de las Comunicaciones y Tecnologías de la Información

CI: 1708600240

**DECLARACIÓN DEL PROFESOR CORRECTOR**

“Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

…….....

Marco Vinicio Vásquez Chávez

Maestro en Administración

CI: 1707997746

## DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

……

Darwin Marcelo Pillo Guanoluisa

CI: 1003319660

AGRADECIMIENTOS

Agradezco a Dios por su infinito amor y misericordia al brindarme salud y la capacidad para cumplir este sueño.

Agradezco a mi Familia y Novia por su apoyo incondicional en cada paso que doy en la vida. Son mi ejemplo e inspiración para cada día seguir adelante y querer ser mejor.

A mi tutor el MSc. Enríquez Reyes Robert Arturo, por su oportuno consejo y guía para sacar este proyecto adelante.

DEDICATORIA

A mi Familia por su apoyo incondicional en cada paso que doy en la vida. Son mi ejemplo e inspiración para cada día seguir adelante y querer ser mejor.

A mi Novia que ha sido motivo de inspiración para cumplir con mis sueños y alcanzar mis metas, ella con sus actos desmedidos de amor ha provocado en mí una felicidad indescriptible, compartiendo conmigo los buenos y malos momentos.

En gran parte este logro es

## RESUMEN

El incremento del presupuesto fiscal destinado para el sector salud ha colaborado considerablemente para el desarrollo de programas de salud y el aumento de la infraestructura hospitalaria pública, sean estos hospitales nuevos o repotenciados. Dentro de la inversión en infraestructura hospitalaria consta el gasto en la parte de Tecnología de la Información, considerando a TI como un aliado para aumentar la eficiencia y mejorar la calidad en la prestación de cuidados de la salud. Actualmente los hospitales públicos requieren cumplir con sus objetivos estratégicos y desarrollar su misión y visión social a través de prestar con eficiencia su cartera de servicios médicos.

Considerando lo anterior, este trabajo de tesis presenta un modelo de Gobierno de TI para hospitales públicos del Ecuador, para asegurar el logro de los objetivos del Hospital a través de TI, alineando los objetivos de TI con los objetivos estratégicos del Hospital, creando valor (Realización de beneficios, optimización de riesgos y recursos) para los interesados; A medida que las organizaciones de salud se vuelven cada vez más dependientes de TI, los eventos de pérdida de integridad, disponibilidad y confidencialidad de la información, puede producir un significativo impacto en el aspecto clínico de los pacientes y en los servicios que presta la organización. Por lo tanto el modelo propuesto de Gobierno de TI tiene un enfoque en la Seguridad de la Información.

En el desarrollo del presente trabajo de tesis, se realiza una revisión del marco legal y normativo relacionado al derecho a la salud en el Ecuador, así mismo se analiza la inversión pública en salud por parte del Estado. Posteriormente se realiza una investigación acerca de estándares internacionales y marcos de trabajo enfocados al Gobierno de TI y la Seguridad de la Información sanitaria.

Posteriormente, a través del uso de buenas prácticas en la Gestión de Proyectos, marco de referencia de Gobierno de TI y normas para la Gestión de

Seguridad de la Información se desarrolla el modelo Gobierno de TI con énfasis en la Seguridad de la Información. La validación del modelo propuesto se aplica en el Hospital General Docente de Calderón.

## ABSTRACT

The increase in the fiscal budget allocated to the health sector has contributed considerably to the development of health programs and the increase of public hospital infrastructure, whether these are new or refurbished hospitals. Within the investment in hospital infrastructure is spending on Information Technology and Communication, considering IT as an ally to increase efficiency and improve the quality of health care delivery. Public hospitals nowadays need to fulfill their strategic objectives and develop their mission and social vision through efficiently rendering their portfolio of medical services.

Considering the above, this thesis presents an IT Governance model for public hospitals in Ecuador, to ensure the achievement of hospital objectives through IT, aligning IT objectives with the hospital's strategic objectives, creating value (Realization of benefits, optimization of risks and resources) for the interested parties; As health organizations become increasingly dependent on IT, events of loss of integrity, availability and confidentiality of information can have a significant impact on the clinical aspect of patients and on the services provided by the organization. Therefore the proposed IT Governance model has a focus on Information Security.

In the development of this thesis, a review of the legal and regulatory framework related to the right to health in Ecuador is carried out, as well as the public investment in health by the State. Subsequently an investigation is made on international standards and frameworks of work focused on IT Governance and health Information Security.

Subsequently, through the use of good practices in project management, IT Governance frameworks and standards for Information Security Management, the IT Governance model is developed with an emphasis on Information Security. The proposed model is validated in the General Hospital of Calderón.

# ÍNDICE

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# INTRODUCCIÓN

El establecimiento de preasignaciones presupuestarias y el derecho a la salud garantizado en la Constitución de la República del año 2008, ha impulsado el desarrollo de programas de salud y el aumento de la infraestructura hospitalaria pública, sean estos hospitales nuevos o repotenciados. Dentro de la inversión en infraestructura hospitalaria consta el gasto en la parte de Tecnología de la Información, considerando a TI como un aliado para aumentar la eficiencia y mejorar la calidad en la prestación de cuidados de la salud. Actualmente los hospitales públicos nuevos o repotenciados requieren cumplir con sus objetivos estratégicos y desarrollar su misión y visión social a través de prestar con eficiencia su cartera de servicios médicos.

Para asegurar el logro de los objetivos del hospital a través de TI, es necesario alinear los objetivos de TI con los objetivos estratégicos del hospital, creando valor (realización de beneficios, optimización de riesgos y recursos) para los interesados. Por lo cual este trabajo de titulación presenta un modelo de Gobierno de TI para hospitales públicos del Ecuador mediante el uso de marcos de referencia y buenas prácticas de la industria.

El uso de las Tecnologías de la Información dentro de las organizaciones del sector sanitario ha proporcionado grandes beneficios para el sector; sin embargo, esto también ha generado nuevos desafíos. Uno de estos desafíos, está relacionado con proteger la seguridad y privacidad de la información personal sobre la salud, creando la necesidad de que el modelo de Gobierno de TI propuesto tenga un enfoque en la Seguridad de la Información. Para lo cual se revisaran las Normas, Leyes y Regulaciones para la Seguridad de la Información aplicable al sector sanitario.

Finalmente, para validar el modelo de Gobierno de TI con enfoque en la Seguridad de la Información, se aplica en el Hospital General Docente de Calderón, para obtener una visión clara del nivel de capacidad en que se

encuentra los procesos del hospital y permita definir los planes de acción para cerrar las brechas y alcanzar el estado deseado.

## Objetivos

### Objetivo General

Proponer un modelo de Gobierno y Gestión de Tecnología de la Información con énfasis en seguridad de la información para hospitales públicos del Ecuador, como caso de estudio el Hospital General Docente de Calderón, mediante el uso de modelos, estándares y normas que permitan alinear los objetivos de TI con los objetivos estratégicos del hospital, permitiéndoles desarrollar su misión y visión social.

### Objetivo Específicos

1. Describir el marco legal y normativo que posee el Ecuador con respecto al derecho a la salud, así como también la inversión realizada por el Estado desde el año 2008 al 2015, que permita conocer la situación actual del sector sanitario en el Ecuador.

2. Realizar una revisión bibliográfica de los estándares, modelos y buenas prácticas enfocados al Gobierno de TI, aplicable para los hospitales públicos del Ecuador.

3. Describir los estándares, normas y reglamentos para la seguridad de la información aplicable al sector sanitario, que permita brindar confidencialidad, integridad y disponibilidad a la información de los hospitales públicos del Ecuador.

4. Proponer un modelo de Gobierno de TI para hospitales públicos del Ecuador con énfasis en seguridad de la información, que proporcione los

elementos necesarios para efectuar una gestión efectiva de TI y posibilite a los hospitales a cumplir con sus objetivos y desarrollar su misión y visión social.

5. Identificar los procesos principales de Gobierno y Gestión de TI de los hospitales públicos del Ecuador, que permita a las casas de salud alinear sus objetivos estratégicos con TI apoyando el uso adecuado de recursos, disminución de costos y riesgos.

6. Realizar una descripción general del Hospital General Docente de Calderón, que permita conocer la situación actual de la organización, como caso de estudio del presente trabajo de titulación.

7. Validar el modelo de Gobierno de TI propuesto, en el Hospital General Docente de Calderón para que las tecnologías de la información puedan aportar de forma estratégica al cumplimiento de los objetivos institucionales, apalancados en los procesos de Gobierno y Gestión de TI.

# 1 Capítulo I. La Salud en el Ecuador

## 1.1 Sector de la Salud en el Ecuador

El Ecuador cuenta con un amplio marco legal y normativo relacionado al derecho a la salud, siendo la Constitución de la República del año 2008 uno de los principales instrumentos legales para un nuevo modelo que fortalezca el Sistema Nacional de Salud (SNS) en el país.

La salud es un derecho garantizado por el Estado para que toda persona alcance el nivel más alto posible de salud física y mental y los mecanismos para su realización, según la actual Constitución que en el artículo 32, de la sección séptima sobre la salud, dice:

> Art. 32.- La salud es un derecho que garantiza el Estado, cuya realización se vincula al ejercicio de otros derechos, entre ellos el derecho al agua, la alimentación, la educación, la cultura física, el trabajo, la seguridad social, los ambientes sanos y otros que sustentan el buen vivir. (Constitución de la República del Ecuador, 2008, pág. 17).

Además, la Constitución de la República del Ecuador hace referencia al establecimiento del Sistema Nacional de Salud, señalando sus principios y componentes, también la conformación de la red pública integral de salud, en donde los servicios estatales serán universales y gratuitos en todos los niveles de atención. Fortalece además la rectoría del Ministerio de Salud como autoridad sanitaria nacional del SNS, según indican los artículos 358, 359, 360, 361 y 362 de la sección segunda sobre la salud:

> Art. 358.- El Sistema Nacional de Salud tendrá por finalidad el desarrollo, protección y recuperación de las capacidades y potencialidades para una vida saludable e integral, tanto individual como colectiva, y reconocerá la diversidad social y cultural. El sistema se guiará por los

> principios generales del sistema nacional de inclusión y equidad social, y por los de bioética, suficiencia e interculturalidad, con enfoque de género y generacional. (Constitución de la República del Ecuador, 2008, pág. 112).
>
> Art. 359.- El Sistema Nacional de Salud comprenderá las instituciones, programas, políticas, recursos, acciones y actores en salud; abarcará todas las dimensiones del derecho a la salud; garantizará la promoción, prevención, recuperación y rehabilitación en todos los niveles; y propiciará la participación ciudadana y el control social (Constitución de la República del Ecuador, 2008, pág. 112).
>
> Art. 360.- El sistema garantizará, a través de las instituciones que lo conforman, la promoción de la salud, prevención y (...).
>
> La red pública integral de salud que será parte del Sistema Nacional de Salud y estará conformada por el conjunto articulado de establecimientos estatales, de la seguridad social y con otros proveedores que pertenecen al Estado, con vínculos jurídicos, operativos y de complementariedad (Constitución de la República del Ecuador, 2008, pág. 112).
>
> Art. 361.- El Estado ejercerá la rectoría del sistema a través de la autoridad sanitaria nacional, será responsable de formular la política nacional de salud, y normará, regulará y controlará todas las actividades relacionadas con la salud, así como el funcionamiento de las entidades del sector (Constitución de la República del Ecuador, 2008, pág. 112).

En la cuestión del financiamiento para el sector salud, la Constitución de la República del Ecuador especifica que los recursos para salud provendrán del Presupuesto General del Estado y garantiza el financiamiento en salud por parte del Estado a través de una pre-asignación presupuestaria, según delinea

el artículo 366 de la sección segunda sobre la salud y 298 de la sección cuarta sobre el Presupuesto General del Estado:

> Art. 366.- El financiamiento público en salud será oportuno, regular y suficiente, y deberá provenir de fuentes permanentes del Presupuesto General del Estado. Los recursos públicos serán distribuidos con base en criterios de población y en las necesidades de salud.
>
> El Estado financiará a las instituciones estatales de salud y podrá apoyar financieramente a las autónomas y privadas siempre que no tengan fines de lucro (…) (Constitución de la República del Ecuador, 2008, pág. 114).

> Art. 298.- Se establecen preasignaciones presupuestarias destinados a los Gobiernos Autónomos Descentralizados, al sector salud, al sector educación, a la educación superior; y a la investigación, ciencia, tecnología e innovación en los términos previstos en la ley. Las transferencias correspondientes a preasignaciones serán predecibles y automáticas. Se prohíbe crear otras preasignaciones presupuestarias (Constitución de la República del Ecuador, 2008, pág. 96).

Después, a través de la vigésima segunda enmienda constitucional indica que “El Presupuesto General del Estado destinado al financiamiento del Sistema Nacional de Salud, se incrementará cada año en un porcentaje no inferior al cero punto cinco por ciento del PIB, hasta alcanzar al menos el cuatro por ciento” (Constitución de la República del Ecuador, 2008, pág. 138).

Las políticas impulsadas en el Gobierno de Alianza País y lideradas por el Presidente del Ecuador electo para el periodo 2007 - 2011 el Economista Rafael Correa Delgado, se concretaron con la Constitución del 2008, que en el sector salud se complementa también con la Ley Orgánica del Sistema Nacional de Salud (LOSNS) vigente desde el año 2002 y los objetivos del Plan

Nacional del Buen Vivir que se constituye en un instrumento de planificación nacional y de política pública.

## 1.2 El Sistema Nacional de Salud en el Ecuador

En el Ecuador la salud como derecho está ratificada en el Sistema Nacional de Salud (SNS) inscrito en la Constitución de la República del Ecuador y expuesto en la Ley Orgánica del Sistema Nacional de Salud (LOSNS) como lo señala el Artículo 2:

> Art. 2.- El Sistema Nacional de Salud tiene por finalidad mejorar el nivel de salud y vida de la población ecuatoriana y hacer efectivo el ejercicio del derecho a la salud. Estará constituido por las entidades públicas, privadas, autónomas y comunitarias del sector salud, que se articulan funcionalmente sobre la base de principios, políticas, objetivos y normas comunes. (Ministerio de Salud Pública, 2012).

La LOSNS tiene como propósito establecer los principios y normas generales para la organización y funcionamiento del SNS que regirá en todo el territorio nacional, éste sistema tiene como objetivo mejorar el nivel de salud y vida de la población ecuatoriana y hacer efectivo el ejercicio del derecho a la salud. En el cuadro a continuación se detallan las cinco funciones fundamentales que ejerce el SNS:

| FUNCIONES DEL SISTEMA NACIONAL DE SALUD | | | | |
|---|---|---|---|---|
| **RECTORÍA** | **COORDINACIÓN** | **PROVISIÓN DE SERVICIOS** | **ASEGURAMIENTO** | **FINANCIAMIENTO** |
| El Estado garantizará la rectoría del sistema a través de la Autoridad Sanitaria Nacional, será responsable de formular la política nacional de salud, y normará, regulará y controlará todas las actividades relacionadas con la salud, así como el funcionamiento de las entidades del sector. | Es la función del sistema que coordina el relacionamiento entre las demás funciones y entre los integrantes del Sistema. Su ejercicio es competencia del Ministerio de Salud Pública, en todos sus niveles, como autoridad sanitaria nacional, apoyado por los Consejos de Salud. | La provisión de servicios de salud es plural y con participación coordinada de las instituciones prestadoras. El Sistema establecerá los mecanismos para que las instituciones garanticen su operación en redes y aseguren la calidad, continuidad y complementariedad de la atención. | Es la garantía de acceso universal y equitativo de la población al Plan Integral de Salud en cumplimiento al derecho ciudadano a la protección social en salud. Se promoverá la ampliación de cobertura de salud de todas las entidades prestadores de servicios y del Seguro General Obligatorio y Seguro Social Campesino, pertenecientes al IESS, de otros seguros públicos, como el Issfa e Isspol. | El financiamiento es la garantía de disponibilidad y sostenibilidad de los recursos financieros necesarios para la cobertura universal en salud de la población. El Consejo Nacional de Salud establecerá mecanismos que permitan la asignación equitativa y solidaria de los recursos financieros entre grupos sociales, provincias y cantones del país, así como su uso eficiente. |
| Constitución de la República del Ecuador Art. 361 | Ley Orgánica del Sistema Nacional de Salud Art. 10 | Ley Orgánica del Sistema Nacional de Salud Art.11 | Ley Orgánica del Sistema Nacional de Salud Art.12 | Ley Orgánica del Sistema Nacional de Salud Art.13 |

Figura 1. Funciones del Sistema Nacional de Salud.
Tomado de (Flores Ma. & Castillo A., 2012, pág. 6).

El SNS del Ecuador está compuesto por instituciones del sector público, privado y mixto, que actúan en el sector de la salud, o en campos directamente relacionados con ella. En el siguiente cuadro se listan las diecisiete entidades que forman parte del SNS.

| | |
|---|---|
| **1.** | Ministerio de Salud Pública y sus entidades adscritas. |
| **2.** | Ministerios que participan en el campo de la salud. |
| **3.** | El Instituto Ecuatoriano de Seguridad Social, IESS; Instituto de Seguridad Social de las Fuerzas Armadas, Issfa; e Instituto de Seguridad Social de la Policía Nacional, Isspol. |
| **4.** | Organizaciones de salud de la Fuerza Pública: Fuerzas Armadas y Policía Nacional. |
| **5.** | Las Facultades y Escuelas de Ciencias Médicas y de la Salud de las Universidades y Escuelas Politécnicas. |
| **6.** | Junta de Beneficencia de Guayaquil. |
| **7.** | Sociedad de Lucha Contra el Cáncer, Solca. |
| **8.** | Cruz Roja Ecuatoriana. |
| **9.** | Organismos seccionales: Consejos Provinciales, Concejos Municipales y Juntas Parroquiales. |
| **10.** | Entidades de salud privadas con fines de lucro: prestadoras de servicios, de medicina prepagada y aseguradoras. |
| **11.** | Entidades de salud privadas sin fines de lucro: organizaciones no gubernamentales (ONG), servicios pastorales y fiscomisionales. |
| **12.** | Servicios comunitarios de salud y agentes de la medicina tradicional y alternativa. |
| **13.** | Organizaciones que trabajan en salud ambiental. |
| **14.** | Centros de desarrollo de ciencia y tecnología en salud. |
| **15.** | Organizaciones comunitarias que actúen en promoción y defensa de la salud. |
| **16.** | Organizaciones gremiales de profesionales y trabajadores de la salud. |
| **17.** | Otros organismos de carácter público, del régimen dependiente o autónomo y de carácter privado que actúen en el campo de la salud. |

Figura 2. Entidades que forman parte del Sistema Nacional de Salud.
Tomado de (Flores Ma. & Castillo A., 2012, pág. 7).

Mediante el ejercicio de las instituciones que pertenecen al SNS, se busca cumplir con cinco objetivos principales, como menciona la LOSNS en su artículo 3:

- Garantizar el acceso equitativo y universal a servicios de atención integral de salud, a través del funcionamiento de una red de servicios de gestión desconcentrada y descentralizada.
- Proteger integralmente a las personas de los riesgos y daños a la salud; al medio ambiente de su deterioro o alteración.
- Generar entornos, estilos y condiciones de vida saludables.
- Promover la coordinación, la complementación y el desarrollo de las instituciones del sector.
- Incorporar la participación ciudadana en la planificación y veeduría en todos los niveles y ámbitos de acción del Sistema Nacional de Salud. (Ministerio de Salud Pública, 2012).

Acorde a lo que estipula el artículo 10 de la LOSNS y el artículo 361 de la Constitución de la República del Ecuador, el Ministerio de Salud Pública creada desde el 16 de junio de 1967 por una Asamblea Nacional Constituyente tiene como misión:

> Ejercer la rectoría, regulación, planificación, coordinación, control y gestión de la Salud Pública ecuatoriana a través de la gobernanza y vigilancia y control sanitario y garantizar el derecho a la salud a través de la provisión de servicios de atención individual, prevención de enfermedades, promoción de la salud e igualdad, la gobernanza de salud, investigación y desarrollo de la ciencia y tecnología; articulación de los actores del sistema, con el fin de garantizar el derecho a la salud. (Ministerio de Salud Pública, 2016).

En la actualidad el Ministerio de Salud Pública, gracias a la reforma y reestructuración del sector salud tiene como finalidad alcanzar la eficiencia y

equidad en materia de salud pública, considerando que para ello maneja recursos económicos del Presupuesto General del Estado, mismo que deben ser utilizados para cumplir con lo que señala las Constitución de la República y el Plan Nacional del Buen Vivir, de tal forma que pueda cubrir con la demanda de la población en todos los niveles.

## 1.3 Objetivos y políticas del Plan Nacional de Desarrollo del Ecuador vinculados al sector Salud

El Plan Nacional de Desarrollo (PND) es el instrumento formal y legal al cual se sujetarán las políticas, programas y proyectos públicos que permitan la consecución de los objetivos del Buen Vivir y la garantía de derechos establecidos en la Constitución del 2008. Según la disposición constitucional contenida en el artículo 280 de la sección sobre régimen de desarrollo:

> El Plan Nacional de Desarrollo [hoy denominado Plan Nacional para el Buen Vivir] es el instrumento al que se sujetarán las políticas, programas y proyectos públicos; la programación y ejecución del presupuesto del Estado; y la inversión y la asignación de los recursos públicos; y coordinará las competencias exclusivas entre el Estado central y los Gobiernos Autónomos Descentralizados. Su observancia será de carácter obligatorio para el sector público e indicativo para los demás sectores. (Constitución de la República del Ecuador, 2008, págs. 91-92)

El Buen Vivir es un principio plasmado en la Constitución, que recoge una visión del mundo centrada en el ser humano, como parte de un entorno natural y social, en donde el Buen Vivir se define como:

> La satisfacción de las necesidades, la consecución de una calidad de vida y muerte digna, el amar y ser amado, el florecimiento saludable de todos y todas, en paz y armonía con la naturaleza y la prolongación indefinida de las culturas humanas. El Buen Vivir supone tener tiempo

> libre para la contemplación y la emancipación, total libertades y oportunidades (…).
> (Secretaría Nacional de Planificación y Desarrollo, 2009)

El ejercicio pleno de los derechos del Buen Vivir: agua, alimentación, salud, educación y vivienda, son algunos de los prerrequisitos para lograr una mejor calidad de vida en la población, como lo establece el artículo 66 de la Constitución “El derecho a una vida digna, que asegure la salud, alimentación y nutrición, agua potable, vivienda, saneamiento ambiental, educación, trabajo, empleo, descanso y ocio, cultura física, vestido, seguridad social y otros servicios sociales necesarios” (Constitución de la República del Ecuador, 2008, pág. 29).

El Buen Vivir y la salud no tienen un sentido netamente individual sino colectivo, evitando enfocarse solo en el aspecto curativo, sino que abarque contextos amplios y den soluciones globales sobre el estado mental y físico de las personas. Es decir, en el Ecuador se ha transformado la concepción de la salud a “un estado de completo bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades” (Organización Mundial de la Salud, 2006). En donde se plantea a la “salud como un instrumento para mejorar la calidad de vida de la población y alcanzar el Buen Vivir, mediante la profundización de esfuerzos en políticas de prevención y en la generación de un ambiente saludable” (Secretaría Nacional de Planificación y Desarrollo, 2013).

El PND 2007-2010 denominado “Planificación para la Revolución Ciudadana”, fue el primer plan implementado posterior a las elecciones presidenciales del año 2006, “elaborado a través de la orientación técnica y metodológica de la Secretaría de Nacional de Planificación y Desarrollo - SENPLADES, en coordinación con los equipos técnicos de los distintos Ministerios y Secretarías de Estado” (Secretaría Nacional de Planificación y Desarrollo, 2007),

convirtiéndose en la base fundamental para la aplicación de políticas públicas en el Ecuador.

El PND 2007–2010 contiene 2 estrategias nacionales, 12 objetivos nacionales, 110 políticas, 922 programas y 95 metas, que establecen los grandes lineamientos de una agenda para el efectivo desarrollo sostenible y equitativo del Ecuador.

En lo que respecta al sector salud, el primer PND enfatiza el aporte de la salud al mejoramiento de la calidad y esperanza de vida de los ecuatorianos mediante una atención integral y de calidad. A través de su objetivo nacional número tres que indica “Aumentar la esperanza y la calidad de vida de la población” (Secretaría Nacional de Planificación y Desarrollo, 2007). Este objetivo propone acciones públicas, con un enfoque intersectorial y de derechos, que se concretan a través de la prestación de servicios de salud integrales e integrados.

Para el cumplimiento de este objetivo se han planteado diferentes políticas y estrategias, que en el tema de recursos económicos para el sector salud se encuentra señalada en la estrategia número cinco “Incremento, asignación oportuna y uso óptimo de los recursos económicos para la función salud” (Secretaría Nacional de Planificación y Desarrollo, 2007) de la “Política 3.1. Promover el desarrollo sectorial, la organización y funcionamiento del Sistema Nacional de Salud” (Secretaría Nacional de Planificación y Desarrollo, 2007).

El segundo PND presentado nuevamente por el Presidente Rafael Correa Delgado, tras ganar de nuevo las elecciones presidenciales en el año 2009, se denominó “Plan Nacional para el Buen Vivir (PNBV) 2009-2013. Construyendo un Estado plurinacional e intercultural” (Secretaría Nacional de Planificación y Desarrollo, 2009). El contenido del PNBV 2009-2013 es muy similar al anterior PND 2007-2010, contiene 2 estrategias nacionales, 12 objetivos nacionales, 87

políticas, 715 programas y 80 metas. Los programas y metas del PND 2007-2010 se retomaron y concluyeron en el PNBV 2009-2013.

El PNBV 2009-2013 es un modelo de desarrollo a largo plazo, dirigido para el cumplimiento de los derechos humanos con el mejoramiento de la calidad de vida de la población. En lo que respecta a garantizar el derecho a la salud de la población, el PNBV 2009-2013, posee políticas y estrategias que garantizan la atención integral de salud sin costo para las y los usuarios, con calidad, calidez y equidad, mediante una red pública de salud mejorada en su infraestructura física y equipamiento.

El PNBV tiene como primer objetivo nacional "Auspiciar la igualdad, cohesión e integración social y territorial en la diversidad" (Secretaría Nacional de Planificación y Desarrollo, 2009), que contiene como estrategia principal la "Política 1.1. Garantizar los derechos del Buen Vivir para la superación de todas las desigualdades (en especial salud, educación, alimentación, agua y vivienda)" (Secretaría Nacional de Planificación y Desarrollo, 2009). Política a cumplirse a través de su lineamiento a) que indica:

> Ampliar la cobertura y acceso de los servicios públicos de salud y educación para toda la población, mejorando la infraestructura física y la provisión de equipamiento, a la vez que se eliminen barreras de ingreso a grupos de atención prioritaria, mujeres, pueblos y nacionalidades (Secretaría Nacional de Planificación y Desarrollo, 2009).

Además, el objetivo tres del PNBV indica "Mejorar la calidad de vida de la población" (Secretaría Nacional de Planificación y Desarrollo, 2009), mediante la "Política 3.3. Garantizar la atención integral de salud por ciclos de vida, oportuna y sin costo para las y los usuarios, con calidad, calidez y equidad" (Secretaría Nacional de Planificación y Desarrollo, 2009), que a través del lineamientos a) se pueda "Articular los diferentes servicios de la red pública de

salud en un sistema único, coordinado e integrado y por niveles de atención" (Secretaría Nacional de Planificación y Desarrollo, 2009).

Las políticas del PNBV están asociadas a una serie de programas y proyectos públicos que viabilizan el cumplimiento de los objetivos nacionales, considerando además que las políticas del PNBV se encuentran vinculadas con las políticas de la Agenda de Desarrollo Social del país. Tomando en cuenta lo antes mencionado y respecto al tema de garantizar la atención integral de salud, la política 3.3 del PNBV 2009-2013 se encuentra articulada con la política 1 perteneciente a la sección salud, de la Agenda de Desarrollo Social 2009-2011, que indica: "Garantizar la atención integral de salud gratuita y oportuna para los usuarios en cada ciclo de vida" (Ministerio de Coordinación de Desarrollo Social, 2009). A continuación, en las siguientes figuras se muestra la relación que existe entre las políticas del PNBV y la Agenda de Desarrollo Social a través de los programas que tiene relación a dichas políticas.

| Objetivo PNVB 2009 -2013 | Políticas PNBV 2009 - 2013 | Política Agenda Social 2009 -2011 |
|---|---|---|
| 3. Mejorar la calidad de vida de la población | Garantizar la atención integral de salud por ciclos de vida, oportuna y sin costo para las y los usuarios, con calidad, calidez y equidad | Garantizar la atención integral de salud gratuita y oportuna para los usuarios en cada ciclo de vida |

Figura 3. Relación entre políticas del PNBV y la Agenda de Desarrollo Social 2009–2011.
Tomado de (Ministerio de Coordinación de Desarrollo Social, 2009, pág. 40).

| Resumen de políticas y programas del sector social | | |
|---|---|---|
| Sector | Política Agenda Social 2009 - 2011 | Programa |
| Salud | Garantizar la atención integral de salud gratuita y oportuna para los usuarios en cada ciclo de vida | Programa de Extensión de la Protección Social en Salud |
| | | Ciclos de Vida - Atención Integral a la Infancia |
| | | Ciclos de Vida - Atención Integral a la Adolescencia |
| | | Ciclos de Vida - Salud Sexual y Reproductiva |
| | | Ciclos de Vida - Atención Integral al Adulto Mayor |
| | | Ciclos de Vida - Atención Integral al Adulto Mayor Enfermedades Crónicas No Transmisibles |
| | | Fortalecimiento de Infraestructura y Equipamiento de las Unidades de Salud |
| | | Salud Intercultural - Fortalecimiento de los Sistemas Médicos Diversos |
| | | Desarrollo de la Ciencia y Tecnología en Salud |

Figura 4. Relación entre Agenda de Desarrollo Social 2009–2011 y programas del sector social.
Tomado de (Ministerio de Coordinación de Desarrollo Social, 2009, pág. 34).

En las páginas siguientes, se describirá la inversión realizada por el Estado en apoyo a programas como el “Fortalecimiento de infraestructura y equipamiento de las unidades de salud” (Secretaría Nacional de Planificación y Desarrollo, 2009), permitiendo dotar y repotenciar la infraestructura, el equipamiento y el mobiliario hospitalario de la red pública de salud, alineado con la Constitución de la República del año 2008 y las políticas del PNBV 2009-2013 y Agenda social de Desarrollo 2009-2011.

Finalmente, el tercer PND que se encuentra vigente actualmente se denominó “Plan Nacional para el Buen Vivir (PNBV) 2013-2017. Todo el mundo mejor” (Secretaría Nacional de Planificación y Desarrollo, 2013), fue presentado por el mismo presidente de la República del Ecuador, Economista Rafael Correa Delgado el 17 de febrero de 2013. Consta asimismo de 2 estrategias nacionales; 12 objetivos nacionales, 100 políticas y 93 metas.

El PNBV 2013-2017, también posee políticas y objetivos alineados a garantizar la salud de la población a través de la prestación universal y gratuita de los

servicios de salud, que permitan mejorar la calidad de vida de los ecuatorianos. La política 3.3 promueve el “Garantizar la prestación universal y gratuita de los servicios de atención integral de salud” (Secretaría Nacional de Planificación y Desarrollo, 2013) a través de sus lineamientos estratégicos a) y c) que delinean “Consolidar y fortalecer la red pública integral de salud de manera coordinada e integrada, para optimizar el uso de recursos, con base en la capacidad de acogida de los territorios” (Secretaría Nacional de Planificación y Desarrollo, 2013) y “Dotar y repotenciar la infraestructura, el equipamiento y el mobiliario hospitalario, según corresponda, a lo largo del territorio ecuatoriano” (Secretaría Nacional de Planificación y Desarrollo, 2013). Políticas y lineamientos que permitan cumplir con el objetivo 3 del PNBV 2013-2017 que indica “Mejorar la calidad de vida de los ecuatorianos” (Secretaría Nacional de Planificación y Desarrollo, 2013).

Los tres Planes Nacionales de Desarrollo tienen en común el objetivo nacional número 3 que se refiere a mejorar la calidad de vida de los ecuatorianos, tomando al sector salud como un instrumento principal para el cumplimiento de dicho objetivo. Para lo cual se han creado políticas que garantizan la atención integral de salud y lineamientos que aseguran el incremento y asignación oportuna de los recursos económicos para la función salud, así como también estrategias y programas que promueven el mejoramiento y repotenciación de la infraestructura, el equipamiento y el mobiliario hospitalario.

Para materializar lo que dispone la Constitución y el objetivo tres del PND sobre mejorar la calidad de vida de la población, en el año 2008 el Ministerio de Salud Pública en su calidad de autoridad sanitaria nacional implementó cambios estructurales en el sector salud, mediante el Modelo de Atención Integral, Familiar, Comunitario e Intercultural (MAIS-FCI) con el cual se pretende que la atención de salud comprenda un conjunto de sistemas, procesos y acciones que permitirán reorganizar la oferta sanitaria o social para cubrir las necesidades de salud de la población.

## 1.4 Modelo de Atención Integral, Familiar, Comunitario e Intercultural (MAIS-FCI)

El MAIS-FCI "es el conjunto de estrategias, normas, procedimientos, herramientas y recursos que al complementarse, organiza el Sistema Nacional de Salud para responder a las necesidades de salud de las personas, las familias y la comunidad, permitiendo la integralidad en los niveles de atención en la red de salud" (Ministerio de Salud Pública, 2012). Esta forma de atención integral de salud se enfoca en consolidar la estrategia de atención primaria en los 3 niveles de atención de salud, reorientando sus servicios para la promoción de la salud y la prevención de enfermedades. Por tanto el MAIS-FCI define:

> Como van a interactuar los actores de los sectores público y privado, los miembros de la red de servicios de salud y la comunidad para llevar a cabo acciones conjuntas que permitan dar soluciones integrales a las necesidades o problemas de salud de la comunidad contribuyendo de esta manera a mejorar su calidad de vida (Ministerio de Salud Pública, 2012).

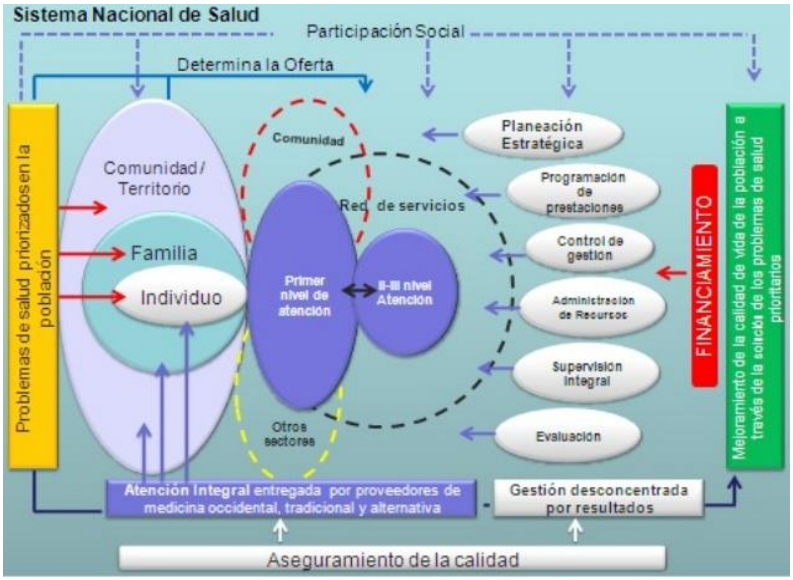



Figura 5. Modelo de Atención Integral de Salud – MAIS.
Tomado de (Ministerio de Salud Pública, 2012).

Como se puede apreciar en el cuadro, el MAIS espera establecer redes que se integren al primer nivel de atención, considerado a este como la puerta de entrada al SNS y enlazando al segundo nivel de hospitales básicos y generales para que coordinen y cada una tenga sus funciones específicas, para llegar a la población con equidad, articulando un sistema integral de salud. Los componentes que hacen viables la operación y desarrollo del MAIS-FCI son los siguientes:

- Componente de provisión de servicios de salud.
- Componente de organización.
- Componente de gestión.
- Componente de financiamiento.

En apoyo a lo que dispone la Constitución y los lineamientos del objetivo tres del PND, el MSP a través del componente de gestión del MAIS, establece una "Gestión de infraestructura, equipamiento y medicamentos de acuerdo a los estándares definidos por la Autoridad Sanitaria Nacional y el cuadro de medicamentos básicos" (Ministerio de Salud Pública, 2012), que conforme a las necesidades nacionales define el plan y estándares para la dotación de nueva infraestructura, equipamiento y el mantenimiento preventivo correctivo de infraestructura y equipamiento, como también el cuadro de medicamentos básicos.

Como parte del MAIS, se creó el proyecto de Infraestructura Física, Equipamiento, Mantenimiento, Estudios y Fiscalización en Salud (PIFEMEFS), que tiene como objetivo "mejorar la calidad de prestación de servicios, mediante el incremento de la cobertura nacional de infraestructura y equipamiento" (Ministerio de Salud Pública, 2016), proyecto que forma parte del programa de "Fortalecimiento del Modelo de Atención Integral en Salud" (Ministerio de Salud Pública, 2016), con el fin de "incrementar la esperanza y calidad de vida de la población, mediante el mejoramiento de la infraestructura,

construcción de unidades nuevas y dotación del equipamiento a las unidades de salud a nivel nacional" (Ministerio de Salud Pública, 2015).

## 1.5 Inversión pública en el sector de la Salud

Desde su posesión como Presidente de la República del Ecuador para el periodo 2007 - 2011, el Econ. Rafael Correa anunció como uno de sus principales pilares de su plan de gobierno, una Revolución en las Políticas Sociales, principios que fueron plasmados en la Constitución del año 2008 estableciendo preasignaciones presupuestarias y garantizando el derecho a la salud.

En el año 2007 el gasto por salud se encontraba en un aproximado de 550 millones de dólares, para el año 2008 el presupuesto de la salud se incrementó a 879 millones de dólares, y hasta el año 2015 esta cifra ascendió a más de 2,500 millones de dólares. En el gráfico a continuación se puede identificar la evolución de la inversión pública en salud durante el periodo 2007 - 2015.


Figura 6. Inversión pública en el sector de la Salud.
Tomado de (Ministerio de Salud Pública, 2015, pág. 5); (Ministerio de Finanzas, 2014).

El mejorar la calidad de vida la población a través de la salud, aumenta sus capacidades de desenvolvimiento y logra que las actividades que desempeñan las personas sean más productivas, tanto para las entidades en las que laboran como para la economía del país. De allí nace la importancia de conocer el gasto en salud respecto del Producto Interior Bruto (PIB).

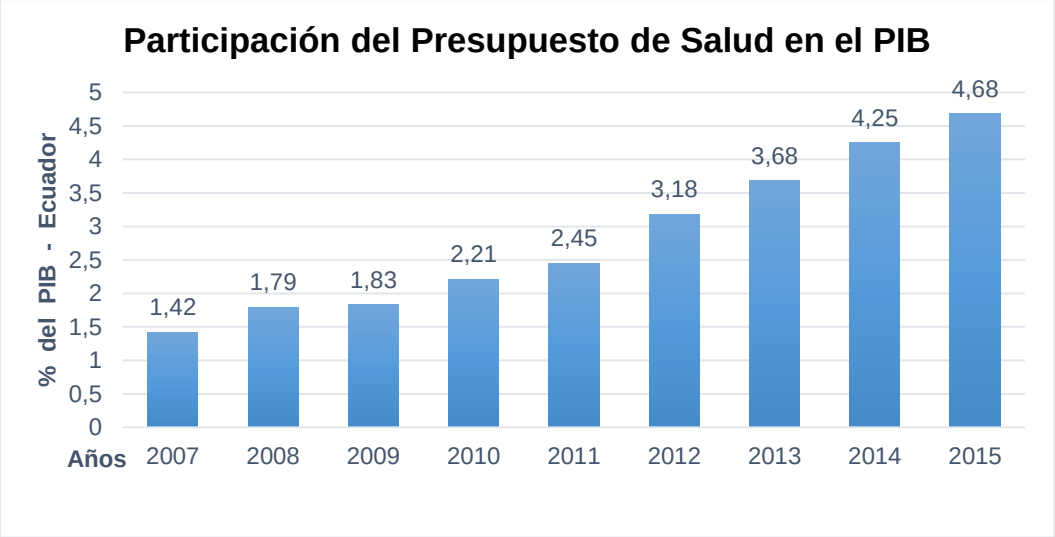



Figura 7. Participación del presupuesto de salud en el PIB.
Tomado de (Ministerio de Salud Pública, 2015, pág. 6); (Baquero, Guerra, & Mieles, 2014).

Para el sector de la salud la Constitución dispone que se incrementará cada año un porcentaje no inferior al cero punto cinco por ciento del PIB, por lo cual en el año 2015 la inversión supera el cuatro por ciento del PIB. La inversión en salud principalmente se realizó en infraestructura, equipamiento, recursos humanos y programas de prevención de salud. En la siguiente figura se describe el presupuesto invertido en salud por tipo y grupo de gasto en el periodo 2008 – 2015.

| Tipo | Grupo Item | Codificado | Devengado |
|---|---|---|---|
| CORRIENTE | Bienes de larga duración | 172.075.988 | 128.810.051 |
| | Gasto en personal | 6.739.671.129 | 5.778.129.061 |
| | Instalación, Mantenimiento y Reparaciones | 154.812.444 | 134.610.520 |
| | Medicinas y Productos Farmacéuticos | 1.365.719.197 | 1.022.374.341 |
| | Otro | 1.405.414.804 | 1.187.447.748 |
| | Servicios Médicos Hospitalarios y Comple.. | 436.956.214 | 348.582.472 |
| | Total | 10.274.649.774 | 8.599.954.193 |
| INVERSIÓN | Bienes de larga duración | 785.054.980 | 371.384.343 |
| | Gasto en personal | 469.173.610 | 425.109.913 |
| | Instalación, Mantenimiento y Reparaciones | 67.115.654 | 35.691.223 |
| | Medicinas y Productos Farmacéuticos | 726.567.630 | 585.480.576 |
| | Obras de Infraestructura | 257.919.545 | 116.435.017 |
| | Otro | 795.786.423 | 571.735.512 |
| | Servicios Médicos Hospitalarios y Comple.. | 39.164.690 | 38.840.907 |
| | Total | 3.140.782.531 | 2.144.677.491 |
| Total general | | 13.415.432.305 | 10.744.631.684 |

Figura 8. Presupuesto público invertido en salud por tipo y grupo de gasto. Tomado de (Ministerio de Salud Pública, 2016).

## 1.6 Gestión en infraestructura de las instituciones del Ministerio de Salud Pública

Coherentes con las disposiciones constitucionales y el PND, el Gobierno Nacional desde el año 2008 ha realizado inversiones en nuevos hospitales y centros de salud, que permita fortalecer el SNS, atender las necesidades de la población y aumentar la oferta de servicios hospitalarios. En el siguiente cuadro se detalla el incremento de los establecimientos de la red pública de salud detallado por nivel y tipología desde el año 2008 al 2015.

Tabla 1.

Establecimientos de la red pública de salud del año 2008 al 2015.

| **Número de establecimientos por nivel y tipología de la red publica de salud desde el año 2008 al 2015** | | | |
|---|---|---|---|
| Nivel de atención | Descripción tipología | 2008 | 2015 |
| Primer nivel | Centro de salud | 1262 | 1446 |
| | Centro de salud tipo A | 134 | 1 |
| | Centro de salud tipo B | | |
| | Centro de salud tipo C | | 1 |
| | Consultorio | | |
| | Consultorio general | | |
| | Puesto de salud | 272 | 517 |
| | Unidad móvil general | | 42 |
| | Unidades anidadas | | 69 |
| | Otros | 9 | |
| | Total | 1677 | 2076 |
| Segundo nivel | Hospital básico | 78 | 83 |
| | Hospital general | 28 | 30 |
| | Hospitales móviles | | 2 |
| | Unidad móvil especializado de oncológica | | 2 |
| | Unidad móvil quirúrgica | | 6 |
| | Total | 106 | 123 |
| Tercer nivel | Centro especializado | 8 | 12 |
| | Hospital de especialidades | 1 | 2 |
| | Hospital especializado | 7 | 14 |
| | Unidad móvil quirúrgica | | 2 |
| | Total | 16 | 30 |
| | **Total final** | **1799** | **2229** |

Adaptado de (Instituto Nacional de Estadística y Censos, 2008), (Ministerio de Salud Pública, 2016).

## 1.7 Normativas sobre confidencialidad de la información para el sector Salud del Ecuador

En el Ecuador a través de la Constitución del año 2008, se garantiza la confidencialidad de la información de los pacientes, que se generen a través de la utilización de los diferentes tipos de servicios de salud, según delinea el artículo 362 de la sección segunda sobre la salud.

> Art. 362.- La atención de salud como servicio público se prestará a través de las entidades estatales, privadas, autónomas, comunitarias y aquellas que ejerzan las medicinas ancestrales alternativas y complementarias. Los servicios de salud serán seguros, de calidad y calidez, y garantizarán el consentimiento informado, el acceso a la información y la confidencialidad de la información de los pacientes (Constitución de la República del Ecuador, 2008, pág. 113).

Para las instituciones de salud, que reciben o administran fondos públicos la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), en su artículo 5 detalla que:

> Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado (Congreso Nacional, 2004).

Y que respecto a la confidencialidad de la información, la LOTAIP en el artículo 6 explica:

> Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República (Congreso Nacional, 2004).

Además, la ley de derechos y amparo del paciente, promueve el derecho a la confidencialidad para los pacientes que utilicen los servicios de las entidades adscritas al SNS, como lo indica en su artículo 4:

> Art. 4.- Derecho a la confidencialidad: Todo paciente tiene derecho a que la consulta, examen, diagnóstico, discusión, tratamiento y cualquier tipo de información relacionada con el procedimiento médico a aplicársele, tenga el carácter de confidencial (Ministerio de Salud Pública, 2006).

Por otra parte, en el año 2015 mediante Acuerdo Ministerial 5216 se expide el Reglamento de Información Confidencial en el SNS que tiene como objetivo "establecer las condiciones operativas de la aplicación de los principios de manejo y gestión de la información confidencial de los pacientes y sus disposiciones serán de cumplimiento obligatorio dentro del Sistema Nacional de Salud" (Ministerio de Salud Pública, 2015). El reglamento considera principios como Confidencialidad, Integridad, Disponibilidad, Seguridad en el manejo de la información y Secreto Médico.

Dentro de los capítulos del reglamento, se toma ya a consideración la confidencialidad en todos los documentos con información de salud, indicando además que "toda persona que intervenga en su elaboración o que tenga acceso a su contenido, está obligada a guardar la confidencialidad respecto de la información" (Ministerio de Salud Pública, 2015).

## 1.8 Justificación y alcance

El incremento del presupuesto fiscal, destinado para el sector salud ha colaborado considerablemente para el desarrollo de programas de salud y el aumento de la infraestructura hospitalaria pública, sean estos hospitales nuevos o repotenciados. Dentro de la inversión en infraestructura hospitalaria consta el gasto en la parte de Tecnología de la Información, considerando a TI como un aliado para aumentar la eficiencia y mejorar la calidad en la prestación de cuidados de la salud.

Las instituciones adscritas al SNS y de forma particular los hospitales públicos requieren cumplir con sus objetivos estratégicos y desarrollar su misión y visión social a través de prestar con eficiencia su cartera de servicios médicos. De ahí que para asegurar el logro de los objetivos del hospital a través de TI, es necesario alinear los objetivos de TI con los objetivos estratégicos del hospital, creando valor (realización de beneficios, optimización de riesgos y recursos) para los interesados. Con lo indicado anteriormente, se puede decir que un modelo de Gobierno de TI, es un proceso sistemático establecido para una correcta implementación del Gobierno de TI en una organización, permitiendo "proveer dirección y control para ayudar a asegurar que las mayores inversiones hechas en TI aporten valor agregado a la empresa, los recursos son usados con responsabilidad y los riesgos sean mitigados" (Coronel, 2015).

Hay que mencionar también, que en la actualidad el sector salud se ha visto beneficiado con el uso de las Tecnología de la Información, en donde la información junto a los procesos y los sistemas que hacen uso de ella, son activos importantes para los hospitales públicos y demás entidades pertenecientes al SNS, que en los diferentes niveles de organización del sistema de salud la información sanitaria es importante para la toma de decisiones.

Según el informe de Salud y Ciberseguridad (health care and cyber security) indica que "En los últimos dos años el 81% de los hospitales y aseguradoras de salud sufrieron una brecha en sus datos" (Bell & Ebert , 2015). En donde todos estos "incidentes provocaron una pérdida en los datos, mostrando que los incidentes registrados no se tratan solo de un malware o un virus, sino que además se trata de una exfiltración por parte del personal que pertenece a la organización" (Bell & Ebert , 2015).

> Según (Areitio, 2008): La Seguridad Informática no solo debe encargarse de los posibles fallos desaprensivos, sino que también debe tener en cuenta los errores que se pudieran generar por el mal funcionamiento

del hardware, así como prevenir acciones involuntarias que puedan afectar la Seguridad de la Información que se encuentre contenida en los sistemas.

La información, junto a los procesos y los sistemas que hacen uso de ella, son activos importantes para los hospitales. En donde la confidencialidad, integridad y disponibilidad de dicha información les faculta a prestar con eficiencia su cartera de servicios. Por lo tanto el tema de tesis se basa en diseñar y proponer un modelo de Gobierno de Tecnologías de la Información para hospitales públicos con énfasis en la Seguridad de la Información, tomando como caso de estudio al Hospital General Docente de Calderón.

# 2 Capítulo II. Estándares, modelos y buenas prácticas para el Gobierno de TI aplicables a Hospitales Públicos

## 2.1 Gobierno de TI

En las organizaciones el rol de las Tecnologías de la Información, ha venido adquiriendo diversos matices y énfasis en la búsqueda de obtener ventaja competitiva, bien sea minimizando costes y riesgos, o también maximizando las ventas o el servicio. Originalmente las TI se centraban en soportar los procesos de apoyo y operativos, que luego evolucionó para soportar los procesos misionales de la organización alineado con los objetivos del negocio, logrando compatibilidad y colaboración.

Las Tecnologías de la Información han evolucionado en las organizaciones siguiendo tres grados de madurez:

- “Automatización progresiva de los procesos.
- Control de los procesos de la organización (inventario, calidad, producción, facturación, compras, etc.).
- Transformación de los procesos de la organización” (Morton, 1991).

El escenario actual genera la necesidad de definir y diseñar estrategias proactivas para gobernar las TI, de tal forma que permitan la adaptación continua del negocio. Son variados los conceptos que existen acerca del Gobierno de TI, cada uno enfocado según la óptica del autor pero con algo en común: Gestión y Tecnologías de la Información. En éstos se coincide puesto que básicamente son la razón de ser de dicho proceso. Algunas de estas definiciones, son:

- (Luftman, 1996):"El gobierno de las TI es la selección y utilización de relaciones, tales como alianzas estratégicas, para alcanzar las principales competencias en TI".

- (Van Grembergen, 2002): "El gobierno de las TI es la capacidad de la que dispone el Consejo de Dirección, la administración ejecutiva y la administración de las TI para controlar la planificación y la implementación de estrategias de TI y así asegurar la alineación entre negocio y TI".

- (IT Governance Institute, 2003): "El Gobierno de las TI es responsabilidad de la administración ejecutiva y del Consejo de Dirección. Es una parte integral del gobierno de una organización y consiste en las estructuras organizacionales y de dirección, y en los procesos que aseguran que la organización mantiene y amplía sus objetivos y estrategias".

- (Doughty & Grieco, 2005):"El principal objetivo del Gobierno de las TI es facilitar y aumentar la habilidad de la organización para atender y cumplir con sus objetivos institucionales y para ofrecer la mejor información para la toma de decisiones relacionadas con la incorporación de TI a sus operaciones, programas y servicios a corto y largo plazo".

- (Webb, Pollard, & Ridley, 2006) "El Gobierno de las TI consiste en la alineación estratégica de las TI con el negocio de tal manera que se alcanza el máximo beneficio (valor) para el negocio a través del desarrollo y mantenimiento del control efectivo y la responsabilidad, gestión del rendimiento y gestión de los riesgos de las TI".

El Gobierno de TI cuenta con 5 principales áreas (alineamiento estratégico, entrega de valor, gestión de riesgos, gestión de los recursos y medición del

desempeño) las cuales funcionan como un ciclo que permite gobernar adecuadamente las tecnologías (IT Governance Institute, 2003).

### 2.1.1 Alineamiento estratégico

La alineación estratégica es uno de los dominios del Gobierno de TI y se encarga de “que la estrategia de TI soporte la estrategia del negocio y que las operaciones en TI estén alineadas con las operaciones actuales de la empresa” (IT Governance Institute, 2003).

Se debe considerar al área de TI como un negocio dentro del negocio de la empresa, donde el Gobierno de TI forme parte integral del Gobierno Corporativo. La Gerencia de TI se enfoca en el logro de sus objetivos, los cuales a su vez deben estar alineados con los objetivos estratégicos de la organización para garantizar que soportan adecuadamente el negocio.

### 2.1.2 Entrega de valor

El Gobierno de TI debe ofrecer beneficios en el aspecto estratégico a la organización, aportando soluciones que faciliten la toma de decisiones, optimizando la inversión y disminuyendo gastos, como lo indica ITGI. La entrega de valor es uno de los dominios del Gobierno de TI, el cual “se encarga de ejecutar la propuesta de valor, garantizando que las TI entreguen los beneficios prometidos, optimizando los costos y probando el valor intrínseco de TI” (IT Governance Institute, 2003).

### 2.1.3 Gestión de riesgos

La gestión de riesgos es uno de los dominios del Gobierno de TI, el cual “se encarga de asegurar que el cumplimiento de los objetivos de la empresa no esté en peligro por las fallas que pueden ocurrir en TI, sean estas operacionales, de seguridad o de proyectos fallidos” (IT Governance Institute,

2003). Por lo cual la Gerencia de TI está obligada a tener una administración efectiva, y un manejo eficiente de la gestión de riesgo, estar en capacidad de detectar y minimizar el riesgo, donde la Dirección General debe estar enterada de los riesgos y vulnerabilidades de su sistema de información y de sus componentes tecnológicos, estando en la capacidad de afrontar y superar las fallas detectadas.

### 2.1.4 Gestión de los recursos

La gestión de recursos es uno de los dominios del Gobierno de TI, que busca "mejorar el rendimiento de TI, optimizando las inversiones, el uso y la asignación los recursos de TI (personas, aplicaciones, infraestructura y datos) para brindar servicios según las necesidades del negocio" (IT Governance Institute, 2003). Los servicios y niveles de servicio que brinda TI a la organización deben estar claramente definidos, con el fin de obtener un eficiente uso de los recursos de TI.

### 2.1.5 Medición del desempeño

La medición del desempeño es uno de los dominios del Gobierno de TI, "que permite saber si está cumpliendo con los objetivos que se han planteado al inicio del proceso del Gobierno de TI" (IT Governance Institute, 2003). Los métodos utilizados para la medición del desempeño depende del tipo de activos o resultados a medir, para los activos tangibles se puede utilizar un cálculo de retorno de la inversión (ROI), o un Cuadro de Mando Integral-CMI (Balanced Scorecard) para medir activos tangible e intangibles.

## 2.2 COBIT 5

Las organizaciones poseen un capital activo muy valioso: información y tecnología. El éxito de una empresa cada vez depende más de la comprensión de ambos componentes. Las buenas prácticas concentradas en el marco de

referencia COBIT (Objetivos de Control para la información y Tecnologías relacionadas), permiten que los objetivos de negocio se alineen con la Tecnología de la Información para así alcanzar los mejores resultados.

COBIT 5 es un marco de trabajo publicado por ISACA (Asociación de Control y Auditoría de Sistemas de Información) en el año 2012, con el objetivo de ayudar a las organizaciones a optimizar el valor de las TI manteniendo un equilibrio entre la generación de valor, la optimización de los niveles de riesgos y el uso eficiente de los recursos de la empresa.

> COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el Gobierno y la Gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. (ISACA, 2012).

Con la versión 5 de COBIT, ISACA ofrece una guía para permitir que las Tecnologías de la Información sean gobernadas y gestionadas de una manera holística en toda la organización, cubriendo las áreas funcionales de responsabilidad de TI y el negocio de extremo a extremo considerando los intereses de las partes interesadas internas y externas.

Para el buen Gobierno y la Gestión de las TI empresariales, COBIT 5 se basa en 5 principios que son útiles para cualquier empresa en las diferentes líneas de negocio en las que se desarrolle. Estos 5 principios permiten a las organizaciones construir un marco de Gobierno y Gestión de TI efectivo que optimice la inversión y el uso de información y tecnología para el beneficio de las partes interesadas.


Figura 9. Principios de COBIT 5.
Tomado de (ISACA, 2012, pág. 13).

### 2.2.1 Principios de COBIT 5

#### 2.2.1.1 Principio 1: Satisfacer las necesidades de las partes interesadas

“Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos” (ISACA, 2012). En consecuencia independiente del tipo de organización se tendrá la creación de valor como un objetivo de Gobierno, Los beneficios pueden tomar muchas formas, por ejemplo, financieros para las empresas comerciales o de servicio público para entidades gubernamentales.

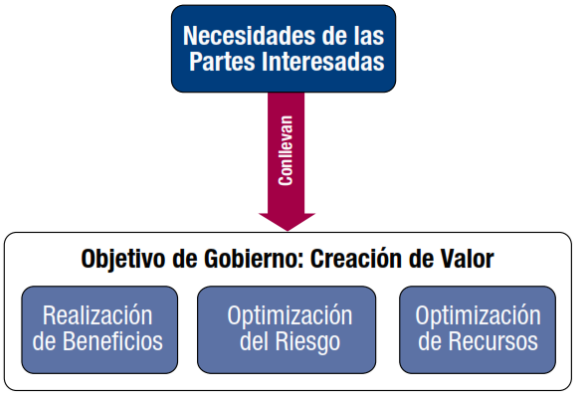



Figura 10. El objetivo de Gobierno: Creación de valor.
Tomado de (ISACA, 2012, pág. 17).

Las necesidades de las partes interesadas, se convierten en una estrategia empresarial llamada cascada de metas, que inicia con las metas corporativas, continúa con las metas relacionadas de TI, que a su vez recaen en lo que COBIT 5 llama procesos y finalmente alcanza a desarrollar las actividades de las metas. Este concepto se visualiza en la figura que se muestra a continuación:


Figura 11. Cascada de metas de COBIT 5.

Tomado de (ISACA, 2012, pág. 18).

#### 2.2.1.1.1 Paso 1: Los motivos de las partes interesadas influyen en las necesidades de las partes interesadas

Las necesidades de los stakeholders (parte interesada o accionista en su traducción al español) están influenciadas por factores internos o externos, como por ejemplo: cambios de estrategia en el modelo de negocio, un entorno regulatorio cambiante o debido a las nuevas tecnologías.

#### 2.2.1.1.2 Paso 2: Las necesidades de las partes interesadas desencadenan metas empresariales

Las necesidades de los stakeholders están relacionadas con un conjunto de metas empresariales genéricas. A través del uso de herramientas como un CMI (Cuadro de Mando Integral) se identifica las metas corporativas, las cuales comúnmente se relacionan con los objetivos genéricos de la empresa.

#### 2.2.1.1.3 Paso 3: Cascada de metas de empresa a metas relacionadas con las TI

El cumplimiento de las metas empresariales está sujeto al alcance de las metas relacionadas con las TI, COBIT 5 define 17 metas relacionadas con las TI asociadas a las mismas dimensiones del CMI. De esta manera, se muestra cómo el lograr resultados relacionados con TI se pueden lograr metas empresariales.

#### 2.2.1.1.4 Paso 4: Cascada de metas relacionadas con las TI hacia metas catalizadoras

Para alcanzar las metas relacionadas con TI se requiere la aplicación y uso satisfactorio de los catalizadores. Los catalizadores identificados a través de la

cascada de metas tienen definidas un conjunto de metas relevantes en apoyo de las metas relacionadas con TI.

“La cascada de metas es importante porque permite la definición de prioridades de implementación, mejora y aseguramiento del Gobierno de TI de la empresa, que se basa en metas corporativas de la empresa y el riesgo relacionado” (ISACA, 2012). El proceso de mapeo entre las metas estratégicas, las metas relacionados con las TI y los procesos o metas catalizadoras no contienen la verdad universal por lo tanto su uso no debe ser de manera mecánica, sino debe ser usado como una guía.

#### 2.2.1.2 Principio 2: Cubrir la empresa de extremo a extremo

COBIT 5 se concentra en el Gobierno y la Gestión de la información y tecnología relacionada, desde una perspectiva integral a nivel de toda la organización, esto significa que COBIT 5:

- Integra el Gobierno de TI propuesto por COBIT 5, con en el Gobierno Corporativo de la empresa.
- “Cubre todas las funciones y procesos necesarios para gobernar y gestionar la información corporativa y las tecnologías relacionadas donde quiera que esa información pueda ser procesada” (ISACA, 2012).
- Todos los procesos de negocios y servicios relevantes de las TI internos y externos son contemplados por COBIT 5.
- “Considera que los catalizadores relacionados con TI para el Gobierno y la Gestión deben ser a nivel de toda la empresa y de principio a fin, es decir toma en cuenta los catalizadores relevantes para el Gobierno y la Gestión de la información de la empresa y TI relacionadas” (ISACA, 2012).

En la siguiente figura se muestra los componentes clave de un sistema de gobierno, que permite cumplir con el enfoque de gobierno extremo-a-extremo que es la base de COBIT 5.

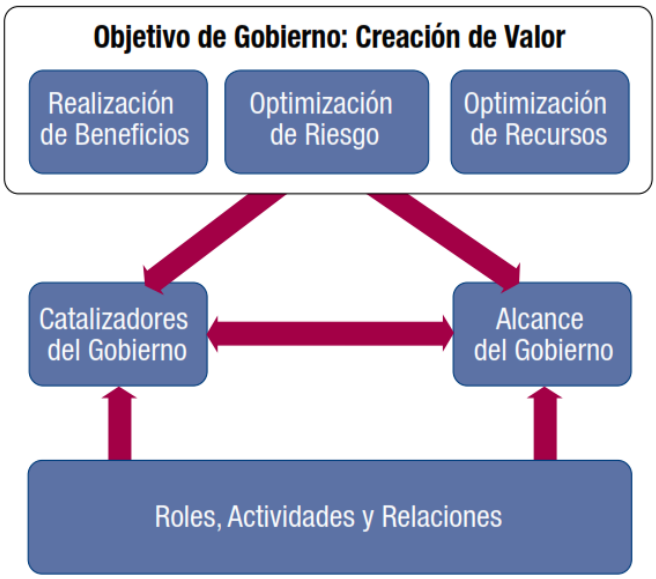



Figura 12. Componentes claves de un sistema de gobierno.
Tomado de (ISACA, 2012, pág. 23).

2.2.1.2.1 Componentes claves de un Sistema de Gobierno

Los Catalizadores de Gobierno son los recursos organizativos para el Gobierno de TI, tales como marcos de referencia, principios, estructuras, procesos y prácticas, que a través de acciones dirigidas permiten cumplir con los objetivos planteados. Las capacidades de servicios de TI (infraestructura TI, aplicaciones, etc.), personas e información son recursos corporativos que también forman parte de los Catalizadores de Gobierno.

2.2.1.2.2 Alcance de Gobierno

El Gobierno puede ser aplicado a toda la empresa, a una entidad, a un activo tangible o intangible, etc. Siendo esencial definir bien el alcance del sistema de gobierno para un uso óptimo de los recursos.

2.2.1.2.3 Roles, actividades y relaciones

Es el equipo de trabajo que está involucrado en el gobierno, definiendo sus roles, responsabilidades, tareas y su interacción dentro del alcance del sistema de gobierno. En la siguiente figura se muestra las interacciones entre los diferentes roles, actividades y relaciones de un sistema de gobierno.

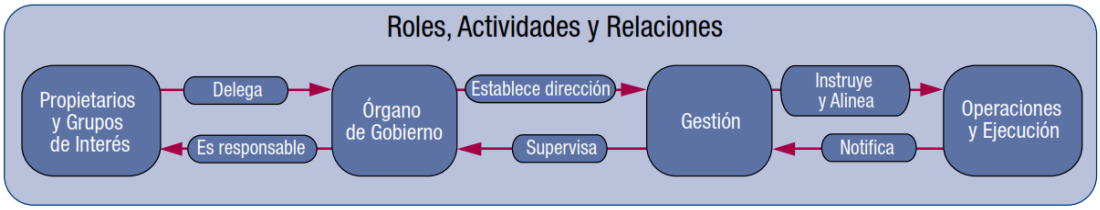



Figura 13. Roles, actividades y relaciones de gobierno.
Tomado de (ISACA, 2012, pág. 24).

2.2.1.3 Principio 3: Aplicar un marco de referencia único integrado

COBIT 5 integra todo el conocimiento disperso de ISACA sobre áreas clave del Gobierno Corporativo como “COBIT, Val IT, Risk IT, BMIS, la publicación Información sobre Gobierno de TI para la Dirección (Board Briefing on IT Governance) e ITAF” (ISACA, 2012). Lo cual le permite alinearse con prácticas y estándares relevantes de alto nivel que constituyen guías para el gobierno y la gestión de la tecnología empresarial, tales como:

- ISO/IEC 38500:2008 – Gobernanza Corporativa de TI.
- ISO 31000:2009 – Principios y directrices de carácter genérico sobre la gestión del riesgo.
- ISO/IEC 27001/27002 – Sistema de Gestión de Seguridad de la Información.
- PRINCE2/PMBOOK – Gestión de Programas y Proyectos.
- TOGAF – Modelo de Arquitectura Empresarial.

- CMMI (Capability Maturity Model Integration) – Procesos de aplicación, construcción y adquisición de aplicaciones incluyendo procesos organizacionales y de calidad.
- Entre otras.

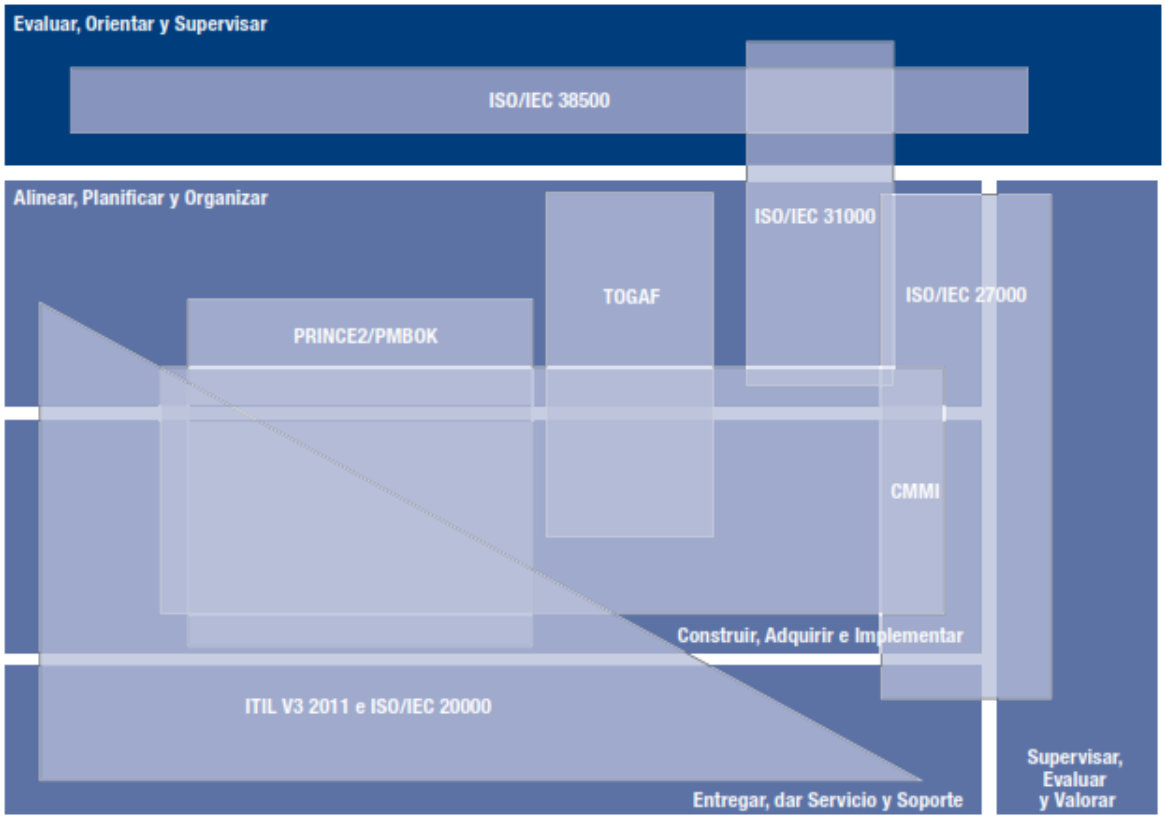



Figura 14. Marco de referencia único e Integrado.
Tomado de (ISACA, 2012, pág. 61).

2.2.1.4 Principio 4: Hacer posible un enfoque holístico

El marco de referencia de COBIT 5, con el propósito de apoyar en la implementación de un sistema integral de Gobierno y Gestión de TI de la organización, propone un conjunto de catalizadores como factores que influyen de manera general sobre el logro de los objetivos de la organización, y están divididos en las siete categorías que se muestran a continuación:

- Los principios, políticas y marcos de referencia.
- Los procesos.

- Las estructuras organizativas.
- La cultura, ética y comportamiento.
- La información.
- Los servicios, infraestructuras y aplicaciones.
- Las personas, habilidades y competencias.

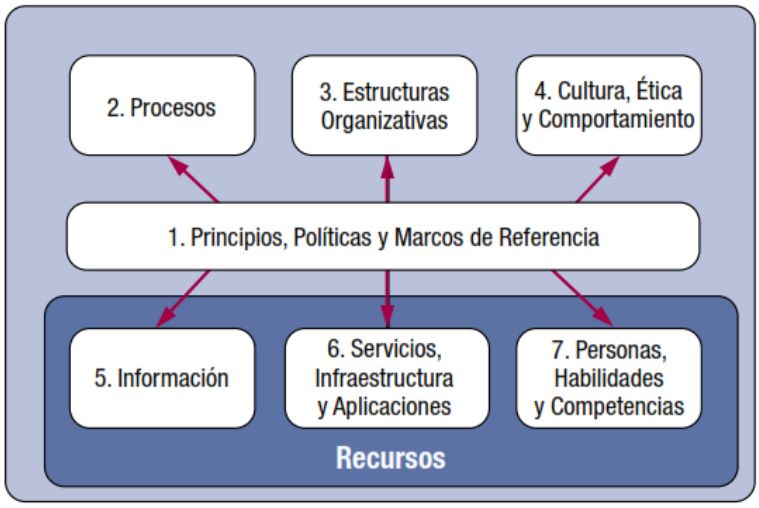



Figura 15. Habilitadores de COBIT 5.
Tomado de (ISACA, 2012, pág. 27).

2.2.1.4.1 Gobierno y Gestión sistémicos mediante catalizadores interconectados

Para lograr los objetivos principales de la organización, siempre debe considerarse una serie interconectada de habilitadores debido a que cada catalizador necesita el resultado de otros catalizadores para ser completamente efectivo, además se debe definir una naturaleza sistémica entre el Gobierno y la Gestión de TI para la toma de buenas decisiones lo que implica un análisis de relevancia de los mismos.

2.2.1.4.2 Dimensiones de los catalizadores

Todos los catalizadores tienen un conjunto de dimensiones comunes que facilitan el uso de los mismos, permitiendo a una organización manipular sus interacciones, facilitando el logro de objetivos.

- **Grupos de Interés:** Son partes que ejecutan un rol activo y/o tienen un interés en el catalizador, los grupos de interés pueden ser internos o externos a la organización, cada uno de ellos con sus propias necesidades e intereses, algunas veces contrarios entre sí.
- **Metas:** Son los resultados esperados del catalizador.
- **Ciclo de vida:** Proceso que describe las fases de los catalizadores desde su inicio, su vida útil operativa hasta su llegar a su eliminación.
- **Buenas prácticas:** Son ejemplos y sugerencias sobre cómo implementar de la mejor manera el catalizador. Las buenas prácticas soportan la consecución de los objetivos del catalizador.

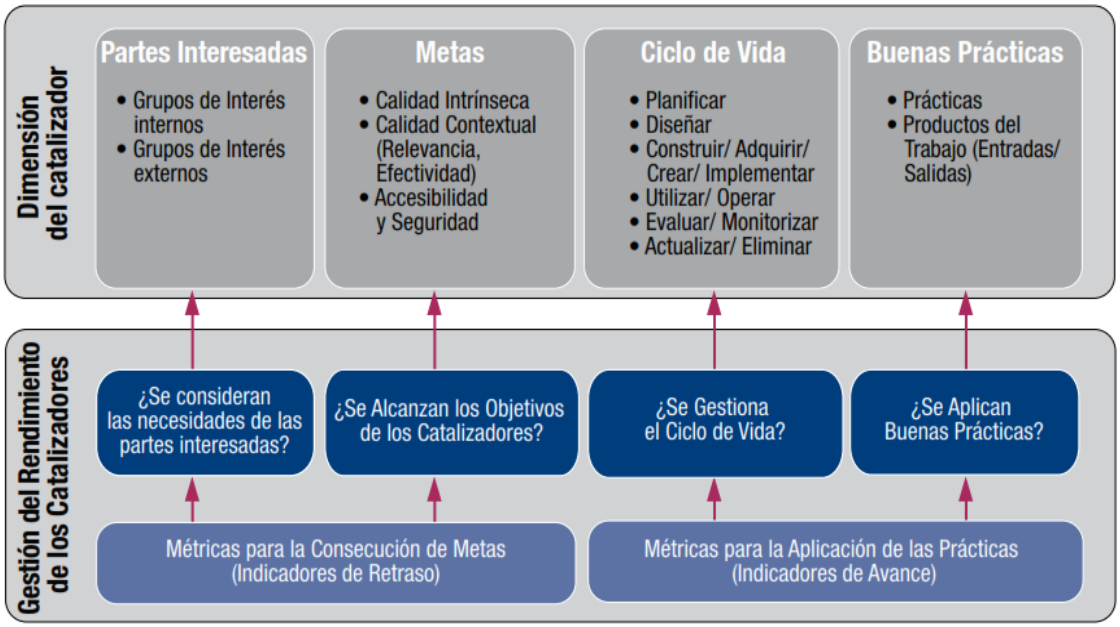



Figura 16. Dimensiones de los catalizadores de COBIT 5.
Tomado de (ISACA, 2012, pág. 28).

2.2.1.5 Principio 5: Separar el Gobierno de la Gestión

El marco de trabajo COBIT 5 plasma una distinción muy clara entre el Gobierno y la Gestión, puesto que cada área cumple diferentes propósitos e involucra actividades y responsabilidades diferentes. Esto se refleja en los dominios del modelo de referencia de procesos, tal como se muestra en la siguiente figura:

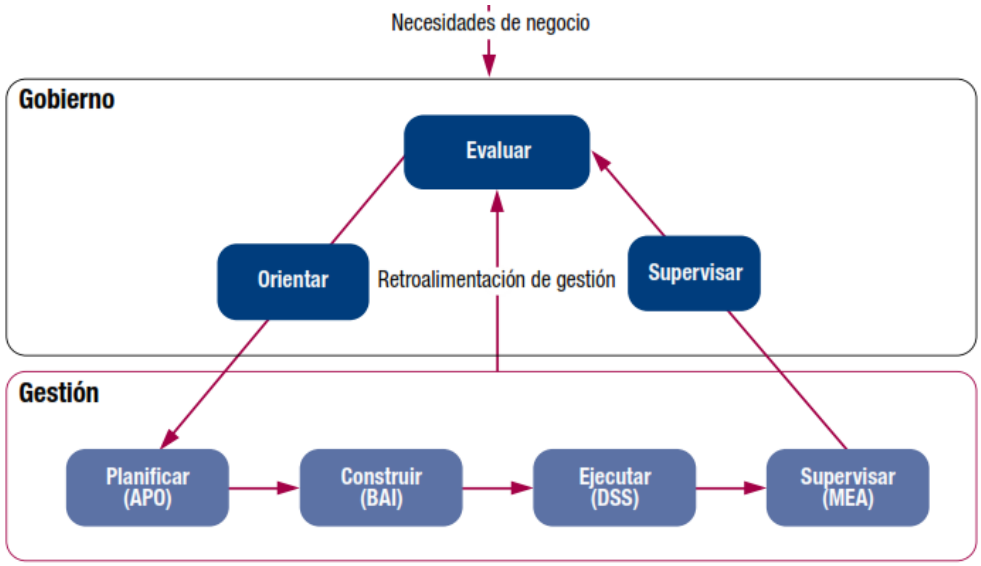



Figura 17. Modelo de referencia de procesos de COBIT 5.
Tomado de (ISACA, 2012, pág. 32).

El modelo de referencia de procesos de COBIT 5 divide los procesos de Gobierno y de Gestión de la TI empresarial en dos dominios principales, los cuales son definidos de la siguiente manera.

2.2.1.5.1 Gobierno

> "El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas". (ISACA, 2012).

2.2.1.5.2 Gestión

“La Gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales” (ISACA, 2012).

En COBIT 5, la Gestión de TI consta de 4 dominios en relación con las áreas responsables de planificar, construir, ejecutar y supervisar, proporcionando una cobertura extremo a extremo de las TI. Los nombres de estos dominios han sido elegidos de acuerdo a estas designaciones de áreas principales:

- Alinear, Planificar y Organizar (APO).
- Construir, Adquirir e Implementar (BAI).
- Entregar, dar Servicio y Soporte (DSS).
- Supervisar, Evaluar y Valorar (MEA).

La siguiente figura muestra el conjunto completo de los 37 procesos de Gobierno y Gestión de TI de COBIT 5.

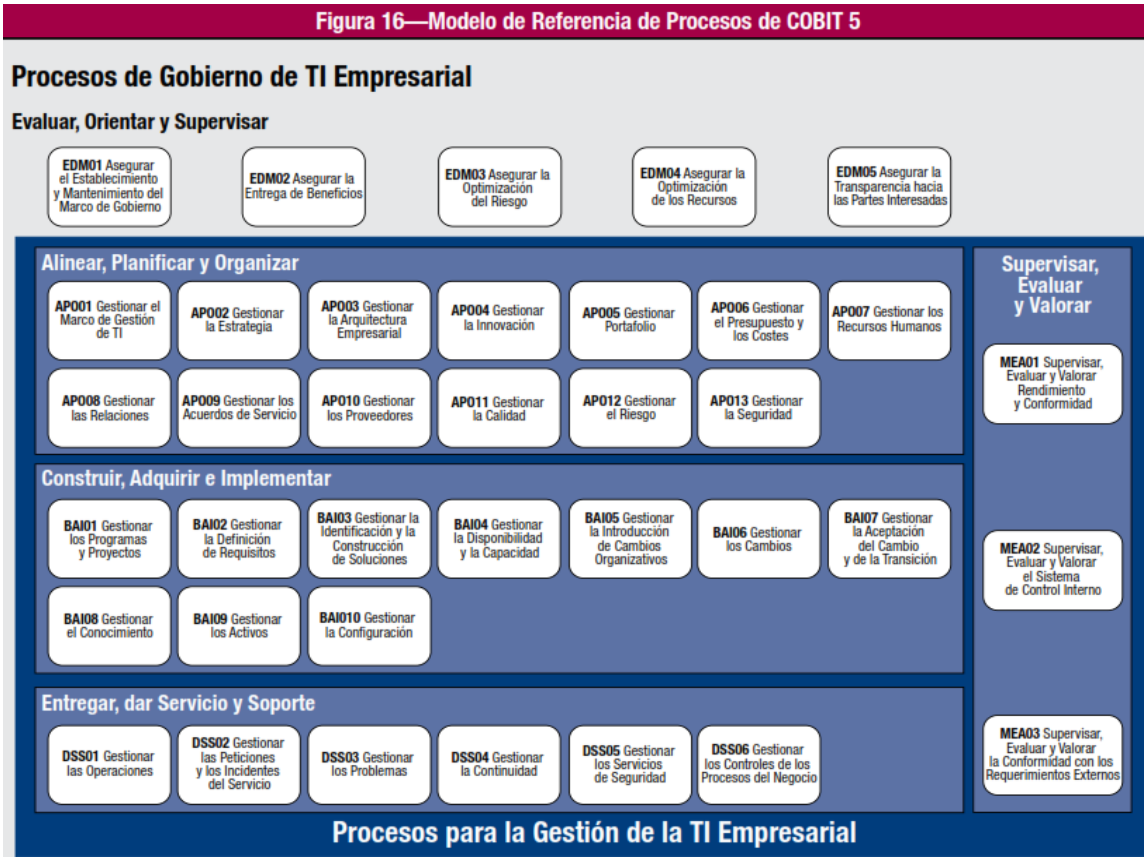



Figura 18. Modelo de referencia de procesos COBIT 5.
Tomado de (ISACA, 2012, pág. 33).

### 2.2.2 Guía de Implementación

ISACA proporciona guías de implementación de COBIT 5, que define la manera cómo aplicar las buenas prácticas de Gobierno y Gestión de TI para las organizaciones, proponiendo un modelo de referencia de 37 procesos de los cuales las empresas deberán analizar y evaluar cuales son necesarios para incrementar su competitividad y lograr eficiencia operativa.

Entre los principales aspectos a ser tomados en cuenta para tener una correcta implementación de COBIT 5 en una organización están:

- **Considerar el Contexto Empresarial:** Entender los factores internos y externos de la empresa, donde cada empresa necesita diseñar su propio plan de implantación.
- **Creando el Entorno Apropiado: "**Es importante para las iniciativas de implementación que se apoyen en COBIT 5 que sean correctamente gobernadas y adecuadamente gestionadas" (ISACA, 2012). El compromiso, apoyo y orientación de los stakeholders clave es crítico para que las mejoras sean adoptadas y mantenidas, además se hace necesario contar con los recursos adecuados para apoyar el programa, considerando que los objetivos y beneficios de la implementación necesitan ser claramente expresados en términos de negocio.
- **Reconociendo las Puntos Débiles y sus Eventos Desencadenantes:** El reconocimiento de puntos débiles pueden indicar una necesidad de mejora del Gobierno y Gestión de la TI empresarial, factores como: bajo retorno de valor al negocio referente a la inversión en TI, Fallos sistemáticos en los niveles de servicio, nuevos requerimientos regulatorios y contractuales, Insuficientes recursos de TI, etc.
- **Facilitando el Cambio:** Una implementación con éxito depende de utilizar los catalizadores apropiados de Gobierno o Gestión de TI en el cambio. En muchas empresas, hay una importante atención en los aspectos esenciales de Gobierno o Gestión de TI, pero no el suficiente énfasis en gestionar los aspectos humanos, culturales y de comportamiento del cambio y motivar a los interesados en involucrarse con el mismo.
- **Un Enfoque de Ciclo de Vida:** "La implementación del ciclo de vida proporciona a las empresas una manera de usar COBIT para solucionar la complejidad y los desafíos que normalmente aparecen durante las implementaciones" (ISACA, 2012). Los tres componentes interrelacionados del ciclo de vida son: Ciclo de vida de Mejora continua, habilitación del cambio y gestión del programa.

En la siguiente figura se muestra el ciclo de vida y sus siete fases:

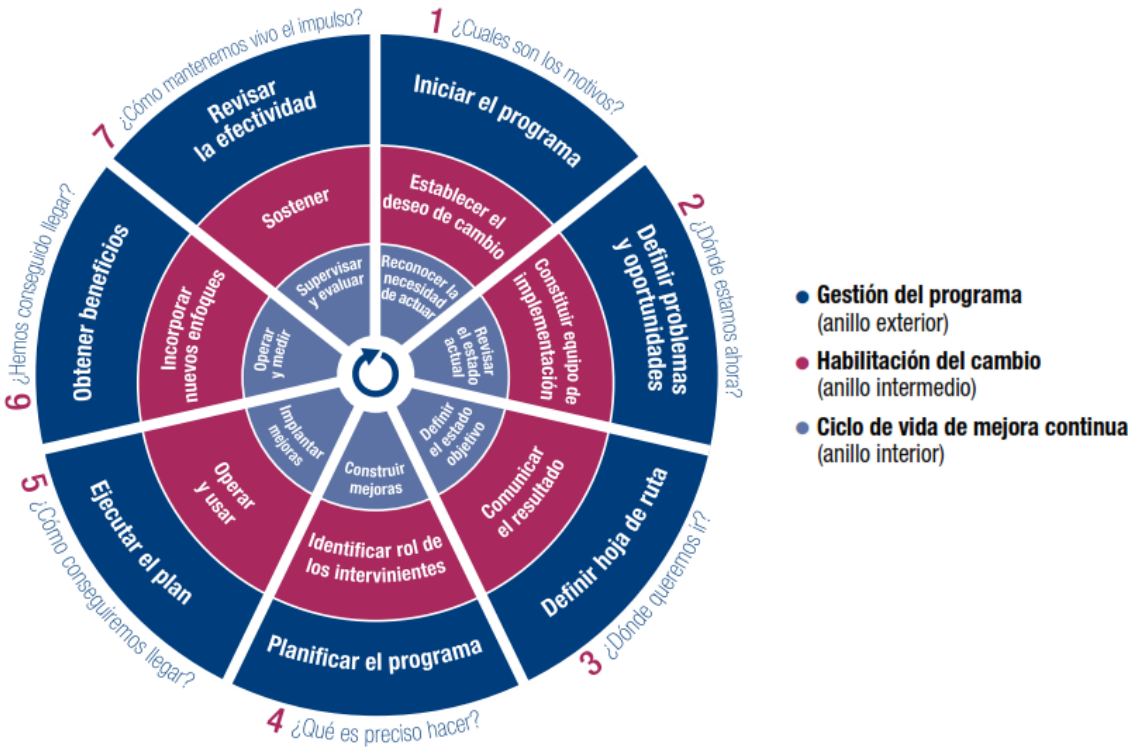



Figura 19. Las siete fases de la implementación del ciclo de vida.
Tomado de (ISACA, 2012, pág. 37).

### 2.2.3 Modelo de Evaluación de Procesos (PAM)

COBIT 5, dentro de su marco de trabajo establece la necesidad de una evaluación de la capacidad de los procesos de TI más rigurosa y confiable por lo que se apoya en la norma “ISO/IEC 15504 de Ingeniería de Software Evaluación de Procesos, este modelo alcanzará los mismos objetivos generales de evaluación de procesos y apoyo a la mejora de procesos, proporcionando un medio para medir el desempeño de los procesos de Gobierno o de Gestión de TI” (ISACA, 2012). El enfoque de COBIT 5 de capacidad de los procesos se puede resumir como se muestra en la siguiente figura:

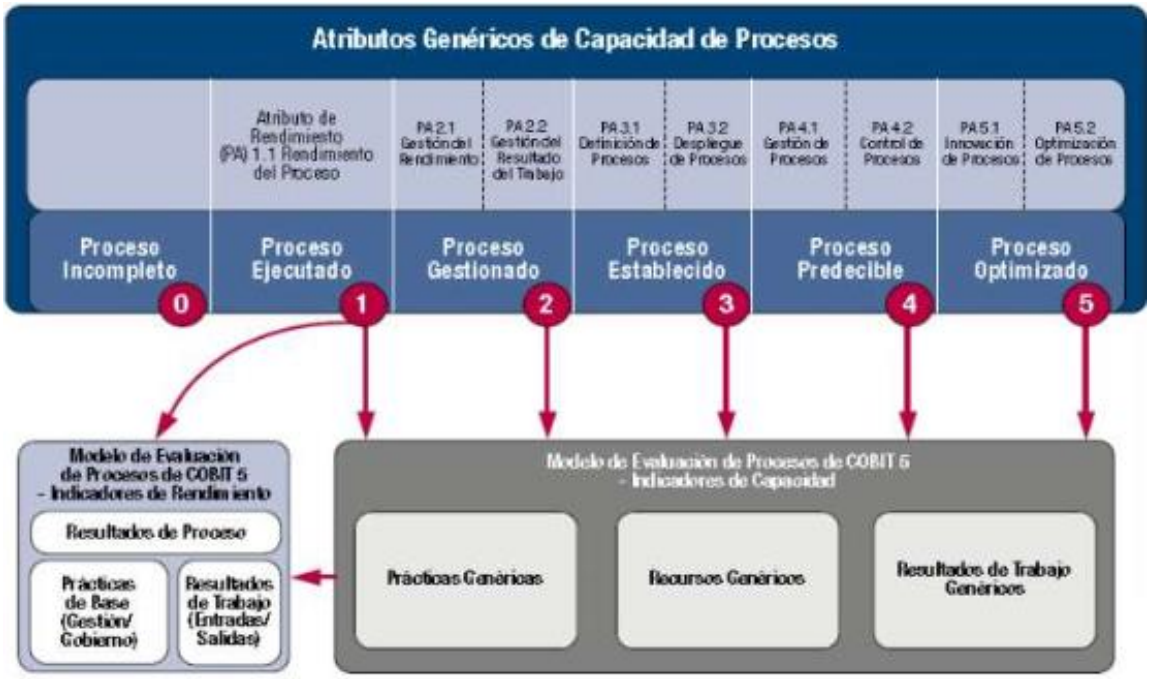



Figura 20. Modelo de Capacidad de Procesos COBIT 5.
Tomado de (ISACA, 2012, pág. 42).

En el anexo 1, se describe el Modelo de evaluación de Procesos (PAM) de COBIT 5 y los elementos de evaluación de la capacidad de procesos.

## 2.3 Normas, Leyes y Regulaciones para la Seguridad de la Información aplicable al sector sanitario

El uso de las Tecnologías de la Información dentro de las organizaciones del sector sanitario ha ido aumentando rápidamente, permitiendo optimizar y mejorar la prestación de sus servicios, convirtiéndose en una herramienta valiosa dentro del proceso de atención médica. Así mismo la continua evolución de la tecnología, indudablemente representa una fuente de posibles riesgos para las organizaciones.

En la actualidad uno de los activos más importantes que poseen las organizaciones es la información; sin embargo, en muchas ocasiones éstas no cuentan con políticas adecuadas para protegerla, generando vulnerabilidades

que pueden ser aprovechadas por las amenazas existentes en el entorno y por ende afectar a la integridad, confidencialidad y disponibilidad de los activos de información.

A medida que las organizaciones de salud se vuelven cada vez más críticamente dependientes de TI, resulta evidente que al existir eventos de pérdida de integridad, disponibilidad y confidencialidad de la información, “puede producir un significativo impacto en el aspecto clínico de los pacientes y en los servicios que presta la organización, conllevando a sanciones económicas y legales” (ISO, 2008).

Por su naturaleza, las organizaciones de salud operan en un entorno donde los trabajadores, pacientes, visitantes y público en general transitan a través de las áreas operativas, así mismo la privacidad de los datos en la atención sanitaria se ve amenazada en muchos niveles porque a menudo los sistemas de TI son altamente distribuidos con muchos usuarios y varios enlaces de comunicación entre los componentes del sistema. Por lo cual la seguridad y la integridad de los sistemas de información sanitaria deben protegerse tanto contra ataques externos como internos.

El dominio de la salud y por consiguiente, los sistemas de TI de atención médica está sujeto a una gran variedad de leyes y reglamentos casi como ninguna otra. Actualmente existe una gran cantidad de normas y regulaciones que se refieren a la Seguridad de la Información para el sector salud, actualmente debido a factores como la escasa coordinación y normalización internacional, se han generado reglamentos específicos para cada país, así mismo algunas regulaciones que fueron adaptadas a los sistemas de TI de atención médica y que inicialmente sólo se dirigían a procesos médicos no computarizados. En las siguientes páginas se describen las normas, leyes y regulaciones más relevantes sobre Seguridad de la Información en el sector sanitario. Por otra parte es importante revisar los conceptos de Seguridad de la

Información, gestión del riesgo y gestión de la Seguridad de la Información, mostrando cómo se relacionan entre sí y su aplicación en el sector sanitario.

### 2.3.1 Seguridad de la Información

El término Seguridad de la Información se divide a menudo en los tres componentes de confidencialidad, integridad y disponibilidad. A continuación se realiza una breve definición de cada uno de estos términos.

- **Confidencialidad:** “La confidencialidad se refiere a que la información no es accesible o revelada a personas no autorizadas” (Wallin & Xu, 2008). La confidencialidad es un estatus que se otorga a los datos o información que indican que es sensible por alguna razón, por lo que debe protegerse contra el robo o divulgación.
- **Integridad:** “Es el mantenimiento de la exactitud y completitud de la información y sus métodos de procesamiento” (Wallin & Xu, 2008). En el sector sanitario la integridad de la información es imprescindible puesto que guía al personal de salud en la toma de decisiones. La información incorrecta sobre el cuidado de la salud puede resultar en eventos peligrosos como la muerte de pacientes o en pacientes que reciben un medicamento equivocado.
- **Disponibilidad:** “La disponibilidad es garantizar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando sea necesario” (Wallin & Xu, 2008), las organizaciones sanitarias debido a su naturaleza y para funcionen adecuadamente, los interesados autorizados deben tener acceso a la información siempre que surja la necesidad.

En este punto y para tener una mejor comprensión de los ítems siguientes es relevante tratar sobre la Seguridad Informática y la Seguridad de la Información, aunque ambas persiguen un fin común que es el proteger la información de la organización, tienen diferencias que radican principalmente

en el enfoque, las metodologías utilizadas, y las zonas de concentración. Dicho esto la Seguridad Informática se centra en proteger las infraestructuras tecnológicas y de comunicación que soportan la operación de una organización (se centra básicamente en hardware y software), y que estas sean utilizadas de la manera indicada. Por otra parte la Seguridad de la Información se puede definir como un conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información. Tanto la Seguridad Informática como la Seguridad de la Información consideran la gestión de riesgos dentro de sus técnicas.

### 2.3.2 Gestión del riesgo

La Gestión de Riesgo es un conjunto de actividades coordinadas que permiten determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo. Las actividades básicas de gestión del riesgo suelen incluir la identificación de riesgos, la evaluación del riesgo y el tratamiento del riesgo.

- **Identificación del riesgo:** Es un proceso que utiliza datos en tiempo real para identificar vulnerabilidades y amenazas relacionadas con tecnología, personas y procesos de seguridad. Una vez que los riesgos han sido identificados, deben ser evaluados en cuanto a la gravedad potencial de la pérdida y la probabilidad de su ocurrencia.
- **Evaluación del riesgo:** La evaluación del riesgo evalúa la gravedad de la pérdida y la probabilidad de ocurrencia después de que se haya identificado el riesgo. Una vez que los riesgos han sido identificados y evaluados, la organización debe buscar tratamiento potencial para los riesgos.
- **Tratamiento del riesgo:** Es el proceso de selección e implementación de medidas para modificar el riesgo.

La implementación de estas técnicas para gestionar los riesgos para una organización puede reducir la probabilidad de una amplia gama de amenazas y, en consecuencia, disminuir el impacto adverso en los sistemas de información de la organización.

Uno de los principales beneficios del proceso de gestión de riesgos es el registro de riesgos. Esto identifica claramente los principales riesgos que deben abordarse y subraya cómo la gestión de riesgos se relaciona con la gestión de la Seguridad de la Información. La gestión de la Seguridad de la Información no puede identificar los mejores controles de gestión de Seguridad de la Información sin identificar los riesgos relevantes.

### 2.3.3 Gestión de la Seguridad de la Información

La gestión de la Seguridad de la Información, implica que las organizaciones clasifiquen sus activos de información en términos de su valor, requerimientos legales, sensibilidad y criticidad, con el propósito de identificar los riesgos que pueden afectar su seguridad. La gestión de la Seguridad de la Información es un proceso continuo que requiere la participación activa de toda la organización, y consiste en garantizar que los riesgos de la Seguridad de la Información sean identificados, valorados, gestionados y tratados por todos los miembros de la organización de una forma documentada, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

### 2.3.4 Norma ISO/IEC 27000

La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI) proporcionan las recomendaciones de mejores prácticas sobre riesgos de Seguridad de la Información, gestión y controles a través de sus normas ISO/IEC 27000 series. Estas normas especifican los requerimientos que deben cumplir las organizaciones para

establecer, implementar, poner en funcionamiento, controlar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI).
Las normas de gestión de la Seguridad de la Información que son relevantes para esta investigación y que hasta la fecha son normadas por el Instituto Ecuatoriano de Normalización (INEN) son:

- ISO/IEC 27001: 2005 - Técnicas de Seguridad de las Tecnologías de la Información: Requisitos de los Sistemas de Gestión de la Seguridad de la Información.
- ISO/IEC 27002: 2005 - Técnicas de Seguridad de las Tecnologías de la Información: Código de Prácticas para la Gestión de la Seguridad de la Información.
- ISO 27799: 2008 - Informática de la Salud: Gestión de la Seguridad de la Información en Salud utilizando ISO / IEC 27002.

#### 2.3.4.1 Norma ISO/IEC 27001:2005

Publicada el 15 de octubre de 2005, es la norma principal de la familia de la ISO/IEC 27000, y promueve la adopción de un enfoque basado en procesos y especifica los “requisitos para la creación, implantación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información” (ISO/IEC, 2005) documentado dentro del contexto de las actividades empresariales de la organización y de los riesgos que ésta afronta. Los requisitos establecidos en esta norma son genéricos y aplicables a todas las organizaciones, cualquiera que sea su tipo, tamaño y naturaleza.
La norma ISO/IEC 27001: 2005, tiene su origen en la BS 7799-2:2002 y es la norma sobre la cual se certifican, por auditores externos, los SGSI de las organizaciones. A pesar de no ser obligatoria la implementación de todos los controles, se debe argumentar la no aplicabilidad de los controles no implementados. Esta norma propone un “modelo PDCA que está compuesto de cuatro pasos que son: Planear – Hacer – Chequear – Actuar, aplicado a los procesos del SGSI, ya que es un modelo de mejoramiento continuo” (ISO/IEC,

2005). La figura 22 muestra el SGSI propuesto por la norma ISO/IEC 27001, el cual, a partir de los requisitos y expectativas de Seguridad de la Información de las partes interesadas y a través de las acciones y procesos necesarios, produce los elementos de salida que responden a dichos requisitos y expectativas.

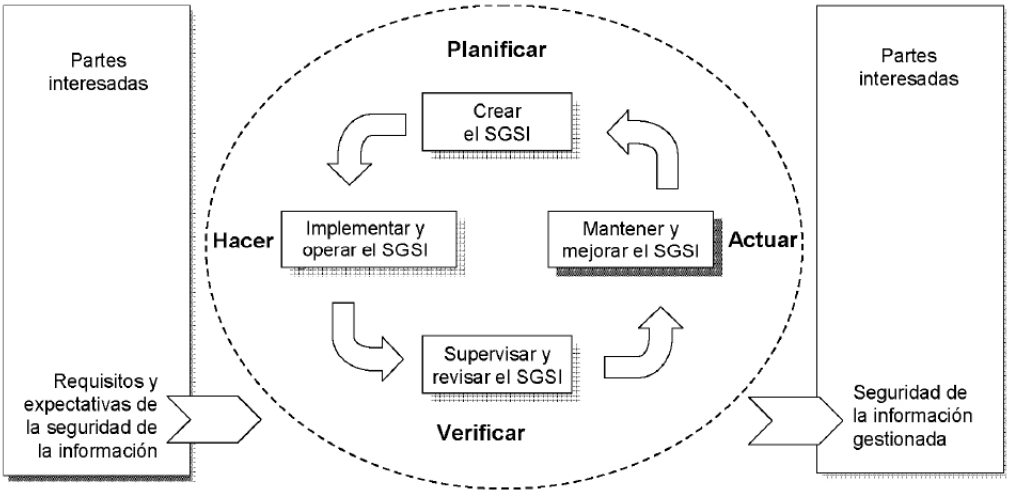



Figura 21. Modelo PDCA aplicado a los procesos SGSI.
Adaptado de (ISO/IEC, 2005, pág. vi).

- **Planear (Plan):** "Establecer políticas, objetivos, procesos y procedimientos del SGSI, los cuales permiten optimizar el manejo del riesgo y obtener una idea macro del mejoramiento de la Seguridad de la Información" (ISO/IEC, 2005), cabe señalar que dichas políticas deberán estar alineadas con las políticas internas de la empresa u organización.
- **Hacer (Do): "**Ejecutar las políticas, objetivos, procesos y procedimientos que se encuentran en el SGSI" (ISO/IEC, 2005).
- **Chequear (Check):** "Hacer un levantamiento de información y verificar si se ha cumplido con los objetivos establecidos en el SGSI, lo cual generará un informe donde se encuentren plasmados los resultados y novedades encontradas" (ISO/IEC, 2005).
- **Actuar (Act)**: "Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna del SGSI y la revisión gerencial u otra

revisión relevante, para lograr el mejoramiento continuo del SGSI" (ISO/IEC, 2005).

ISO/IEC 27001:2005 está estructurada en ocho cláusulas. Las tres primeras cláusulas tratan el alcance, la aplicación de la norma y las definiciones. Las cláusulas cuatro a la ocho están orientadas a procesos y definen los requisitos para la implementación y mejora de un SGSI.

Tabla 2.
Estructura de la norma ISO/IEC 27001:2005.

| | | |
|---|---|---|
| **ISO/IEC 27001:2005** | Clausulas | 1.- Alcance |
| | | 2.- Referencias normativas |
| | | 3.- Términos y definiciones |
| | | 4.- Sistema de gestión de seguridad de la información |
| | | 5.- Responsabilidad de la gerencia |
| | | 6.- Auditorías internas SGSI |
| | | 7.- Revisión Gerencial del SGSI |
| | | 8.- Mejoramiento del SGSI |
| | Anexos | A.- Normativo |
| | | B.- Informativo |
| | | C.- informativo |

2.3.4.2 Norma ISO/IEC 27002:2005

La norma ISO/IEC 27002:2005, anteriormente conocida como ISO/IEC 17799, establece "las directrices y los principios generales para iniciar, implantar y mantener la gestión de la Seguridad de la Información en una organización" (ISO/IEC, 2005). Esta norma pretende ser una guía práctica para desarrollar estándares organizacionales de seguridad y prácticas de gestión de la seguridad efectivas, así como para fortalecer la confianza a la hora de llevar a cabo actividades interorganizacionales.

Los objetivos y controles de la norma ISO/IEC 27002:2005 proporcionan una guía general sobre las metas de gestión de la Seguridad de la Información más comúnmente aceptadas. De manera que se obtenga una reducción de riesgos

debido al establecimiento y seguimiento de controles sobre ellos, logrando reducir las amenazas hasta tener un nivel de riesgo asumible por la organización.


Figura 22. Dominios de seguridad de la norma ISO/IEC 27002:2005.

Los dominios de la norma ISO/IEC 27002:2005 no solo hace referencia a la área de Tecnología de la Información, sino que también enfoca asuntos organizaciones, seguridades físicas, gestión de personal, administración de políticas, etc. Como se puede ver en la siguiente tabla esta norma contiene 11 dominios de controles con un total de 39 categorías y 133 controles de seguridad.

Tabla 3.

Estructura de la norma ISO/IEC 27002:2005.

| Dominios | Categorías | Controles |
|---|---|---|
| 5.- Política de seguridad | 1 | 2 |
| 6.- Aspectos organizativos de la seguridad de la información | 2 | 11 |
| 7.- Gestión de activos | 2 | 5 |
| 8.- Seguridad ligada a los recursos humanos | 3 | 9 |
| 9.- Seguridad física y ambiental | 2 | 13 |
| 10.- Gestión de comunicaciones y operaciones | 10 | 32 |
| 11.- Control de acceso | 7 | 25 |
| 12.- Adquisición, desarrollo y mantenimiento de los sistemas de información | 6 | 16 |
| 13.- Gestión de incidentes de seguridad de la información | 2 | 5 |
| 14.- Gestión de la continuidad del negocio | 1 | 5 |
| 15.- Cumplimiento | 3 | 10 |
| Total | 39 | 133 |

Cada categoría de la norma ISO/IEC 27002:2005, contiene un objetivo que expone aquello que se pretende conseguir, y también uno o más controles de seguridad que pueden ser aplicados para satisfacer el objetivo de cada categoría.

### 2.3.4.3 Norma ISO 27799:2008

La ISO 27799:2008 fue publicada en junio del año 2008 y desarrollada por el Comité Técnico ISO/TC-215 responsable de Salud Informática. La ISO 27799:2008 aborda el área de la información personal de salud y cómo proteger su confidencialidad e integridad, al tiempo que garantiza su disponibilidad para la prestación de servicios de salud. Esta norma “establece un conjunto de controles detallados para la gestión de la Seguridad de la Información de salud y proporciona directrices de buenas prácticas de Seguridad de la Información de salud” (ISO, 2008). Mediante la implementación de esta Norma Internacional, las organizaciones sanitarias y otros custodios de la información de salud podrán garantizar un nivel mínimo de seguridad que sea apropiado a las circunstancias de su organización y que mantenga la confidencialidad, integridad y disponibilidad de la información de salud.

Se prevé que la adopción de la norma ISO 27799:2008 ayudará a tener una mejor adopción de las nuevas tecnologías que colaboran en la prestación de servicios de salud. Esto debido a que los profesionales de la salud contribuyeron con su experiencia durante la definición de las directrices para apoyar específicamente la interpretación e implementación de la ISO/IEC 27002 en informática de salud. La norma ISO 27799:2008 “está pensada como un documento complementario a la ISO/IEC 27002. No pretende suplantar la norma ISO/IEC 27002 e ISO/IEC 27001. Más bien, es un complemento a estas normas más genéricas” (ISO, 2008).

La ISO 27799:2008 se aplica a la información de salud en todos sus aspectos: Cualquiera que sea la forma que tome la información (palabras y números, grabaciones sonoras, dibujos, imágenes de vídeo e imágenes médicas), cualquier medio utilizado para almacenarla (impresión o escritura en papel o almacenamiento electrónico) y cualquier medio utilizado para transmitirlo (a mano, vía fax, redes informáticas o por correo), ya que la información siempre debe estar debidamente protegida. (ISO, 2008).

Aunque la norma ISO 27799:2008 se basa en la ISO/IEC 27002, la estructura de la ISO 27799:2008 difiere. Comienza con un prólogo y una introducción (sin numerar) y tiene otras siete secciones numeradas de 1 a 7. Al igual que la ISO/IEC 27002:2005, la introducción y las secciones del 1 a 6 abordan aspectos introductorios e informativos como una introducción a la Seguridad de la Información de salud, el alcance de la norma, las referencias normativas, los términos y definiciones de Seguridad de la Información de la salud y un extenso plan de acción práctico para la aplicación de la norma ISO/IEC 27002. La mayor parte de la norma está establecida en la sección 7 que abarca las cláusulas de seguridad, control de objetivos y controles de la norma. La última parte de la norma comprende tres anexos y una bibliografía.

Es importante señalar que la norma ISO 27799:2008 incorpora aspectos de la ISO/IEC 27001:2005 en su sección 6, que discute un plan de acción para

implementar la ISO/IEC 27002. A continuación, en la tabla número 5 se muestra la estructura de la norma ISO 27799:2008.

Tabla 4.

Estructura de la norma ISO 27799:2008.

| **ISO 27799:2008** | |
|---|---|
| 1.- Alcance | |
| 2.- Referencias normativas | |
| 3.- Términos y definiciones | • Términos de salud.<br>• Términos de seguridad de la información. |
| 4.- Términos abreviados | |
| 5.- Seguridad de la información sanitaria | • Objetivos de seguridad de la información en salud<br>• Seguridad de la información dentro de la gobernanza de la información<br>• Gobernanza de la información dentro del gobierno corporativo y clínico<br>• Información de salud a proteger<br>• Amenazas y vulnerabilidades en la seguridad de la información de salud |
| 6.- Plan de acción práctico para la aplicación de la norma ISO/IEC 27002 | • Taxonomía de las normas ISO/IEC 27002 e ISO/IEC 27001<br>• Compromiso de la administración con la implementación de ISO/IEC 27002<br>• Establecer, operar, mantener y mejorar el SGSI<br>• Planificar: establecimiento del SGSI<br>• Hacer: implementar y operar el SGSI<br>• Comprobar: monitoreo y revisión del SGSI<br>• Actuar: mantener y mejorar el SGSI |
| 7.- Implicaciones para la salud de ISO/IEC 27002. | • General<br>• Política de seguridad de la información<br>• Organización de la seguridad de la información<br>• Gestión de activos<br>• Seguridad de los recursos humanos<br>• Seguridad física y medio ambiental<br>• Comunicaciones y gestión de operaciones<br>• Control de acceso<br>• Adquisición, desarrollo y mantenimiento de sistemas de información<br>• Gestión de incidentes de seguridad de la información<br>• Aspectos de la seguridad de la información en la gestión de la continuidad del negocio (BCM)<br>• Conformidad |
| Anexo A (informativo): Las amenazas a la seguridad informática de la salud | |
| Anexo B: Tareas y documentación del SGSI | |
| Anexo C: Beneficios potenciales y atributos de las herramientas de apoyo | |

### 2.3.5 Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA)

HIPAA es una ley estadounidense diseñada para establecer mecanismos estandarizados para proporcionar seguridad y confidencialidad de todos los datos relacionados con la salud, la ley “fue aprobada el 21 de agosto 1996 por el congreso de los Estados Unidos y entró en vigor el 14 de abril de 2003” (Beaver & Herold, 2004). Los objetivos fundamentales de la ley son:

- Facilitar a las personas el obtener y mantener un seguro médico.
- Proteger la confidencialidad y la Seguridad de la Información del cuidado médico.
- Ayudar a la industria de la salud a controlar costos administrativos.

HIPAA se divide en cinco títulos, en donde cada título trata un aspecto único de la reforma del seguro de salud, como lo muestra la siguiente tabla:

Tabla 5.
Estructura de la ley HIPAA.

| | Títulos | Descripción |
|---|---|---|
| **HIPAA** | Título I – Portabilidad | Portabilidad, se refiere a que las personas puedan llevar su seguro médico de un trabajo a otro sin que colapse su cobertura. Restringe a los planes médicos sobre el tema de condiciones preexistentes cuando se cambia de un plan a otro. |
| | Título II – Simplificación Administrativa | Define las políticas, procedimientos y directrices para mantener la privacidad y seguridad de información de salud identificable individualmente, así como esbozar numerosos delitos relativos a la salud y establece sanciones civiles y penales por violaciones.<br>• Regla de privacidad<br>• Transacciones y código establece reglas<br>• Regla de seguridad<br>• Regla de identificadores únicos<br>• Aplicación de la regla |
| | Título III – Disposiciones de Salud Relacionadas a Impuestos | Estandariza la cantidad que puede ser salvada por persona en una cuenta de ahorros médica antes de impuestos. |
| | Título IV – Aplicación y Cumplimiento de los Requisitos de Planes Grupales de Salud. | Especifica las condiciones para planes de salud colectivos con respecto a la cobertura de las personas con condiciones preexistentes. |
| | Título V – Retenciones de Ingresos | Contiene disposiciones relacionadas con la propiedad de la compañía de seguros de vida. |

HIPAA se ocupa de la seguridad y privacidad de la información de salud a través de la regla de privacidad (normas de privacidad de la información de salud individualmente identificable) y la regla de seguridad (normas de seguridad para la protección de la información de salud electrónica).

#### 2.3.5.1 Regla de privacidad

La regla de privacidad HIPAA permite que el "personal médico use y revele solo la información médica protegida para su tratamiento, pago y operaciones de atención médica sin autorización escrita. La mayoría de los usos adicionales y revelaciones requieren del permiso del paciente" (Office for Civil Rights, 2003). Bajo la regla de privacidad, el paciente tiene derecho a:

- Recibir copia del comunicado de prácticas de privacidad del sistema médico militar.
- Solicitar acceso a la información personal de salud (PHI - Protected Health Information).
- Solicitar corrección de la PHI.
- Solicitar un resumen de todas las divulgaciones de la PHI.
- Solicitar restricción en el uso y divulgación de la PHI.
- Presentar una queja en relación con infracciones a la privacidad.

#### 2.3.5.2 Regla de seguridad

La regla de seguridad HIPAA especifica un "conjunto de procesos empresariales y requisitos técnicos que los proveedores, planes médicos y oficinas de compensación deben seguir para garantizar la Seguridad de la Información médica" (Office for Civil Rights, 2003). La regla de seguridad se orienta a tres áreas:

- **Salvaguardias Administrativas:** estas son prácticas diseñadas para controlar las medidas de seguridad y la conducta del personal que

accede, ve, procesa y distribuye electrónicamente información médica protegida.

- **Salvaguardias Físicas:** estos son procesos que protegen equipo físico y edificios relacionados, de peligros naturales y medio ambientales, así como de intrusiones físicas.
- **Salvaguardias Técnicas:** estos son mecanismos técnicos y procesos diseñados para proteger, controlar y monitorear el acceso a la información.

Control de acceso:

- Restringir el acceso sólo al personal autorizado.
- El acceso por función o usuario particular es una manera de ayudar a divulgar el mínimo necesario.
- Uso de contraseña para controlar el acceso y autentificar al usuario.

### 2.3.6 Ley de Salud para la Salud Económica y Clínica (HITECH)

La ley HITECH aprobada en el año 2009, impone requisitos regulatorios más estrictos bajo las reglas de seguridad y privacidad de HIPAA, aumenta las sanciones civiles por una violación de HIPAA. HITECH provee fondos para la adopción de tecnología de información de salud en hospitales y servicios particulares de médicos.

Aparte de hacer cumplir las reglas de la HIPAA, HITECH “toma en cuenta la notificación de incumplimiento y acceso a los registros de salud electrónicos” (Freedman, 2009). La ley HITECH requiere que cualquier uso y divulgación no autorizados genere una notificación de violación de datos, por ejemplo, los pacientes serán notificados de cualquier incumplimiento no garantizado. La ley otorga a las personas el derecho a obtener sus registros médicos electrónicos y también pueden designar a un tercero para que reciba esta información.

### 2.3.7 Legislación de la Unión Europea (UE) sobre protección de la información personal

La situación normativa en Europa para el tratamiento de los datos médicos es compleja, ya que existen diferentes fuentes de regulación. La Unión Europea a través de su órgano ejecutivo la Comisión Europea (CE) propone leyes, así como cada Estado miembro posea sus propias legislaciones. Esto aplica tanto a los reglamentos que tienen relación con la protección de datos en general, así como las regulaciones dirigidas específicamente a los datos médicos. Para los reglamentos sobre protección de la información personal, la Unión Europea emite directivas generales, que son implementadas en las leyes nacionales por los estados miembros.

#### 2.3.7.1 Directiva 95/46/CE de la Unión Europea

La primera Directiva emitida por la Unión Europea en el año 1995 sobre protección de datos, es la 95/46/CE “relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos” (Parlamento Europeo y Consejo de la UE, 1995). La Directiva tiene como objetivo “proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo los criterios fundamentales para que el tratamiento sea lícito y los principios relativos a la calidad de los datos” (Parlamento Europeo y Consejo de la UE, 1995). El principio general de la Directiva 95/46/CE establece que los datos personales no deben ser procesados en absoluto, a menos que se cumplan las siguientes condiciones:

- El tratamiento de los datos es lícito, si: El interesado ha dado inequívocamente su consentimiento, forma parte para el cumplimiento de un contrato, forma parte para el cumplimiento de una obligación legal, proteger los intereses vitales de la persona.

- Para favorecer la transparencia, el interesado tiene derecho a ser informado sobre el tratamiento de sus datos personales.
- El procesamiento de datos tiene que ser proporcional a su propósito: cuanto más sensibles sean los datos, más esfuerzo debe hacerse para asegurar la privacidad y el anonimato.

En lo que se refiere a la protección de la información médica, El artículo 8, apartado 1, de la Directiva 95/46/CE “prohíbe el tratamiento de los datos personales relativos a la salud en general” (Parlamento Europeo y Consejo de la UE, 1995).

#### 2.3.7.2 Directiva de la Unión Europea 2002/58/EC

La información se intercambia a través de servicios de comunicaciones electrónicas como Internet y la telefonía móvil y fija, así como de sus redes de apoyo. Estos servicios y redes exigen normas y salvaguardias específicas para garantizar el derecho de los usuarios a la intimidad y la confidencialidad. Por lo cual en el año 2002 el Parlamento Europeo emite la Directiva 2002/58/CE “relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)” (Parlamento Europeo y Consejo de la UE, 2002) en apoyo a la Directiva 95/46/CE.

La Directiva 2002/58/EC “Establece normas para garantizar la seguridad en el tratamiento de los datos personales, la notificación de las violaciones de los datos personales y la confidencialidad de las comunicaciones. Asimismo, prohíbe las comunicaciones no solicitadas en las que el usuario no ha dado su consentimiento” (Parlamento Europeo y Consejo de la UE, 2002). Los datos relacionados con la salud están específicamente sujetos a regulaciones más estrictas (Artículo 8 - 95/46/CE). Su procesamiento es generalmente prohibido, a menos que el sujeto de los datos haya dado su consentimiento o los datos

sean manejados por personal médico para tratamiento o propósitos preventivos.

2.3.7.3 Reglamento de la Unión Europea 2016/679

El 25 de Mayo de 2016 se aprueba el “reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE” (Parlamento Europeo y Consejo de la UE, 2016). Este reglamento, a diferencia de las directivas anteriores, tiene como principal efecto ser de directa aplicación en toda Europa, sin necesidad de incorporación por los Estados miembros a su ordenamiento interno. No obstante, debido al calado y trascendencia de las nuevas normas y derechos regulados, será aplicable a partir del 25 de mayo de 2018. Así, durante los dos próximos años, cada Estado y todas las empresas y administraciones públicas podrán realizar las modificaciones y ajustes necesarios para garantizar su cumplimiento.

La principal diferencia entre el reglamento 2016/679 y la Directiva 95/46/CE es que se establecen normas específicas para “proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales” (Parlamento Europeo y Consejo de la UE, 2016) y además incluye normas para posibilitar la libre circulación de tales datos en la UE.

### 2.3.8 Ley Canadiense de Protección de la Información de Salud

La estrategia canadiense para la protección de la privacidad de la información está en capas y sectoriales, asumiendo que la protección de la privacidad requiere múltiples soluciones. En la capa superior, la legislación federal para la protección de la información consiste en la banca, las telecomunicaciones y el transporte, mientras que en la capa inferior, la legislación sobre privacidad y protección de la información que cubren todos los dominios. En Canadá el

derecho a la privacidad está asegurada por Corte Suprema a través de la “Ley de Protección de Información de Salud Personal, también conocida como PHIPA establecida en el año 2004, para proteger la información personal de salud” (Ministerio de Salud y Atención a Largo Plazo, 2005). PHIPA se divide en siete partes con un total de 75 secciones. Cada una de estas secciones contiene varias reglas que especifican que los custodios de información de salud (por ejemplo, hospitales) deben obtener datos con consentimiento de las personas.

Los principales objetivos de la PHIPA son los siguientes:

- Establecer reglas para la recopilación, uso y divulgación de la información personal de salud, que protejan la confidencialidad de esa información y la privacidad de las personas, al mismo tiempo que faciliten la provisión efectiva de atención médica.
- Proporcionar a los individuos el derecho de exigir el acceso, corrección o enmienda de la información personal sobre su salud.
- Proveer para revisión independiente y resolución de quejas con respecto a información de salud personal.
- Establecer que los custodios de la información de salud traten toda la información de salud personal como confidencial y mantengan su seguridad.

### 2.3.9 Ley Japonesa de Protección de Datos Personales (PDP)

La ley japonesa de Protección de Datos Personales (PDP), es una norma legal, promulgada en Japón en el año 2005 como una respuesta a la necesidad de limitar la forma en que la información personal era manipulada y compartida sin tener en cuenta los principios de privacidad y seguridad.

La Ley PDP se “aplica a todos los negocios u organizaciones que recopilan y almacenan información personal de más de cinco mil personas. El propósito del

uso es el núcleo de la nueva ley" (Legislatura Bi-Cameral Japonesa, 2005) y obliga a todas las empresas del país, incluidas las extranjeras a cumplir con las estrictas normas de la legislación.

- Sobre datos personales: Se prohíbe la entrega de datos personales. Estos son, por ley, el nombre de una persona, su dirección, fecha de nacimiento, sexo, lugar de nacimiento y números de teléfono.
- Designación de encargado de privacidad: Las empresas deben designar a un Gerente de Privacidad Corporativa que se encargará de hacer cumplir las disposiciones de la ley.
- Sobre penas y multas: Se establecen multas económicas o penas de cárcel de hasta seis meses para el Gerente o Administrador de Datos que viole la ley.

### 2.3.10 Seguridad de la Información en instituciones públicas del Ecuador

La Seguridad de la Información en el Ecuador se ha enfocado en el ámbito investigativo por parte de los centros de educación superior y también en la realización de proyectos conjuntos con las entidades del Estado como la Superintendencia de Telecomunicaciones (SUPERTEL). Como una buena práctica la SUPERTEL ha promovido la creación de un Equipo de Respuestas ante Emergencias Informáticas (CERT). Su implementación se lo realizó con una consultoría en cooperación con el Gobierno de Corea y se denominó CERT Ecuador/CC, que tiene como misión:

> "En convertirse en el centro de alerta nacional que coordine, controle y contribuya con las instituciones del sector público y privado en lo concerniente a administración y gestión de incidentes de Seguridad Informática. Además de responder de forma rápida y eficiente a los incidentes de seguridad que pudieran surgir, y afrontar de forma proactiva las nuevas amenazas en los sistemas y redes de Tecnologías de la Información internacional" (SUPERTEL, s.f.).

Para las instituciones públicas la Secretaría Nacional de la Administración Pública (SNAP) tiene como misión “Mejorar la eficiencia de las instituciones del Estado Central a través de políticas y procesos que optimicen la calidad, la transparencia y la calidez del Servicio Público” (Secretaría Nacional de la Administración Pública, s.f.). Y que mediante el Acuerdo Ministerial 166 se emite el Esquema Gubernamental de Seguridad de la Información (EGSI), donde la “SNAP dispone a las entidades de la Administración Pública Central, Institucional, y que dependen de la Función Ejecutiva, el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información (SGI)” (Secretaría Nacional de la Administración Pública, 2013).

La norma técnica Ecuatoriana NTE INEN – ISO/IEC 27002 vigente en la fecha de elaboración del presente trabajo es una traducción idéntica de la norma internacional ISO/IEC 27002:2005.

## 2.4 Resumen de Normas, Leyes y Regulaciones para la Seguridad de la Información aplicable al sector salud

El intercambio de información de salud está sujeto a muchas cuestiones de privacidad. Estos datos consisten, en muchos casos, en condiciones médicas de pacientes, información de facturación y asesoramiento médico. La importancia de la confidencialidad, integridad y disponibilidad de la información del sector sanitario ha aumentado especialmente desde la era de la computadora. Para garantizar la seguridad general de los datos en el sector salud, se han especificado varias normas internacionales, leyes o regulaciones dependiendo del país o región, indicando sobre cómo trabajar con la información de salud. A continuación se realiza un resumen de las normas, leyes y regulaciones antes descritas:

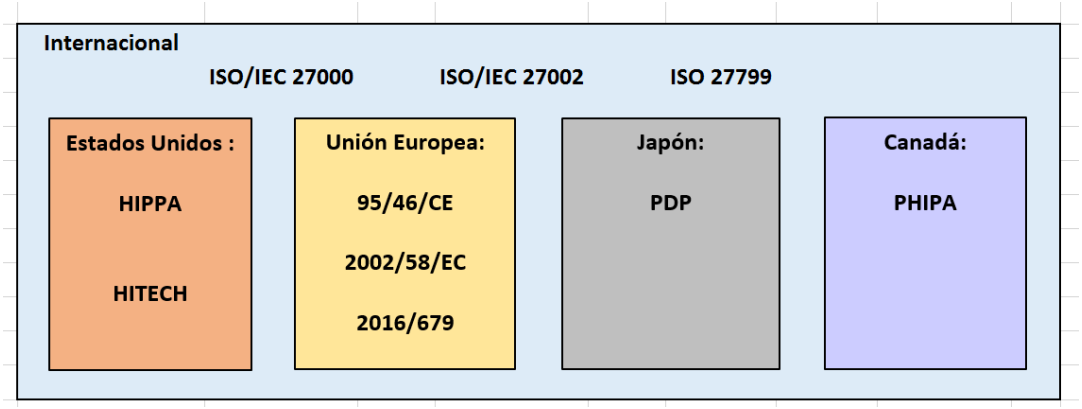



Figura 23. Resumen de normas, leyes y regulaciones para la Seguridad de la Información aplicable al sector salud.

# 3 Capítulo III. Modelo de Gobierno de TI con énfasis en Seguridad de la Información para hospitales públicos del Ecuador

Las organizaciones dependiendo de muchos factores como, el tipo de industria, los productos o servicios que comercializa, la cultura y las personas, tienen distintas necesidades y debilidades para brindar valor a sus stakeholders, así como también asegurar la confidencialidad, integridad y disponibilidad de sus activos de información. Esto ocasiona que cada empresa deba adaptar los distintos marcos de trabajo o buenas prácticas de Gobierno de TI y Seguridad de la Información a su entorno. El presente trabajo propone un modelo que sirva como referencia para los hospitales públicos del Ecuador y como se ha manifestado anteriormente cada casa de salud tendrá sus propias necesidades y deberá adaptar los procesos en base a dichas necesidades y requerimientos.

Teniendo en cuenta que el marco de Gobierno de TI sobre el que se apoya el presente trabajo es COBIT 5, se procede a generar un artefacto que contenga el mapeo de procesos y prácticas de COBIT 5 con los marcos de trabajo o buenas prácticas que apoyan la Seguridad de la Información, conforme a lo revisado en la sección 2.2.10 la SNAP dispone el uso de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información (SGI) para las entidades públicas.

## 3.1 Relación entre frameworks y buenas prácticas

COBIT por una parte define los procesos y elementos generales que intervienen en el Gobierno y Gestión de TI, junto con sus mecanismos de evaluación como son los niveles de capacidad, necesarios para las organizaciones que brindan servicios de TI a clientes internos o externos. Por otra parte la ISO/IEC 27001:2005 contiene los requisitos a cumplir para implantar un SGSI certificable. Además, la norma ISO/IEC 27002:2005

presenta directrices para los controles de Seguridad de la Información que son genéricas para todas las empresas que han considerado implementar la gestión de la Seguridad de la Información para sus actividades. Hay que mencionar también que la ISO 27799:2008, aborda el área de la información personal de salud y cómo proteger su confidencialidad e integridad, tomando como base la ISO/IEC 27002:2005. La relación entre el marco de referencia COBIT 5 y las normas ISO/IEC 27002:2005 e ISO 27799:2008 se muestran en los siguientes ítems.

### 3.1.1 Relación entre la Norma ISO/IEC 27002:2005 e ISO 27799:2008

Como se mencionó en la sección 2.4.4.3 la norma ISO 27799:2008 - Gestión de la Seguridad de la Información en Salud, contiene un conjunto detallado de controles para la gestión de la Seguridad de la Información específica para el ámbito sanitario, aclarando ser un complemento para la norma ISO/IEC 27002:2005. En este ítem se pretende determinar qué valor aporta la norma ISO 27799:2008 a la norma ISO 27002:2005 para satisfacer las necesidades de gestión de la Seguridad de la Información del sector de la salud.

Se iniciará con una comparación de alto nivel entre las dos normas que muestra las similitudes y diferencias en la estructura general de las mismas, posteriormente se realiza una comparación detallada entre las cláusulas, categorías de seguridad y controles de la norma ISO/IEC 27002:2005 y la ISO 27799:2008, que nos permita identificar las nuevas o enmendadas cláusulas, categorías de seguridad y controles incluidos en la norma ISO 27799:2008.

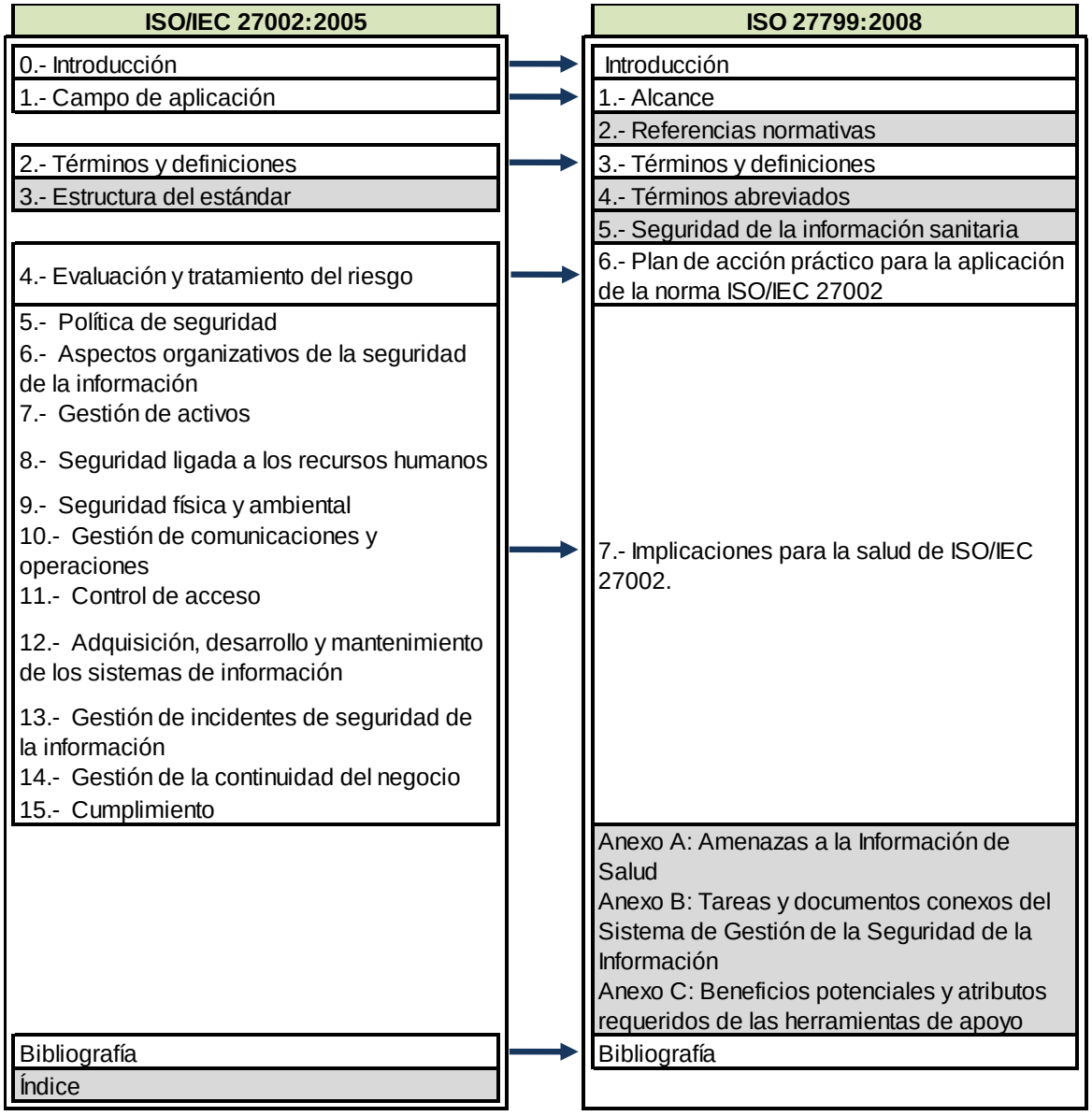
#### 3.1.1.1 Comparación de alto nivel entre la Norma ISO/IEC 27002:2005 e ISO 27799:2008

Como punto de partida, se analiza las normas ISO/IEC 27002:2005 e ISO 27799:2008 desde la perspectiva de entender a un alto nivel, cómo las secciones contenidas en las normas se corresponden entre sí. La comparación

de las dos normas se muestra esquemáticamente en la tabla 6. Donde las secciones de las normas ISO/IEC 27002:2005 e ISO 27799.2008 está representado por un rectángulo que muestra el número y nombre de la sección. Esto no implica que el contenido de las secciones sea el mismo, sino que las secciones incluidas en las normas tienen el mismo fin, por ejemplo, introducir la sección de alcance en cada norma o definir los términos y definiciones aplicables en la norma pertinente.

Tabla 6.

Comparación de alto nivel de la Norma ISO/IEC 27002:2005 e ISO 27799:2008.



Para una correcta interpretación de la tabla se debe considerar que:

- Las secciones que tienen un propósito similar entre las norma ISO/IEC 27002:2005 e ISO 27799:2008, se muestran señaladas con una flecha y representa el mapeo entre las secciones de las normas.
- Existen varias secciones que pueden clasificarse como "secciones únicas"; Es decir, estas secciones se cubren principalmente en una de las normas y no en la otra, estas secciones únicas se destacan con un sombreado en los rectángulos.

Con el fin de facilitar la comparación de alto nivel entre las secciones de las normas ISO/IEC 27002:2005 e ISO 27799:2008, en la tabla 7 se realiza una descripción de cada sección.

Tabla 7.

Descripción de las secciones de las normas ISO/IEC 27002:2005 e ISO 27799:2008.

| ISO/IEC 27002:2005 | ISO 27799:2008 |
|---|---|
| **Sección 0: Introducción**<br>Se define de manera general la seguridad de la información y su importancia en las organizaciones al proporcionar confidencialidad, integridad y disponibilidad a los activos de información importantes para el negocio. Además se describe brevemente temas como:<br>• Definición de la seguridad de la información;<br>• Importancia de la seguridad de la información en la organización;<br>• Métodos para establecer requisitos de seguridad;<br>• Evaluación de los riesgos de seguridad;<br>• La selección de los controles;<br>• Factores críticos de éxito para implementar la seguridad de la información dentro de una organización. | **Introducción**<br>Se explica la necesidad de una gestión eficaz de la seguridad informática en la asistencia sanitaria debido creciente uso de la tecnología de la información en el sector salud, indicando además que hay requisitos especiales que deben cumplirse para garantizar la confidencialidad, integridad, y disponibilidad de la información personal de salud. Se describe brevemente temas como:<br>• La importancia de SGSI adaptado para el sector salud.<br>• La relación directa que existe con la norma ISO/IEC 27002.<br>• Describir los beneficios de su uso de la norma ISO 27799. |

| | |
|---|---|
| **Sección 1: Campo de aplicación**<br>Esta sección define el alcance de la norma en términos de prácticas de gestión de la seguridad de la información, indicando que puede servir como guía práctica para el desarrollo de normas de la seguridad de una organización. | **Sección 1: Alcance**<br>Se describe el papel de la norma para la gestión de la seguridad de la información de salud. Se hace hincapié en el hecho de que es neutra desde el punto de vista tecnológico. Se confirma su aplicabilidad a la información sanitaria en todos sus aspectos y formas. Se observa la relación con la norma ISO/IEC 27002. Se identifican y se enumeran las áreas de seguridad de la información que no forman parte de la ISO 27799 por ejemplo: La calidad de servicio de la red y la calidad de los datos (a diferencia de la integridad de los datos). |
| | **Sección 2: Referencias normativas**<br>Esta sección es única. Enumera la ISO/IEC 27002 como una referencia normativa en el uso de la ISO27799. |
| **Sección 2: Términos y definiciones**<br>Se define la terminología de administración de seguridad de información general. | **Sección 3: términos y definiciones**<br>Se definen términos específicos de atención médica y alguna terminología genérica de administración de seguridad de la información. |
| **Sección 3: Estructura del estándar**<br>Esta sección es única. Explica la estructura de la norma en el número de cláusulas y categorías principales de seguridad que contiene. Se explica además que la composición de las categorías principales de seguridad comprende un objetivo de control y uno o más controles. | **Sección 4: Términos abreviados**<br>La sección 4 es única. Proporciona una lista de acrónimos utilizados en la ISO 27799. Es una lista breve que contiene solamente cinco términos. |
| | **Sección 5: Seguridad de la Información de Salud**<br>La sección 5 es única. Se realiza un esfuerzo concertado para contextualizar la seguridad de la información de salud. Los principales temas de interés en esta sección incluyen:<br>• Objetivos de seguridad de la información en salud;<br>• Seguridad de la información dentro de la gobernanza de la información;<br>• Gobernanza de la información dentro de la gobernabilidad corporativa y clínica.<br>• Información de salud a ser protegida.<br>• Amenazas y vulnerabilidades en la seguridad de la información de salud. |

| | |
|---|---|
| **Sección 4: Evaluación y tratamiento del riesgo**<br>Hace referencia sobre la evaluación de los riesgos de seguridad y se describe brevemente las posibles opciones de tratamiento. Estos temas comprenden una página y media del estándar y se discuten de forma superficial. | **Sección 6: Tratamiento / Plan de Acción Práctico para la Implementación de la Norma ISO / IEC 27002**<br>Esta sección proporciona una breve taxonomía de las normas ISO 27001 e ISO 27002. Se explica que el cumplimiento de la norma ISO 27002 no es un asunto sencillo y requiere un SGIS operacional en el que existan procesos adecuados de auditoría de cumplimiento.<br>En la sección se define la importancia de introducir un SGSI cuando exista un requisito para la acreditación formal o la certificación. Se afirma que las organizaciones sanitarias necesitan un apoyo evidente de la administración al intentar implementar un SGSI.<br>El resto de la sección proporciona una discusión detallada de establecer, operar, mantener y mejorar un SGSI en un ambiente de atención médica. |
| **Sección 5 – 15 de la ISO/IEC 27002**<br>En la sección del 5 – 15 de la ISO/IEC 27002, contiene la guía de buenas prácticas para la gestión de la seguridad de la información, La ISO/IEC 27002 contiene Dominios (11), Objetivos de control (39) y Controles (133). | **Sección 7: Implicaciones para la salud de ISO/IEC 27002.**<br>En esta sección la norma ISO 27799, establece todos los objetivos de control que son relevantes para la seguridad informática del sector sanitario, indicando que se toman en cuenta todos los objetivos de control de seguridad descritos en ISO/IEC 27002, por otro lado existen algunos controles que requieren una explicación adicional sobre su uso en la protección de la seguridad de la información de salud. También queda claro que la norma ISO 27799 es un complemento para la norma ISO/IEC 27002. |
| | **Anexo A: Amenazas a la Seguridad de la Información de Salud.**<br>El Anexo A contiene una lista informativa de los tipos de amenazas que deben ser consideradas por las organizaciones de salud al evaluar los riesgos para la confidencialidad, integridad y disponibilidad de los activos de salud.<br>**Anexo B: Tareas y Documentos Relacionados del Sistema de Gestión de la Seguridad de la Información.**<br>En el Anexo B se describen brevemente las tareas y documentos relacionados con la operación de un SGSI en un ambiente de salud. Completa el resumen del proceso del SGSI y la discusión proporcionada en la Sección 6 de la norma.<br>**Anexo C: Beneficios potenciales y atributos requeridos de las herramientas de soporte.**<br>El Anexo C discute las ventajas de las herramientas de apoyo como una ayuda para implementar la gestión de la seguridad de la información. |
| **Bibliografía**<br>Enumera las normas relacionadas con la seguridad de la información. | **Bibliografía**<br>Enumera los estándares relacionados en la seguridad de la información de salud. |
| **Índice**<br>Esta sección hace referencia a una lista alfabética de términos en relación con las cláusulas, objetivos de control y controles de la ISO/IEC 27002 utilizando los números de sección asignados. | |

Con respecto a la tabla 7, se puede declarar que:

a) Las secciones Introducción, Alcance, Términos y Definiciones de ambos estándares abordan aspectos que son requeridos para contextualizar los estándares, es decir para la norma ISO/IEC 27002:2005 estas secciones contextualizan el estándar en términos de Seguridad de la Información y Seguridad Informática, mientras que para la ISO 27799:2008 estas secciones contextualizan el Estándar en términos de la ISO/IEC 27002:2005, la Seguridad de la Información de salud y la gestión de la Seguridad de la Información de salud.

b) El contenido de las secciones únicas de la ISO 27799:2008 (es decir, las secciones 2, 4 y 5) satisface un objetivo básico, que es proporcionar la información suficiente sobre cuestiones de relevancia en el contexto de la atención sanitaria. Esto contribuye a la naturaleza de la ISO 27799:2008 como una versión específica de la industria de la ISO/IEC 27002:2005.

c) Si bien la Sección 3 de la ISO/IEC 27002:2005 es una sección única que no está cubierta en la ISO 27799:2008, la información que contiene es de relevancia directa para la ISO 27799:2008. Por lo tanto, tiene sentido que no se repita en la norma ISO 27799:2008, debido que utiliza las mismas entidades estructurales (por ejemplo: cláusulas de seguridad, principales categorías de seguridad, objetivos de control, etc.).

d) La ISO/IEC 27002:2005 establece que sus objetivos de control y controles están destinados a ser implementados para satisfacer los requisitos identificados por una evaluación de riesgos. Esto explica la inclusión de la Sección 4 en la norma, que proporciona una breve visión general de los temas de evaluación y tratamiento del riesgo. Estos temas de igual manera se tratan en la Sección 6 de la ISO 27799:2008. Además la Sección 6 de la ISO 27799:2008 revela que la sección

incluye información relacionada con el contexto de atención médica. Por ejemplo, las "reacciones de los pacientes" como un factor a tomar en cuenta en los criterios de aceptación del riesgo.

e) Se muestra que las secciones 5-15 de la ISO/IEC 27002:2005 se corresponden con la Sección 7 de la ISO 27799:2008. Estas secciones que comprenden la mayor parte de las normas, se comparan de forma detallada en el ítem 3.1.1.2.

f) Respecto a los apéndices (incluyendo bibliografía, índice y anexos) sirven como herramientas para contextualizar las normas ISO/IEC 27002:2005 e ISO 27799:2008.

#### 3.1.1.2 Comparación de las cláusulas, categorías de seguridad y controles de las Normas ISO/IEC 27002:2005 e ISO 27799:2008

La norma ISO 27799:2008 establece que “todos los objetivos de control de seguridad descritos en ISO/IEC 27002 son relevantes para la informática de la salud, pero algunos controles requieren explicaciones adicionales con respecto a cómo pueden usarse mejor para proteger la información de salud” (ISO, 2008). Las secciones 5-15 de la ISO/IEC 27002:2005 se corresponden con la Sección 7 de la ISO 27799:2008, por lo cual la comparación comienza examinando el número de cláusulas, categorías de seguridad y controles contenidos en cada norma. La tabla 8 presenta una visión general de las similitudes y diferencias en la estructura de las cláusulas de seguridad en las normas.

Tabla 8.

Cláusulas, categorías de seguridad y controles de las normas ISO/IEC 27002:2005 e ISO 27799:2008.

| | | | ISO/IEC 27002:20005 | | | ISO 27799:2008 | | |
|---|---|---|---|---|---|---|---|---|
| ISO 27002 | ISO 27799 | Clausula de seguridad | Número de sección | Números de Categorías de Seguridad | Número de Controles | Número de sección | Número de Categorías de Seguridad | Número de Controles |
| | 7.1 | General | | | | 0 | 0 | 0 |
| 5 | 7.2 | Política de Seguridad<br>Política de Seguridad de la Información | 5.1 | 1 | 2 | | 0 | 2 |
| 6 | 7.3 | Organizaciones de la seguridad de la información | | | | 7.3.1 | 3 | 0 |
| | | Organización de la seguridad de la información | 6.1 | 2 | 8 | 7.3.2 | | 4 |
| | | | 6.2 | | 3 | 7.3.3 | | 3 |
| 7 | 7.4 | Gestión de Activos | 7.1 | 2 | 3 | 7.4.1 | 2 | 0 |
| | | | 7.2 | | 2 | 7.4.2 | | 2 |
| 8 | 7.5 | Seguridad ligada a los Recursos Humanos | 8.1 | 3 | 3 | 7.5.1 | 3 | 3 |
| | | | 8.2 | | 3 | 7.5.2 | | 3 |
| | | | 8.3 | | 3 | 7.5.3 | | 2 |
| 9 | 7.6 | Seguridad Física y del Entorno | 9.1 | 2 | 6 | 7.6.1 | 2 | 3 |
| | | | 9.2 | | 7 | 7.6.2 | | 5 |
| 10 | 7.7 | Gestión de Comunicaciones y Operaciones | 10.1 | 10 | 4 | 7.7.1 | 10 | 4 |
| | | | 10.2 | | 3 | 7.7.2 | | 0 |
| | | | 10.3 | | 2 | 7.7.3 | | 2 |
| | | | 10.4 | | 2 | 7.7.4 | | 2 |
| | | | 10.5 | | 1 | 7.7.5 | | 0 |
| | | | 10.6 | | 2 | 7.7.6 | | 2 |
| | | | 10.7 | | 4 | 7.7.7 | | 4 |
| | | | 10.8 | | 5 | 7.7.8 | | 4 |
| | | | 10.9 | | 3 | 7.7.9 | | 2 |
| | | | 10.10 | | 6 | 7.7.10 | | 7 |
| 11 | 7.8 | Control de Accesos | 11.1 | 7 | 1 | 7.8.1 | 6 | 2 |
| | | | 11.2 | | 4 | 7.8.2 | | 4 |
| | | | 11.3 | | 3 | 7.8.3 | | 0 |
| | | | 11.4 | | 7 | 7.8.4 | | 0 |
| | | | 11.5 | | 6 | | | |
| | | | 11.6 | | 2 | 7.8.5 | | 2 |
| | | | 11.7 | | 2 | 7.8.6 | | 2 |
| 12 | 7.9 | Adquisición, Desarrollo y Mantenimiento de Sistemas de Información | 12.1 | 6 | 1 | 7.9.1 | 5 | 0 |
| | | | 12.2 | | 4 | 7.9.2 | | 5 |
| | | | 12.3 | | 2 | 7.9.3 | | 2 |
| | | | 12.4 | | 3 | 7.9.4 | | 3 |
| | | | 12.5 | | 5 | 7.9.5 | | 0 |
| | | | 12.6 | | 1 | | | |
| 13 | 7.10 | Gestión de Incidentes de Seguridad de la Información | 13.1 | 2 | 2 | 7.10.1 | 2 | 0 |
| | | | 13.2 | | 3 | 7.10.2 | | 3 |
| 14 | 7.11 | Gestión de Continuidad del Negocio<br>Aspectos de la seguridad de la información en la gestión de la continuidad del negocio | 14.1 | 1 | 5 | | 0 | 0 |
| 15 | 7.12 | Conformidad | | 3 | 0 | 7.12.1 | 4 | 0 |
| | | | 15.1 | | 6 | 7.12.2 | | 3 |
| | | | 15.2 | | 2 | 7.12.3 | | 0 |
| | | | 15.3 | | 2 | 7.12.4 | | 0 |

En la tabla 8, debe tomarse en cuenta que los bloques sombreados en las columnas usadas para la ISO 27799:2008, significa que no se proporciona una guía adicional por encima de la información contenida en la ISO/IEC 27002:2005. El número total de categorías de seguridad y controles de la ISO

27799:2008 es discutible ya que en esta norma no se muestra claramente las 39 categorías de seguridad y 133 controles de la ISO/IEC 27002:2005 en su estructura. Por lo cual se ha realizado una comparación detallada de cláusulas, categorías de seguridad y controles de la ISO/IEC 27002:2005 y la ISO 27799:2008, que consta en el anexo 2.

A partir de la información proporcionada en la tabla 8 y el anexo 2, se puede deducir lo siguiente:

a) La mayoría de las cláusulas ISO/IEC 27002:2005 e ISO 27799:2008 comparten los mismos nombres, pero los nombres de tres cláusulas son ligeramente diferentes la 7.2, 7.3 y 7.11 de la ISO 27799:2008.

b) Adición de nuevas cláusulas (1), categorías de seguridad (2) y controles (3) en la ISO 27799:2008:

- **Cláusula 7.1 - General:** Esta cláusula contiene consejos específicos sobre las cláusulas y categorías de seguridad descritas en la norma ISO/IEC 27002:2005. Básicamente motiva la necesidad de la ISO 27799:2008 y declara explícitamente que la guía dada en la ISO 27799:2008 es adicional, y no sustituye a la norma ISO/IEC 27002:2005.
- **Categoría de seguridad 7.3.1 - General:** Esta principal categoría de seguridad hace hincapié en la necesidad de una infraestructura explícita y sólida de gestión de la Seguridad de la Información, especialmente cuando las organizaciones dependen de servicios médicos gestionados prestados por terceros.
- **Categoría de seguridad 7.12.1 - General:** El foco principal de esta categoría está en un programa de auditoría para los sistemas de TI sanitarios y que aborde todo el ciclo de operaciones. Dicho programa no sólo debe identificar áreas problemáticas sino también revisar los resultados y decidir actualizaciones del SGSI. Se sugiere un ciclo de

12 meses a 18 meses para los programas de auditoría de las organizaciones de salud, durante el cual deben cubrirse todos los elementos de la norma.

- **Control 7.7.10.1 - General:** Este control hace hincapié en la importancia de los requisitos de seguridad relacionados con la auditoría y el registro. Destaca la importancia de garantizar la rendición de cuentas y afirma que la una auditoría y registro eficaces pueden ayudar a descubrir el uso indebido de los sistemas de información de salud o de información personal de salud.
- **Control 7.8.1.1 - General:** Este control se centra en el acceso a la información personal de salud. Hace hincapié en que los usuarios de los sistemas de información sanitaria sólo deben tener acceso a la información personal sobre la salud si existe una relación entre el usuario y el sujeto de la atención (persona afectada).
- **Control 7.9.2.1 - Identificación Exclusiva de los Pacientes:** Este control indica que es obligatorio que los sistemas de información sanitaria garanticen que los sujetos de atención (pacientes) pueden ser identificados de forma única en el sistema y también ser capaces de fusionar registros duplicados o multiplicados si tales registros fueron creados intencionalmente o durante una emergencia médica.

c) Declaraciones de control modificadas, algunas declaraciones de control en la ISO 27799:2008 se amplían para tratar cuestiones de importancia en la Seguridad de la Información de salud. En general, estas declaraciones de control enumeran requisitos más estrictos o requisitos más específicos que la norma ISO/IEC 27002:2005.

Un ejemplo de una instrucción de control modificada es la 7.2.2 “Revisión del documento de política de Seguridad de la Información”, indicando que se requiere revisiones por etapas de tal manera que la totalidad de la política se revise al menos anualmente. Además, requiere que la política se revise obligatoriamente después de la ocurrencia de un

incidente de seguridad grave. Estos requisitos no se incluyen como parte de la declaración de control en la norma ISO 27002:2005, que requiere que la política se revise a intervalos planificados o si se produjeran cambios significativos.

d) Categoría de seguridad no numeradas en la norma ISO 27799:2008, en la comparación estructural de las dos normas se identifica que secciones de la norma ISO/IEC 27002:2005 no han recibido un número de sección en la ISO 27799:2008, Por ejemplo, Categoría principal de seguridad 14.1 y los controles 14.1.1 a 14.1.5 de la ISO/IEC 27002 no se han asignado números de sección en la ISO/IEC 27799:2008. Esto confirma que la ISO 27799:2008 no puede utilizarse aisladamente, ya que conducirá a una implementación incompleta de la ISO/IEC 27002:2005.

e) Consolidación de categorías de seguridad y controles en la ISO 27799:2008, en la comparación estructural de las dos normas se muestra que se han consolido categorías principales de seguridad y controles de la ISO/IEC 27002:2005 en la ISO 27799:2008, por ejemplo los controles 6.1.1 a 6.1.8 (ocho controles) en la ISO/IEC 27002:2005 se han consolidado como controles 7.3.2.1 - 7.3.2.4 (cuatro controles) en la norma ISO 27799:2008.

f) El número total de cláusulas, categorías de seguridad y controles contenidos en las normas puede resumirse como sigue:

Tabla 9.
Total de cláusulas, categorías de seguridad y controles de las normas ISO/IEC 27002:2005 e ISO 27799:2008.

| | **ISO/IEC 27002:2005** | **ISO 27799:2008** |
|---|---|---|
| Número de Clausulas | 11 | 12 |
| Número de Categorías de Seguridad | 39 | 41 |
| Número de Controles | 133 | 136 |

Cabe indicar que los totales calculados para la norma ISO 27799:2008 se basan en los totales de la ISO/IEC 27002:2005 más el número de nuevas cláusulas, categorías de seguridad y controles. Tomando en cuenta que la ISO 27799:2008 agrega recomendaciones especiales para la Gestión de la Seguridad de la Información en Salud y “se considera una guía adicional y no como un reemplazo para la orientación encontrada en ISO/IEC 27002:2005” (ISO, 2008).

### 3.1.2 Combinación entre COBIT 5 e ISO/IEC 27002:2005

COBIT 5 e ISO/IEC 27002:2005 son marcos de referencia y estándares ampliamente utilizados, sus contenidos han evolucionado a través de los años y representan el aporte de expertos, consultores y profesionales de la industria de TI; por tanto, pueden ser de gran utilidad para establecer lineamientos claros para el diseño de un modelo de Gobierno de Tecnologías de la Información para hospitales públicos con énfasis en la Seguridad de la Información.

Los principios de COBIT 5, permite diferenciar claramente los roles de Gobierno y Gestión de TI, describe responsabilidades en los distintos niveles de la empresa y cubre todas las etapas de proceso de principio a fin. Sin embargo, COBIT 5 no incluye una guía exhaustiva para la definición de procedimientos o tareas específicas para la Seguridad de la Información, es decir se enfoca en lo que una empresa necesita hacer pero no cómo lo tiene que hacer. La audiencia objetivo es la Alta Gerencia, los Gerentes Funcionales, los Gerentes de TI y los Auditores. Esta característica ubica a COBIT 5 como un marco de gestión y control, más no como un manual de referencia de procesos aun cuando esté orientado a los mismos. La combinación de los objetivos de control y controles de la norma ISO/IEC 27002:2005 con los procesos de COBIT 5 permitirá definir los siguientes aspectos:

- Objetivos de control y controles para los procesos de COBIT.

- Enfoque de Seguridad de la Información bajo un criterio de gestión de riesgos.
- Verificación de cumplimiento de buenas prácticas.
- Definición de niveles de servicio y métodos de control para los mismos.
- Políticas específicas.

Hay que mencionar además, que el objetivo del estándar ISO/IEC 27002:2005 es “brindar información a los responsables de la implementación de Seguridad de la Información de una organización” (IT Governance Institute, 2008). Donde su contenido representa los requisitos legales o las mejores prácticas generalmente aceptadas, que permiten mantener y desarrollar normas de seguridad y prácticas de gestión que garanticen la protección de la información. Siendo este un motivo principal para elegir la ISO/IEC 27002:2005 sobre la ISO/IEC 27001:2005 en el presente trabajo de investigación.

Para establecer la relación entre los procesos de COBIT 5 e ISO/IEC 27002:2005 utilizaremos una guía de implementación proporcionada por ISACA denominada, COBIT 5 for Information Security (COBIT 5 para Seguridad de la Información) como una guía que “se centra en la Seguridad de la Información y proporciona una orientación más detallada y práctica para los profesionales de la Seguridad de la Información y demás partes interesadas en todos los niveles de la empresa” (ISACA, 2012). A continuación en la tabla 10, se muestra el mapeo de los procesos de COBIT 5 con la ISO/IEC 27002:2005 específicos para la Seguridad de la Información.

Tabla 10.

Mapeo entre COBIT 5 e ISO/IEC 27002:2005.

| COBIT 5 | | | ISO/IEC 27002:2005 |
|---|---|---|---|
| (EDM) | EDM01 | Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno. | 6.1.1 Compromiso de gerencia con la seguridad de la información |
| | EDM02 | Asegurar la entrega de beneficios | N/A |
| | EDM03 | Asegurar la optimización del riesgo | 14.1.2 Continuidad del negocio y evaluación de riesgos. |
| | EDM04 | Asegurar la optimización de los recursos | N/A |

| | | | |
|---|---|---|---|
| Evaluar, Orientar y Supervisar | EDM05 | Asegurar la transparencia hacia las partes interesadas | 6.1.1 Compromiso de gerencia con la seguridad de la información |
| | | | 6.1.2 Coordinación de la seguridad de la información |
| | | | 6.1.3 Asignación de las responsabilidades de la seguridad de la información |
| | | | 6.1.4 Proceso de autorización de recursos para el tratamiento de la información |
| | | | 6.1.5 Acuerdos de confidencialidad |
| | | | 6.1.6 Contacto con las autoridades |
| | | | 6.1.7 Contacto con grupos de interés especial |
| | | | 6.1.8 Revisión independiente de la seguridad de la información |
| Alinear, Planificar y Organizar (APO) | APO01 | Gestionar el Marco de Gestión de TI | 6. Organización de seguridad de la información |
| | APO02 | Gestionar la Estrategia | N/A |
| | APO03 | Gestionar la Arquitectura Empresarial | N/A |
| | APO04 | Gestionar la Innovación | N/A |
| | APO05 | Gestionar Portafolio | N/A |
| | APO06 | Gestionar el Presupuesto y Costo | N/A |
| | APO07 | Gestionar los Recursos Humanos | 8. Seguridad ligada a los Recursos Humanos |
| | APO08 | Gestionar las Relaciones | N/A |
| | APO09 | Gestionar los Acuerdos de Servicios | 10.2.1 Provisión de servicios |
| | | | 10.2.2. Supervisión y revisión de los servicios prestados por terceros. |
| | | | 10.2.3. Gestión del cambio en los servicios prestados por terceros. |
| | APO10 | Gestionar Proveedores | 6.1.5 Acuerdos de confidencialidad |
| | | | 6.2.1 Identificación de los riesgos derivados del acceso de terceros |
| | | | 6.2.3 Tratamiento de la seguridad en contratos con terceros |
| | | | 8.1.2 Investigación de antecedentes |
| | | | 8.1.3. Términos y condiciones de la relación laboral |
| | | | 10.2.3. Gestión del cambio en los servicios prestados por terceros. |
| | | | 10.8.2 Acuerdos de intercambio |
| | | | 12.4.2. Protección de los datos de prueba del sistema. |
| | | | 12.5.5. Externalización del desarrollo de software |
| | | | 15.1.4. Protección de datos y privacidad de la información de carácter personal. |
| | APO11 | Gestionar la Calidad | N/A |
| | APO12 | Gestionar el Riesgo | 13.1.1. Notificación de los eventos de seguridad de la información. |
| | | | 13.1.2. Notificación de puntos débiles de seguridad. |
| | | | 14.1.1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio. |
| | | | 14.1.2. Continuidad del negocio y evaluación de riesgos. |
| | APO13 | Gestionar la Seguridad | Tratado a lo Largo de esta Norma |

| | | | |
|---|---|---|---|
| Construir, Adquirir e Implementar (BAI) | BAI01 | Gestionar los Programas y Proyectos | N/A |
| | BAI02 | Gestionar la Definición de Requisitos | 10.1.1. Documentación de los procedimientos operativos. |
| | | | 10.3.2 Aceptación del sistema |
| | | | 11.6.2. Aislamiento de sistemas sensibles. |
| | | | 12.1.1 Análisis y especificación de requisitos de seguridad |
| | BAI03 | Gestionar la Identificación y la Construcción de Soluciones | Tratado a lo Largo de esta Norma |
| | BAI04 | Gestionar la Disponibilidad y Capacidad | 10.3.1. Gestión de capacidades. |
| | BAI05 | Gestionar la Introducción de Cambios Organizados | N/A |
| | BAI06 | Gestionar los Cambios | 10.1.2 Gestión de cambios |
| | | | 11.5.4. Uso de los servicios del sistema. |
| | | | 12.5.1 Procedimientos de control de cambios |
| | | | 12.5.3. Restricciones a los cambios en los paquetes de software. |
| | | | 12.6.1 Control de las vulnerabilidades técnicas |
| | BAI07 | Gestionar la Aceptación del Cambio y de la Transición | 6.1.4 Proceso de autorización de recursos para el tratamiento de la información |
| | | | 8.2.2. Conocimiento, educación y capacitación en seguridad de la información |
| | | | 9.1.6. Áreas de acceso público, entrega y carga |
| | | | 10.1.4. Separación de los recursos de desarrollo, prueba y operación. |
| | | | 10.3.2 Aceptación del sistema |
| | | | 12.4.2. Protección de los datos de prueba del sistema. |
| | | | 12.4.3. Control de acceso al código fuente de los programas. |
| | | | 12.5.1. Procedimientos de control de cambios. |
| | | | 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. |
| | BAI08 | Gestionar el Conocimiento | 10.1.1. Documentación de los procedimientos operativos. |
| | | | 10.3.2 Aceptación del sistema |
| | | | 10.7.4. Seguridad de la documentación del sistema |
| | | | 13.2.2. Aprendizaje de los incidentes de seguridad de la información. |
| | BAI09 | Gestionar los Activos | 7.1.1 Inventario de activos |
| | | | 7.1.2 Propiedad de los activos |
| | | | 7.2.2 Etiquetado y manejo de la información |
| | | | 10.7.4. Seguridad de la documentación del sistema |
| | | | 11.4.3. Identificación de los equipos en las redes |
| | | | 12.4.1 Control del software en explotación |
| | | | 12.4.2 Protección de los datos de prueba del sistema |
| | | | 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. |
| | | | 12.5.3. Restricciones a los cambios en los paquetes de software. |
| | | | 12.6.1 Control de las vulnerabilidades técnicas |
| | | | 15.1.5. Prevención del uso indebido de recursos de tratamiento de la información. |
| | BAI10 | Gestionar la Configuración | 7.1.1 Inventario de activos |
| | | | 7.1.2 Propiedad de los activos |
| | | | 7.2.2 Etiquetado y manejo de la información |
| | | | 10.7.4. Seguridad de la documentación del sistema |
| | | | 11.4.3 Identificación de los equipos en las redes |

| | | | |
|---|---|---|---|
| Construir, Adquirir e Implementar (BAI) | BAI10 | Gestionar la Configuración | 7.1.1 Inventario de activos |
| | | | 7.1.2 Propiedad de los activos |
| | | | 7.2.2 Etiquetado y manejo de la información |
| | | | 10.7.4. Seguridad de la documentación del sistema |
| | | | 11.4.3 Identificación de los equipos en las redes |
| | | | 12.4.1. Control del software en explotación. |
| | | | 12.4.2 Protección de los datos de prueba del sistema |
| | | | 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. |
| | | | 12.5.3. Restricciones a los cambios en los paquetes de software. |
| | | | 12.6.1. Control de las vulnerabilidades técnicas. |
| | | | 15.1.5. Prevención del uso indebido de recursos de tratamiento de la información. |
| Entrega, Servicio y Soporte (DSS) | DSS01 | Gestionar las Operaciones | 10. Gestión de Comunicaciones y Operaciones |
| | DSS02 | Gestionar las Peticiones y los Incidentes del Servicio | 13. Gestión de Incidentes en la Seguridad de la Información |
| | DSS03 | Gestionar los Problemas | 13.2.2. Aprendizaje de los incidentes de seguridad de la información. |
| | DSS04 | Gestionar la Continuidad | 14. Gestión de Continuidad del Negocio |
| | DSS05 | Gestionar los Servicios de Seguridad | Tratado a lo Largo de esta Norma |
| | DSS06 | Gestionar los Controles de los Procesos del Negocio | 8.2.1 Responsabilidades de la dirección |
| | | | 10.1.3 Segregación de tareas |
| | | | 10.1.4. Separación de los recursos de desarrollo, prueba y operación. |
| | | | 10.5.1 Copias de seguridad de la información |
| | | | 10.6.1 Controles de red |
| | | | 10.7.3. Procedimientos de manipulación de la información |
| | | | 10.8.3 Soportes físicos en tránsito |
| | | | 10.8.4 Mensajería electrónica |
| | | | 12.4.2. Protección de los datos de prueba del sistema. |
| | | | 12.4.3. Control de acceso al código fuente de los programas. |
| Supervisar, Evaluar y Valorar (MEA) | MEA01 | Supervisar, Evaluar y Valorar el Rendimiento y Conformidad | 10.10.2. Supervisión del uso del sistema. |
| | | | 5.1.2 Revisión de la política de seguridad de la información |
| | | | 6.1.8 Revisión independiente de la seguridad de la información |
| | | | 10.10.2 Supervisión del uso del sistema |
| | MEA02 | Supervisar, Evaluar y Valorar el Sistemas de Control Interno | 5.1.1 Documento de la Política de Seguridad de la Información |
| | | | 5.1.2 Revisión de la política de seguridad de la información |
| | | | 6.1.8 Revisión independiente de la seguridad de la información |
| | | | 6.2.3. Tratamiento de la seguridad en contratos con terceros |
| | | | 10.2.2. Supervisión y revisión de los servicios prestados por terceros. |
| | | | 10.10.2 Supervisión del uso del sistema |
| | | | 10.10.4 Registros de administración y operación |
| | | | 15.2.1 Cumplimiento de políticas y normas de seguridad |
| | | | 15.2.2 Comprobación del cumplimiento técnico |
| | | | 15.3.1 Controles de auditoría de los sistemas de información |
| | MEA03 | Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos | 6.1.6 Contacto con las autoridades |
| | | | 15.1.1 Identificación de la legislación aplicable |
| | | | 15.1.2 Derechos de propiedad intelectual (DPI) |
| | | | 15.1.4. Protección de datos y privacidad de la información de carácter personal. |

| | | | |
|---|---|---|---|
| BAI | BAI10 | Gestionar la Configuración | 12.4.1. Control del software en explotación. |
| | | | 12.4.2 Protección de los datos de prueba del sistema |
| | | | 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. |
| | | | 12.5.3. Restricciones a los cambios en los paquetes de software. |
| | | | 12.6.1. Control de las vulnerabilidades técnicas. |
| | | | 15.1.5. Prevención del uso indebido de recursos de tratamiento de la información. |
| Entrega, Servicio y Soporte (DSS) | DSS01 | Gestionar las Operaciones | 10. Gestión de Comunicaciones y Operaciones |
| | DSS02 | Gestionar las Peticiones y los Incidentes del Servicio | 13. Gestión de Incidentes en la Seguridad de la Información |
| | DSS03 | Gestionar los Problemas | 13.2.2. Aprendizaje de los incidentes de seguridad de la información. |
| | DSS04 | Gestionar la Continuidad | 14. Gestión de Continuidad del Negocio |
| | DSS05 | Gestionar los Servicios de Seguridad | Tratado a lo Largo de esta Norma |
| | DSS06 | Gestionar los Controles de los Procesos del Negocio | 8.2.1 Responsabilidades de la dirección |
| | | | 10.1.3 Segregación de tareas |
| | | | 10.1.4. Separación de los recursos de desarrollo, prueba y operación. |
| | | | 10.5.1 Copias de seguridad de la información |
| | | | 10.6.1 Controles de red |
| | | | 10.7.3. Procedimientos de manipulación de la información |
| | | | 10.8.3 Soportes físicos en tránsito |
| | | | 10.8.4 Mensajería electrónica |
| | | | 12.4.2. Protección de los datos de prueba del sistema. |
| | | | 12.4.3. Control de acceso al código fuente de los programas. |
| Supervisar, Evaluar y Valorar (MEA) | MEA01 | Supervisar, Evaluar y Valorar el Rendimiento y Conformidad | 10.10.2. Supervisión del uso del sistema. |
| | | | 5.1.2 Revisión de la política de seguridad de la información |
| | | | 6.1.8 Revisión independiente de la seguridad de la información |
| | | | 10.10.2 Supervisión del uso del sistema |
| | MEA02 | Supervisar, Evaluar y Valorar el Sistemas de Control Interno | 5.1.1 Documento de la Política de Seguridad de la Información |
| | | | 5.1.2 Revisión de la política de seguridad de la información |
| | | | 6.1.8 Revisión independiente de la seguridad de la información |
| | | | 6.2.3. Tratamiento de la seguridad en contratos con terceros |
| | | | 10.2.2. Supervisión y revisión de los servicios prestados por terceros. |
| | | | 10.10.2 Supervisión del uso del sistema |
| | | | 10.10.4 Registros de administración y operación |
| | | | 15.2.1 Cumplimiento de políticas y normas de seguridad |
| | | | 15.2.2 Comprobación del cumplimiento técnico |
| | | | 15.3.1 Controles de auditoría de los sistemas de información |
| | MEA03 | Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos | 6.1.6 Contacto con las autoridades |
| | | | 15.1.1 Identificación de la legislación aplicable |
| | | | 15.1.2 Derechos de propiedad intelectual (DPI) |
| | | | 15.1.4. Protección de datos y privacidad de la información de carácter personal. |

Adaptado de (ISACA, 2012, pág. 207).

A través de la tabla 11, se puede identificar los procesos de COBIT 5 que tiene relación con la Seguridad de la Información, siendo los procesos que se tomarán para la presente propuesta de modelo de Gobierno de Tecnologías de la Información para hospitales públicos con énfasis en la Seguridad de la Información. Sin embargo, cabe aclarar que en cada proyecto de aplicación se deberá seleccionar los procesos necesarios dependiendo de la planificación y naturaleza de la organización de salud.

Los procesos del grupo EDM identificados se consideran importantes debido que definen el Gobierno de TI de cara a la Junta Directiva, que en el caso de los hospitales podría ser el Gerente o el Comité de Gestión Hospitalaria. Respecto a los procesos de Gestión de TI (APO, BAI, DSS y MEA) permitirán aplicar las mejores prácticas y controles que mejoren el desempeño de la Seguridad de la Información en las organizaciones de salud.

Tabla 11.

Procesos de COBIT 5 relacionados con la Seguridad de la Información.

| **COBIT 5** | | |
|---|---|---|
| Evaluar, Orientar y Supervisar (EDM) | EDM01 | Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno |
| | EDM03 | Asegurar la optimización del riesgo |
| | EDM05 | Asegurar la transparencia hacia las partes interesadas |
| Alinear, Planificar y Organizar (APO) | APO01 | Gestionar el Marco de Gestión de TI |
| | APO07 | Gestionar los Recursos Humanos |
| | APO09 | Gestionar los Acuerdos de Servicios |
| | APO10 | Gestionar Proveedores |
| | APO12 | Gestionar el Riesgo |
| | APO13 | Gestionar la Seguridad |
| Construir, Adquirir e Implementar (BAI) | BAI02 | Gestionar la Definición de Requisitos |
| | BAI03 | Gestionar la Identificación y la Construcción de Soluciones |
| | BAI04 | Gestionar la Disponibilidad y Capacidad |
| | BAI06 | Gestionar los Cambios |
| | BAI07 | Gestionar la Aceptación del Cambio y de la Transición |
| | BAI08 | Gestionar el Conocimiento |
| | BAI09 | Gestionar los Activos |
| | BAI10 | Gestionar la Configuración |

| | | |
|---|---|---|
| Entrega, Servicio y Soporte (DSS) | DSS01 | Gestionar las Operaciones |
| | DSS02 | Gestionar las Peticiones y los Incidentes del Servicio |
| | DSS03 | Gestionar los Problemas |
| | DSS04 | Gestionar la Continuidad |
| | DSS05 | Gestionar los Servicios de Seguridad |
| | DSS06 | Gestionar los Controles de los Procesos del Negocio |
| Supervisar, Evaluar y Valorar (MEA) | MEA01 | Supervisar, Evaluar y Valorar el Rendimiento y Conformidad |
| | MEA02 | Supervisar, Evaluar y Valorar el Sistemas de Control Interno |
| | MEA03 | Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos |

### 3.1.3 Combinación entre COBIT 5, ISO/IEC 27002:2005 e ISO 27799:2008

COBIT 5 se ha definido como una arquitectura multinivel dado que pretende cubrir gran cantidad de áreas relacionadas con las Tecnologías de la Información. Concretamente, la estructura de COBIT 5 se basa en los siguientes niveles ordenados de mayor a menor: Inicialmente se definen dos áreas que son la de Gestión y Gobierno, luego dentro de las dos áreas se encuadran los cinco dominios de COBIT 5, internamente los cinco dominios poseen 37 procesos entre Gobierno y Gestión de TI, cada proceso contiene prácticas que son los objetivos de control de COBIT 5. Las prácticas que contiene cada proceso de COBIT 5 es el nivel de granularidad utilizado para integrar con las normas ISO/IEC 27002:2005 e ISO 27799:2008.

La información utilizada para la combinación entre COBIT 5, ISO/IEC 27002:2005 e ISO 27799:2008 es la tabla 8, el anexo 2, la tabla 10, las publicaciones oficiales de las normas ISO/IEC 27002:2005 e ISO 27799:2008 y la guía proporcionada por la organización ISACA denominada Alineando COBIT 4.1, ITIL V3 e ISO/IEC 27002 en beneficio de la empresa. Siendo estos la base documental para mapear las prácticas de Gobierno y Gestión de COBIT 5 con las categorías de seguridad de la norma ISO/IEC 27002:2005 e ISO 27799:2008.

### 3.1.3.1 Estrategia de integración

Para facilitar la integración entre COBIT 5, ISO/IEC 27002:2005 e ISO 27799:2008 se realizaron los siguientes pasos:

a) Identificación de los procesos de COBIT 5 que serán parte del mapeo detallados en la tabla 11.

b) Establecimiento de la metodología de mapeo con enfoque en la Seguridad de la Información aplicado al sector sanitario.

   En esta sección se definirán los criterios generales utilizados para el mapeo de las categorías de seguridad de las normas ISO/IEC 27002:2005 e ISO 27799:2008 con las prácticas de Gobierno y Gestión de COBIT 5. Dado el alto número de controles que poseen el marco de trabajo y las normas incluidas en el mapeo, es importante definir de qué modo se considerará que un control tiene relación con otro. La metodología utilizada se ha adaptado a partir de la propuesta realizada por ISACA en su libro “Alineando COBIT 4.1, ITIL V3 e ISO/IEC 27002 en beneficio de la empresa” (IT Governance Institute, 2008), los cuales se detallan a continuación:

   **Parcial (P):** El conjunto de actividades comprendidas dentro de la práctica de COBIT 5 es más amplia que el/los controles especificados por las normas ISO/IEC 27002:2005 e ISO 27799:2008. Significa que a efectos del modelo propuesto se evidencia un nivel de cumplimiento satisfactorio con la práctica de COBIT 5, sobre entendiéndose que los controles de las normas ISO/IEC 27002:2005 e ISO 27799:2008 están cubiertos por las actividades de la práctica de COBIT 5. Debido que el modelo propuesto tiene una aplicabilidad en el sector sanitario y por su propia naturaleza del sector se recomienda tomar en consideración cuando corresponda las guías y controles adicionales sugeridos por la norma ISO 27799:2008.

**Completo (C):** El conjunto de actividades comprendidas dentro de la práctica de COBIT 5 es semejante y pueden considerarse iguales con los controles de la norma ISO/IEC 27002:2005 e ISO 27799:2008. Para efectos del modelo propuesto en el mapeo completo se debe tomar en cuenta que discernir entre usar una u otra modalidad no es un proceso matemático y por tanto puede estar sujeto a interpretaciones o al entorno de la organización. En este caso puede entenderse la relación como bidireccional, por lo que si se demuestra el cumplimiento en uno de los lados del mapeo, se podrá entender que el otro lado también está cubierto. De igual manera se recomienda tomar en cuenta las guías y controles adicionales sugeridos por la norma ISO 27799:2008 debido que el modelo tiene una aplicabilidad en el sector sanitario.

**Excede (E):** El conjunto de actividades comprendidas dentro de la práctica de COBIT 5 es menos amplia que el conjunto de controles especificados por la norma ISO/IEC 27002:2005 e ISO 27799:2008. Esto significa que el conjunto de controles de las normas de referencia tiene un alcance mayor que las actividades definidas por COBIT 5. En este caso para efecto del modelo propuesto con aplicabilidad en el sector sanitario se debe obligatoriamente tomar en cuenta las guías y controles adicionales sugeridos por la norma ISO 27799:2008.

Se debe agregar que aunque resulte evidente, no todas las actividades de las prácticas de COBIT 5, tienen correspondencia con los controles de ISO/IEC 27002:2005 e ISO 27799:2008, por lo que necesariamente existirán controles vacíos en la tabla de mapeo detallado del anexo 3.

### 3.1.3.2 Mapeo de COBIT 5, ISO/IEC 27002:2005 e ISO 27799:2008

Con el objetivo de ilustrar la metodología de mapeo mostrada en el ítem 3.1.3.1, y debido al tamaño de la tabla de mapeo contenida en el anexo 3, se incluye a continuación diversos ejemplos representativos de cada caso.

a) **Mapeo parcial:** El primer ejemplo corresponde con un mapeo parcial. Se puede observar en la siguiente figura que la práctica o control de COBIT 5 corresponde con el código DSS01.02 y trata de gestionar servicios externalizados de TI. COBIT 5 define cuatro actividades o buenas prácticas para la implantación del control.

| Práctica de Gestión | Entradas | | Salidas | |
|---|---|---|---|---|
| **DSS01.02 Gestionar servicios externalizados de TI. .** Gestionar la operación de servicios externalizados de TI para mantener la protección de la información empresarial y la confiabilidad de la entrega del servicio. | **De** | **Descripción** | **Descripción** | **A** |
| | APO09.03 | • OLAs<br>• ANSs | Planes de aseguramiento independientes | MEA02.06 |
| | BAI05.05 | Plan de operación y uso | | |
| **Actividades** | | | | |
| 1. Asegurar que los procesos de información se adhieren a los requerimientos de seguridad de la empresa y conformes con los contratos y ANSs con terceros que alojan o proveen servicios. | | | | |
| 2. Asegurar que los requerimientos operativos del negocio y de procesamiento de TI, así como a las prioridades en la entrega del servicio se adhieren y son conformes a los contratos y ANSs con terceros que alojan o proveen servicios. | | | | |
| 3. Integrar los procesos críticos de gestión interna de TI con los de los proveedores de servicios externalizados cubriendo, por ejemplo, la planificación de la capacidad y el rendimiento, la gestión del cambio, la gestión de la configuración, la gestión de peticiones de servicio y de incidentes, la gestión de problemas, la gestión de la seguridad, la continuidad del negocio y la monitorización y notificación del desempeño de los procesos. | | | | |
| 4. Planificar la realización de auditorías y aseguramientos independiente de los entonos operativos de los proveedores de externalización (outsourcing) para confirmar que los requerimientos acordados están recibiendo el tratamiento adecuado. | | | | |

Figura 24. DSS01.02: Gestionar servicios externalizados de TI.
Tomado de (ISACA, 2012, pág. 141).

Seguidamente, observamos el resultado del mapeo entre las actividades de la práctica DSS01.02 de COBIT 5 con los controles de las normas ISO/IEC 27002:2005 e ISO 27799:2008.

| COBIT 5 | ISO/IEC 27002:2005 | ISO 27799:2008 | Mapeo |
|---|---|---|---|
| • DSS01.02 Gestionar servicios externalizados de TI | **6.2 Grupos o personas externas:**<br>• 6.2.3. Tratamiento de la seguridad en contratos con terceros.<br>**10.2. Gestión de la provisión de servicios por terceros:**<br>• 10.2.2. Supervisión y revisión de los servicios prestados por terceros. | **7.3.3 Grupos o personas externas:**<br>• 7.3.3.3 Tratamiento de la seguridad en contratos con terceros.<br>**7.7.2 Gestión de la provisión de servicios por terceros:** | P |

Figura 25. Mapeo de la práctica DSS01.02: Gestionar servicios externalizados de TI.

En base a los resultados obtenidos en el mapeo, se puede indicar que los controles de las normas ISO/IEC 27002:2005 e ISO 27799:2008 brindan alguna información de soporte sobre la protección de la

información empresarial, auditorías periódicas y la revisión de los servicios prestados por terceros, cubriendo así algunas de las actividades de la práctica DSS01.02 de COBIT 5. Sin embargo, las cuatro actividades que contiene la práctica DSS01.02 proporcionan un mejor detalle para el cumplimiento del objetivo de la práctica de gestión, puesto que dentro sus actividades tratan temas adicionales sobre planes de aseguramiento independientes para los proveedores e integrar los procesos críticos de la gestión interna de TI de la organización, con los procesos de los proveedores de servicios de TI externalizados.

**b) Mapeo completo:** Para este ejemplo de mapeo completo el control elegido es APO01.06 relativo a la propiedad de la información (datos) y del sistema. En este caso COBIT 5 incluye cuatro actividades para esta práctica, que son las que se muestran en la siguiente figura.

| Práctica de Gestión | Entradas | | Salidas | |
|---|---|---|---|---|
| **APO01.06 Definir la propiedad de la información (datos) y del sistema.**<br>Definir y mantener las responsabilidades de la propiedad de la información (datos) y los sistemas de información. Asegurar que los propietarios toman decisiones sobre la clasificación de la información y los sistemas y su protección de acuerdo con esta clasificación. | **De** | **Descripción** | **Descripción** | **A** |
| | | | Directrices para la clasificación de datos | APO03.02<br>BAI02.01<br>DSS05.02<br>DSS06.01 |
| | | | Directrices para el control y seguridad de datos | BAI02.01 |
| | | | Procedimientos de integridad de datos | BAI02.01<br>DSS06.01 |
| **Actividades** | | | | |
| 1. Proveer políticas y directrices para asegurar la adecuación y consistencia de la clasificación de la información (datos) en toda la empresa. | | | | |
| 2. Definir, mantener y proporcionar herramientas adecuadas, técnicas y directrices para garantizar la seguridad y control efectivo sobre la información y los sistemas en colaboración con el propietario. | | | | |
| 3. Crear y mantener un inventario de la información (sistemas y datos) que incluya un listado de los propietarios, custodios y clasificaciones. Incluir los sistemas subcontratados y aquellos cuya propiedad debe permanecer dentro de la empresa. | | | | |
| 4. Definir e implementar procedimientos para asegurar la integridad y consistencia de toda la información almacenada en formato electrónico, tales como bases de datos, almacenes de datos (*data warehouses*) y archivos de datos. | | | | |

Figura 26. APO01.06: Definir la propiedad de la información (datos) y del sistema.

Tomado de (ISACA, 2012, pág. 141).

Seguidamente, observamos el resultado del mapeo entre las actividades de la práctica APO01.06 de COBIT 5 con los controles de las normas ISO/IEC 27002:2005 e ISO 27799:2008.

| COBIT 5 | ISO/IEC 27002:2005 | ISO 27799:2008 | Mapeo |
|---|---|---|---|
| • APO01.06 Definir la propiedad de la información (datos) y del sistema. | **7.1 Responsabilidad sobre los activos:**<br>• 7.1.1. Inventario de activos.<br>• 7.1.2. Propiedad de los activos.<br>• 7.1.3. Acuerdos sobre el uso aceptable de los activos.<br>**7.2 Clasificación de la información:**<br>• 7.2.1 Directrices de Clasificación. | **7.4.1 Responsabilidad sobre los activos de información de salud:**<br>**7.4.2 Clasificación de información de salud:**<br>• 7.4.2.1 Directrices de Clasificación. | **C** |

Figura 27. Mapeo de la práctica APO01.06: Definir la propiedad de la información (datos) y del sistema.

En este caso se ha definido el mapeo como completo, puesto que las actividades de la práctica de COBIT 5 están cubiertas por los controles de las normas ISO/IEC 27002:2005 e ISO 27799:2008. Por lo cual se estima que el cumplimiento en uno de los lados podría corresponderse con el cumplimiento en la otra parte.

En este caso debido al enfoque de Seguridad de la Información aplicado al sector sanitario se debe tomar en cuenta los controles y las guías de implementación sugeridas por la norma ISO 27799:2008, como un complemento de la norma ISO/IEC 27002:2005. Por ejemplo el control 7.4.2.1 directrices de clasificación indica que “toda la información de salud personal debe clasificarse uniformemente como confidencial” (ISO, 2008), el análisis entre los controles de las normas ISO/IEC 27002:2005 e ISO 27799:2008 se trató a mayor detalle en el ítem 3.1.1.2 y en el anexo 3.

**c) Mapeo excede:** Finalmente, para mostrar un ejemplo de mapeo tipificado como excede se ha escogido la práctica DSS05.01 relativo a proteger contra software malicioso (malware). En COBIT 5 se definen seis actividades como se muestra la siguiente figura.

| DSS05 Prácticas, Entradas/Salidas y Actividades del Proceso | | | | |
|---|---|---|---|---|
| **Prácticas de Gestión** | **Entradas** | | **Salidas** | |
| **DSS05.01 Proteger contra software malicioso (*malware*).**<br>Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura). | **De** | **Descripción** | **Descripción** | **A** |
| | | | Política de prevención de software malicioso | AP001.04 |
| | | | Evaluaciones de amenazas potenciales | AP012.02<br>AP012.03 |
| **Actividades** | | | | |
| 1. Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención. | | | | |
| 2. Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente). | | | | |
| 3. Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios. | | | | |
| 4. Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad). | | | | |
| 5. Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing). | | | | |
| 6. Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado. | | | | |

Figura 28. DSS05.01: Proteger contra software malicioso (malware). Tomado de (ISACA, 2012, pág. 192)

Seguidamente, observamos el resultado del mapeo entre las actividades de la práctica DSS05.01 de COBIT 5 con los controles de las normas ISO/IEC 27002:2005 e ISO 27799:2008.

| COBIT 5 | ISO/IEC 27002:2005 | ISO 27799:2008 | Mapeo |
|---|---|---|---|
| • DSS05.01 Proteger contra software malicioso (malware). | **6.1 Organización interna:**<br>• 6.1.7 Contacto con grupos de interés especial.<br>**7.1 Responsabilidad sobre los activos:**<br>• 7.1.3. Acuerdos sobre el uso aceptable de los activos.<br>**10.4 Protección contra software malicioso y código móvil:**<br>• 10.4.1. Controles contra software malicioso.<br>• 10.4.2. Medidas y controles contra códigos móviles (cliente). | **7.3.2 Organización interna:**<br>• 7.3.2.4 Contacto con las autoridades, contacto con grupos de intereses especiales y revisión independiente de la seguridad de la información.<br>**7.4.1 Responsabilidad sobre los activos de información de salud:**<br>**7.7.4 Protección contra software malicioso y código móvil:**<br>• 7.7.4.1 Controles contra software malicioso.<br>• 7.7.4.2 Medidas y controles contra códigos móviles (cliente). | **E** |

Figura 29. Mapeo de la práctica DSS05.01: Proteger contra software malicioso (malware).

En este caso se ha definido el mapeo como excede, puesto que los controles de las normas ISO/IEC 27002:2005 e ISO 27799:2008 cubren por completo a las actividades de la práctica de COBIT 5, y además agregan controles adicionales dedicados a proteger la información

contra software malicioso (malware) y brindan un mejor detalle para el cumplimiento del objetivo de la práctica de gestión de COBIT 5. Entre los controles adicionales relacionados con la protección de la información contra código malicioso se tiene la creación de “planes adecuados de continuidad de negocio para la recuperación de los ataques de código malicioso, políticas contra la descarga y uso de código no autorizado por el cliente” (ISO/IEC, 2005) y “mantener el contacto adecuado con grupos especializados en Seguridad de la Información” (ISO/IEC, 2005). Además, la norma ISO 27799:2008 sugiere una “capacitación de concientización para protegerse contra software malintencionado, de una forma diferenciada y apropiada para el personal médico y administrativo” (ISO, 2008) de la organización de salud.

## 3.2 Metodología de implementación del modelo

La metodología de implementación del modelo Gobierno de TI para hospitales públicos con énfasis en la Seguridad de la Información propuesto se componen de los siguientes pasos:

### 3.2.1 Analizar los procesos actuales del hospital

Se realiza un análisis y descripción de la situación actual del hospital que será objeto de estudio, para conocer su funcionamiento y en qué forma la gestión de TI puede contribuir a desarrollar su misión y visión social.

### 3.2.2 Planificar la Implementación del modelo

Para alcanzar los objetivos se sugiere la implementación del modelo propuesto como un proyecto de la organización de salud, para lo cual se utilizará los fundamentos para la dirección de proyectos proporcionada por PMBOK y el libro de implementación de COBIT 5 proporcionada por ISACA que “provee un enfoque de buenas prácticas a la hora de implementar Gobierno de TI basado

en un ciclo de vida de mejora continua que debe adaptarse a las necesidades específicas de la empresa" (ISACA, 2012), las fases de la guía de implementación del modelo con sus actividades y entregables se explican en el ítem 3.3.

### 3.2.3 Identificar los motivadores actuales de cambio

Identificar los motivadores actuales de cambio y aceptación de la necesidad de una iniciativa de implementar o mejorar los procesos de Gobierno y Gestión de TI. A través de un análisis del estado actual del caso de negocio se debe crear el ánimo de cambio desde la Gerencia o Comité de Gestión Hospitalario para todos los involucrados de la organización y obtener el patrocinio ejecutivo.

### 3.2.4 Alinear los objetivos relacionados con TI con la estrategia del hospital

En esta fase se definirá el alcance de la iniciativa de implementación o mejora de los procesos de Gobierno y Gestión de TI. "Se alineará los objetivos relacionados con TI con la estrategia de la empresa y el riesgo y prioriza los principales objetivos de la empresa, los objetivos relacionados con TI y los procesos" (ISACA, 2012), además se identifican los procesos críticos que se necesitan para asegurar resultados exitosos. Así mismo se realizará una evaluación de la situación actual del hospital identificando los problemas y deficiencias mediante la ejecución de un proceso de revisión de capacidad de procesos.

### 3.2.5 Establecer los objetivos de mejora y priorizar los proyectos a implementar

Después de realizar un análisis de la situación actual de los procesos críticos del hospital, "se establecerán los objetivos de mejora seguidos por un análisis comparativo para identificar las potenciales soluciones" (ISACA, 2012). Algunas

de estas soluciones pueden proporcionar beneficios inmediatos y otras actividades pueden ser más desafiantes y de largo plazo. La prioridad deberían ser aquellas iniciativas que son más fáciles de conseguir y aquellas que podrían proporcionar los mayores beneficios.

### 3.2.6 Definir proyectos apoyados por casos de negocios

En esta fase se “planifica soluciones prácticas y viables mediante la definición de proyectos apoyados por casos de negocios justificados; además, se desarrolla un plan de cambios para la implementación” (ISACA, 2012). Considerando que un caso de negocio bien planificado y desarrollado ayudará a asegurar que los beneficios del proyecto son identificados y continuamente supervisados.

### 3.2.7 Implementación, establecimiento de medidas y supervisión del proyecto propuesto

Las soluciones propuestas en la fase anterior son implementadas en prácticas diarias. Se pueden determinar las mediciones e instaurar la supervisión del proyecto, empleando las metas y métricas de COBIT 5 para asegurar que se consigue y mantiene la alineación de TI con las metas del hospital. Como en las anteriores fases, “el éxito requiere la participación, sensibilización y comunicación, el entendimiento y el compromiso de la Alta Dirección y los dueños de los procesos de negocio y TI afectados” (ISACA, 2012).

### 3.2.8 Transición y supervisión de las prácticas de Gobierno y de Gestión mejoradas

En esta fase se debe centrar en la transición sostenible de las prácticas de gobierno y/o de gestión nueva o mejorada, así como también en las operaciones cotidianas del hospital. “Las mejoras descritas en el programa deben ser supervisadas a través de los objetivos TI relacionados y los objetivos

de los procesos utilizando técnicas adecuadas, tales como un cuadro de mandos TI (CMI, en inglés, Balanced Scorecard, BSC)" (ISACA, 2012). La supervisión de las mejoras se debe realizar mediante métricas de rendimiento y obtención de los beneficios. Para cada métrica, se deben fijar los objetivos, compararlos regularmente contra la realidad y comunicar con un informe de rendimiento. "Esto asegurará que las iniciativas permanecen en el buen camino de acuerdo a los objetivos iniciales de negocio y TI, y continúan ofreciendo los beneficios de negocio deseados" (ISACA, 2012).

### 3.2.9 Evaluar los resultados y la experiencia adquirida en la implementación del modelo

En esta fase se comprueba el éxito global del proyecto, identificando los requisitos adicionales para el modelo de Gobierno de TI y reforzando la necesidad de mejora continua. De igual manera se comprueba el éxito global del proyecto, mediante la evaluación de los resultados y la experiencia adquirida en el programa, como también el registrar y compartir las lecciones aprendidas. Por otra parte se debe "mejorar las estructuras organizativas, procesos, roles y responsabilidades para cambiar el comportamiento de la empresa de manera que el Gobierno de TI se convierta en la forma normal del negocio y se optimice continuamente" (ISACA, 2012). A lo largo del tiempo de implementación de la iniciativa, las mejoras identificadas se utilizarán como entrada a la siguiente iteración del ciclo de vida.

## 3.3 Guía de implementación del modelo

Según lo indicado por guía del PMBOK la "aplicación de conocimientos, habilidades, herramientas y técnicas aumenta las posibilidades de conseguir los objetivos de un proyecto" (PMI, 2013), siendo esta una motivación para el uso de dicha herramienta en la implementación del modelo propuesto para hospitales públicos. El marco de trabajo PMBOK es una colección de 47 procesos que se agrupan en diez áreas de conocimiento diferenciadas y cinco

grupos de procesos que forman parte del ciclo de vida de un proyecto. “Las fases y procesos del PMBOK deben ser adaptadas a cada proyecto en particular para que se puedan alcanzar los objetivos planteados por la organización” (PMI, 2013).

### 3.3.1 Fase 1: Iniciación

En la etapa de iniciación del proyecto se tiene como propósito “desarrollar un documento que autoriza formalmente la existencia de un proyecto y confiere al Director del Proyecto la autoridad para asignar los recursos de la organización a las actividades del proyecto” (PMI, 2013). Las entradas de la presente fase estarán en base a los procesos y necesidades actuales del hospital que hacen referencia a la necesidad del negocio o los objetivos estratégicos de la institución. Finalmente el beneficio clave de esta fase es un inicio y unos límites del proyecto bien definidos, la creación de un registro del proyecto y el establecimiento de una forma directa para que la Gerencia del hospital acepte formalmente y se comprometa con el proyecto.

**Actividades:**

- Presentar el modelo de Gobierno de TI a la Gerencia o Comité de Gestión Hospitalario de la casa de salud.
- Explicar el alcance del proyecto.
- Definir los roles y responsable de la implementación del proyecto.
- Informar a los miembros del equipo del proyecto.

**Entregables:**

- Acta de Constitución del Proyecto.
- Declaración Inicial del alcance del proyecto.

### 3.3.2 Fase 2: Planificación

La fase de planificación está “compuesto por aquellos procesos realizados para establecer el alcance total del esfuerzo, definir y refinar los objetivos, y desarrollar la línea de acción requerida para alcanzar dichos objetivos” (PMI, 2013). El beneficio clave de esta fase es un documento central denominado Plan para la Dirección del Proyecto que “define la estrategia y las tácticas, así como la línea de acción o ruta para completar con éxito el proyecto o fase. El contenido del Plan para la Dirección del Proyecto es variable en función del área de aplicación y de la complejidad del proyecto” (PMI, 2013).

#### 3.3.2.1 Identificación y/o creación de estructuras organizativas

Una parte del modelo propuesto es la definición de las estructuras organizativas requeridas para proporcionar el apoyo necesario a todo el ciclo de vida del proyecto. Por lo cual, en esta fase del proceso de implementación se inicia por la identificación y/o creación de dichas estructuras organizativas del hospital. “La correcta identificación de las estructuras organizativas determina que los recursos humanos posean las habilidades requeridas para el éxito del proyecto” (PMI, 2013).

**Actividades:**

- Identificación y/o creación de las estructuras organizativas del hospital.

**Entregables:**

- Documento con la identificación y/o creación de la estructura organizativa del hospital y sus responsables.

#### 3.3.2.2 Aplicación de la técnica de cascada de metas de COBIT 5

Como parte del modelo propuesto se designó a la técnica de cascada de metas de COBIT 5 como herramienta para asegurar el alineamiento de TI con los

objetivos estratégicos y metas del Hospital. La herramienta utilizada en el presente ítem permite “identificar y describir los límites del proyecto, especificando cuáles de los requisitos recopilados serán incluidos y cuáles excluidos del alcance del proyecto” (PMI, 2013).

**Actividades:**

- Aplicación de la técnica de cascada de metas de COBIT 5, teniendo como insumo los objetivos estratégicos del Hospital.
- Definir una escala de valoración para cada proceso de mapeo.
- Establecer entre los miembros del Equipo de Proyecto el nivel de valoración que debe tener cada meta corporativa, meta relacionada con TI, proceso de Gobierno y Gestión de TI para ser considerada dentro del proceso de mapeo.

**Entregables:**

- Documento con las matrices resultantes de los distintos mapeos que proporciona la aplicación de la técnica de cascada de metas de COBIT 5;
- Documentación con la definición de los procesos de Gobierno y de Gestión resultado de la cascada de metas de COBIT 5.

#### 3.3.2.3 Priorización de los procesos con enfoque en la Seguridad de la Información

Es necesario definir el orden en que se implementará los procesos dependiendo de la importancia para la operación del hospital, en este caso debido al enfoque de Seguridad de la Información que tiene el modelo de Gobierno de TI, se utilizará la información de la tabla 11.

**Actividades:**

- Identificación de los procesos de Gobierno y de Gestión de TI, que tienen un enfoque de Seguridad de la Información.

**Entregables:**

- Documentación con la definición de los procesos de Gobierno y de Gestión de TI que tienen un enfoque de Seguridad de la Información.
- Plan de Gestión del Alcance.

3.3.2.4 Elaboración del Plan de Gestión del Cronograma

En este ítem se proporcionará una guía y dirección sobre cómo se gestionará el cronograma del proyecto a lo largo del mismo.

**Actividades:**

- Analizar las actividades y entregables definidos en el Plan de Gestión del Alcance.
- Referirse al Acta de Constitución del Proyecto.
- Analizar los factores ambientales del hospital.

**Entregables:**

- Plan de Gestión del Cronograma.

3.3.2.5 Elaboración de la Matriz de Asignación de Responsabilidades (RACI) para la estructura organizativa del Hospital

La matriz RACI se utilizará como herramienta para establecer los mecanismos de relación entre los diferentes recursos que conforman la estructura organizativa del hospital establecida en el ítem 3.3.2.1. Se debe agregar que “una matriz RACI es una herramienta útil cuando el equipo está constituido por recursos internos y externos, a fin de asegurar una diferenciación clara de roles y expectativas de los miembros del equipo del proyecto” (PMI, 2013).

**Actividades:**

- Definición de la matriz RACI.

**Entregables:**

- Documento con la matriz RACI definida.
- Plan de Gestión de los Recursos Humanos.

3.3.2.6 Elaboración del Plan de Gestión de los Costos

El Plan de Gestión de los Costos define los recursos necesarios para completar las actividades del proyecto.

**Actividades:**

- Definir los recursos necesarios para completar las actividades del Proyecto.

**Entregables:**

- Plan de Gestión de los Costos.

3.3.2.7 Elaboración del Plan de Gestión de las Comunicaciones

El Plan de Comunicación del proyecto definirá los tipos de comunicación que existirán durante el desarrollo del proyecto y la manera que se llevarán a cabo cada tipo de comunicación.

**Actividades:**

- Registro de los interesados.
- Análisis de los requisitos de comunicación.
- Modelos y métodos de comunicación.

**Entregables:**

- Plan de Gestión de las Comunicaciones.

#### 3.3.2.8 Elaborar el Plan de Gestión de Riesgos

El Plan de Riesgos define las posibles amenazas que podrían afectar a la ejecución del proyecto.

**Actividades:**

- Registro de los interesados.
- Definir las posibles amenazas que podrían afectar a la ejecución del Proyecto.

**Entregables:**

- Plan de Gestión de Riesgos.

#### 3.3.2.9 Identificación del estado actual

En esta fase se identifica el estado actual del hospital, para lo cual se realiza un diagnóstico inicial sobre cómo se encuentran los procesos de Gobierno y de Gestión de TI que componen el modelo propuesto. Para efectuar dicha evaluación se utiliza el PAM de COBIT 5 y cuya descripción se encuentra en el anexo 1 de este documento.

**Actividades:**

- Realizar la evaluación de capacidad de cada uno de los procesos de Gobierno y Gestión de TI.
- Registrar los participantes de la evaluación de los procesos del modelo de Gobierno de TI.

**Entregables:**

- Documentación con la evaluación realizada a los procesos del hospital, considerando los niveles establecidos dentro del modelo de capacidad propuesto por COBIT 5.

#### 3.3.2.10 Identificar y definir el estado deseado

Considerando los resultados obtenidos en la evaluación realizada en el punto anterior así como las necesidades del hospital se establece el estado deseado. Se determinara las brechas a cerrarse con la finalidad de avanzar en la implementación del proyecto y debido que el modelo propuesto tiene un enfoque de Seguridad de la Información se tomarán en cuenta los controles de las normas ISO/IEC 27002:2005 e ISO 27799:2008, así como también las actividades adicionales de la Guía de COBIT 5 para Seguridad de la Información, “que permita “mejorar la integración de la Seguridad de la Información en la empresa” (ISACA, 2012).

**Actividades:**

- Definir el estado deseado.
- Identificar las brechas existentes entre el estado actual y el estado deseado.
- Definir las actividades que permitan alcanzar el estado deseado.
- Incluir las actividades adicionales de la Guía COBIT 5 para Seguridad de la Información.
- Incluir los controles adicionales de las normas ISO/IEC 27002:2005 e ISO 27799:2008, en base al anexo 3.
- Establecer el orden de implementación de los procesos del Hospital.

**Entregables:**

- Plan de Acción para alcanzar el estado deseado en cada proceso.

### 3.3.3 Fase 3: Ejecución

En esta fase se ejecutara el proyecto autorizado por la Gerencia y se realizarán una a una, las actividades diseñadas en la Fase de Planificación. Es así que la Fase de Ejecución efectúa “la coordinación de personas y recursos, se gestiona las expectativas de los interesados, así como la integración y

realización de las actividades del proyecto conforme a la planificación" (PMI, 2013). La Fase de Ejecución, Monitoreo, Control y Cierre no se encuentra en el alcance de esta tesis.

**Actividades:**

- Implementación de las actividades que permitan alcanzar el estado deseado.
- "Dirigir y gestionar el equipo de trabajo del proyecto.
- Realizar el aseguramiento de Calidad.
- Gestionar las comunicaciones.
- Gestionar la participación de los interesados" (PMI, 2013).

**Entregables:**

- "Datos de desempeño del trabajo.
- Solicitudes de cambio.
- Actualizaciones al Plan para la Dirección del Proyecto.
- Actualizaciones a los documentos del proyecto" (PMI, 2013).

### 3.3.4 Fase 4: Monitoreo y control

Esta fase tiene como objetivo dar seguimiento, revisar e informar el avance del proyecto, a fin de cumplir con los objetivos de desempeño definidos en el Plan para la Dirección del Proyecto. El beneficio clave del monitoreo y control es que permite medir y analizar el desempeño del proyecto en intervalos regulares, así mismo permite controlar los cambios y realizar acciones correctivas a posibles problemas. "Este monitoreo continuo proporciona al equipo del proyecto conocimiento sobre la salud del proyecto y permite identificar las áreas que requieren más atención" (PMI, 2013).

**Actividades:**

- "Validar y controlar el alcance del proyecto.
- Controlar el avance del proyecto en función del tiempo.

- Controlar la calidad.
- Controlar las comunicaciones y riesgos del proyecto.
- Controlar la participación de los interesados” (PMI, 2013).

**Entregables:**

- “Solicitudes de cambio.
- Informes de desempeño del trabajo.
- Actualizaciones al Plan para la Dirección del Proyecto.
- Actualizaciones a los documentos del proyecto” (PMI, 2013).

### 3.3.5 Fase 5: Cierre

Los procesos de la Fase de Cierre se encargan de finalizar todas las actividades a través de todos los grupos de procesos de la dirección de proyectos, permitiendo completar formalmente el proyecto. El beneficio clave de este “proceso es que proporciona las lecciones aprendidas, la finalización formal del trabajo del proyecto, y la liberación de los recursos de la organización para afrontar nuevos esfuerzos” (PMI, 2013).

**Actividades:**

- El Director del Proyecto debe revisar toda la información anterior procedente de los cierres de las fases previas para asegurarse de que todo el trabajo del proyecto está completo.
- Recopilar los registros del proyecto, reunir las lecciones aprendidas y archivar la información del proyecto.

**Entregables:**

- Acta de Cierre del Proyecto.
- “Transferencia del producto, servicio o resultado final para el que se autorizó el proyecto” (PMI, 2013).

En el anexo 4 se encuentran las plantillas para los documentos indicados en cada una de las fases del modelo.

# 4 Capítulo IV. Implementación del modelo de Gobierno de TI con énfasis en Seguridad de la Información en el Hospital General Docente de Calderón.

En el presente capítulo se realiza una aplicación práctica del modelo propuesto, en el Hospital General Docente de Calderón como caso de estudio.

## 4.1 Descripción del caso estudio

### 4.1.1 Descripción

El Hospital General Docente de Calderón inaugurado el jueves 16 de julio del 2015, es un Hospital público de segundo nivel que beneficia a los habitantes del norte de Quito y parroquias aledañas, el hospital tiene 156 camas y cuenta con 21 especialidades, como ginecología, pediatría, odontología, traumatología, neurocirugía, entre otros.

Esta nueva casa de salud cuenta con un área de emergencia que funciona las 24 horas, como también posee una ludoteca y una sección para residencia médica. En la construcción del hospital el Estado ha invertido aproximadamente 74 millones de dólares que involucra la parte de infraestructura y equipamiento,

Tabla 12.
Inversión en infraestructura y equipamiento del Hospital General Docente de Calderón.

| Nro. | Año | Hospital Inaugurado | Inversión Infraestructura | Inversión Equipamiento | Total Inversión |
|---|---|---|---|---|---|
| 1 | 2015 | Hospital General Docente de Calderón | $ 54.847.809,54 | $ 19.761.229,03 | $ 74.609.038,57 |

Tomado de (Ministerio de Salud Pública, 2016)

Hasta la fecha de elaboración del presente trabajo, el Hospital General Docente de Calderón no posee un Plan Estratégico aprobado y autorizado por el Comité de Gestión Hospitalario de la casa de salud. Por lo cual los lineamientos que sigue actualmente el hospital están dados por el Estatuto Orgánico de Gestión Organizacional por Procesos de los Hospitales del MSP.

Figura 30. Hospital General Docente de Calderón.
Tomado de (ANDES, 2012).

### 4.1.2 Misión y Visión

El Hospital General Docente de Calderón tiene como Misión:

> Prestar servicios de salud con calidad y calidez en el ámbito de la asistencia especializada, a través de nuestra cartera de servicios, cumpliendo con la responsabilidad de promoción, prevención, recuperación, rehabilitación de salud integral, docencia e investigación, conforme a las políticas del Ministerio de Salud Pública y el trabajo en red, en el marco de la justicia y equidad social (Hospital General Docente de Calderón, 2015).

Y como Visión:

> Ser reconocidos por la ciudadanía como un Hospital accesible, que presta una atención de calidad, que satisface las necesidades y expectativas de la población bajo principios fundamentales de la salud pública y bioética, utilizando la tecnología y los recursos públicos de forma eficiente y transparente (Hospital General Docente de Calderón, 2015).

### 4.1.3 Objetivos estratégicos

Los objetivos estratégicos que permitirán cumplir con la Misión y Visión del Hospital son:

- **Objetivo 1:** Garantizar la equidad en el acceso y gratuidad de los servicios.
- **Objetivo 2:** Trabajar bajo los lineamientos del Modelo de Atención Integral de Salud (MAIS) de forma integrada y en red con el resto de las Unidades Operativas de Salud del Ministerio de Salud Pública y otros actores de la red pública y privada complementaria que conforman el sistema nacional de salud del Ecuador.
- **Objetivo 3:** Mejorar la accesibilidad y el tiempo de espera para recibir atención, considerando la diversidad de género, cultural, generacional, socio económica, lugar de origen y discapacidades.
- **Objetivo 4:** Involucrar a los profesionales en la gestión del Hospital, aumentando su motivación, satisfacción y compromiso con la misión del Hospital.
- **Objetivo 5:** Garantizar una atención de calidad y respeto a los derechos de las y los usuarios, para lograr la satisfacción con la atención recibida.

- **Objetivo 6:** Desarrollar una cultura de excelencia con el fin de optimizar el manejo de los recursos públicos, y la rendición de cuentas. (Ministerio de Salud Pública, 2012).

### 4.1.4 Estructura organizacional de gestión por procesos

La estructura organizacional del Hospital General Docente de Calderón, se encuentra alineada con la “misión del Ministerio de Salud Pública, el Modelo de Atención, al Modelo de Gestión Hospitalaria, políticas determinadas en la Constitución de la República del Ecuador, las Políticas del Estado, leyes y otras normas vigentes” (Ministerio de Salud Pública, 2012).

Los procesos del Hospital se ordenan y clasifican en función de su grado de contribución o valor agregado al cumplimiento de su misión. Estos son:

- **Los Procesos Gobernantes:** que orientan la gestión institucional a través de la formulación de propuestas de políticas, directrices, normas, procedimientos, planes, acuerdos y resoluciones para la adecuada administración y ejercicio de la representación legal de la institución.
- **Los Procesos Agregadores de Valor:** son los encargados de generar y administrar los productos y servicios destinados a usuarios y permiten cumplir con la misión institucional y los objetivos estratégicos.
- **Los Procesos Habilitantes de Asesoría y de Apoyo:** que generan productos y servicios para los procesos gobernantes, agregadores de valor y para sí mismos, apoyando y viabilizando la Gestión Institucional.

### 4.1.5 Procesos Internos del Hospital

El Hospital General Docente de Calderón para el cumplimiento de su misión y visión social, desarrolla los siguientes procesos internos:

Tabla 13.

Procesos internos del Hospital General Docente de Calderón.

| |
|---|
| **1. Proceso Gobernante** |
| 1.1. Gerencia Hospitalaria |
| 1.2. Comité de Gestion y Direccionamiento Estratégico del Hospital |
| **2. Procesos Agregadores de Valor** |
| 2.1. Gestión Asistencial |
| 2.1.1. Gestión de Especialidades Clínicas y/o Quirúrgicas (De acuerdo al tipo, complejidad y nivel resolutivo de cada hospital) |
| 2.1.2. Gestión de Cuidados de Enfermería |
| 2.1.3. Gestión de Apoyo Diagnóstico y Terapéutico (De acuerdo al tipo, complejidad y nivel resolutivo de cada hospital) |
| 2.1.4. Gestión de Docencia e Investigación (De acuerdo a la acreditación en docencia e investigación) |
| **3. Procesos Habilitantes de Asesoría** |
| 3.1. Gestión de Planificación, Seguimiento y Evaluación de Gestión |
| 3.2. Gestión de Asesoría Jurídica |
| 3.3. Gestión de Comunicación |
| 3.4. Gestión de Calidad |
| **4. Procesos Habilitantes de Apoyo** |
| 4.1. Gestión de Atención al Usuario |
| 4.2. Gestión de Admisiones |
| 4.3. Gestión Administrativa y Financiera |
| 4.3.1. Gestión de Talento Humano |
| 4.3.2. Gestión Financiera |
| 4.3.3. Gestión Administrativa |
| 4.3.4. Gestión de Tecnologías de la Información y Comunicaciones |

Adaptado de (Ministerio de Salud Pública, 2012).

### 4.1.6 Cadena de valor y mapa de procesos

En la siguiente figura se muestra cómo se desarrollan las actividades dentro del Hospital y la forma de interactuar entre los diferentes procesos internos.

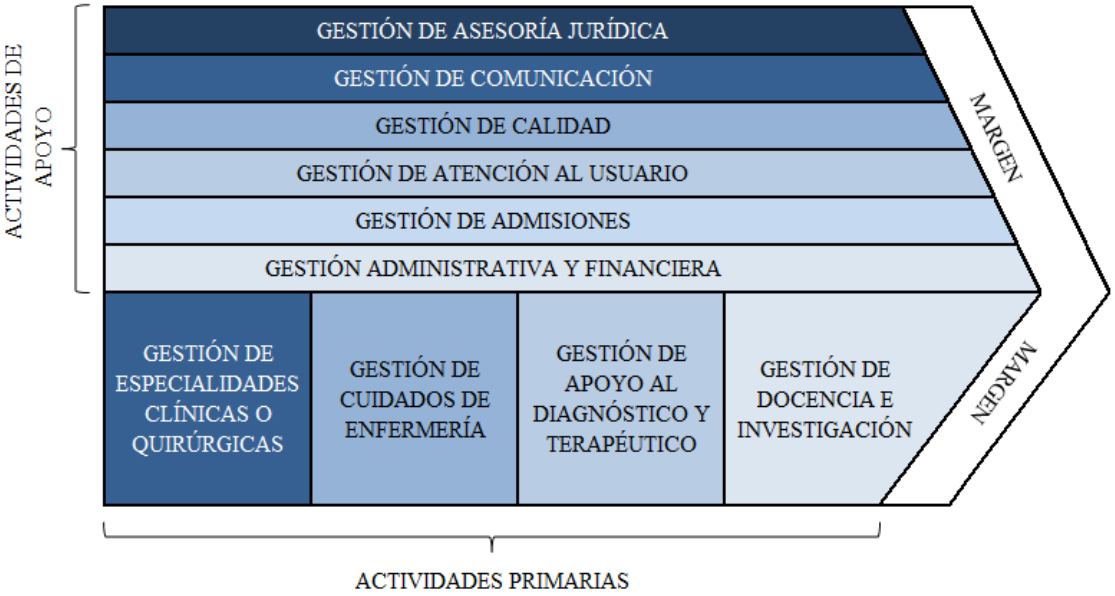



Figura 31. Cadena de valor del Hospital General Docente de Calderón. Adaptado de (Ministerio de Salud Pública, 2012).


Figura 32. Mapa de Procesos del Hospital General Docente de Calderón. Adaptado de (Ministerio de Salud Pública, 2012).

### 4.1.7 Organigrama estructural

A continuación se detalla el organigrama estructural del Hospital General Docente de Calderón.

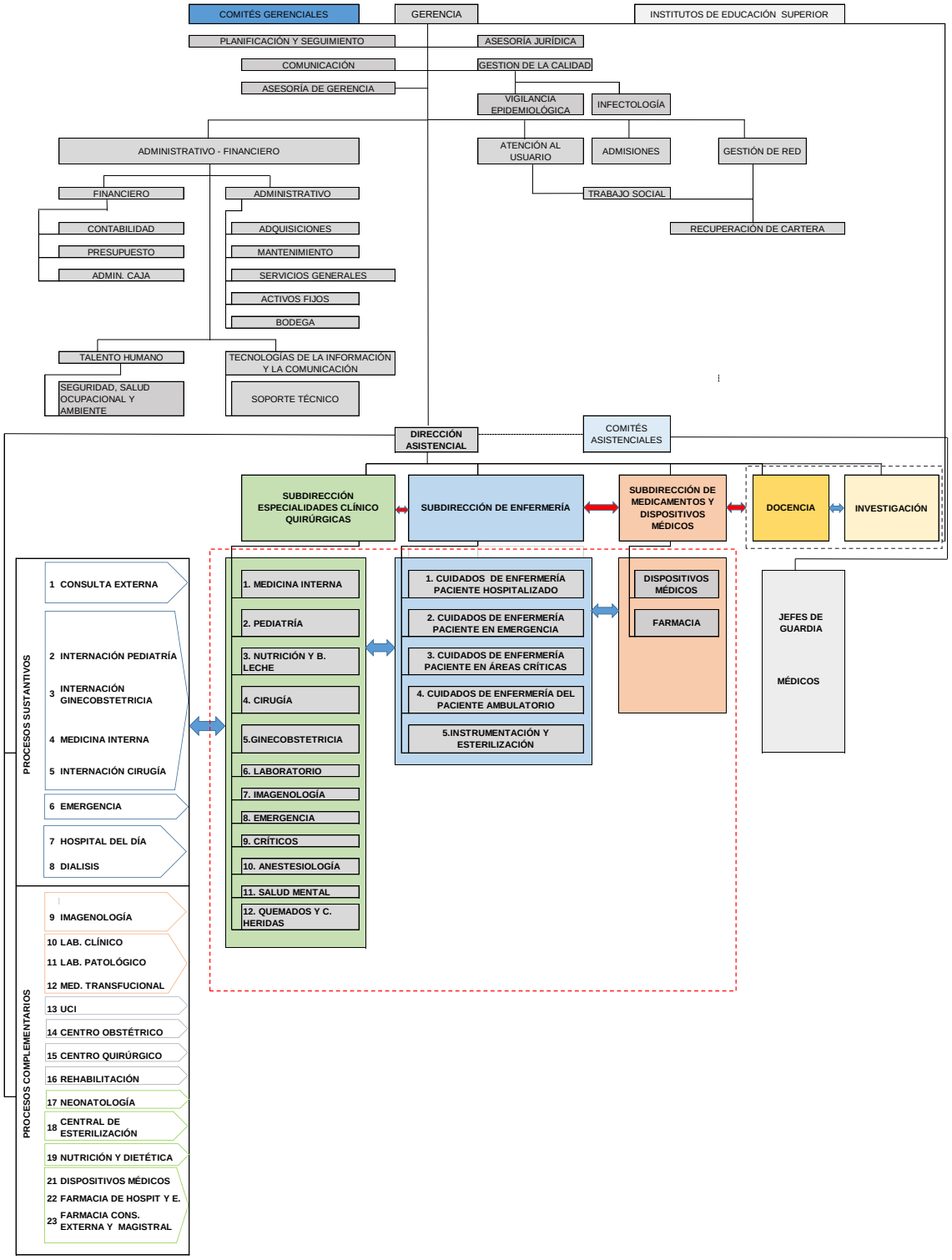



Figura 33. Organigrama estructural del Hospital General Docente de Calderón. Tomado de (Hospital General Docente de Calderón, 2017)

### 4.1.8 Estado de la Unidad de Gestión de Tecnología de la Información y Comunicaciones

La Unidad de Gestión de Tecnologías de la Información y Comunicaciones (TIC), se encuentra conformado por 8 profesionales de TI y 2 pasantes, distribuidos en la Jefatura, Infraestructura, Redes de Comunicación, Desarrollo de Software, Soporte y Mesa de Ayuda.

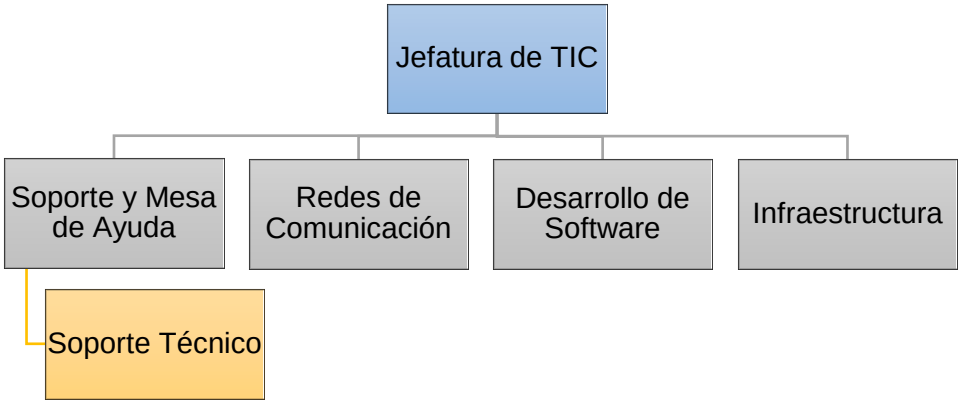



Figura 34. Estructura organizacional actual de Unidad de Gestión de Tecnologías de la Información y Comunicaciones.

Las principales funciones de la unidad de TIC son las siguientes:

- Mantenimiento a las líneas de red.
- Acciones preventivas y correctivas de software y hardware.
- Informes sobre las acciones preventivas y correctivas de software y hardware realizados.
- Informes sobre las redes de conectividad.
- Plan de mejoramiento de redes.
- Ejecución de Plan de Continuidad (BCP) y Recuperación de Desastres (DRP).
- Mantenimiento de programas informáticos existentes.
- Sistemas de información en las diferentes áreas y página WEB del hospital.

- Mantenimiento de la central telefónica digital.
- Servicio de Internet a las diferentes unidades del Hospital.
- Correo institucional.
- Inventario de los equipos tecnológicos computacionales y comunicacionales.
- Actas de la entrega recepción de los equipos adquiridos en coordinación con las áreas de Activos Fijos y Bodega. (Ministerio de Salud Pública, 2012).

## 4.2 Aplicación del Modelo

En este ítem se realiza la aplicación del Modelo de Gobierno de TI con énfasis en Seguridad de la Información propuesto, en el Hospital General Docente de Calderón para lo cual, se hará uso de las recomendaciones detalladas en el apartado 3.3 de este documento.

### 4.2.1 Fase 1: Iniciación

En esta fase se realiza el Acta de Constitución del Proyecto, en la cual se compromete el apoyo de la Gerencia del Hospital para la implementación del proyecto y una definición inicial del alcance del mismo.

Tabla 14.
Acta de Constitución del Proyecto.

| **Acta de Constitución del Proyecto** | |
|---|---|
| Nombre del proyecto | Siglas del proyecto |
| Gobierno de Tecnología de la Información con énfasis en la Seguridad de la Información para el Hospital General Docente de Calderón. | GOBTISI |
| Descripción del proyecto: ¿qué, quién, cómo, cuándo y dónde? | |

El Proyecto GOBTISI consiste en la implementación de un modelo de Gobierno de Tecnología de la Información con énfasis en la Seguridad de la Información en el Hospital General Docente de Calderón.

El Proyecto GOBTISI se desarrollara siguiendo las siguientes fases:

a) Realizar una descripción del Hospital.
b) Presentar el Modelo de Gobierno de TI a la Gerencia y Comité de Gestión Hospitalario.
c) Informe sobre la estructura organizativa del Hospital para el Proyecto.
d) Identificar y documentar los roles y responsabilidades del recurso humano para la ejecución del Proyecto.
e) Definir los tipos de comunicación que existirán durante el desarrollo del Proyecto.
f) Identificar las posibles amenazas que podrían afectar a la ejecución del Proyecto.
g) Identificar el estado de capacidad actual de los procesos seleccionados.
h) Identificar el estado de capacidad objetivo de los procesos seleccionados.
i) Analizar las brechas existentes y plantear las actividades que permitan alcanzar el estado deseado.
j) Ejecutar y monitorear la implementación del Proyecto.
k) Cerrar el proyecto y utilizar las lecciones aprendidas para adaptar y mejorar el enfoque de TI en iniciativas futuras.

La responsabilidad del Proyecto estará a cargo de la jefatura de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones y de la persona designada como Director de Proyecto.

Definición del producto del proyecto: descripción del producto, servicio o capacidad a generar.

El Proyecto GOBTISI asegura el logro de los objetivos estratégicos del Hospital a través de TI, permitiendo a la casa de salud cumplir con su Misión y Visión. El Proyecto incluirá los siguientes entregables:

a) Acta de Constitución del Proyecto.
b) Plan de Gestión del Alcance.
c) Plan de Gestión del Cronograma.
d) Plan de Gestión de los Recursos Humanos.
e) Plan de Gestión de los Costos.
f) Plan de Gestión de las Comunicaciones.
g) Plan de Gestión de Riesgos.
h) Documentación sobre el estado de capacidad actual de los procesos seleccionados.
i) Documentación sobre el estado de capacidad objetivo de los procesos seleccionados.
j) Documentación sobre las actividades que permitan alcanzar el estado deseado.
k) Informe del desempeño en la ejecución del proyecto y gestión de solicitudes de cambio.
l) Acta de Cierre del Proyecto.

Objetivos del proyecto: metas hacia las cuales se debe dirigir el trabajo del Proyecto en términos de la triple restricción.

| Concepto | Objetivos |
|---|---|
| 1. Alcance | a) Acta de Constitución del Proyecto.<br>b) Informe sobre la estructura organizativa del Hospital para el Proyecto.<br>c) Documentación sobre el estado de capacidad actual de los procesos seleccionados.<br>d) Informe sobre el estado de capacidad objetivo de los procesos seleccionados.<br>e) Documentación sobre las actividades que permitan alcanzar el estado deseado. |

| | |
|---|---|
| | f) Plan de Gestión del Cronograma.<br>g) Plan de Gestión de los Recursos Humanos.<br>h) Plan de Gestión de los Costos.<br>i) Plan de Gestión de las Comunicaciones.<br>j) Plan de Gestión de Riesgos.<br>k) Informe del desempeño en la ejecución del proyecto y gestión de solicitudes de cambio<br>l) Acta de Cierre del Proyecto y documentación con las lecciones aprendidas para adaptar y mejorar el enfoque de TI a iniciativas futuras. |
| 2. Tiempo | 365 días calendario |
| 3. Costo | La implementación del Proyecto se realizará en su mayoría con los recursos internos del Hospital. Sin embargo, este tema se lo trata a más detalle en el Plan de Gestión de los Costos. |
| Finalidad del proyecto: fin último, propósito general, u objetivo de nivel superior por el cual se ejecuta el Proyecto. Enlace con programas, portafolios, o estrategias de la organización. | |
| Asegurar el cumplimiento de los objetivos estratégicos del Hospital General Docente de Calderón. | |
| Justificación del proyecto: motivos, razones, o argumentos que justifican la ejecución del Proyecto. | |
| El Hospital General Docente de Calderón requiere cumplir con sus objetivos estratégicos, para poder prestar con eficiencia su cartera de servicios médicos y desarrollar su misión y visión social. De ahí que para asegurar el logro de los objetivos del Hospital a través de TI, es necesario alinear los objetivos de TI con los objetivos del Hospital, creando valor (realización de beneficios, optimización de riesgos y recursos) para la Gerencia y el Comité de Gestión | |
| Designación del Director del Proyecto. | |
| Nombre: | Responsable de la Jefatura de Gestión de Planificación, Seguimiento y Evaluación de Gestión. |
| Niveles de autoridad: | |

| | | |
|---|---|---|
| Reporta a: | Gerencia Hospitalaria | Exigir el cumplimiento de los entregables |
| Supervisa a: | Equipo del Proyecto | |
| Principales amenazas del proyecto (riesgos negativos). | | |
| No contar con el personal profesional clave (habilidades y competencias). | | |
| No contar con el compromiso de la Gerencia del Hospital. | | |
| Principales oportunidades del proyecto (riesgos positivos). | | |
| La ejecución del Proyecto GOBTISI permitirá asegurar el logro de los objetivos del Hospital a través de TI. | | |
| El Gobierno de TI en el Hospital posibilita la creación de valor (realización de beneficios, optimización de riesgos y recursos) para la Gerencia y el Comité de Gestión Hospitalario | | |

| Sponsor que autoriza el proyecto. | | | |
|---|---|---|---|
| Nombre: | Empresa / Organización: | Cargo: | Fecha: |
| Dr. Marco Andrés Sotomayor Paredes | Hospital General Docente de Calderón - HGDC | Gerente del Hospital General Docente de Calderón. | 25 de febrero de 2017 |

### 4.2.2 Fase 2: Planificación

En esta fase se define la estrategia y tácticas, así como la línea de acción o ruta para completar con éxito el proyecto.

4.2.2.1 Identificación y/o creación de la estructura organizativa

Se define la estructura organizativa del Hospital que proporcionará el apoyo necesario en todo el ciclo de vida de implementación del Gobierno de TI. Para la identificación se utiliza la estructura orgánica definida en el Estatuto Orgánico de Gestión Organizacional por Procesos de los Hospitales del MSP y las recomendaciones de COBIT 5 en su Guía un Marco de Negocio para el Gobierno y la Gestión de las TI de la empresa.

Tabla 15.

Identificación de la estructura organizativa.

| Hospital General Docente de Calderón | Función | Roles y Estructuras Organizativas de COBIT 5 |
|---|---|---|
| **1. Proceso Gobernante** | | |
| 1.1. Gerencia Hospitalaria | Gerenciar el funcionamiento global del Hospital como máxima autoridad y representante legal de la institución, en el marco de las directrices y acuerdos emanados por el Ministerio de Salud Pública y en cumplimiento de la normativa legal vigente. | Director General Ejecutivo CEO |
| 1.2. Comité de Gestión y Direccionamiento Estratégico del Hospital | Responsables del Gobierno del Hospital como autoridades máximas de cada proceso interno, en el marco de las directrices y acuerdos emanados por el Ministerio de Salud Pública y en cumplimiento de la normativa legal vigente. | Consejo de Administración |
| **2. Procesos Agregadores de Valor** | | |
| 2.1. Gestión Asistencial | Dirigir y coordinar actividades médico sanitarias de todas las especialidades, a fin de que éstas otorguen al paciente los servicios médicos y hospitalarios con oportunidad, alta calidad, eficiencia y efectividad. Garantizar el funcionamiento de los departamentos productores de salud dentro de los parámetros estandarizados de eficiencia y calidad. | Ejecutivo de Negocio |
| **3. Proceso Habilitantes de Asesoría** | | |
| 3.1. Gestión de Planificación, Seguimiento y Evaluación de Gestión | Articular los recursos, procedimientos y planes de salud en función de las estratégicas y objetivos institucionales. Implementar sistemas de seguimiento y control que contribuyan a la evaluación del cumplimiento de objetivos y metas y a la reducción de la brecha de oferta y demanda de los servicios de salud que ofrece el Hospital, con el propósito de generar satisfacción de los clientes internos, externos y el mejoramiento de los servicios que se ofrece a la población. | Oficina de Gestión de Programas y Proyectos (PMO) |
| 3.2. Gestión de Asesoría Jurídica | Asesorar en temas relacionados a la correcta aplicación de la carta magna, leyes, reglamentos, acuerdos, decretos y otros instrumentos legales relacionados con el andamiaje legal, a fin de que la institución y su gestión se encuentren siempre amparada en la ley. | Cumplimiento |

| | | |
|---|---|---|
| 3.3. Gestión de Calidad | Velar por la implementación y el cumplimiento del sistema integral de gestión de calidad y de los procedimientos e indicadores de calidad de cada uno de los servicios provistos por el hospital para satisfacer las necesidades de la demanda y la interacción con otros sistemas en su contexto. | Propietario del Proceso de Negocio |
| **4. Proceso Habilitantes de Apoyo** | | |
| 4.1. Gestión de Talento Humano | Administrar, seleccionar y desarrollar el talento humano del Hospital, garantizando su desarrollo constante mediante una verdadera capacitación, bienestar social y seguridad, con el fin de potencializar las habilidades y capacidades de su personal en cumplimiento a la ley, reglamentos, normas, políticas y otros documentos legales vigentes. | Jefe de Recursos Humanos |
| 4.2. Gestión Financiera | Administrar, organizar y controlar las actividades financiero-contables del Hospital, proporcionando ágil, oportuna y transparentemente los recursos financieros requeridos para la ejecución de los planes, programas y proyectos de la institución. | Director General Financiero (CFO) |
| 4.3. Gestión Administrativa | Administrar con eficiencia, eficacia y efectividad los recursos materiales, suministros, bienes y servicios requeridos para la ejecución de los planes, programas, proyectos y actividades del hospital. | Director General Operativo (COO) |
| 4.4. Gestión de Tecnologías de la Información y Comunicaciones | Aplicar las normas y procedimientos que efectivicen la gestión y administración de las tecnologías de la información y comunicaciones, orientadas a la optimización de los recursos y fortalecimiento de la red interna para mejorar la eficiencia en la atención a los pacientes. | Director de Informática/Sistemas (CIO) |

Adaptada de (Ministerio de Salud Pública, 2012); (ISACA, 2012, pág. 76).

#### 4.2.2.2 Aplicación de la técnica de cascada de metas de COBIT 5

Para asegurar el alineamiento de TI con los objetivos estratégicos del Hospital se utilizará la cascada de metas de COBIT 5 y la información del ítem 4.1.3. Como primer paso se realiza el mapeo entre las Metas Corporativas Genéricas y los objetivos del Hospital, para lo cual se utilizaron dos escalas:

- La escala “P” para principal, cuando las Metas Genéricas de COBIT 5 correspondan a los objetivos del Hospital y tendrá una valoración de 5.
- La escala “S” para secundario, cuando las Metas Genéricas de COBIT 5 no corresponden pero están enlazadas a los objetivos del Hospital y tendrá una valoración de 1.

En este punto se define que para la selección de las Metas Corporativas Genéricas, Metas Relacionadas con TI, Procesos de Gobierno y Gestión de TI, deben tener un nivel de valoración alto, así como también poseer mínimo dos (2) escalas “P” denominadas como principal y estar relacionados directamente en cumplir los objetivos del Hospital a consideración del Equipo del Proyecto.

Tabla 16.

Mapeo entre las Metas Corporativas Genéricas de COBIT 5 y los objetivos del Hospital General Docente de Calderón.

| Mapeo entre las Metas Corporativas de COBIT 5 y las Preguntas del Gobierno y la Gestión | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Metas Corporativas | | | | | | | | | | | | | | | | |
| | Financiera | | | | | Cliente | | | | | Interna | | | | | Aprendizaje y C. | |
| | Valor para las partes interesadas de las inversiones de negocio | Cartera de productos y servicios competitivos | Riesgos de negocio gestionados (salvaguarda de activos) | Cumplimiento de leyes y regulaciones externas | Transparencia financiera | Cultura de servicio orientada al cliente | Continuidad y disponibilidad del servicio de negocio | Respuestas ágiles a un entorno de negocio cambiante | Toma estratégica de decisiones basada en información | Optimización de costes de entrega del servicio | Optimización de la funcionalidad de los procesos de negocio | Optimización de los costes de los procesos de negocio | Programas gestionados de cambio en el negocio | Productividad operacional y de los empleados | Cumplimiento con las políticas internas | Personas preparadas y motivadas | Cultura de innovación de producto negocio |
| **Necesidades de las partes interesadas** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| Garantizar la equidad en el acceso y gratuidad de los servicios. | S | S | | S | | P | P | P | P | S | P | S | | P | S | P | |
| Trabajar bajo los lineamientos del Modelo de Atención Integral de Salud (MAIS) de forma integrada y en red con el resto de las Unidades Operativas de Salud del Ministerio de Salud Pública y otros actores de la red pública y privada complementaria que conforman el sistema nacional de salud del Ecuador. | | | | P | | | | | | | | | S | S | P | | |
| Mejorar la accesibilidad y el tiempo de espera para recibir atención, considerando la diversidad de género, cultural, generacional, socio económica, lugar de origen y discapacidades. | S | P | | S | | P | P | S | P | S | P | S | | P | S | S | |
| Involucrar a los profesionales en la gestión del hospital, aumentando su motivación, satisfacción y compromiso con la misión del hospital. | | | | | | S | | | | | | | | | S | S | P |
| Garantizar una atención de calidad y respeto a los derechos de las y los usuarios, para lograr la satisfacción con la atención recibida. | S | | | S | | P | P | S | S | S | | | | P | P | P | |
| Desarrollar una cultura de excelencia con el fin de optimizar el manejo de los recursos públicos, y la rendición de cuentas. | P | S | | P | S | | | | | S | | S | | S | | S | |
| **Sumatoria** | 8 | 7 | 0 | 13 | 1 | 16 | 15 | 7 | 11 | 4 | 10 | 3 | 1 | 17 | 13 | 13 | 5 |

En la siguiente tabla se resume las Metas Corporativas Genéricas planteadas por COBIT 5 que proporcionan el soporte para el cumplimiento de los objetivos estratégicos del Hospital General Docente de Calderón.

Tabla 17.
Resumen de las Metas Corporativas Genéricas de COBIT 5, aplicables al Hospital General Docente de Calderón.

| | | |
|---|---|---|
| Metas Corporativas | Financiera | 4.- Cumplimiento de leyes y regulaciones externas |
| | Cliente | 6.- Cultura de servicio orientada al cliente |
| | | 7.- Continuidad y disponibilidad del servicio de negocio |
| | | 9.- Toma estratégica de decisiones basada en información |
| | Interna | 11.- Optimización de la funcionalidad de los procesos de negocio |
| | | 14.- Productividad operacional y de los empleados |
| | | 15. Cumplimiento con las políticas internas |
| | Aprendizaje y Crecimiento | 16.- Personas preparadas y motivadas |

Una vez identificadas las Metas Corporativas Genéricas relacionadas con el Hospital se procede a identificar su correspondencia con las Metas Relacionadas con TI que incluye los datos, sistemas y procesos de información. COBIT 5 propone diecisiete Metas Relacionadas con TI, con las cuales se realiza el mapeo. De igual manera que en el ítem anterior, se utilizarán las siguientes escalas para realizar el mapeo:

- La escala “P” para principal, cuando exista una importante relación, es decir, las Metas Relacionadas con TI son el pilar imprescindible para conseguir los objetivos del Hospital y tendrá una valoración de 5.
- La escala “S” para secundario, cuando todavía existe un vínculo fuerte, pero menos importante, es decir, las Metas Relacionadas con las TI son un soporte secundario para cumplir con los objetivos del Hospital y tendrá una valoración de 1.

Tabla 18.

Mapeo entre las Metas Relacionadas con TI y las Metas Corporativas Genéricas de COBIT 5.

| Mapeo entre las Metas Corporativas de COBIT 5 y las Metas Relacionadas con las TI | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Metas Corporativas | | | | | | | | | | | | | | | | | | | |
| | | | 1. Valor para las partes interesadas de inversiones de negocio | 2. Cartera de productos y servicios competitivos | 3. Riesgos de negocio gestionados (salvaguarda de activos) | 4. Cumplimiento de Leyes y regulaciones externas | 5 Transparencia financiera | 6. Cultura de servicio orientada al cliente | 7. Continuidad y disponibilidad del servicio de negocio | 8. Respuestas ágiles a un entorno de negocio cambiante | 9. Toma estratégica de decisiones basada en información | 10. Optimización de costes de entrega del servicio | 11. Optimización de la funcionalidad de los procesos de negocio | 12. Optimización de los costes de los procesos de negocio | 13. Programas gestionados de cambio en el negocio | 14. Productividad operacional y de los empleados | 15. Cumplimiento con las políticas internas | 16. Personas preparadas y motivadas | 17. Cultura de innovación de producto negocio | |
| | | **Meta relacionada con las TI** | Financiera | | | | | Cliente | | | | | Interna | | | | | Aprendizaje y Crecimiento | | **Sumatoria** |
| Financiera | 1 | Alineamiento de TI y estrategia de negocio | P | P | S | | | P | S | P | P | S | P | S | P | | | S | S | 17 |
| | 2 | Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas | | | S | P | | | | | | | | | | | P | | | 10 |
| | 3 | Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI | P | S | S | | | | | S | S | | S | | P | | | S | S | 3 |
| | 4 | Riesgos de negocio relacionados con las TI gestionados | | | P | S | | | P | S | | P | | | S | | S | S | | 8 |
| | 5 | Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI | P | P | | | | S | | S | | S | S | P | | S | | | S | 3 |
| | 6 | Transparencia de los costes, beneficios y riesgos de las TI | S | | S | | P | | | | S | P | | P | | | | | | 1 |
| Cliente | 7 | Entrega de servicios de TI de acuerdo a los requisitos del negocio | P | P | S | S | | P | S | P | S | | P | S | S | | | S | S | 14 |
| | 8 | Uso adecuado de aplicaciones, información y soluciones tecnológicas | S | S | S | | | S | S | | S | S | P | S | | P | | S | S | 14 |

| Mapeo entre las Metas Corporativas de COBIT 5 y las Metas Relacionadas con las TI | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Metas Corporativas | | | | | | | | | | | | | | | | | | | | |
| | | | 1. Valor para las partes interesadas de las inversiones de negocio | 2. Cartera de productos y servicios competitivos | 3. Riesgos de negocio gestionados (salvaguarda de activos) | 4. Cumplimiento de Leyes y regulaciones externas | 5. Transparencia financiera | 6. Cultura de servicio orientada al cliente | 7. Continuidad y disponibilidad del servicio de negocio | 8. Respuestas ágiles a un entorno de negocio cambiante | 9. Toma estratégica de decisiones basada en información | 10. Optimización de costes de entrega del servicio | 11. Optimización de la funcionalidad de los procesos de negocio | 12. Optimización de los costes de los procesos de negocio | 13. Programas gestionados de cambio en el negocio | 14. Productividad operacional y de los empleados | 15. Cumplimiento con las políticas internas | 16. Personas preparadas y motivadas | 17. Cultura de innovación de producto negocio | |
| | | **Meta relacionada con las TI** | Financiera | | | | | Cliente | | | | | Interna | | | | | Aprendizaje y Crecimiento | | **Sumatoria** |
| Interna | 9 | Agilidad de las TI | S | P | S | | | S | | P | | | P | | S | S | | S | P | 8 |
| | 10 | Seguridad de la información, infraestructura de procesamiento y aplicaciones | | | P | P | | | P | | | | | | | | P | | | 15 |
| | 11 | Optimización de activos, recursos y capacidades de las TI | P | S | | | | | | S | | P | S | P | S | S | | | S | 2 |
| | 12 | Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio | S | P | S | | | S | | S | | S | P | S | S | S | | | S | 7 |
| | 13 | Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad. | P | S | S | | | S | | | | S | | S | P | | | | | 1 |
| | 14 | Disponibilidad de información útil y fiable para la toma de decisiones | S | S | S | S | | | P | | P | | S | | | | | | | 12 |
| | 15 | Cumplimiento de las políticas internas por parte de las TI | | | S | S | | | | | | | | | | | P | | | 6 |
| Aprendizaje y C. | 16 | Personal del negocio y de las TI competente y motivado | S | S | P | | | S | | S | | | | | | P | | P | S | 11 |
| | 17 | Conocimiento, experiencia e iniciativas para la innovación de negocio | S | P | | | | S | | P | S | | S | | S | | | S | P | 4 |

Como resultado del mapeo se identificaron las siguientes Metas Relacionadas con TI:

Tabla 19.

Resumen de las Metas Relacionadas con TI y las Metas Corporativas Genéricas de COBIT 5.

| | | | |
|---|---|---|---|
| Meta relacionada con las TI | Financiera | 1 | Alineamiento de TI y estrategia de negocio |
| | | 2 | Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas |
| | Cliente | 7 | Entrega de servicios de TI de acuerdo a los requisitos del negocio |
| | | 8 | Uso adecuado de aplicaciones, información y soluciones tecnológicas |
| | Interna | 10 | Seguridad de la información, infraestructura de procesamiento y aplicaciones |
| | | 14 | Disponibilidad de información útil y fiable para la toma de decisiones |
| | Aprendizaje y Crecimiento | 16 | Personal del negocio y de las TI competente y motivado |

Siguiendo con la técnica de cascada de metas de COBIT 5, se efectuó el mapeo entre las Metas Relacionadas con las TI y los Procesos de Gobierno y de Gestión de COBIT 5. Este mapeo se realizó usando la siguiente escala:

- “P” para principal, cuando existe una relación importante, es decir, el Proceso de COBIT 5 es un soporte primario para conseguir la Meta Relacionada con TI y tendrá una valoración de 5.
- “S” para secundario, cuando todavía existe una relación fuerte, pero menos importante, es decir, el Proceso de COBIT 5 es un soporte secundario para conseguir la Meta Relacionada con TI y tendrá una valoración de 1.

Tabla 20.

Mapeo entre las Metas Relacionadas con TI y los Procesos de COBIT 5.

| Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Meta relacionada con las TI | | | | | | | | | | | | | | | | |
| | | Financiera | | | | | | Cliente | | Interna | | | | | | | Aprendizaje y Crecimiento | |
| Procesos de COBIT 5 | | Alineamiento de TI y estrategia de negocio | Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas | Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI | Riesgos de negocio relacionados con las TI gestionados | Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI | Transparencia de los costes, beneficios y riesgos de las TI | Entrega de servicios de TI de acuerdo a los requisitos del negocio | Uso adecuado de aplicaciones, información y soluciones tecnológicas | Agilidad de las TI | Seguridad de la información, infraestructura de procesamiento y aplicaciones | Optimización de activos, recursos y capacidades de las TI | Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio | Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad. | Disponibilidad de información útil y fiable para la toma de decisiones | Cumplimiento de las políticas internas por parte de las TI | Personal del negocio y de las TI competente y motivado | Conocimiento, experiencia e iniciativas para la innovación de negocio | Sumatoria |
| **Evaluar, Orientar y Supervisar** | | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | |
| EDM01 | Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno | P | S | P | S | S | S | P | | S | S | S | S | S | S | S | S | S | 14 |
| EDM02 | Asegurar la entrega de beneficios | P | | S | | P | P | P | S | | | S | S | S | S | | S | P | 13 |
| EDM03 | Asegurar la optimización de riesgos | S | S | S | P | | P | S | S | | P | | | S | S | P | S | S | 11 |
| EDM04 | Asegurar la optimización de recursos | S | | S | S | S | S | S | S | P | | P | | S | | | P | S | 8 |
| EDM05 | Asegurar la transparencia hacia las partes nteresadas | S | S | P | | | P | P | | | | | | S | S | S | | S | 8 |
| **Alinear, Planificar y Organizar** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | |
| APO01 | Gestionar el Marco de Gestión de TI | P | P | S | S | | | S | | P | S | P | S | S | S | P | P | P | 18 |
| APO02 | Gestionar la Estrategia | P | | S | S | S | | P | S | S | | S | S | S | S | S | S | P | 13 |
| APO03 | Gestionar la Arquitectura Empresarial | P | | S | S | S | S | S | S | P | S | P | S | | S | | | S | 9 |
| APO04 | Gestionar la Innovación | S | | | S | P | | | P | P | | P | S | | S | | | P | 7 |
| APO05 | Gestionar el Portafolio | P | | S | S | P | S | S | S | S | | S | | P | | | | S | 7 |
| APO06 | Gestionar el Presupuesto y los Costos | S | | S | S | P | P | S | S | | | S | | S | | | | | 3 |
| APO07 | Gestionar los Recursos Humanos | P | S | S | S | | | S | | S | S | P | | P | | S | P | P | 13 |
| APO08 | Gestionar las Relaciones | P | | S | S | S | S | P | S | | | S | P | S | | S | S | P | 12 |

| Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Meta relacionada con las TI | | | | | | | | | | | | | | | | | |
| | | Financiera | | | | | | Cliente | | Interna | | | | | | | Aprendizaje y Crecimiento | | |
| Procesos de COBIT 5 | | Alineamiento de TI y estrategia de negocio | Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas | Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI | Riesgos de negocio relacionados con las TI gestionados | Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI | Transparencia de los costes, beneficios y riesgos de las TI | Entrega de servicios de TI de acuerdo a los requisitos del negocio | Uso adecuado de aplicaciones, información y soluciones tecnológicas | Agilidad de las TI | Seguridad de la información, infraestructura de procesamiento y aplicaciones | Optimización de activos, recursos y capacidades de las TI | Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio | Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad. | Disponibilidad de información útil y fiable para la toma de decisiones | Cumplimiento de las políticas internas por parte de las TI | Personal del negocio y de las TI competente y motivado | Conocimiento, experiencia e iniciativas para la innovación de negocio | |
| APO09 | Gestionar los Acuerdos de Servicios | S | | | S | S | S | P | S | S | S | S | | S | P | S | | | 13 |
| APO10 | Gestionar los Proveedores | | S | | P | S | S | P | S | P | S | S | | S | S | S | | S | 9 |
| APO11 | Gestionar la Calidad | S | S | | S | P | | P | S | S | | S | | P | S | S | S | S | 10 |
| APO12 | Gestionar los Riesgos | | P | | P | | P | S | S | S | P | | | P | S | S | S | S | 14 |
| APO13 | Gestionar la Seguridad | | P | | P | | P | S | S | | P | | | | P | | | | 17 |
| **Construcción, Adquisición e** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | |
| BAI01 | Gestionar Programas y Proyectos | P | | S | P | P | S | S | S | | | S | | P | | | S | S | 8 |
| BAI02 | Gestionar la Definición de Requisitos | P | S | S | S | S | | P | S | S | S | S | P | S | S | | | S | 14 |
| BAI03 | Gestionar la Identificación y Construcción de Soluciones | S | | | S | S | | P | S | | | S | S | S | S | | | S | 8 |
| BAI04 | Gestionar la Disponibilidad y Capacidad | | | | S | S | | P | S | S | | P | | S | P | | | S | 11 |
| BAI05 | Gestionar la Introducción de Cambios Organizados | S | | S | | S | | S | P | S | | S | S | P | | | | P | 7 |
| BAI06 | Gestionar los Cambios | | | S | P | S | | P | S | S | P | S | S | S | S | S | | S | 12 |
| BAI07 | Gestionar la Aceptación del Cambio y de la Transición | | | | S | S | | S | P | S | | | P | S | S | S | | S | 7 |
| BAI08 | Gestionar el Conocimiento | S | | | | S | | S | S | P | S | S | | | S | | S | P | 6 |
| BAI09 | Gestionar los Activos | | S | | S | | P | S | | S | S | P | | | S | S | | | 4 |
| BAI10 | Gestionar la Configuración | | P | | S | | S | | S | S | S | P | | | P | S | | | 12 |

| Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Meta relacionada con las TI | | | | | | | | | | | | | | | | |
| | | Financiera | | | | | | Cliente | | Interna | | | | | | | Aprendizaje y Crecimiento | |
| Procesos de COBIT 5 | | Alineamiento de TI y estrategia de negocio | Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas | Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI | Riesgos de negocio relacionados con las TI gestionados | Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI | Transparencia de los costes, beneficios y riesgos de las TI | Entrega de servicios de TI de acuerdo a los requisitos del negocio | Uso adecuado de aplicaciones, información y soluciones tecnológicas | Agilidad de las TI | Seguridad de la información, infraestructura de procesamiento y aplicaciones | Optimización de activos, recursos y capacidades de las TI | Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio | Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad. | Disponibilidad de información útil y fiable para la toma de decisiones | Cumplimiento de las políticas internas por parte de las TI | Personal del negocio y de las TI competente y motivado | Conocimiento, experiencia e iniciativas para la innovación de negocio | |
| **Entregar, dar Servicio y Soporte** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | |
| DSS01 | Gestionar las Operaciones | | S | | P | S | | P | S | S | S | P | | | S | S | S | S | 10 |
| DSS02 | Gestionar las Peticiones y los Incidentes del Servicio | | | | P | | | P | S | | S | | | | S | S | | S | 8 |
| DSS03 | Gestionar los Problemas | | S | | P | S | | P | S | S | | P | S | | P | S | | S | 12 |
| DSS04 | Gestionar la Continuidad | S | S | | P | S | | P | S | S | S | S | S | | P | S | S | S | 15 |
| DSS05 | Gestionar los Servicios de Seguridad | S | P | | P | | | S | S | | P | S | S | | S | S | | | 14 |
| DSS06 | Gestionar los Controles de Procesos del Negocio | | S | | P | | | P | S | | S | S | S | | S | S | S | S | 10 |
| **Supervisión, Evaluación y** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | |
| MEA01 | Supervisar, Evaluar y Valorar el Rendimiento y Conformidad | S | S | S | P | S | S | P | S | S | S | P | | S | S | P | S | S | 11 |
| MEA02 | Supervisar, Evaluar y Valorar el Sistemas de Control Interno | | P | | P | | S | S | S | | S | | | | S | P | | S | 9 |
| MEA03 | Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos | | P | | P | S | | S | | | S | | | | | S | | S | 7 |

Como resultado de la aplicación de la técnica de cascada de metas de COBIT 5 se identifica los Procesos de Gobierno y Gestión de TI, para alcanzar los objetivos estratégicos del Hospital.

Tabla 21.

Procesos de COBIT 5 primarios para alcanzar los objetivos estratégicos del Hospital General Docente de Calderón.

| | | |
|---|---|---|
| 1 | EDM01 | Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno |
| 2 | EDM02 | Asegurar la entrega de beneficios |
| 3 | APO01 | Gestionar el Marco de Gestión de TI |
| 4 | APO02 | Gestionar la Estrategia |
| 5 | APO07 | Gestionar los Recursos Humanos |
| 6 | APO09 | Gestionar los Acuerdos de Servicios |
| 7 | APO12 | Gestionar los Riesgos |
| 8 | APO13 | Gestionar la Seguridad |
| 9 | BAI02 | Gestionar la Definición de Requisitos |
| 10 | DSS04 | Gestionar la Continuidad |
| 11 | DSS05 | Gestionar los Servicios de Seguridad |

#### 4.2.2.3 Priorización de los procesos con enfoque en la Seguridad de la Información

Es necesario priorizar los procesos que se implementaran en el Hospital, en este caso debido al enfoque de Seguridad de la Información que tiene el modelo de Gobierno de TI, se utilizará la información de la tabla 11 para priorizar los procesos de la tabla 21.

Tabla 22.

Procesos de COBIT 5 con énfasis en la Seguridad de la Información para el Hospital General Docente de Calderón.

| | | |
|---|---|---|
| 1 | EDM01 | Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno |
| 2 | APO01 | Gestionar el Marco de Gestión de TI |
| 3 | APO07 | Gestionar los Recursos Humanos |
| 4 | APO09 | Gestionar los Acuerdos de Servicios |
| 5 | APO12 | Gestionar los Riesgos |
| 6 | APO13 | Gestionar la Seguridad |
| 7 | BAI02 | Gestionar la Definición de Requisitos |
| 8 | DSS04 | Gestionar la Continuidad |
| 9 | DSS05 | Gestionar los Servicios de Seguridad |

A continuación se presenta el Plan de Gestión del Alcance del Proyecto:

Tabla 23.

Plan de Gestión del Alcance del proyecto.

| **Plan de Gestión del Alcance** | |
|---|---|
| Nombre del proyecto | Siglas del proyecto |
| Gobierno de Tecnología de la Información con énfasis en la Seguridad de la Información para el Hospital General Docente de | GOBTISI |
| Descripción del alcance del producto | |
| Requisitos: Condiciones o capacidades que debe poseer o satisfacer el producto para cumplir con contratos, normas, especificaciones u otros documentos | Características: Propiedades físicas, energéticas, o que son distintivas del producto, y/o que describen su singularidad. |
| 1. Alinear los objetivos de TI con los objetivos estratégicos del Hospital. | 1. Identificación y priorización de los procesos primarios relacionados con TI y que tienen un enfoque de Seguridad de la Información. |

| | |
|---|---|
| 2. Los servicios y funciones de TI se proporcionen con el máximo valor posible o de la forma más eficiente. | 2. Prácticas y actividades que faciliten la toma de decisiones, optimizando la inversión y disminuyendo gastos. |
| 3. Mantener los riesgos relacionados con TI en un nivel aceptable. | 3. Prácticas y actividades que permitan una administración efectiva, y un manejo eficiente de la gestión de riesgo en TI. |
| 4. Cumplimiento de leyes, regulaciones, acuerdos contractuales y políticas aplicables a la Seguridad de la Información. | 4. Políticas y prácticas que permitan brindar integridad, confidencialidad y disponibilidad a los activos de información del Hospital. |

| Entregables del proyecto: productos entregables intermedios y finales que se generarán en cada fase del proyecto. | |
|---|---|
| Fase del proyecto | Productos entregables |
| 1. Inicio | 1.1 Acta de Constitución del Proyecto. |
| 2. Planificación | 2.1. Informe sobre la estructura organizativa del Hospital para el Proyecto.<br>2.2. Plan de Gestión del Alcance.<br>2.3. Plan de Gestión del Cronograma.<br>2.4. Plan de Gestión de los Recursos Humanos.<br>2.5. Plan de Gestión de las Comunicaciones.<br>2.6. Plan de Gestión de los Costos.<br>2.7. Plan de Gestión de Riesgos.<br>2.8. Documentación sobre el estado actual de los procesos seleccionados.<br>2.9. Informe sobre el estado objetivo de los procesos seleccionados.<br>2.10. Documentación sobre las actividades que permitan alcanzar el estado deseado. |
| 3. Ejecución | 3.1. Datos de desempeño del trabajo.<br>3.2. Solicitudes de cambio.<br>3.3. Actualizaciones al Plan para la Dirección del Proyecto. |

| | |
|---|---|
| 4. Monitoreo y Control | 4.1. Datos de desempeño del trabajo.<br>4.2. Solicitudes de cambio.<br>4.3. Actualizaciones al Plan para la Dirección del Proyecto. |
| 5. Cierre | 5.1. Acta de Cierre del Proyecto. |
| Restricciones del proyecto: factores que limitan el rendimiento del proyecto, el rendimiento de un proceso del proyecto, o las opciones de planificación del proyecto. | |
| Sólo se emplearán los recursos internos del Hospital asignados para el | |
| Supuestos del proyecto: factores que para propósitos de la planificación del proyecto se consideran verdaderos, reales o ciertos. | |
| Sólo se emplearán los recursos internos del Hospital asignados para el | |

4.2.2.4 Elaboración del Plan de Gestión del Cronograma

En este ítem se proporcionará una guía y dirección sobre cómo se gestionará el cronograma del proyecto a lo largo del mismo.

Tabla 24.

Plan de Gestión del Cronograma.

| **Plan de Gestión del Cronograma** | |
|---|---|
| Nombre del proyecto | Siglas del proyecto |
| Gobierno de Tecnología de la Información con énfasis en la Seguridad de la Información para el Hospital General Docente de Calderón. | GOBTISI |

| Nombre de la tarea | Duración (Dias) | Inicio | Fin |
|---|---|---|---|
| **1.0 Inicio** | **5** | **20-feb-17** | **25-feb-17** |
| 1.1 Acta de Constitución del Proyecto. | 5 | 20-feb-17 | 25-feb-17 |
| **2.0 Planificación** | **26** | **25-feb-17** | **23-mar-17** |
| 2.1 Informe sobre la estructura organizativa del Hospital para el Proyecto. | 2 | 25-feb-17 | 27-feb-17 |
| 2.2 Plan de Gestión del Alcance | 2 | 27-feb-17 | 01-mar-17 |
| 2.3 Plan de Gestión del Cronograma. | 3 | 01-mar-17 | 04-mar-17 |
| 2.4 Plan de Gestión de los Recursos Humanos. | 2 | 04-mar-17 | 06-mar-17 |
| 2.5 Plan de Gestión de las Comunicaciones. | 2 | 06-mar-17 | 08-mar-17 |
| 2.6 Plan de Gestión de Costos y Riesgos. | 2 | 08-mar-17 | 10-mar-17 |
| 2.8 Documentación sobre el estado actual de los procesos seleccionados. | 5 | 10-mar-17 | 15-mar-17 |
| 2.9 Informe sobre el estado objetivo de los procesos seleccionados. | 3 | 15-mar-17 | 18-mar-17 |
| 2.10 Documentación sobre las actividades que permitan alcanzar el estado deseado. | 5 | 18-mar-17 | 23-mar-17 |
| **3.0 Ejecución** | **198** | **23-mar-17** | **07-oct-17** |
| 3.1 Implementación de las actividades que permitan alcanzar el estado deseado. | 180 | 23-mar-17 | 19-sep-17 |
| 3.2 Datos de desempeño del trabajo. | 5 | 19-sep-17 | 24-sep-17 |
| 3.3 Solicitudes de cambio. | 8 | 24-sep-17 | 02-oct-17 |
| 3.4 Actualizaciones al Plan para la Dirección del Proyecto. | 5 | 02-oct-17 | 07-oct-17 |
| **4.0 Monitoreo y Control** | **16** | **07-oct-17** | **23-oct-17** |
| 4.1 Datos de desempeño del trabajo. | 6 | 07-oct-17 | 13-oct-17 |
| 4.2 Solicitudes de cambio. | 5 | 13-oct-17 | 18-oct-17 |
| 4.3 Actualizaciones al Plan para la Dirección del Proyecto. | 5 | 18-oct-17 | 23-oct-17 |
| **5.0 Cierre** | **3** | **23-oct-17** | **26-oct-17** |
| 5.1 Acta de Cierre del Proyecto. | 3 | 23-oct-17 | 26-oct-17 |

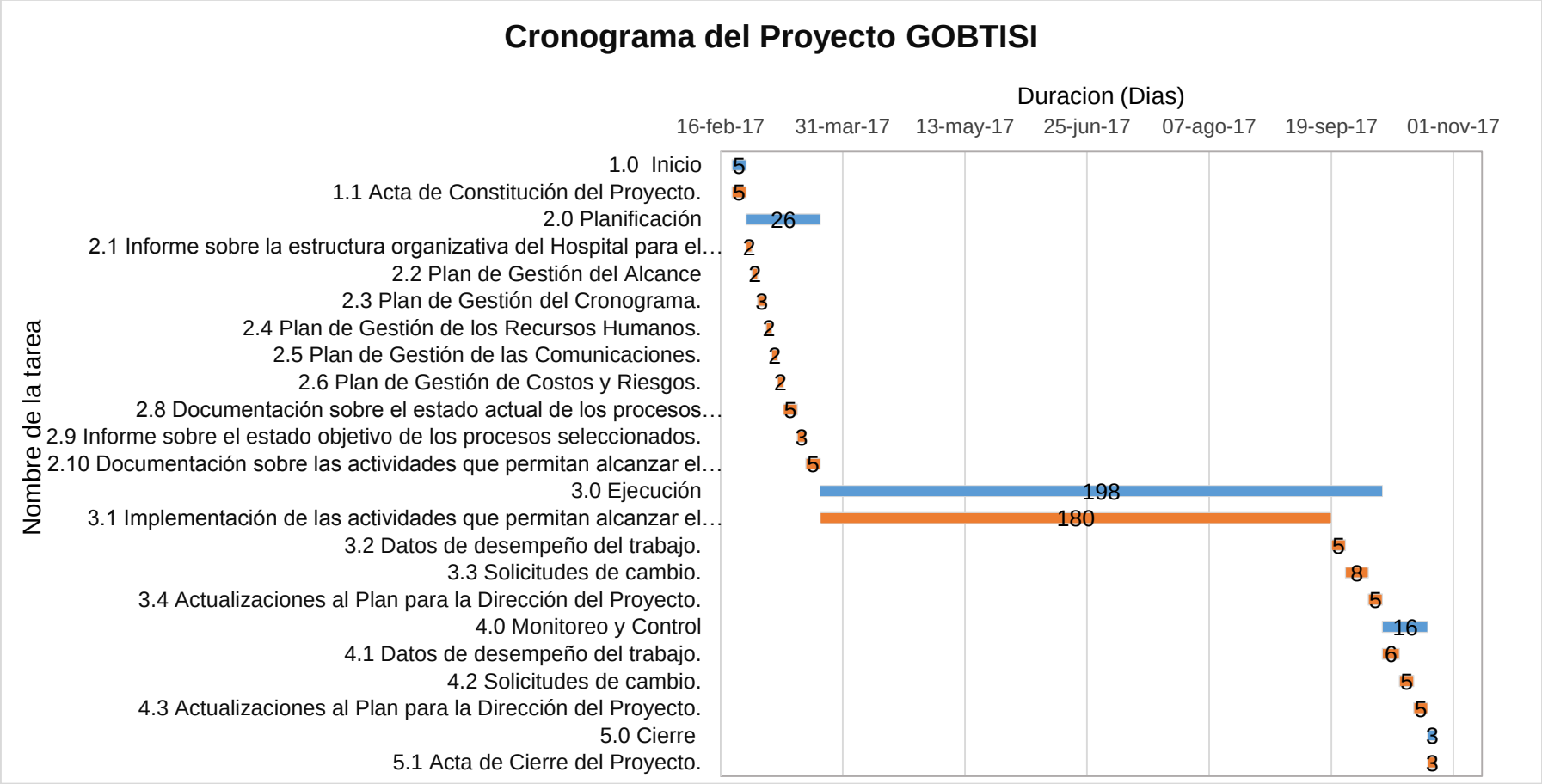



Figura 35. Cronograma del Proyecto GOBTISI.

### 4.2.2.5 Elaboración de la Matriz de Asignación de Responsabilidades (RACI) para la estructura organizativa

En las siguientes tablas se muestran las responsabilidades de cada miembro del Equipo del Proyecto y el Plan de Gestión de los Recursos Humanos.

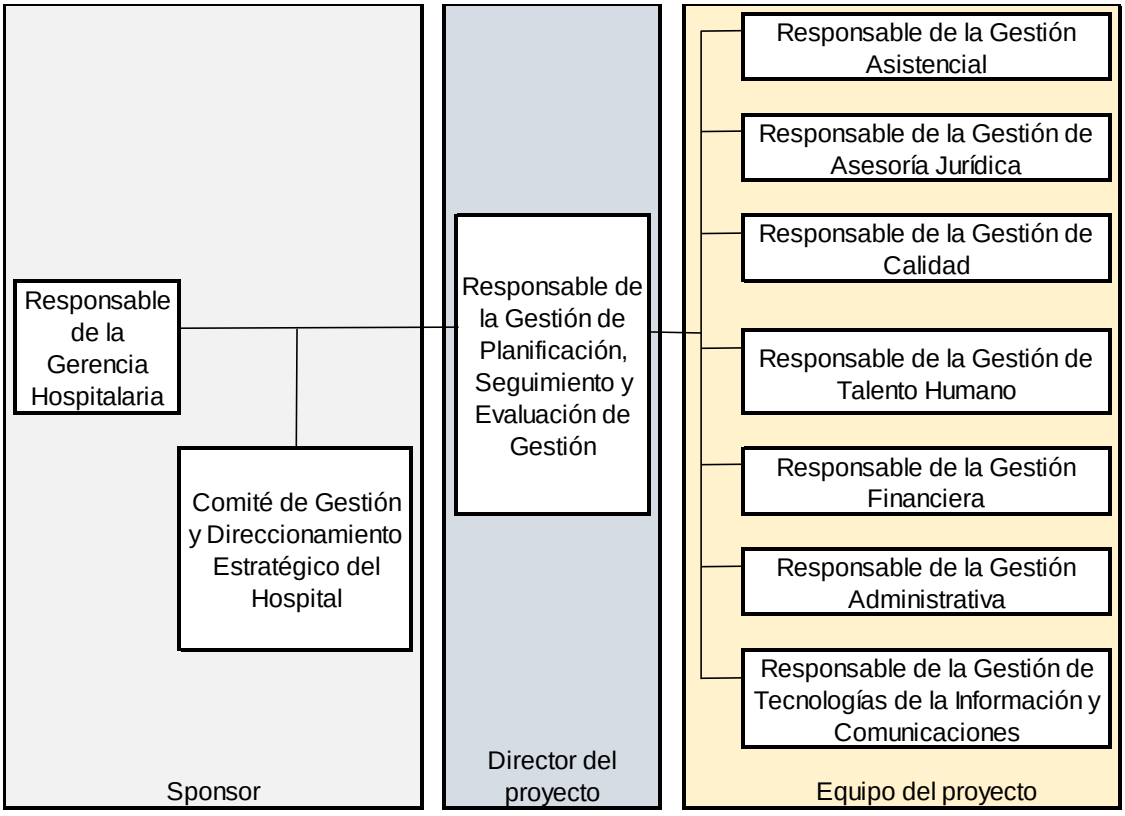
Tabla 25.

Matriz de responsabilidades de Proyecto GOBTISI.

| | Estructura organizativa | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Nombre de la tarea | Gerencia Hospitalaria. | Comité de Gestión y Direccionamiento Estratégico del Hospital. | Gestión Asistencial. | Gestión de Planificación, Seguimiento y Evaluación de Gestión. | Gestión de Asesoría Jurídica. | Gestión de Calidad. | Gestión de Talento Humano. | Gestión Financiera. | Gestión Administrativa. | Gestión de Tecnologías de la Información y Comunicaciones. |
| **1.0 Inicio** | | | | | | | | | | |
| 1.1 Acta de Constitución del Proyecto. | A | A | I | R | I | I | I | I | I | C |
| **2.0 Planificación** | | | | | | | | | | |
| 2.1 Informe sobre la estructura organizativa del Hospital para el Proyecto. | A | A | C | R | I | I | I | I | I | C |
| 2.2 Plan de Gestión del Alcance | A | I | C | R | I | I | I | I | C | C |
| 2.3 Plan de Gestión del Cronograma. | I | I | I | A | I | I | C | I | R | C |
| 2.4 Plan de Gestión de los Recursos Humanos. | I | I | I | A | I | I | R | I | C | I |
| 2.5 Plan de Gestión de las Comunicaciones. | A | A | I | R | I | I | I | I | C | I |
| 2.6 Plan de Gestión de los Costos. | A | A | I | R | I | I | I | I | C | I |
| 2.7 Plan de Gestión de los Riesgos. | A | A | I | R | I | I | I | I | C | C |
| 2.8 Documentación sobre el estado actual de los procesos seleccionados. | A | I | I | R | I | I | I | I | C | R/A |
| 2.9 Informe sobre el estado objetivo de los procesos seleccionados. | A | A | C | R | C | C | C | C | C | R/C |
| 2.10 Documentación sobre las actividades que permitan alcanzar el estado deseado. | A | A | C | R | I | I | I | I | I | R/A |
| **3.0 Ejecución** | | | | | | | | | | |
| 3.1 Implementación de las actividades que permitan alcanzar el estado deseado. | I | I | I | R/A | R | R | R | R | R | R |
| 3.2 Datos de desempeño del trabajo. | I | I | I | R/A | R | R | R | R | R | R |
| 3.3 Solicitudes de cambio. | I | I | I | R/A | R | R | R | R | R | R |
| 3.4 Actualizaciones al Plan para la Dirección del Proyecto. | I | I | I | R/A | R | R | R | R | R | R |
| **4.0 Monitoreo y Control** | | | | | | | | | | |
| 4.1 Datos de desempeño del trabajo. | I | I | I | R/A | R | R | R | R | R | R |
| 4.2 Solicitudes de cambio. | I | I | I | R/A | R | R | R | R | R | R |
| 4.3 Actualizaciones al Plan para la Dirección del Proyecto. | I | I | I | R/A | R | R | R | R | R | R |
| **5.0 Cierre** | | | | | | | | | | |
| 5.1 Acta de Cierre del Proyecto. | A | A | I | R | C | C | C | C | C | C |

Tabla 26.

Plan de Gestión de los Recursos Humanos.

| **Plan de Gestión de los Recursos Humanos** | |
|---|---|
| Nombre del proyecto | Siglas del proyecto |
| Gobierno de Tecnología de la Información con énfasis en la Seguridad de la Información para el Hospital General Docente de Calderón | GOBTISI |
| Organigrama del proyecto: especificar el organigrama del proyecto. | |
|  | |
| Roles y responsabilidades: especificar la matriz de asignaciones de responsabilidades. | |
| Referirse a la Tabla 25. Matriz de responsabilidades de Proyecto GOBTISI. | |
| Capacitación, entrenamiento, tutoría requerido: | |

| |
|---|
| • Para aprovechar la ejecución del Proyecto GOBTISI, el Director del Proyecto hará el proceso de tutoría a los miembros del equipo menos experimentados, permitiéndoles desarrollar sus habilidades en la Gestión de Proyectos.<br>• La casa de salud deberá capacitar y entrenar al personal que participará en el Proyecto. |
| Cumplimiento de regulaciones, pactos, y políticas: |
| • Sólo se deberá tomar en cuenta al personal que como mínimo posea título de tercer nivel y que pertenezcan al personal interno del Hospital, se debe considerar la opción de solicitar una acreditación o especialización en su área de gestión.<br>• Todo el personal del Hospital que participará en el Proyecto pasará por una evaluación de desempeño al final del mismo, y dicha evaluación se guardará en su perfil óptimo, realizado por la Unidad de Gestión de Recursos Humanos al final de cada año. |

.

4.2.2.6 Elaboración del Plan de Gestión de los Costos

En esta fase se definen los recursos necesarios para completar las actividades del Proyecto GOBTISI.

Tabla 27.

Plan de Gestión de los Costos.

| **Plan de Gestión de los Costos** | |
|---|---|
| Nombre del proyecto | Siglas del proyecto |
| Gobierno de Tecnología de la Información con énfasis en la Seguridad de la Información para el Hospital General Docente de Calderón | GOBTISI |
| Consideraciones: | |

- Se toma en cuenta para el cálculo del presupuesto las horas hombre utilizadas para cada actividad según el cronograma con una hora de dedicación por cada tarea.
- Se utiliza software libre para herramientas de Gestión de Proyectos y ofimática, pero se toma en cuenta un servidor de repositorio digital de documentos con un costo en el mercado de $ 2.000,00.
- Las personas involucradas en cada actividad están definidas en la Matriz de Responsabilidades de Proyecto y la duración de cada actividad en el Plan de Gestión del Cronograma.
- Como se indicó en el Acta de Constitución del Proyecto, para la implementación del proyecto se utilizará únicamente los recursos humanos internos del Hospital.
- El costo unitario de cada hora dedicada al Proyecto GOBTISI por parte de los recursos humanos está definida por el sueldo de cada funcionario, puesto que los involucrados en el proyecto son los líderes de sus respectivas unidades de gestión, tienen una categoría de servidor público 7 con una remuneración de $ 1.676,00, a excepción del Gerente del Hospital que tiene un salario mensual de $ 5.009,00 con una categoría de coordinadores / asesor 1.

Costos de implementación del proyecto:

| Nombre de la Tarea | Duración (Días) | Horas Trabajadas | Costo Unitario ($) | Total Unitario ($) |
|---|---|---|---|---|
| **1.0 Inicio** | | | | |
| 1.1 Acta de Constitución del Proyecto. | 5 | 5 | 10,47 | 52,35 |
| **2.0 Planificación** | | | | |
| 2.1 Informe sobre la estructura organizativa del Hospital para el Proyecto. | 2 | 2 | 10,47 | 20,94 |
| 2.2 Plan de Gestión del Alcance | 2 | 2 | 10,47 | 20,94 |
| 2.3 Plan de Gestión del Cronograma. | 3 | 3 | 10,47 | 31,41 |
| 2.4 Plan de Gestión de los Recursos Humanos. | 2 | 2 | 10,47 | 20,94 |
| 2.5 Plan de Gestión de las Comunicaciones. | 2 | 2 | 10,47 | 20,94 |
| 2.6 Plan de Gestión de los Costos y Riesgos. | 2 | 2 | 10,47 | 20,94 |
| 2.7 Documentación sobre el estado actual de los procesos seleccionados. | 5 | 10 | 10,47 | 104,7 |

| | | | | |
|---|---|---|---|---|
| 2.8 Informe sobre el estado objetivo de los procesos seleccionados. | 3 | 6 | 10,47 | 62,82 |
| 2.9 Documentación sobre las actividades que permitan alcanzar el estado deseado. | 5 | 10 | 10,47 | 104,7 |
| **3.0 Ejecución** | | | | |
| 3.1 Implementación de las actividades que permitan alcanzar el estado deseado. | 180 | 1080 | 10,47 | 11307,6 |
| 3.2 Datos de desempeño del trabajo. | 5 | 30 | 10,47 | 314,1 |
| 3.3 Solicitudes de cambio. | 8 | 48 | 10,47 | 502,56 |
| 3.4 Actualizaciones al Plan para la Dirección del Proyecto | 5 | 25 | 10,47 | 261,75 |
| **4.0 Monitoreo y Control** | | | | |
| 4.1 Datos de desempeño del trabajo. | 6 | 36 | 10,47 | 376,92 |
| 4.2 Solicitudes de cambio. | 5 | 30 | 10,47 | 314,1 |
| 4.3 Actualizaciones al Plan para la Dirección del Proyecto. | 5 | 30 | 10,47 | 314,1 |
| **5.0 Cierre** | | | | |
| 5.1 Acta de Cierre del Proyecto. | 3 | 3 | 10,47 | 31,41 |
| Costo total horas trabajadas | | | | **13883,22** |
| **Herramientas adicionales** | | | | |
| Project Libre | | | | **0** |
| Open Office | | | | **0** |
| Repositorio digital | | | | **2000** |
| **Total** | | | | **15883,22** |

### 4.2.2.7 Elaboración del Plan de Gestión de las Comunicaciones

En la siguiente tabla se muestra el Plan de Gestión de las Comunicaciones del Proyecto GOBTISI:

Tabla 28.

Plan de Gestión de las Comunicaciones.

| **Plan de Gestión de las Comunicaciones** | |
|---|---|
| Nombre del proyecto | Siglas del proyecto |
| Gobierno de Tecnología de la Información con énfasis en la Seguridad de la Información para el Hospital General Docente de Calderón | GOBTISI |
| Procedimiento para tratar polémicas: defina el procedimiento para procesar y resolver las polémicas, especificando la forma de capturarlas y registrarlas, el modo en que se abordará su tratamiento y resolución. | |

1. Se captarán las diferencias a través de la observación y conversación, de alguna persona o grupo que los exprese formalmente.
2. Se codificaran y registraran las polémicas en un documento de Control de Polémicas.
3. Se revisará el documento de Control de Polémicas en la reunión semanal de Coordinación del Proyecto, con el fin de determinar las soluciones a aplicar y revisar si las soluciones aplicadas han sido efectivas.
4. En caso que una polémica no pueda ser resuelta o en caso que haya evolucionado hasta convertirse en un problema, se deberá escalar el

Guías para eventos de comunicación: defina guía para reuniones, conferencias, correo electrónico, etc.

1. Reuniones formales del Equipo de Proyecto: Para las reuniones del Equipo de Proyecto se deberá seguir los siguientes pasos
   a) Se debe fijar la agenda con anterioridad.
   b) Se debe coordinar e informar la fecha, hora y lugar con los participantes.
   c) Se debe empezar puntual.
   d) Se deben fijar los objetivos de la reunión, los roles, los procesos grupales de trabajo, y los métodos de solución de polémicas.
   e) Se debe cumplir a cabalidad los roles de facilitador (dirige el proceso grupal de trabajo) y de anotador (toma nota de los resultados formales de la reunión).
   f) Se debe terminar puntual.
   g) Se debe emitir un acta de reunión la cual se debe repartir a los participantes (previa revisión por parte de ellos).
2. Comunicaciones entre miembros del equipo: Serán realizadas principalmente por correo electrónico o utilizando un repositorio digital de documentos para compartir la información.
3. Comunicaciones masivas a todos los colaboradores del Proyecto: Será vía correo electrónico, así como también las capacitaciones sobre las políticas y procesos definidos.

4. Entrega de documentos del Proyecto: Serán subidos a un repositorio digital compartido, una vez que sean aprobados en la reunión por el Equipo de Proyecto. El responsable de almacenar y organizar la información será la Unidad de Gestión Administrativa.

4.2.2.8 Elaborar el Plan de Gestión de los Riesgos

El Plan de Riesgos del Proyecto GOBTISI, define las posibles amenazas que podrían afectar a la ejecución del proyecto y las posibles soluciones que permitan mitigar dichas amenazas.

Tabla 29.
Plan de Gestión de los Riesgos.

| **Plan de Gestión de los Riesgos** | |
|---|---|
| Nombre del proyecto | Siglas del proyecto |
| Gobierno de Tecnología de la Información con énfasis en la Seguridad de la Información para el Hospital General Docente de Calderón | GOBTISI |
| Identificación y descripción de las posibles amenazas que podrían afectar a la ejecución del proyecto. | |
| 1. Falta de conocimiento por parte de los miembros del Equipo de Proyecto, respecto a los marcos de referencia de Gestión de TI: Es posible que los miembros del Equipo de Proyecto no cuenten con la misma experiencia y conocimiento de los marcos de referencia de Gobierno de TI, de ser así se espera retrasos en el desarrollo del proyecto.<br>2. Problemas Técnicos: Existe la posibilidad de que se presenten problemas técnicos como fallas en los equipos de cómputo, pérdida de información, cortes de energía, etc. que podría retrasar el desarrollo del proyecto.<br>3. Problemas de Comunicación: Los problemas de comunicación dentro | |

4. Dificultad de adopción de los procesos: Es probable que los colaboradores de la empresa tengan dificultad y cierta resistencia para adoptar las políticas y procesos en la puesta en producción y los resultados no serían los esperados.

Análisis cualitativo los riesgos.

| Núm. | Riesgo | Probabilidad | Impacto |
|---|---|---|---|
| 1 | Falta de conocimiento por parte de los miembros del Equipo de Proyecto, respecto a los marcos de referencia de Gobierno de TI | Alta | medio |
| 2 | Problemas Técnicos | baja | medio |
| 3 | Problemas de Comunicación | medio | alto |
| 4 | Dificultad de adopción de los procesos | medio | alto |

Plan de Contingencia.

Acorde a las amenazas identificadas se realiza el Plan de Contingencia que permita evitar o mitigar el riesgo.

1. **Falta de conocimiento por parte de los miembros del Equipo de Proyecto, respecto a los marcos de referencia de Gobierno de TI:** Para mitigar el riesgo, Se le preguntará a cada miembro del equipo por la experiencia y conocimiento que posee en marcos de referencia de Gobierno de TI, en caso de tener falencias se dará una capacitación previa sobre el tema para que exista una comunicación más fluida sobre temas de Gobierno y Gestión de TI. El encargado de la capacitación será la Unidad de Gestión de Tecnologías de la Información y Comunicaciones.
2. **Problemas Técnicos:** Para mitigar el riesgo, se instalará un repositorio de información en el Hospital organizado por fechas y versiones para almacenar la información generada del Proyecto GOBTISI, que permita sacar respaldos automáticos.

3. **Problemas de Comunicación:** Para mitigar el riesgo, el Director de Proyecto permitirá la participación a todos los miembros del equipo en cada reunión, con la finalidad de conocer los diferentes puntos de vista de cada persona y que se establezca un diálogo sano y amigable. Los acuerdos y responsabilidades deben ser comunicados a todos los integrantes del equipo, para evitar malos entendidos.
4. **Dificultad de adopción de los procesos:** Se mitigará el riesgo con una capacitación sobre los procesos a implementar a todos los actores del Proyecto.

4.2.2.9 Identificación del estado actual

En esta fase se identifica el estado actual de los procesos que contribuirán alcanzar los objetivos estratégicos del Hospital, para lo cual se realiza una evaluación de capacidad de procesos a través del PAM (Modelo de Evaluación de Procesos) de COBIT 5 como método de evaluación. Los pasos realizados para la evaluación de los procesos son:

a) Se realiza una encuesta a los responsables de cada área de gestión del Hospital. La encuesta se realizara vía WEB mediante la herramienta Google Forms, donde los resultados y participantes son registrados por la misma herramienta de software. Las preguntas de la encuesta y resultados se presentan en el anexo 5 y 6 respectivamente. Se debe agregar que la encuesta puede ser accedida mediante el enlace: https://goo.gl/forms/tVy94ObXMNLPBIGp1.

b) La calificación de las metas de cada proceso de COBIT 5 (una pregunta por cada meta), se realiza conforme a la siguiente escala de calificación.

Tabla 30.

Escala de calificación.

| N : No logrado (0 a 15% ) | P: Parcialmente logrado (>15% a 50%) | L: Logrado en gran medida (>50% a 85%) | F: Logrado Totalmente (>85% a 100%) |
|---|---|---|---|

Adaptado de (ISACA, 2013).

c) Llenar la tabla de evaluación detallada de los procesos de COBIT 5.

d) Registrar los datos en la tabla de resultados de evaluación del proceso.

e) Describir el nivel de capacidad obtenido en la evaluación realizada a los procesos de COBIT 5.

A continuación, se muestran las tablas de resultados de evaluación de los proceso de Hospital.

Tabla 31.

Resultados de la evaluación del proceso EDM01.

| **Nombre de Proceso : EDM01 - Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno** | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Niveles de Capacidad:** | Nivel 0 | Nivel 1 | Nivel 2 | | Nivel 3 | | Nivel 4 | | Nivel 5 | |
| | | PA 1.1 | PA 2.1 | PA 2.2 | PA 3.1 | PA 3.2 | PA 4.1 | PA 4.2 | PA 5.1 | PA 5.2 |
| **Puntuación de los criterios:** | | P | N | N | | | | | | |
| **Nivel de capacidad alcanzado:** | 0 | | | | | | | | | |
| **Escala de calificación:** | N : No logrado (0 a 15% ) | | P: Parcialmente logrado (>15% a 50%) | | L: Logrado en gran medida (>50% a 85%) | | | F: Logrado Totalmente (>85% a 100%) | | |

Adaptado de (ISACA, 2013)

El nivel de capacidad alcanzado por el proceso EDM01 - Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno es cero (0).

Las decisiones o iniciativas de TI para aportar a los objetivos estratégicos del Hospital, actualmente son gestionadas por la Unidad de Planificación y Administrativa - Financiera del Hospital, por lo tanto existen decisiones, como la provisión de nuevos servicios o el abastecimiento de infraestructura TI, sin una

previa planificación e investigación del retorno de inversión, realizada por prestigio interinstitucional. Además por iniciativa propia la unidad de Gestión de Tecnologías de la Información y Comunicaciones del Hospital realiza encuestas de satisfacción a los usuarios sobre los servicios de TI proporcionados, para un posterior reporte a la Gerencia Hospitalaria. Sin embargo, por no encontrarse bien definidos los roles y responsabilidades dentro del sistema de gobierno del Hospital dichos informes son desestimados o revisados en forma tardía.

Tabla 32.

Resultados de la evaluación del proceso APO01.

| **Nombre de Proceso : APO01 - Gestionar el Marco de Gestión de TI** | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Niveles de Capacidad:** | Nivel 0 | Nivel 1 | Nivel 2 | | Nivel 3 | | Nivel 4 | | Nivel 5 | |
| | | PA 1.1 | PA 2.1 | PA 2.2 | PA 3.1 | PA 3.2 | PA 4.1 | PA 4.2 | PA 5.1 | PA 5.2 |
| **Puntuación de los criterios:** | | P | N | N | | | | | | |
| **Nivel de capacidad alcanzado:** | 0 | | | | | | | | | |
| **Escala de calificación:** | N : No logrado (0 a 15% ) | | P: Parcialmente logrado (>15% a 50%) | | L: Logrado en gran medida (>50% a 85%) | | F: Logrado Totalmente (>85% a 100%) | | | |

Adaptado de (ISACA, 2013, pág. 16)

El nivel de capacidad alcanzado por el proceso APO01 - Gestionar el marco de Gestión de TI es cero (0).

El funcionamiento del Hospital se realiza a travez de un modelo de Gestion por procesos conforme lo establece el Estatuto Orgánico de Gestión Organizacional para Hospitales; Sin embargo, los procesos y autoridades actuales para la gestión de la información y uso TI no se encuentran alineados con los objetivos del Hospital. El Área de Gestión de Tecnologías de la Información y Comunicaciones del Hospital es considerada solo como un departamento de apoyo y no como una parte integral y estratégica para lograr los objetivos de la casa de salud.

Existen políticas y habilitadores documentados provistos por la Dirección Nacional de Tecnología del MSP pero no se encuentran actualizadas; su edición tiene más de (3) tres años y no son parte integral de las operaciones del Hospital. Hay algunos proveedores externos de servicios de TI que no tienen contratos con los requisitos de control estandarizados y definidos como:

acuerdos de servicio, penalidades, multas etc., por lo tanto, no hay un seguimiento adecuado y métricas del servicio.

El bajo número de políticas, buenas prácticas y estándares que se encuentren ya involucradas en los procesos internos del Hospital, conlleva a que no exista el ambiente propicio para poder implementar y mantener un marco de Gobierno y Gestión de TI permita alcanzar los objetivos estratégicos de la casa de salud a través de TI.

Tabla 33.

Resultados de la evaluación del proceso APO07.

| **Nombre de Proceso : APO07 - Gestionar los Recursos Humanos** | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Niveles de Capacidad:** | Nivel 0 | Nivel 1 | Nivel 2 | | Nivel 3 | | Nivel 4 | | Nivel 5 | |
| | | PA 1.1 | PA 2.1 | PA 2.2 | PA 3.1 | PA 3.2 | PA 4.1 | PA 4.2 | PA 5.1 | PA 5.2 |
| **Puntuación de los criterios:** | | P | N | N | | | | | | |
| **Nivel de capacidad alcanzado:** | 0 | | | | | | | | | |
| **Escala de calificación:** | N: No logrado (0 a 15% ) | | P: Parcialmente logrado (>15% a 50%) | | L: Logrado en gran medida (>50% a 85%) | | F: Logrado Totalmente (>85% a 100%) | | | |

Adaptado de (ISACA, 2013, pág. 16)

El nivel de capacidad alcanzado por el proceso APO07 - Gestionar los Recursos Humanos es cero (0).

Debido a que la estructura organizacional actual del Hospital está definida por el Estatuto Orgánico de Gestión Organizacional por Procesos de los Hospitales del MSP y la no existencia de políticas o buenas prácticas implementadas en los procesos internos del Área de Gestión de Tecnologías de la Información y Comunicaciones, ha conllevado que las relaciones de TI con las demás Áreas no sea flexible y permita dar una respuesta ágil a las incidencias. En ciertas ocasiones los incidentes que no pudieron resolverse dentro de las estructuras de gestión, se escalaron a las estructuras de Gobierno del Hospital.

El porcentaje de rotación de personal en el Hospital es bajo en los procesos de apoyo y de asesoría; sin embargo, respecto al personal médico la rotación de personal es alto ocasionado por una falta de cultura del cliente interno,

programas de inducción, crecimiento profesional, sistema de evaluación de méritos,etc.

Tabla 34.

Resultados de la evaluación del proceso APO09.

| Nombre de Proceso : APO09 - Gestionar los Acuerdos de Servicios | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Niveles de Capacidad:** | Nivel 0 | Nivel 1 | Nivel 2 | | Nivel 3 | | Nivel 4 | | Nivel 5 | |
| | | PA 1.1 | PA 2.1 | PA 2.2 | PA 3.1 | PA 3.2 | PA 4.1 | PA 4.2 | PA 5.1 | PA 5.2 |
| **Puntuación de los criterios:** | | P | N | N | | | | | | |
| **Nivel de capacidad alcanzado:** | 0 | | | | | | | | | |
| **Escala de calificación:** | N : No logrado (0 a 15% ) | | P: Parcialmente logrado (>15% a 50%) | | L: Logrado en gran medida (>50% a 85%) | | F: Logrado Totalmente (>85% a 100%) | | | |

Adaptado de (ISACA, 2013, pág. 16)

El nivel de capacidad alcanzado por el proceso APO09 - Gestionar los acuerdos de servicios es cero (0).

Los servicios de TI que proporciona la Unidad de Gestión de Tecnologías de la Información y Comunicaciones, en su gran mayoría no tienen definidos completamente los Acuerdos de Nivel de Servicio (SLA), ocasionando usuarios de TI insatisfechos porque el servicio no cumple los niveles acordados.

Tabla 35.

Resultados de la evaluación del proceso APO12.

| Nombre de Proceso : APO12 - Gestionar los Riesgos | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Niveles de Capacidad:** | Nivel 0 | Nivel 1 | Nivel 2 | | Nivel 3 | | Nivel 4 | | Nivel 5 | |
| | | PA 1.1 | PA 2.1 | PA 2.2 | PA 3.1 | PA 3.2 | PA 4.1 | PA 4.2 | PA 5.1 | PA 5.2 |
| **Puntuación de los criterios:** | | P | N | N | | | | | | |
| **Nivel de capacidad alcanzado:** | 0 | | | | | | | | | |
| **Escala de calificación:** | N : No logrado (0 a 15% ) | | P: Parcialmente logrado (>15% a 50%) | | L: Logrado en gran medida (>50% a 85%) | | F: Logrado Totalmente (>85% a 100%) | | | |

Adaptado de (ISACA, 2013, pág. 16)

El nivel de capacidad alcanzado por el proceso APO12 - Gestionar los riesgos es cero (0).

La falta de consideración de la Gerencia y el Comite de Gestion del Hospital, respecto al impacto que tienen los riesgos relacionados con TI en las operaciones y entrega de servicios a los usuarios de TI. Ha ocasionado que

existan frecuentes interrupciones en el funcionamiento de los procesos agregadores de valor del Hospital. Para poder mitigar las interrupciones de los servicios de TI se ha considerado el uso métodos de recoleccion, clasificación y análisis de datos relacionados con riesgo de TI.

Tabla 36.

Resultados de la evaluación del proceso APO13.

| Nombre de Proceso : APO13 - Gestionar la Seguridad | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Niveles de Capacidad:** | Nivel 0 | Nivel 1 | Nivel 2 | | Nivel 3 | | Nivel 4 | | Nivel 5 | |
| | | PA 1.1 | PA 2.1 | PA 2.2 | PA 3.1 | PA 3.2 | PA 4.1 | PA 4.2 | PA 5.1 | PA 5.2 |
| **Puntuación de los criterios:** | | P | N | N | | | | | | |
| **Nivel de capacidad alcanzado:** | 0 | | | | | | | | | |
| **Escala de calificación:** | N : No logrado (0 a 15% ) | | P: Parcialmente logrado (>15% a 50%) | | L: Logrado en gran medida (>50% a 85%) | | F: Logrado Totalmente (>85% a 100%) | | | |

Adaptado de (ISACA, 2013, pág. 16)

.

El nivel de capacidad alcanzado por el proceso APO13 - Gestionar la seguridad es cero (0).

El Hospital actualmente no tiene establecido un Sistema de Gestión de Seguridad de la Información (SGSI) que proteja los activos de información de la casa de salud y permita preservar su confidencialidad, integridad y disponibilidad. Dentro de los procesos internos que se realiza en el Hospital los usuarios de TI, no tienen definidos claramente sus tareas y los recursos informáticos a los que tienen acceso, ocasionando incidentes relacionados con la Seguridad de la Información. Las técnicas de Seguridad Informática establecida y usada dentro del Hospital son provistas por la Dirección Nacional de Tecnología del MSP.

Tabla 37.

Resultados de la evaluación del proceso BAI02.

| Nombre de Proceso : BAI02 - Gestionar la Definición de Requisitos | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Niveles de Capacidad:** | Nivel 0 | Nivel 1 | Nivel 2 | | Nivel 3 | | Nivel 4 | | Nivel 5 | |
| | | PA 1.1 | PA 2.1 | PA 2.2 | PA 3.1 | PA 3.2 | PA 4.1 | PA 4.2 | PA 5.1 | PA 5.2 |
| **Puntuación de los criterios:** | | P | N | N | | | | | | |
| **Nivel de capacidad alcanzado:** | 0 | | | | | | | | | |
| **Escala de calificación:** | N : No logrado (0 a 15% ) | | P: Parcialmente logrado (>15% a 50%) | | L: Logrado en gran medida (>50% a 85%) | | F: Logrado Totalmente (>85% a 100%) | | | |

Adaptado de (ISACA, 2013, pág. 16)

El nivel de capacidad alcanzado por el proceso BAI02 - Gestionar la definición de requisitos es cero (0).

Dentro del Hospital existen procesos informales para definir las características, el propósito, la dirección y el tamaño de la solución tecnológica que va a ser desarrollada o adquirida. Además el inadecuado entendimiento de las necesidades de los usuarios de TI ocasiona que la solución propuesta no alcance a cumplir sus objetivos o en la mayoría de casos la solución tecnológica no salga a producción.

Tabla 38.

Resultados de la evaluación del proceso DSS04.

| **Nombre de Proceso : DSS04 - Gestionar la Continuidad** | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Niveles de Capacidad:** | Nivel 0 | Nivel 1 | Nivel 2 | | Nivel 3 | | Nivel 4 | | Nivel 5 | |
| | | PA 1.1 | PA 2.1 | PA 2.2 | PA 3.1 | PA 3.2 | PA 4.1 | PA 4.2 | PA 5.1 | PA 5.2 |
| **Puntuación de los criterios:** | | P | N | N | | | | | | |
| **Nivel de capacidad alcanzado:** | 0 | | | | | | | | | |
| **Escala de calificación:** | N : No logrado (0 a 15% ) | | P: Parcialmente logrado (>15% a 50%) | | L: Logrado en gran medida (>50% a 85%) | | F: Logrado Totalmente (>85% a 100%) | | | |

Adaptado de (ISACA, 2013, pág. 16)

El nivel de capacidad alcanzado por el proceso DSS04 - Gestionar la continuidad es cero (0).

El Hospital no dispone de un Plan de Continuidad (BCP), basado en la estrategia de la continuidad, que asegure su efectividad frente a desastres o incidentes de TI. Actualmente los respaldos y recursos críticos para la restauración y recuperación de los servicios de TI se realizan de manera manual y periódica. Sin embargo, luego de un incidente existen servicios de TI que en ocasiones frecuentes no cumplen con los niveles de servicio mínimos requeridos por el Hospital.

Tabla 39.

Resultados de la evaluación del proceso DSS05.

| Nombre de Proceso : DSS05 - Gestionar los Servicios de Seguridad | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Niveles de Capacidad:** | Nivel 0 | Nivel 1 | Nivel 2 | | Nivel 3 | | Nivel 4 | | Nivel 5 | |
| | | PA 1.1 | PA 2.1 | PA 2.2 | PA 3.1 | PA 3.2 | PA 4.1 | PA 4.2 | PA 5.1 | PA 5.2 |
| **Puntuación de los criterios:** | | P | N | N | | | | | | |
| **Nivel de capacidad alcanzado:** | 0 | | | | | | | | | |
| **Escala de calificación:** | N : No logrado (0 a 15% ) | | P: Parcialmente logrado (>15% a 50%) | | L: Logrado en gran medida (>50% a 85%) | | | F: Logrado Totalmente (>85% a 100%) | | |

Adaptado de (ISACA, 2013, pág. 16)

El nivel de capacidad alcanzado por el proceso TI DSS05 - Gestionar los servicios de seguridad es cero (0).

Para proteger los activos de información del Hospital, en la transmisión de la información crítica, actualmente se aplican técnicas básicas de encriptación, apoyados mediante el software libre. Se han implantado medidas físicas para proteger los activos de información de accesos no autorizados, pero debido a la naturaleza del negocio del Hospital, han existido incidentes relacionados con seguridad física. La mayoría de incidentes que afectan la confidencialidad, integridad y disponibilidad de los activos de información están relacionados con la falta concienciación de los usuarios de TI en aspectos de Seguridad de la Información, dispositivos de usuario final no autorizados detectados en la red o en el entorno y accesos no autorizados a la información.

Las pòliticas y prácticas sobre Seguridad Informática y Seguridad de la Información que maneja actualmente el Hospital son provistas por la Dirección Nacional de Tecnología del MSP.

#### 4.2.2.10 Identificar y definir el plan de acción para el estado deseado

Considerando los resultados de nivel de capacidad obtenidos en el punto anterior se establece el estado deseado para los procesos del Hospital, según lo acordado por la Gerencia y el Equipo del Proyecto en el anexo 7.

Tabla 40.

Identificación del nivel de capacidad alcanzado y deseado.

| Núm. | Código | Nombre del proceso | Nivel de capacidad alcanzado | Nivel de capacidad deseado | Puntuación deseada |
|---|---|---|---|---|---|
| 1 | EDM01 | Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno | 0 | 1 | L |
| 2 | APO01 | Gestionar el Marco de Gestión de TI | 0 | 1 | L |
| 3 | APO07 | Gestionar los Recursos Humanos | 0 | 1 | L |
| 4 | APO09 | Gestionar los Acuerdos de Servicios | 0 | 1 | L |
| 5 | APO12 | Gestionar los Riesgos | 0 | 1 | L |
| 6 | APO13 | Gestionar la Seguridad | 0 | 1 | L |
| 7 | BAI02 | Gestionar la Definición de Requisitos | 0 | 1 | L |
| 8 | DSS04 | Gestionar la Continuidad | 0 | 1 | L |
| 9 | DSS05 | Gestionar los Servicios de Seguridad | 0 | 1 | L |

En la siguiente tabla se presenta el orden de implementación de los procesos de Gobierno y Gestión de acuerdo al nivel de valoración obtenido en la tabla 20 y la importancia otorgada por los miembros del Equipo de Proyecto, conforme lo registra el anexo 7.

Tabla 41.

Orden de implementación de los procesos del Hospital.

| Núm. | Código | Nombre del proceso | Sumatoria | Nivel de Importancia |
|---|---|---|---|---|
| 1 | APO01 | Gestionar el Marco de Gestión de TI | 18 | Muy Importante |
| 2 | APO13 | Gestionar la Seguridad | 17 | Muy Importante |
| 3 | EDM01 | Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno | 14 | Muy Importante |
| 4 | DSS05 | Gestionar los Servicios de Seguridad | 14 | Muy Importante |
| 5 | APO12 | Gestionar los Riesgos | 14 | Importante |
| 6 | APO07 | Gestionar los Recursos Humanos | 13 | Importante |
| 7 | DSS04 | Gestionar la Continuidad | 15 | Poco importante |
| 8 | BAI02 | Gestionar la Definición de Requisitos | 14 | Poco importante |
| 9 | APO09 | Gestionar los Acuerdos de Servicios | 13 | Poco importante |

A continuación se plantea una serie de actividades a realizar en cada proceso con la finalidad de alcanzar el nivel de capacidad deseado.

Tabla 42.

Plan de acción para alcanzar el estado deseado en el proceso APO01.

| APO01 - Gestionar el Marco de Gestión de TI |
| --- |
| Para proveer un enfoque de gestión consistente que permita que los requerimientos de Gobierno del Hospital sean conocidos, posean procesos de gestión, estructuras organizacionales, roles y responsabilidades, actividades seguras y repetibles, habilidades y competencias. Se sugiere:<br>a) **Definir la estructura organizativa:** Revisar y establecer una estructura organizativa en el Hospital, que incorpore dentro de dicha estructura las necesidades del Hospital y las prioridades de TI. Permitiendo que la toma de decisiones se realice de manera eficaz y eficiente, para lo cual se sugiere las siguientes actividades:<br>• Identificar las decisiones y actividades necesarias para alcanzar los objetivos estratégicos del Hospital y las metas de TI, de igual manera para la gestión y ejecución de servicios de TI.<br>• Establecer una matriz de responsabilidades, que muestre el nivel de participación de las partes interesadas críticas del Hospital en la toma de decisiones (quiénes rendirán cuentas, quiénes son responsables, quiénes deben ser consultados y quiénes informados).<br>• Incorporar modelos organizativos corporativos en la organización interna de TI del Hospital.<br>• Definir el enfoque, los roles y las responsabilidades de cada función dentro de la estructura organizativa interna de TI.<br>• Establecer un Comité Estratégico de TI (o equivalente) a nivel del Comité de Gestión o Gerencia Hospitalaria, que permita asegurar que el Gobierno de TI forma parte del Gobierno Corporativo del Hospital y que se encuentra contemplado de manera adecuada para realizar sugerencias sobre la dirección estratégica y las inversiones principales de TI.<br>• Establecer un Comité Directivo de TI (o equivalente) que permita determinar las prioridades de los programas de |

inversión de TI de acuerdo con la estrategia y prioridades del Hospital; realizar un seguimiento del estado de los proyectos de TI y resolver los conflictos de recursos; y supervisar los niveles de servicio y las mejoras en el servicio.

- Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre los procesos agregadores de valor y las funciones de TI dentro del Hospital.
- Establecer un Comité Directivo de Seguridad de la Información dentro de la casa de salud.
- Alinear la estrategia de Seguridad de la Información con los objetivos estratégicos del Hospital.
- Definir la función de la Seguridad de la Información en el Hospital, incluyendo capacidades y roles internos y externos.

b) **Establecer roles y responsabilidades:** Establecer, acordar y comunicar los roles y responsabilidades del personal de TI, así como de las otras Unidades del Hospital con responsabilidades en los procesos de TI. Para lo cual se sugiere las siguientes actividades:

- Establecer, acordar y comunicar los roles y responsabilidades de TI para todo el personal del Hospital alineándose con las necesidades y objetivos estratégicos. Delimitar claramente las responsabilidades y la rendición de cuentas, especialmente para la aprobación y toma de decisiones.
- Contribuir al proceso de continuidad del servicio de TI manteniendo actualizada la información de contacto y las descripciones de roles del personal de TI del Hospital.
- Asegurar que la rendición de cuentas queda definida a través de los roles y responsabilidades.
- Estructurar los roles y las responsabilidades para reducir las posibilidades de que un solo rol de TI pueda comprometer un proceso crítico del Hospital.
- Determinar las obligaciones de Seguridad de la Información, responsabilidades y tareas de los otros roles organizacionales

del Hospital (incluyendo grupos e individuos).

c) **Mantener los elementos catalizadores del sistema de gestión:** Garantizar que los elementos facilitadores del sistema de gestión y del entorno de control de TI, estén integrados y alineados con el Gobierno y Gestión del Hospital. Se debe fomentar la cooperación interdepartamental y el trabajo en equipo promoviendo el cumplimento y la mejora continua. Para lograrlo se sugiere:
   - Reforzar el entorno interno del Hospital, incluyendo la cultura y filosofía de gestión, nivel de tolerancia al riesgo, seguridad, valores éticos, código de conducta y rendición de cuentas e integrar los principios de TI con los principios de la casa de salud.
   - Crear, evaluar un conjunto de políticas de control de TI en temas relevantes, como calidad, seguridad, confidencialidad, controles internos, uso de activos de TI, ética y derechos de propiedad intelectual.
   - Revisar como mínimo una vez al año, las políticas de TI y procedimientos para mantenerlos revisados y actualizados.

d) **Comunicar los objetivos y la dirección de gestión:** Comunicar los objetivos y la dirección de la Gestión de TI a todo el personal del Hospital. Para ello se recomienda:
   - Comunicar continuamente los objetivos y dirección de la Gestión de TI por todos los canales disponibles del Hospital.
   - Garantizar que la información a comunicar engloba una clara visión, objetivo de servicio, seguridad, calidad, código ética, etc. La información debe tener el nivel de detalle para la respectiva audiencia dentro del Hospital.
   - Definir las expectativas y desarrollar un programa de concientización sobre la Seguridad de la Información.

e) **Optimizar la ubicación de la función de TI:** Posicionar la capacidad de TI dentro de la estructura organizativa, de tal manera que se refleje la importancia de TI para el Hospital. La línea de reporte del

responsable de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones debe ser proporcional a la importancia de las TI en el Hospital.

- Identificar, evaluar y priorizar las opciones de ubicación de la organización de TI, dentro de la estructura organizativa del Hospital. Mostrando la capacidad de TI dentro de la casa de salud.
- Entender el contexto de la función de TI en el Hospital, a través de una evaluación de la estrategia institucional, la importancia de TI, la situación y las opciones de provisión. Que permita definir la importancia y función operacional de TI dentro de la estructura organizativa del Hospital

f) **Definir la propiedad de la información (datos) y del sistema:** Definir y mantener las responsabilidades de la propiedad de la información (datos) y los sistemas de información.

- Proveer políticas y directrices para asegurar la integridad y consistencia de la información (datos) del Hospital.
- Definir, mantener y proporcionar herramientas adecuadas, técnicas y directrices para garantizar el control y seguridad de la información del Hospital.
- Registrar todos los activos de información del Hospital y asignar un responsable por cada uno. La implantación de los controles específicos puede ser delegada por el propietario del activo según éste considere, pero la responsabilidad de la protección adecuada de los activos permanece en el propietario.
- Definir e implementar procedimientos para asegurar la integridad y consistencia de toda la información almacenada en formato electrónico, tales como bases de datos, almacenes de datos (Data warehouses) y archivos de datos.
- Identificar y clasificar de manera especial los dispositivos médicos únicos que registran o transmiten información de salud de los pacientes, considerando el nivel de seguridad necesario

debido el entorno en el que operan.

g) **Gestionar la mejora continua de los procesos:** Evaluar, planificar y ejecutar la mejora continua de los procesos y su capacidad para asegurar que son capaces de entregarse conforme a los objetivos del Hospital.
    - Identificar los procesos críticos de negocio del Hospital basándose en el rendimiento, cumplimiento y los riesgos relacionados. Así como también evaluar la capacidad del proceso e identificar objetivos de mejora.
    - Implementar las oportunidades de mejoras de proceso y establecer objetivos y métricas de rendimiento que permitan el seguimiento de las mejoras del proceso.

h) **Mantener el cumplimiento con las políticas y procedimientos:** Implementar procedimientos para mantener el cumplimiento y medición del funcionamiento de las políticas y procedimientos del marco de referencia.
    - Realizar evaluaciones periódicas para determinar el grado de cumplimiento de políticas y procedimientos.
    - Analizar el incumplimientos de las políticas y procedimientos en el Hospital, para adoptar acciones de remediación por no cumplimiento.
    - Programar y realizar evaluaciones periódicas para determinar el cumplimiento de las políticas y procedimientos de Seguridad de la Información.

Tabla 43.

Plan de acción para alcanzar el estado deseado en el proceso APO13.

| APO13 - Gestionar la Seguridad |
| --- |
| Para mantener el impacto y ocurrencia de los incidentes de la Seguridad de la Información dentro de los niveles de aceptables de riesgo del Hospital. Se sugiere:<br>a) **Establecer y mantener un SGSI:** Definir y mantener un Sistema de Gestión de la Seguridad de la Información (SGSI) que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información en el Hospital.<br>• Definir el alcance y los límites del SGSI de acuerdo a las características de la casa de salud, sus políticas, activos y tecnología.<br>• Obtener la autorización y el compromiso de la Gerencia Hospitalaria para implementar y operar o cambiar el SGSI.<br>• Describir el alcance del SGSI a través de una declaración de aplicabilidad.<br>• Definir y comunicar los roles y las responsabilidades de la gestión de la Seguridad de la Información.<br>b) **Definir y gestionar un Plan de Gestión del Riesgo de la seguridad de la información:** Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de Seguridad de la Información con la estrategia y estructura organizativa del Hospital.<br>• Diseñar, mantener y aplicar un Plan de Gestión de Riesgos de Seguridad de la Información alineado con los objetivos estratégicos del Hospital.<br>• Desarrollar propuestas para implementar el plan de Gestión de Riesgos de Seguridad de la Información en el Hospital, sustentados en casos de negocio adecuados que consideren además la financiación, la asignación de roles y responsabilidades.<br>• Definir la forma de medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables.<br>• Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de Seguridad de la Información y otros controles que permitan la prevención y detección temprana de |

eventos de seguridad, así como la respuesta a incidentes de seguridad.

- Las actividades relativas a la Seguridad de la Información deberían ser coordinadas entre los representantes de las diferentes partes del Hospital con sus correspondientes roles y funciones de trabajo.
- determinar y revisar periódicamente la necesidad de establecer acuerdos de confidencialidad o no revelación del Plan de Gestión de Riesgos, que reflejen las necesidades del Hospital para la protección de la información.
- Considerar dentro del Plan de Riesgos del Hospital, el establecer, documentar y revisar una política de control de acceso basada en los requisitos del negocio y de seguridad para el acceso.
- Considerar dentro del Plan de Riesgos del Hospital, implementar una política formal para la protección contra los riesgos de la utilización de ordenadores portátiles y comunicaciones móviles. Así como también para actividades relacionadas con teletrabajo.
- Considerar dentro del Plan de Riesgos y políticas a implementar en el Hospital, que únicamente los usuarios autorizados del sistema de información de salud, tendrán acceso a la información de los pacientes.

c) **Supervisar y revisar el SGSI:** Controlar y revisar el Sistema de Gestión de la Seguridad de la Información.

- Realizar revisiones periódicas del SGSI incluyendo las políticas, objetivos definidos en la etapa de concepción del SGSI.
- Realizar evaluaciones o auditorías al SGSI de forma periódica para determinar su cumplimiento e identificar mejoras en el proceso.
- Registrar acciones y eventos que podrían tener impacto en la efectividad o desempeño del SGSI.
- Las revisiones de la política de Seguridad de la Información del Hospital debe realizarse mínimo una vez al año o después de la ocurrencia de un incidente de seguridad grave.

Tabla 44.

Plan de acción para alcanzar el estado deseado en el proceso EDM01.

| EDM01 - Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno |
| --- |
| Para garantizar que las decisiones relativas a TI, se han adoptado en línea con los objetivos del Hospital, garantizando el cumplimiento de los requerimientos regulatorios y legales, así como también que se han alcanzado los requerimientos de Gobierno de la Gerencia Hospitalaria, se recomienda:<br>a) **Evaluar el Sistema de Gobierno:** Identificar y comprometerse continuamente con las partes interesadas del Hospital, realizar una estimación del actual y futuro diseño del Gobierno de TI de la casa de salud. Para lo cual se sugiere las siguientes actividades:<br>• Analizar e identificar los factores del entorno interno y externo (obligaciones legales, contractuales y regulatorias) y tendencias en el entorno de prestación de servicios de salud pública que pueden influir en el diseño del Gobierno de TI.<br>• Determinar la relevancia de TI y su papel con respecto a prestación de servicio de salud.<br>• Alinear las capacidades de TI con los intereses de la Gerencia y Comité de Gestión, así como también con los objetivos, misión y visión del Hospital.<br>• Articular los principios de un modelo de toma de decisiones, para que las TI sean efectivas y estén alineadas con los objetivos estratégicos, Misión y Visión del Hospital.<br>• Acordar un modelo de delegación, que determine los niveles apropiados para la delegación de autoridad dentro del Hospital, incluyendo reglas de umbrales, para las decisiones de TI.<br>• Identificar en qué medida la Seguridad de la Información cumple con las necesidades del negocio del Hospital.<br>• Establecer principios que guíen el diseño de facilitadores de la Seguridad de la Información y promueven un ambiente positivo |

para la seguridad.

- Determinar con la Gerencia y Comité de Gestión del Hospital un modelo óptimo en la toma de decisiones para la Seguridad de la Información.

b) **Orientar el Sistema de Gobierno:** Comunicar los principios del Gobierno de TI a la Gerencia Hospitalaria y obtener su apoyo, su aceptación y su compromiso. Así mismo se deberá orientar que las estructuras, procesos y prácticas para el Gobierno de TI estén en línea con:

- Comunicar los principios del Gobierno de TI (alineamiento estratégico, entrega de valor, gestión de riesgos, gestión de los recursos y medición del desempeño) y acordar con la Gerencia Hospitalaria la manera de establecer un liderazgo informado y comprometido.
- Establecer las estructuras, procesos y prácticas del Gobierno de TI en el Hospital, procurando que estén en línea con los principios de diseños de Gobierno, los modelos de toma de decisión y de delegación acordados.
- Asignar un responsable con autoridad dentro del Hospital, encargado de que se apliquen los principios de diseños de Gobierno, los modelos de toma de decisión y de delegación acordados.
- Implementar mecanismos de notificación y de comunicación en el Hospital, que proporcionen la información adecuada a las personas que tienen la responsabilidad de la supervisión y toma de decisiones sobre las estructuras, procesos y prácticas del Gobierno de TI.
- Establecer dentro de la casa de salud un sistema de recompensa para promover el cambio cultural deseable en los funcionarios médicos y administrativos del Hospital.
- Establecer un Comité Directivo de Seguridad de la Información dentro de la casa de salud.

- Alinear la estrategia de Seguridad de la Información con los objetivos estratégicos del Hospital.
- Crear planes para fomentar una cultura y un ambiente de Seguridad de la Información positiva en el Hospital.

c) **Supervisar el Sistema de Gobierno:** Supervisar la ejecución y efectividad del Gobierno de TI en el Hospital. Así mismo analizar si el sistema de Gobierno y los mecanismos implementados (incluyendo estructuras, principios y procesos) está operando de forma efectiva y proporcionan una supervisión apropiada de TI. Para lo cual se sugiere las siguientes actividades:

- Evaluar la efectividad y rendimiento de las personas responsables del Gobierno de TI de la casa de salud.
- Evaluar periódicamente si los mecanismos para el Gobierno de TI acordados (estructuras, principios, procesos, etc.) están establecidos y operando efectivamente en el Hospital.
- Mantener la supervisión sobre el punto (estructuras, principios, procesos, etc.) hasta el que TI satisfaga los intereses de la Gerencia Hospitalaria, así como también los objetivos, misión y visión del Hospital.
- Verificar que los sistema de monitoreo de la Seguridad de la Información del Hospital, cumplan con las legislación y reglamentación actual.

Tabla 45.

Plan de acción para alcanzar el estado deseado en el proceso DSS05.

| DSS05 - Gestionar los Servicios de Seguridad |
|---|
| Para minimizar el impacto en el negocio del Hospital, con las vulnerabilidades e incidentes operativos de seguridad en la información. Se sugiere:<br>a) **Proteger contra software malicioso (malware):** Implementar y mantener medidas preventivas, de detección y correctivas a lo largo del Hospital, para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía – |

spyware- y correo basura).

- Difundir políticas de prevención para software malicioso y generar planes de concienciación sobre los efectos del software malicioso en los activos de información del Hospital.
- Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso de información, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi automáticamente).
- Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.
- Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).
- Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).
- Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.
- Mantenerse en continuo contacto con los grupos de interés especial, foros y asociaciones profesionales especializadas en Seguridad de la Información que traten temas sobre software malicioso.
- identificar, documentar e implantar reglas para el uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información del Hospital.
- Cuando se autorice el uso de código descargado por el usuario de TI, la configuración debería garantizar que dicho código autorizado funciona de acuerdo con una política de seguridad claramente definida, y se debería evitar que se ejecute el

código no autorizado.

b) **Gestionar la seguridad de la red y las conexiones:** Utilizar medidas de seguridad y procedimientos de gestión para proteger la información en todos los modos de conexión.

- Establecer y mantener políticas para Seguridad de la Información en los modos de conexión, basándose en el análisis de riesgos y en los requerimientos del negocio del Hospital.
- Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red del Hospital. Configurar estos dispositivos para forzar la solicitud de contraseña.
- Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico de red entrante y saliente.
- Cifrar la información en tránsito de acuerdo con su clasificación.
- Configurar los equipamientos de red de forma segura.
- Establecer mecanismos de seguridad de confianza para dar soporte a la transmisión y recepción segura de información del Hospital.
- Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.
- identificar los riesgos e implantar los controles apropiados para los activos de información del Hospital, que requieran el acceso de terceros.
- proporcionar a los usuarios únicamente el acceso a los servicios para que los que hayan sido específicamente autorizados.
- Utilizar los métodos apropiados de autenticación para controlar el acceso de los usuarios remotos.
- Controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración de los equipos de red del Hospital.

- Los grupos de servicios de información, usuarios y sistemas de información del Hospital deberían estar segregados en redes.
- Implementar controles de encaminamiento (routing) de redes para asegurar que las conexiones de los ordenadores y los flujos de información no violan la política de control de acceso de los sistemas Hospitalarios.
- Los sistemas Hospitalarios sensibles del Hospital deberían tener un entorno dedicado (aislado) de ordenadores.

c) **Gestionar la seguridad de los puestos de usuario final:** Asegurar que los puestos de usuario final (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados acorde a los requerimientos de Seguridad de la Información del Hospital.

- Configurar los sistemas operativos que utiliza el Hospital de forma segura.
- Implementar mecanismos de bloqueo de los dispositivos de usuario final.
- Cifrar la información almacenada de acuerdo a su clasificación.
- Gestionar el acceso y control remoto a los sistemas informáticos del Hospital.
- Gestionar la configuración de la red de forma segura.
- Implementar el filtrado del tráfico de la red en dispositivos de usuario final.
- Proteger la integridad de los sistemas informáticos que posee el Hospital.
- Proveer de protección física a los dispositivos de usuario final.
- Deshacerse de los dispositivos de usuario final, que ya no se utilicen de una forma segura.
- Desarrollar e implementar políticas de seguridad para dispositivos de usuario final y uso de dispositivos móviles.
- Proteger la información que sea objeto de mensajería

electrónica.

- Formular e implementar una política para el uso de los controles criptográficos y gestión de claves para proteger la información del usuario de TI.

d) **Gestionar la identidad del usuario y el acceso lógico:** Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo a las funciones y procesos de negocio que desarrollen en el Hospital.

- Revisar y mantener que todos los usuarios tengan derechos de acceso a la información de acuerdo a las funciones y procesos de negocio que desarrollen en el Hospital. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos.
- Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas, documentadas y autorizadas por los responsables del proceso del Hospital.
- Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.
- identificarse los riesgos e implantar los controles apropiados para los activos de información del Hospital, que requieran el acceso de terceros.
- Definir e Implementar los requisitos de seguridad, antes de otorgar acceso a los usuarios de TI a los activos o a la información del Hospital.
- Revisar los derechos de acceso a la información y a los recursos de tratamiento de la información de todos los funcionarios del Hospital, en el proceso de cese de funciones o cambio de puesto de trabajo.
- Establecer, documentar y revisar una política de control de acceso basada en los requisitos del negocio del Hospital y de

seguridad para el acceso.

- Establecerse un procedimiento formal de registro y de anulación de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información.
- Revisar los derechos de acceso de usuario de TI en intervalos regulares y utilizando un proceso formal.

e) Gestionar el acceso físico a los activos de TI: Definir e implementar procedimientos para conceder, limitar y revocar el acceso físico a los activos de TI del Hospital.

- Gestionar las peticiones y concesiones de acceso físico a los activos de TI del Hospital. Las peticiones formales de acceso deben ser completadas y autorizadas por la Unidad de Gestión de Tecnologías de la Información y Comunicaciones y se debería registrar de petición.
- Asegurar que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.
- Registrar y supervisar todos los accesos a las instalaciones del Hospital donde se encuentren los activos de información, incluyendo a los contratistas y vendedores.
- Implementar técnicas de autenticación de los equipos en las redes, como también puede complementarse con otras técnicas de autenticación de usuario del equipo.
- Controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración de los equipos de red del Hospital.
- Implementar recursos de seguridad para restringir el acceso de usuarios autorizados a los sistemas operativos permitiendo identificar usuarios no autorizados, registrar los intentos exitosos y fallidos de autenticación, restringir el tiempo de conexión, disparar alarmas cuando se infrinjan las políticas de seguridad.

- Considerar el implementar una política formal de control de accesos, para utilización de ordenadores portátiles y comunicaciones móviles. Así como también para actividades relacionadas con teletrabajo.
- Implementar procesos de notificación de puntos débiles de seguridad, de cumplimiento obligatorio por parte de empleados, contratistas, y terceros que sean usuarios de los sistemas y servicios de información del Hospital.
- Realizar actividades de comprobación de cumplimiento técnico a los sistemas de información, verificando que cumplen las normas de aplicación para la implantación y uso para los usuarios de TI.
- Proteger el acceso a las herramientas de auditoría de los sistemas de información, para proteger de un acceso indebido o denegación de servicio.

f) **Gestionar documentos sensibles y dispositivos de salida:** Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para los activos sensibles de TI.

- Realizar y mantener un inventario de los documentos sensibles y dispositivos de salida de la información del Hospital.
- Establecer procedimientos operativos apropiados para proteger los documentos sensibles, los soportes informáticos (por ejemplo: cintas, discos) y dispositivos de salida de información del Hospital.
- Establecer procedimientos para la manipulación y el almacenamiento de la información, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido.

g) **Supervisar la infraestructura para detectar eventos relacionados con la seguridad:** Usar herramientas de detección de intrusiones y supervisar la infraestructura para detectar accesos no autorizados. Las amenazas identificadas deben estar integradas con la supervisión

general de eventos y la Gestión de Incidentes.

- Registrar los incidentes de Seguridad de la Información del Hospital, a través de herramientas de monitorización de seguridad de la infraestructura.
- Definir y comunicar las características de los incidentes relacionados con la Seguridad de la Información, de manera que sean fácilmente reconocibles en futuros incidentes y permita brindar una respuesta adecuada.
- Gestionar que los tiques de incidentes de Seguridad de la Información se creen de manera oportuna, al identificar una amenaza potencial para los activos de información del Hospital.
- Restringir el acceso a la información y a las aplicaciones a los usuarios y al personal de soporte, de acuerdo con la política de control de acceso definida.
- Implementar procesos de notificación de los puntos débiles de seguridad en los sistemas y servicios de información del Hospital.
- Realizar actividades de comprobación del cumplimiento técnico a los sistemas de información e infraestructura, verificando que cumplen las normas de aplicación para la implantación y uso para los usuarios de TI.

Tabla 46.

Plan de acción para alcanzar el estado deseado en el proceso APO12.

| APO12 - Gestionar los Riesgos |
| --- |
| Para integrar la gestión de riesgos relacionados con TI con la gestión de riesgos del hospital y equilibrar los costes y beneficios de gestionar riesgos relacionados con TI. Se sugiere: |
| a) **Recopilar datos:** Identificar y recopilar datos relevantes para agilitar la identificación, análisis y notificación efectiva de riesgos relacionados con TI.<br>• Establecer y mantener un método para la recolección, clasificación y análisis de datos relacionados con riesgo de TI en el Hospital.<br>• Registrar datos relevantes sobre el entorno de operación interno y externo del Hospital que pudieran jugar un papel significativo en la gestión del riesgo de TI.<br>• Registrar datos sobre eventos de riesgo que han causado o puedan causar impactos al beneficio/valor facilitado por TI, a la entrega de programas y proyectos de TI y/o a las operaciones y entrega de servicio de TI al Hospital.<br>• Ejecutar análisis periódicos de eventos y de factores de riesgo relacionado con TI, que permita identificar asuntos nuevos o emergentes relacionados con el riesgo.<br>• Recopilar datos sobre riesgos, ataques, incumplimientos e incidentes relacionados con la Seguridad de la Información; Incluir datos externos y estadísticas, según proceda.<br>b) **Analizar el riesgo:** Elaborar información útil para toma de decisiones relacionadas con los riesgos de TI en el Hospital.<br>• Definir el alcance del análisis de riesgos considerando todos los factores de riesgo y la criticidad en los procesos agregadores de valor del Hospital.<br>• Construir y actualizar regularmente escenarios de riesgo de TI, que incluyan escenarios compuestos en cascada y/o tipos de amenaza coincidentes, que permita desarrollar actividades de control específicas, capacidades para detectar y otras medidas de respuesta.<br>• Especificar los requerimientos de alto nivel para los proyectos o programas que se implementarán para mitigar los riesgos de TI.<br>• Validar los resultados de análisis de riesgos antes de usarlos para la |

toma de decisiones, confirmando que los análisis se alinean con requerimientos del Hospital y verificando que las estimaciones fueron apropiadamente calibradas y examinadas ante una posible parcialidad.

- Realizar un análisis de riesgo de la Seguridad de la Información en el Hospital y validar los resultados.

c) **Mantener un perfil de riesgo:** Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.

- Inventariar los procesos de negocio del Hospital, incluyendo el personal de soporte, aplicaciones, infraestructura, instalaciones, vendedores, proveedores y documentar la dependencia de los procesos de gestión de servicio TI y de los recursos de infraestructuras de TI.
- Determinar y acordar qué servicios TI y recursos de infraestructuras de TI son esenciales para sostener la operación de procesos de negocio del Hospital.
- Documentar los escenarios de riesgo actuales, por categoría, línea de negocio y área funcional.
- Capturar toda la información sobre el perfil de riesgo y definir un conjunto de indicadores de riesgo que permitan la identificación rápida del perfil de riesgo.
- Documentar los escenarios de riesgo que tengan relación con la Seguridad de la Información, por categoría, línea de negocio y área funcional.

d) **Expresar el riesgo:** Proporcionar información sobre el análisis de riesgos a la Gerencia y Comité de Gestión del Hospital para una respuesta apropiada.

- Informar de los resultados del análisis de riesgos a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones del Hospital.
- Informar el perfil de riesgo actual a todas las partes involucradas del Hospital, incluyendo la efectividad del proceso de gestión de riesgos, la efectividad de los controles, estado de la remediación y sus impactos en el perfil de riesgo.

- Desarrollar y comunicar estrategias de respuesta para ataques, incumplimientos e incidentes que tengan relación con la Seguridad de la Información.

e) **Definir un portafolio de acciones para la gestión de riesgos:** Definir un portafolio de acciones que permita reducir el riesgo relacionado a TI a un nivel aceptable.
   - Mantener un inventario de las actividades de control que estén en marcha para gestionar el riesgo relativo a TI y que permitan que el riesgo que se tome esté dentro de un nivel de tolerancia.
   - Definir un conjunto de propuestas de proyecto equilibradas diseñadas para reducir el riesgo.
   - Definir propuestas de proyectos que permitan reducir el riesgo relacionado con la Seguridad de la Información.

f) **Responder al riesgo:** Responder de una forma oportuna al riesgo, con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.
   - Preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente de impacto grave a los procesos del Hospital.
   - Examinar los eventos adversos y determinar sus causas raíz relacionada con el riesgo de TI. Comunicar la causa raíz para que se incluyan en los procesos de Gobierno del riesgo.
   - Definir prácticas de mitigación y respuesta al riesgo relacionado con Seguridad de la Información.

Tabla 47.

Plan de acción para alcanzar el estado deseado en el proceso APO07.

| APO07 - Gestionar los Recursos Humanos |
|---|
| Para optimizar las capacidades de los recursos humanos y cumplir con los objetivos estratégicos del Hospital. Se sugiere:<br>a) **Mantener la dotación de personal suficiente y adecuado:** Evaluar las necesidades de personal en forma regular o en cambios importantes del Hospital, para asegurar que la empresa tiene los suficientes recursos humanos para apoyar las metas y objetivos del Hospital. El personal incluye |

solo a recursos internos.

- Evaluar las necesidades de personal de forma regular o ante cambios importantes para asegurar, que la función de TI cuenta con recursos suficientes para apoyar de manera adecuada y apropiada las metas y objetivos del Hospital.
- Implementar planes de desarrollo de carrera y de competencias, así como también asegurar que exista respaldo para el personal clave de TI que permita reducir la dependencia de una sola persona en procesos críticos.
- Definir los requisitos para la dotación del personal de Seguridad de la Información del Hospital.

b) **Identificar personal clave de TI**: Identificar el personal clave de TI y reducir al mínimo la dependencia de una sola persona en la realización de una función crítica de trabajo o proceso de TI.

- Minimizar la dependencia en una sola persona en la realización de una función crítica de trabajo mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión, el respaldo (backup) del personal, el entrenamiento cruzado e iniciativas de rotación de puestos.

c) **Mantener las habilidades y competencias del personal:** Verificar regularmente que el personal tenga las competencias necesarias para cumplir con sus funciones sobre la base de su educación, formación y/o experiencia y verificar que estas competencias se mantienen, con programas de capacitación y certificación en su caso.

- Elaborar una matriz de habilidades y competencias necesarias y disponibles actualmente del personal de TI del Hospital para lograr los objetivos del Hospital, de TI y de procesos.
- Fomentar el desarrollo de competencias, oportunidades de progreso personal y una menor dependencia de personas clave a través de planes de desarrollo de carrera y profesional.
- Definir un plan de formación o entrenamiento sobre Seguridad de la Información en el sector salud.
- Desarrollar un programa de concienciación sobre Seguridad de la Información para el personal del Hospital.

d) **Evaluar el desempeño laboral de los empleados:** Evaluar el rendimiento

del personal de TI, respecto a los objetivos individuales derivados de los objetivos del Hospital, las normas establecidas, las responsabilidades específicas del trabajo y el marco de habilidades y competencias.

- Establecer metas individuales en el personal, considerando los objetivos funcionales del Hospital.
- Implementar un plan de mejora del desempeño basados en los resultados del proceso de evaluación y los requisitos de capacitación y desarrollo de competencias identificados.
- Recibir preparación sobre el desempeño y conducta siempre que sea apropiado.

e) **Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio:** Comprender y realizar un seguimiento de la demanda actual y futura de recursos humanos de TI y de los procesos agregadores de valor del Hospital. Que permita identificar las carencias y recopilar información para el aprovisionamiento oportuno de recurso humano para el Hospital.

- Crear y mantener un inventario de recursos humanos de TI y de los procesos agregadores de valor del Hospital.
- Analizar e identificar las deficiencias en el proceso de obtención de recursos humanos para de TI y los procesos agregadores de valor del Hospital.

f) **Gestionar el personal contratado:** Garantizar que el personal contratado de TI conoce y cumplen las políticas del Hospital así como los requisitos contractuales previamente acordados.

- Implementar políticas y procedimientos de contratación de personal.
- Llevar a cabo revisiones periódicas para asegurarse de que el personal contratado ha firmado y aceptado todos los acuerdos necesarios.

Tabla 48.

Plan de acción para alcanzar el estado deseado en el proceso DSS04.

| DSS04 - Gestionar la Continuidad |
| --- |
| Para continuar con las operaciones críticas del Hospital y mantener la disponibilidad de la información a un nivel aceptable para la casa de salud ante un evento de una interrupción significativa. Se sugiere:<br>a) **Definir la política de continuidad de negocio, objetivos y alcance:** Establecer la política y alcance de la continuidad de las operaciones críticas, que se encuentren alineados con los objetivos estratégicos del Hospital y de las partes interesadas.<br>• Identificar las partes interesadas clave del Hospital, los roles y responsabilidades para definir y acordar la política y objetivos de continuidad y su alcance.<br>• Documentar los escenarios de incidentes que causan una interrupción en las operaciones, servicios de TI del Hospital.<br>b) **Mantener una estrategia de continuidad:** Evaluar las opciones de gestión de la continuidad de negocio del Hospital y escoger una estrategia de continuidad viable y efectiva en coste, que permita asegurar la continuidad y recuperación del Hospital frente a una interrupción significativa.<br>• Realizar un análisis de impacto en el negocio del Hospital, que permita evaluar el impacto en tiempo de una disrupción en funciones críticas de los servicios médicos y el efecto que tendría en ellas.<br>• Analizar los requerimientos de continuidad para identificar las posibles estrategias de negocio del Hospital y opciones técnicas.<br>• Obtener la aprobación de la Gerencia y el Comité de Gestión del Hospital, para las opciones estratégicas de continuidad seleccionadas.<br>c) **Desarrollar e implementar una respuesta a la continuidad del negocio**: Elaborar un Plan de Continuidad de Negocio (BCP), basado en la estrategia de documentar los procedimientos y la información, para facilitar que el Hospital continúe con sus actividades críticas luego de sufrir un incidente mayor o disrupción.<br>• Definir las acciones y comunicaciones de respuesta a incidentes que deben ser realizadas al sufrir un evento de disrupción en el Hospital. Además se debe definir los roles y responsabilidades relacionados, |

incluyendo la responsabilidad para la política y la implementación.

- Desarrollar y mantener planes de continuidad que contengan los procedimientos que deben ser seguidos para permitir continuar operando los procesos críticos de negocio del Hospital.
- Definir y documentar los recursos necesarios para soportar los procedimientos de continuidad y recuperación, considerando personas, instalaciones e infraestructura de TI que posee el Hospital.
- Determinar las habilidades necesarias para los individuos implicados en la ejecución de los planes y procedimientos.

d) **Ejercitar, probar y revisar el BCP:** Probar regularmente los acuerdos de continuidad, que permita ejercitar los planes de recuperación para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará eficientemente.

- Definir los objetivos para ejercitar y probar el Plan de Continuidad de Negocio (BCP) y enfrentarse a los riesgos relacionados con TI y el negocio del Hospital.
- Definir y acordar con la Gerencia y el Comité de Gestión del Hospital los ejercicios, que permitan validar los principios de continuidad, incluyendo roles y responsabilidades. Los ejercicios deben ocasionar una mínima disrupción en los procesos de TI del Hospital.
- Desarrollar recomendaciones para mejorar el Plan de Continuidad de Negocio actual en base a los resultados de la revisión.

e) **Revisar, mantener y mejorar el BCP:** Revisar, mantener y mejorar el Plan de Continuidad de Negocio, para asegurar que el plan de continuidad se mantiene actualizado y refleja continuamente los requerimientos actuales del Hospital.

- Revisar el plan y la capacidad de continuidad de forma regular frente a las asunciones hechas y los objetivos de negocio actuales del Hospital, tanto estratégica como operativa.
- Recomendar y comunicar los cambios en la política, planes, procedimientos, infraestructura, roles y responsabilidades para la aprobación de la Gerencia del Hospital y su realización mediante el proceso de gestión de cambios.

f) **Proporcionar formación en el BCP:** Proporcionar a todas las partes implicadas, internas y externas del Hospital, de sesiones formativas

regulares que contemplen los procedimientos y sus roles y responsabilidades en caso de disrupción.

- Definir y mantener planes de formación para quienes realicen de manera frecuente planificación de la continuidad, análisis de impacto, evaluaciones de riesgos y respuesta a incidentes.
- Supervisar las habilidades y competencias basándose en los resultados de los ejercicios y las pruebas de las personas involucradas en el proceso de gestión de continuidad.

g) **Gestionar acuerdos de respaldo:** Mantener la disponibilidad de la información crítica del negocio del Hospital.

- Realizar copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo a una planificación definida internamente.
- Extender la concienciación y la formación en Planes de Continuidad de Negocio (BCP) en el Hospital.
- Probar y mantener legibles las copias de seguridad y las archivadas periódicamente.

h) **Efectuar revisiones post-reanudación:** Evaluar el Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio del Hospital y servicios de TI después de una disrupción.

- Documentar la evaluación del Plan de Continuidad de Negocio.
- Identificar debilidades u omisiones en el plan y las capacidades y hacer recomendaciones para la mejora.
- Obtener la aprobación de la Gerencia y el Comité de Gestión del Hospital para realizar cambios en el plan y aplicarlos mediante el proceso de control de cambios del Hospital.

Tabla 49.

Plan de acción para alcanzar el estado deseado en el proceso BAI02.

| BAI02 - Gestionar la Definición de Requisitos |
|---|
| Para crear soluciones viables y óptimas que cumplan con las necesidades de la organización mientras minimizan el riesgo. Se sugiere:<br>a) **Definir y mantener los requerimientos técnicos y funcionales de negocio**: Identificar, priorizar, especificar y acordar los requerimientos de información, funcionales, técnicos y de control que cubra el alcance |

de todas las iniciativas y permita alcanzar los resultados esperados de la solución de TI propuesta.

- Definir e implementar la definición de requerimientos y un repositorio de requisitos acorde al tamaño, complejidad, objetivos y riesgos de la iniciativa que el Hospital está considerando emprender.
- Obtener, analizar y confirmar que los requerimientos de todas las partes interesadas son considerados, obtenidos, priorizados y registrados de un modo comprensible durante toda la implementación de la iniciativa
- Confirmar que todos los requerimientos de las partes interesadas incluyendo los criterios de aceptación relevantes, son considerados, obtenidos, priorizados y registrados de un modo comprensible para el personal médico y el personal de la implementación técnica.
- Tomar en consideración los requerimientos relativos a políticas y estándares Hospitalarios, planes de TI estratégicos y tácticos, procesos de TI internos, requerimientos de Seguridad de la Información, requerimientos regulatorios, competencias del personal, estructura organizativa y tecnologías catalizadoras.
- Definir los requisitos relacionados con Seguridad de la Información.

b) **Realizar un estudio de viabilidad de las potenciales soluciones alternativas**: Realizar un estudio de viabilidad de las potenciales soluciones alternativas, evaluando su viabilidad y seleccionando la opción preferida.

- Definir y ejecutar un estudio de viabilidad o solución básica funcional que clara y concisamente describa las soluciones alternativas que cumplan con los requerimientos funcionales y de negocio. Además se debe Incluir una evaluación de su viabilidad técnica y económica.
- Revisar las soluciones alternativas con Gerencia y el Comité de

Gestión del Hospital, para seleccionar la solución más apropiada basada en criterios de viabilidad, incluyendo costes y riesgos.

- Definir y documentar las acciones que permitirán mitigar el riesgo relacionado con Seguridad de la Información.

c) **Gestionar los riesgos de los Requerimientos**: Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de las partes interesadas del Hospital y la solución propuesta.

- Analizar y priorizar los riesgos de los requerimientos conforme probabilidad e impacto. Si aplica, determinar los impactos en coste y tiempo.
- Identificar los métodos de controlar, evitar o mitigar los riesgos de los requerimientos en orden de prioridad.

d) **Obtener la aprobación de los requerimientos y soluciones:** Obtener la aprobación de la Gerencia y el Comité de Gestión del Hospital, en aspectos como los requerimientos técnicos y funcionales, de los estudios de viabilidad, de los análisis de riesgos y de las soluciones recomendadas.

- Asegurar que el patrocinador o propietario del producto toman la decisión final con respecto a la elección de la solución, enfoque de adquisición y diseño de alto nivel acorde al caso de negocio del Hospital.
- Realizar revisiones periódicas de calidad completas y de cada fase clave del proyecto, iteración o versión comparando los resultados obtenidos contra los
- Disponer de la firma de la Gerencia o propietario del producto en cada revisión de calidad.
- Obtener la aprobación para las soluciones y requisitos de Seguridad de la Información.

Tabla 50.

Plan de acción para alcanzar el estado deseado en el proceso APO09.

| APO09 - Gestionar los Acuerdos de Servicios |
| --- |
| Para asegurar que los servicios de TI y los niveles de servicio cubren las necesidades presentes y futuras del Hospital. Se sugiere: |
| a) **Identificar servicios TI:** Determinar los servicios de TI y los niveles de servicio que soportan los procesos de negocio del Hospital.<br>• Valorar los servicios TI y niveles de servicio actuales que permita identificar lagunas entre los servicios existentes y las necesidades reales de los procesos de negocio del Hospital.<br>• Analizar, estudiar y estimar la futura demanda y confirmar la capacidad de los servicios de TI existentes.<br>• Crear servicios de TI estandarizados que relacione la demanda de los procesos de negocio con los paquetes de servicio, para obtener una eficiencia global.<br>b) **Catalogar servicios basados en TI:** Definir y mantener un catálogo de servicios de TI, para la Gerencia y Comité de Gestión del Hospital.<br>• Definir y publicar los servicios TI, paquetes de servicios y opciones de nivel del servicio que se encuentran activos de la cartera de servicios.<br>• Definir un catálogo de servicios relacionados con la Seguridad de la Información.<br>c) **Definir y preparar acuerdos de servicio:** Establecer y preparar los acuerdos de servicio basándose en el catálogo de servicio de TI. Además se debe incluir acuerdos de nivel de operaciones interno.<br>• Esbozar borradores de Acuerdos de Nivel de Servicio (SLA) con los clientes de TI, basados en los servicios, paquetes de servicios y opciones del nivel de servicio del catálogo de servicios<br>• Determinar, acordar y documentar los acuerdos de nivel operativo (OLA) internos para cimentar los acuerdos de servicio con los clientes de TI, siempre que sea aplicable.<br>• Evaluar los Acuerdos de Nivel de Servicios (SLA) y de operación (OLA), de acuerdo con los criterios y requisitos de la Seguridad de la Información.<br>d) **Supervisar e informar de los niveles de servicio:** Supervisar los niveles de servicios y proporcionar la información de gestión apropiada para ayudar |

en la gestión del rendimiento.

- Establecer y mantener medidas para supervisar y recolectar datos del nivel del servicio.
- Evaluar el rendimiento y proporcionar informes regular y formalmente sobre el rendimiento del acuerdo del servicio, incluyendo desviaciones con respecto a los valores acordados.
- Acordar planes de acción y remedio para los incidentes del rendimiento o tendencias negativas del mismo.
- Realizar informes de rendimiento del nivel de servicio de Seguridad de la Información.

e) **Revisar acuerdos de servicio y contratos:** Llevar a cabo revisiones periódicas de los acuerdos de servicio y revisarlos cuando sea necesario.

- Revisar los términos de los acuerdos de servicio regularmente para asegurar que son efectivos y están actualizados.
- Revisar los términos que estén relacionadas con la Seguridad de la Información en los contratos, según corresponda y actualizar los SLA según sea necesario.

Para complementar el Modelo de Gobierno de TI propuesto en el presente trabajo y aportar un valor adicional a la investigación realizada, en el anexo 8 se elabora una de las políticas de Seguridad de la Información para el Hospital General Docente de Calderón como una guía para utilizar la información del anexo 3, que combina los objetivos de control y controles de la norma ISO/IEC 27002:2005 e ISO 27799:2008 con los procesos de COBIT 5. Las políticas de Seguridad de la Información es una herramienta que permitirá resguardar los activos de información, proporcionando además una dirección gerencial y apoyo a la Seguridad de la Información de acuerdo con las necesidades del hospital, las leyes y reglamentos pertinentes a salud.

# 5 Conclusiones y Recomendaciones

## 5.1 Conclusiones

El Ecuador cuenta con un amplio marco legal y normativo relacionado al derecho a la salud, siendo la Constitución de la República del año 2008 uno de los principales instrumentos legales para el nuevo modelo que fortalezca el Sistema Nacional de Salud en el país. De igual forma la Ley Orgánica del Sistema Nacional de Salud (LOSNS) ratifica el derecho a la salud, en concordancia con el objetivo tres del PNBV que indica “Mejorar la calidad de vida de la población”, siendo el PNBV el instrumento formal y legal al cual se sujetarán las políticas, programas y proyectos públicos que permitan la consecución de los objetivos del Buen Vivir y la garantía del derecho a la salud.

La inversión pública en salud por parte del Estado se incrementó de 550 millones de dólares en el año 2008 a 2,500 millones de dólares en el año 2015, reflejando de esta forma el cumplimiento de lo establecido en la Constitución de la República del año 2008 de superar el cuatro por ciento del PIB y de otorgar prioridad al gasto social especialmente el relacionado con el sector salud con inversión en infraestructura, equipamiento tecnológico, recursos humanos y programas de prevención de salud.

El marco referencial COBIT 5 es robusto, flexible e integrador, y permite a las organizaciones alinear sus objetivos estratégicos con TI apoyando el uso adecuado de recursos, disminución de costos y riesgos, con un modelo integral que cubre de extremo a extremo a las organizaciones. Además tiene varios principios, prácticas, herramientas y modelos de análisis que permiten abordar aspectos críticos, por lo que constituyó una base sólida para el diseño del modelo de Gobierno de TI para hospitales públicos, con énfasis en la Seguridad de la Información.

El sector de la salud y por consiguiente, los sistemas de TI de atención médica está sujeto a una gran cantidad de normas y regulaciones que se refieren a la Seguridad de la Información. Sin embargo, debido a factores como la escasa coordinación y normalización internacional la mayoría de dichas normas y regulaciones son específicos para cada país o región.

El uso de las Tecnologías de la Información dentro de las organizaciones del sector sanitario ha proporcionado grandes beneficios para el sector; sin embargo, esto también ha generado nuevos desafíos. Uno de estos desafíos, está relacionado con proteger la seguridad y privacidad de la información personal sobre la salud. Es por esto que para reducir las amenazas hasta un nivel de riesgo asumible por la organización, se implementan programas integrales de Seguridad de la Información basados en estándares y buenas prácticas como las normas ISO/IEC 27000 para la Gestión de Seguridad de la Información (SGI).

Por su naturaleza, las organizaciones de salud operan en un entorno donde los trabajadores, pacientes, visitantes y público en general transitan a través de los activos de información y áreas operativas. Por lo cual la utilización de la norma ISO 27799:2008 que contiene un conjunto de controles específicos para la gestión de la Seguridad de la Información sanitaria, garantiza un nivel mínimo de seguridad acorde a las circunstancias de la organización de salud y manteniendo la confidencialidad, integridad y disponibilidad de la información de salud.

La herramienta generada a través del mapeo entre el marco de referencia COBIT 5 y las normas ISO/IEC 27002:2005 e ISO 27799:2008, puede concluirse que su uso supone una mejora en los procesos de Gobierno y Gestión de TI que tienen relación con la Seguridad de la Información para las organizaciones del sector salud. Debido que los controles de las normas ISO/IEC 27002:2005 e ISO 27799:2008 tiene un alcance mayor que las actividades definidas por COBIT 5 en las practicas del proceso.

El uso de estándares, modelos y buenas prácticas enfocados al Gobierno de TI y seguridad de la información, permitió diseñar un modelo de Gobierno de TI para hospitales públicos con énfasis en la Seguridad de la Información, que alinea los objetivos de TI con los objetivos estratégicos de la casa de salud.

El uso de las buenas prácticas en Gestión de Proyectos como el PMBOK, aumenta las posibilidades de conseguir los objetivos del modelo Gobierno de TI con énfasis en la Seguridad de la Información, debido que contiene la información necesaria para iniciar, planificar, ejecutar, supervisar, controlar y cerrar un proyecto. Es así que modelo de Gobierno de TI propuesto puede ser repetible y acoplarse a diferentes hospitales públicos.

La priorización de procesos a través del mecanismo de la cascada de metas de COBIT 5, identifica los procesos críticos de Gobierno y Gestión de TI que se necesitan para asegurar resultados exitosos en la implementación del modelo de Gobierno de TI con énfasis en la Seguridad de la Información para hospitales públicos del Ecuador.

La implementación del modelo de Gobierno de TI con énfasis en la Seguridad de la Información en el Hospital General Docente de Calderón, proporciona una visión clara del nivel de capacidad en que se encuentra cada proceso del Hospital, permitiendo definir los planes de acción para cerrar las brechas y alcanzar el estado deseado. Para asegurar el logro de los objetivos estratégicos del Hospital y crear valor (realización de beneficios, optimización de riesgos y recursos) para los interesados de la casa de salud.

## 5.2 Recomendaciones

Se recomienda que el equipo designado responsable de la implantación del modelo posea un amplio conocimiento en el marco de referencia COBIT 5 y las normas ISO/IEC 27002:2005 e ISO 27799:2008, así como en el modelo de evaluación PAM; o en su defecto realizar un proceso de capacitación continua

al personal del Hospital para facilitar el entendimiento y la familiarización del marco de referencia y normas utilizadas.

Debido al enfoque de Seguridad de la Información que tiene el modelo propuesto, se sugiere que en la fase de implementación se considere la incorporación de un Comité Directivo de Seguridad de la Información responsable de desarrollar y proponer para aprobación de la Gerencia, las políticas e iniciativas que permitan incrementar los niveles de seguridad de información en el Hospital.

Se recomienda el desarrollo completo de las políticas de Seguridad de la Información, utilizando la herramienta generada a través del mapeo entre el marco de referencia COBIT 5 y las normas ISO/IEC 27002:2005 e ISO 27799:2008. Las políticas de Seguridad de la Información es un elemento imprescindible para gestionar la Seguridad de la Información en el Hospital.

# REFERENCIAS

ANDES, A. (2012). *Obras en el sector social de Ecuador no se detendrán en 2016 reitera Presidente Correa*. Recuperado el 01 de octubre de 2016 de http://www.andes.info.ec/es/noticias/obras-sector-social-ecuador-no-detendran-2016-reitera-presidente-correa.html

Areitio, J. (2008). *Seguridad de la información. Redes, Informática y Sistemas de Información.* Madrid:Paraninfo.

Baquero, Guerra, & Mieles. (2014). Presupuesto del Estado y reformas al mercado de valores. *Revista Carta Económica.11(1)*,1-2. Recuperado el 04 de octubre de 2016 de http://www.cordes.org/images/publicaciones/2014/CE_Noviembre_2014.pdf.

Beaver, K., & Herold, R. (2004). *The Practical Guide to HIPAA Privacy and Security compliance* (1st ed.). Florida: Auerbach-publications.

Bell , G., & Ebert , M. (2015). Health care and cyber security. *Revista KPMG, 1(1)*, 2-3. Recuperado el 02 de octubre de 2016 de https://www.kpmg.com/LU/en/IssuesAndInsights/Articlespublications/Documents/cyber-health-care-survey-kpmg-2015.pdf

Congreso Nacional. (2004). *Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP).* Registro Oficial Suplemento 337 de 18 de mayo de 2004. Quito. Recuperado el 10 de octubre de 2016 de http://www.seguridad.gob.ec/wpcontent/uploads/downloads/2015/04/ley_organica_de_transparencia_y_acceso_a_la_informacion_publica.pdf

*Constitución de la República del Ecuador.* (2008). Registro Oficial 449 de 20 de octubre de 2008. Reformas en Registro Oficial Suplemento de 13 de julio de 2011. Recuperado el 05 de octubre de 2016 de http://www.pucesi.edu.ec/web/wp-content/uploads/2016/04/Constituci%C3%B3n-de-la-Rep%C3%BAblica-2008.pdf

Coronel, K. (2015). *Gobierno de la Tecnologia de la Informacion* [diapositivas de PowerPoint]. Quito, Ecuador. Recuperado el 08 de octubre de 2016

de http://www2.udla.edu.ec/maestrias/mod/resource/view.php?id=28187.

Doughty, K., & Grieco, F. (2005). *IT Governance: Pass or Fail?, Information Systems Audit and Control Association.* ISACA. Recuperado el 20 de octubre de 2016, de http://www.isaca.org/Journal/archives/2005/Volume2/Documents/jopdf052-IT-Gov-Pass-or-Fail.pdf

Flores Ma. & Castillo A. (2012). Una mirada desde la sociedad civil a la Gobernanza del Sistema Nacional de Salud. *Revista Esfera Publica. 4(1)*, 6-7. Recuperado el 16 de noviembre de 2016, de http://www.grupofaro.org/content/una-mirada-desde-la-sociedad-civil-la-gobernanza-del-sistema-nacional-de-salud.

Freedman, L. (2009). The Health Information Technology for Economic and Clinical Health Act (HITECH Act): implications for the adoption of health information technology, HIPAA, and privacy and security issues. *Revista Nixon Peabody. 1*(1), 1-3. Recuperado el 29 de enero de 2017 de https://www.nixonpeabody.com/-/media/Files/Alerts/Health_Law_Alert_ 02_23_2009.ashx

Hospital General Docente de Calderón. (2017). *Organigrama del Hospital General Docente de Calderón*. Recuperado el 29 de noviembre de 2017 de http://www.hgdc.gob.ec/index.php/hospital/organigrama

Hospital General Docente de Calderón. (2015). *Misión y Visión del Hospital General Docente de Calderón.* Recuperado el 29 de noviembre de 2016 de http://www.hgdc.gob.ec/index.php/hospital/mision-y-vision

Instituto Nacional de Estadística y Censos. (2008). *Anuario de recursos y actividades de salud. En Instituto Nacional de Estadisticas y Censos*. (1ª ed.). Ecuador. Recuperado el 29 de noviembre de 2016 de http://www.ecuadorencifras.gob.ec//documentos/web-inec/Estadisticas_Sociales/Recursos_Actividades_de_Salud/Publicaciones/Anuario_Rec_Act_Salud_2008.zip

ISACA. (2012). *COBIT 5: For Information Security.* (1.ª ed.). [versión electrónica] Recuperado el 02 de octubre de 2016 de http://www.isaca.org/cobit/pages/info-sec.aspx

ISACA. (2012). *COBIT 5: Implementacion.* (1.ª ed.). [versión electrónica] Recuperado el 02 de octubre de 2016 de http://www.isaca.org/cobit/pages/cobit-5-implementation-product-page.aspx

ISACA. (2012). *COBIT 5: Procesos Catalizadores.* (1.ª ed.). [versión electrónica] Recuperado el 02 de octubre de 2016 de http://www.isaca.org/cobit/pages/cobit-5-enabling-processes-product-page.aspx

ISACA. (2012). *COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la empresa*. (1.ª ed.). [versión electrónica] Recuperado el 02 de octubre de 2016 de https://www.isaca.org/cobit/pages/cobit-5-framework-product-page.aspx

ISACA. (2013). *COBIT 5: Guia de autoevaluación.* (1.ª ed.). [versión electrónica] Recuperado el 02 de octubre de 2016 de http://www.isaca.org/cobit/pages/self-assessment-guide.aspx

ISO. (2008). *ISO 27799: Health informatics - Information security management in health using ISO/IEC 27002.* (1.ª ed.). [versión electrónica] Recuperado el 03 de octubre de 2016 de https://www.iso.org/standards-catalogue/browse-by-ics.html

ISO/IEC. (2005). *ISO/IEC 27001: Information Technology - Security Techniques - Information Security Management Systems – Requirements.* (1.ª ed.). [versión electrónica] Recuperado el 03 de octubre de 2016 de https://www.iso.org/standards-catalogue/browse-by-ics.html

ISO/IEC. (2005). *ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management.* (1.ª ed.). [versión electrónica] Recuperado el 03 de octubre de 2016 de https://www.iso.org/standards-catalogue/browse-by-ics.html

IT Governance Institute. (2003). *Board Briefing on IT Governance*. (2.ª ed.). [versión electrónica] Recuperado el 05 de octubre de 2016 de

https://www.isaca.org/restricted/Documents/26904_Board_Briefing_final.pdf

IT Governance Institute. (2008). *Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit*. (1.ª ed.). [versión electrónica] Recuperado el 05 de octubre de 2016 de http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_Eng_1108.pdf

Legislatura Bi-Cameral Japonesa. (2005). *Act on the Protection of Personal Information.* Japon. Recuperado el 10 de octubre de 2016 de http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf

Luftman, J. (1996). *Managing in the Information Age: Practical Application of the Strategic.* (2.ª ed.). [versión electrónica] Recuperado el 15 de noviembre de 2016 de https://books.google.com.ec/books?id=lAE3uWq6x5kC&pg=PA47&lpg=PA47&dq=Luftman,+J.+(1996).+Managing+in+the+Information+Age&source=bl&ots=oen393DGv6&sig=igE1fc0UhS7SwBgt-90jPUWquFc&hl=es-419&sa=X&ved=0ahUKEwj29LLGoOHTAhXFdSYKHfCNBWYQ6AEISzAG#v=onepage&q=Luftman%2C%20J.%20(1996).%20Managing%20in%20the%20Information%20Age&f=false

Ministerio de Coordinación de Desarrollo Social. (2009). *Agenda de Desarrollo Social 2009–2011.* Quito. Recuperado el 20 de octubre de 2016 de http://www.desarrollosocial.gob.ec/wp-content/uploads/downloads/2012/ 07/2_Agenda_Social_09_11.pdf

Ministerio de Finanzas. (2014). *Informe Ejecución Presupuestaria Ejercicio Fiscal.* Quito. Recuperado el 04 de octubre de 2016 de http://www.finanzas.gob.ec/wp-content/uploads/downloads/2015/04/ Informe-Ejecuci%C3%B3n-Presupuestaria-Ejercicio-Fiscal-2014_2.pdf

Ministerio de Salud Pública. (2006). *Ley de Derechos y Amparo al Paciente. Ecuador.* Registro Oficial 626 de 03 febrero de 1995. Recuperado el 16 de noviembre de 2016 de http://www.salud.gob.ec/wp-

content/uploads/downloads/2014/09/Normativa-Ley-de-Derechos-y-Amparo-del-Paciente.pdf

Ministerio de Salud Pública. (2012). *Estatuto Orgánico de Gestión Organizacional por Procesos de los Hospitales del MSP.* Registro Oficial 339 de 25 septiembre de 2012. Recuperado el 11 de diciembre de 2016 http://instituciones.msp.gob.ec/somossalud/images/guia/documentos/estatuto_de_hosp_acuerdo.pdf

Ministerio de Salud Pública. (2012). *Ley Orgánica del Sistema Nacional de Salud*. Registro Oficial 457 de 30 octubre de 2008. Recuperado el 10 de noviembre de 2016 de http://www.salud.gob.ec/wp-content/uploads/downloads/2014/09/Reglamento-a-la-Ley-Org%C3%A1 nica-de-Salud.pdf

Ministerio de Salud Pública. (2012). *Manual del Modelo de Atención Integral de Salud - MAIS.* Quito. Recuperado el 09 de noviembre de 2016 de http://instituciones.msp.gob.ec/somossalud/images/documentos/guia/Manual_MAIS-MSP12.12.12.pdf

Ministerio de Salud Pública. (2015). *Ficha Informativa de Proyecto 2015.* Quito. Recuperado el 10 de noviembre de 2016 de http://www.hgdc.gob.ec/images/lotaip/2016/julio/anexo%20Literal%20k%20Reporte%20GPR%20Proyecto%20PIFEMEFS.pdf

Ministerio de Salud Pública. (2015). *Reglamento de Información Confidencial en el Sistema Nacional de Salud.* Registro Oficial 427 de 29 de enero de 2015. Recuperado el 10 de noviembre de 2016 de http://instituciones.msp.gob.ec/cz6/images/lotaip/Enero2015/Acuerdo%20Ministerial%205216.pdf

Ministerio de Salud Pública. (2015). *Rendicion de cuentas 2015 - MSP.* Recuperado el 11 de noviembre de 2016 de http://www.salud.gob.ec/wp-content/uploads/2016/03/ppt_rc_29.04.15.pdf

Ministerio de Salud Pública. (2016). *Informe de rendición de cuentas 2015*. Recuperado el 08 de noviembre de 2016 de

http://www.salud.gob.ec/wp-content/uploads/2016/04/estructura_informe_resumen_23.03.2016_vr12.pdf

Ministerio de Salud Pública. (2016). *Planes y programas de la institución en ejecución - MSP.* Recuperado el 10 de noviembre de 2016 de http://instituciones.msp.gob.ec/images/Documentos/Ley_de_Transparencia/2016/Julio/k-Planes-y-programas-en-ejecucion.pdf

Ministerio de Salud Pública. (2016). *Planificación, gestión, coordinación y control de la salud pública*. Recuperado el 12 de octubre de 2016 de http://www.salud.gob.ec/valores-mision-vision/

Ministerio de Salud Pública. (2016). *Presupuesto MSP 2008 - 2014*. Recuperado el 12 de Noviembre de 2016 de http://www.salud.gob.ec/informacion-estadistica-de-produccion-de-salud/

Ministerio de Salud y Atención a Largo Plazo. (2005). *PHIPA: Personal Health Information Protection Act.* Registro 20 de mayo de 2004. Recuperado el 01 de Noviembre de 2016 de https://www.ontario.ca/laws/statute/04p03

Morton, M. (1991). *The Corporation of the 1990s: Information Technology and Organizational Transformation.* Reino Unido:Oxford University Press.

Office for Civil Rights, (OCR). (2003). *Summary of the HIPAA privacy rule.* (1.ª ed.). [versión electrónica] Recuperado el 19 de octubre de http://web.archive.org/web/20041016111930/http://www.hhs.gov/ocr/privacysummary.pdf

Organización Mundial de la Salud,OMS. (2006). *Constitución de la OMS.* Registro Oficial octubre de 2006. Recuperado el 10 de noviembre de 2016 de de http://www.who.int/governance/eb/who_constitution_sp.pdf

Parlamento Europeo y Consejo de la UE. (1995). *Directive 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Registro Oficial 281 de 23 de noviembre de 1995. Recuperado el 10 de noviembre de 2016 de

http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

Parlamento Europeo y Consejo de la UE. (2002). *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).* Registro Oficial 201 de 31 de julio de 2002. Recuperado el 10 de noviembre de 2016 de http://ec.europa.eu/justice/data-protection/law/files/recast_20091219_en.pdf

Parlamento Europeo y Consejo de la UE. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.* Registro Oficial 119 de 4 de mayo de 2016. Recuperado el 10 de noviembre de 2016 de http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/reglamentos/common/pdfs/Reglamento_UE_2016-679_Proteccion_datos_DOUE.pdf

PMI. (2013). *Fundamentos para la Dirección de Proyectos (Guía del PMBOK)*. (5.ª ed.). Pensilvania, Estados Unidos de America: Project Management Institute, Inc.

Secretaría Nacional de la Administración Pública. (2013). *Esquema Gubernamental de Seguridad de la Información.* Registro Oficial Suplemento 88 de 25 de septiembre de 2013. Recuperado el 25 de noviembre de 2016 de http://www.administracionpublica.gob.ec/wp-content/uploads/downloads/2016/02/Esquema-Gubernamental-de-Seguridades-de-la-Informacion.pdf

Secretaría Nacional de la Administración Pública. (En línea). *La Secretaría*. Recuperado el 23 de diciembre de 2016 de http://www.administracionpublica.gob.ec/la-secretaria/

Secretaría Nacional de Planificación y Desarrollo. (2007). *Plan Nacional de Desarrollo 2007-2010.* Recuperado el 17 de octubre de 2016 de http://www.planificacion.gob.ec/wp-

content/uploads/downloads/2013/09/ Plan-Nacional-Desarrollo-2007-2010.pdf

Secretaría Nacional de Planificación y Desarrollo. (2009). *Plan Nacional para el Buen Vivir 2009-2013.* Recuperado el 17 de octubre de 2016, de http://www.planificacion.gob.ec/wp-content/uploads/downloads/2012/07/ Plan_Nacional_para_el_Buen_Vivir.pdf

Secretaría Nacional de Planificación y Desarrollo. (2013). *Plan Nacional para el Buen Vivir 2013-2017.* Recuperado el 20 de octubre de 2016 de http://www.buenvivir.gob.ec/versiones-plan-nacional

SUPERTEL. (En línea). *Proyecto CERT Ecuador/CC*. Recuperado el 23 de diciembre de 2016 de https://sites.google.com/site/certecuadorcc/home

Van Grembergen, J. (2002). Introduction to the Minitrack: IT governance and its. Proceedings of the 35th Hawaii International Conference on System. IEEE. *Revista IEEE Xplore*. 1(1). 1-2 Recuperado el 23 de diciembre de 2016 de http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=994349

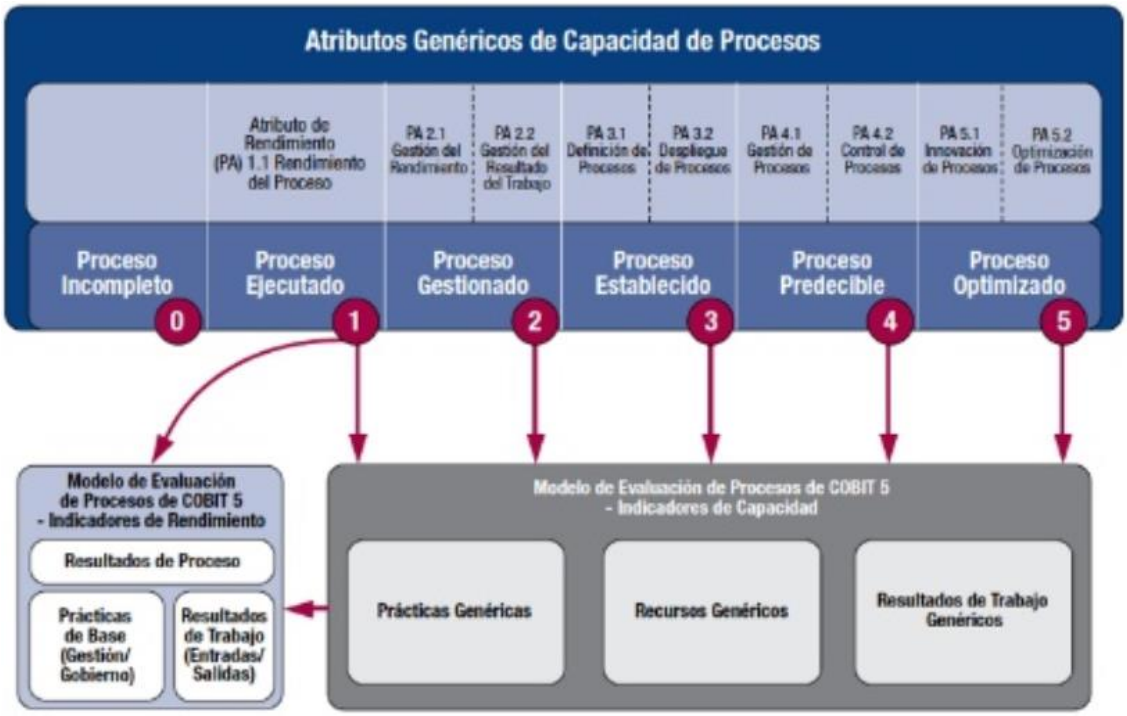
Wallin, E., & Xu, Y. (2008). Managing Information Security in Healthcare: A Case Study in Region Skåne. (Tesis de Maestria). Lund University. Suecia. Recuperado el 10 de diciembre de 2016 de https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=1336692&fileOId=1646720

Webb, P., Pollard, C., & Ridley, G. (2006). *Attempting to Define IT Governance: Wisdom or Folly. Proceedings of the 39th Hawaii.International Conference on System Science.* IEEE Computer Society.

# ANEXOS

## Anexo 1: Modelo de Capacidad de los procesos de COBIT 5

El conjunto de productos de COBIT 5 incluye un modelo de capacidad de procesos que es compatible con la norma ISO/IEC 15504 de Ingeniería de Software-Evaluación de Procesos. Este modelo se utiliza como base para la realización de una evaluación de la capacidad de cada uno de los procesos de Gobierno y Gestión de COBIT 5 y que está basado en la evidencia permitiendo una forma fiable, consistente y repetible de evaluar las capacidades de los procesos de TI.




Modelo de Capacidad de Procesos COBIT 5.

Existen seis niveles de capacidad que se pueden alcanzar por un proceso:

- 0 Proceso incompleto: El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.
- 1 Proceso ejecutado (un atributo): El proceso implementado alcanza su propósito.
- 2 Proceso gestionado (dos atributos): El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.

- 3 Proceso establecido (dos atributos): El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso.
- 4 Proceso predecible (dos atributos): El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.
- 5 Proceso optimizado (dos atributos): El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con las metas empresariales presentes y futuros.

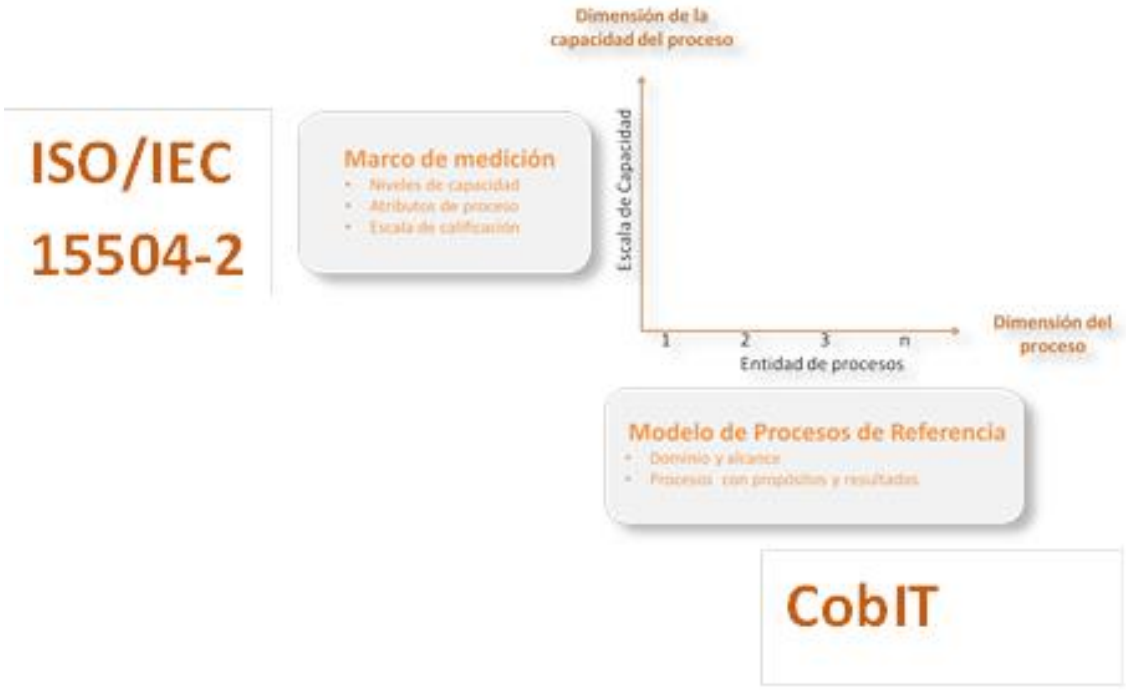
Cada nivel de capacidad puede ser alcanzado sólo cuando el nivel inferior se ha alcanzado por completo. Por ejemplo, un nivel 3 de capacidad de proceso (establecido) requiere que los atributos de definición y despliegue del proceso se hayan alcanzado ampliamente, sobre la consecución completa de los atributos del nivel 2 de capacidad de procesos (proceso gestionado).

Para calificar si se ha llegado a un nivel de capacidad determinado, se utiliza escalas y ratios las cuales son:

- N (No alcanzado): No se muestra una evidencia satisfactoria del atributo (0 al 15%).
- P (Parcialmente alcanzado): Se muestra alguna evidencia de algún logro del atributo. Ciertos factores del logro del atributo pueden ser impredecibles (15 al 50%).
- L (Ampliamente alcanzado): Se muestran evidencias en forma sistémica visualizando un logro significativo del atributo. Pueden encontrarse algunas debilidades (50 al 85%).
- F (Completamente alcanzado): Se evidencia un completo y sistemático enfoque a más de un logro completo del atributo. No existen debilidades significativas (85 al 100%).

1. **Elementos de evaluación de la capacidad de procesos (PAM)**

Para llevar a cabo una evaluación de la capacidad de un proceso de Gobierno o de Gestión de TI, se necesitan varias fuentes de evidencias las cuales se dividen en dos grupos según a la dimensión que pertenecen:




- Dimensión de Proceso (Evidencias de realización del proceso): Utiliza el modelo de referencia de procesos (PRM) de COBIT 5 con las definiciones de procesos en su ciclo de vida y relacionados con los resultados del proceso (Outcomes/Metas del proceso) descritos en cada uno de los procesos COBIT 5.
- Dimensión de Capacidad (Evidencias de la capacidad del proceso): Proporciona una medida de la capacidad del proceso, con el fin de lograr los objetivos estratégicos. El nivel de capacidad del proceso se determina en base a la consecución de los atributos de un proceso específico.

Como ya se comentó anteriormente, el PAM de COBIT 5 se compone de un conjunto de indicadores de desempeño y capacidad del proceso, los cuales se utilizan como base para recopilar pruebas objetivas que permitan asignar calificaciones.

**2. Indicadores de Evaluación**

Los indicadores de evaluación se utilizan para evaluar si los atributos del proceso se han alcanzado. Hay dos tipos de indicadores de evaluación:

- Indicadores de Desempeño (Prácticas de Base y Productos de Trabajo): son específicos para cada proceso y se utilizan para determinar si un

proceso se encuentra en un nivel de capacidad 1. Estos indicadores de desempeño consisten en Prácticas Base (BP's) y Productos de Trabajo (WP's) y son exclusivos para el nivel 1.

- Indicadores de Capacidad: Son genéricos para cada atributo de proceso en los niveles de capacidad del 1 al 5. Los indicadores de capacidad de proceso utilizados en la evaluación de COBIT son: Prácticas Genéricas (GP's) y Productos de Trabajo Genérico (GWP's)
- Los procesos se describen en términos de nombre del proceso, propósito y resultado esperado, basado en COBIT 5. Además, la dimensión de proceso del PAM proporciona información en forma de:
- Prácticas Base (BP's) para los procesos: Proporciona una definición de las actividades necesarias para lograr el propósito del proceso y cumplir con los resultados de cada proceso. Cada BP's esta explícitamente asociado a un resultado esperado.
- Producto de Trabajo (WP's) de Entradas y Salidas: Están asociados a cada proceso y relacionados con uno o más de sus resultados esperados.
- Características asociadas con cada producto de trabajo.

# Anexo 2: Comparación de las cláusulas, categorías de seguridad y controles de las Normas ISO/IEC 27002:2005 e ISO 27799:2008

| ISO/IEC 27002:2005 | ISO 27799:2008 | Situación | Análisis de las guías y controles adicionales proporcionadas por la ISO 27799 |
|---|---|---|---|
| | 7.1 General. | Nuevo Control | Esta cláusula contiene consejos específicos sobre las cláusulas y categorías de seguridad descritas en ISO/IEC 27002. Esencialmente motiva la necesidad de la ISO 27799 e indica explícitamente que la guía dada en la ISO 27799 es adicional y no reemplaza a la ISO/IEC 27002. |
| **5. Política de Seguridad.** | **7.2 Política de Seguridad de la Información.** | | |
| 5.1. Política de seguridad de la información. | | | |
| 5.1.1 Documento de la Política de Seguridad de la Información. | 7.2.1 Documento de la Política de Seguridad de la Información. | > | **Control**<br>Las organizaciones que procesen información de salud, incluyendo información personal de salud, deberán tener una política escrita de seguridad de la información aprobada por la administración, publicada y luego comunicada a todos los empleados y partes externas relevantes.<br>**Guía de implementación**<br>Además de seguir la orientación dada por ISO/IEC 27002 sobre lo que debe contener una política de seguridad de la información, esta política debe contener declaraciones sobre:<br>• 7.2.1 (literales a-e)<br>La justificación, objetivos, cumplimiento regulatorio, notificación incidentes, implementación de políticas guiadas por un análisis de riesgos de la organización. Ejemplo: B) los objetivos de la seguridad de la información en salud.<br>• 7.2.1 (literales f-n)<br>Las políticas de seguridad de la información en las organizaciones de salud tendrán que considerar específicamente los siguientes factores, que son únicos para el sector salud: derechos y responsabilidades éticas del personal, consentimiento informativo de los pacientes, intercambio de información con fines de investigación y ensayos clínicos, derechos de los pacientes sobre confidencialidad, integridad y disponibilidad de su información. |
| 5.1.2 Revisión de la política de seguridad de la información. | 7.2.2 Revisión del documento de política de seguridad de la información. | > | **Control**<br>La política de seguridad de la información de la organización de salud debe estar sujeta a una revisión continua y escalonada de manera que la totalidad de la política se trate al menos anualmente. La política debe ser revisada después de la ocurrencia de un incidente de seguridad grave.<br>**Guía de implementación**<br>• 7.2.2 (Literales a-g)<br>Además de seguir la orientación dada por la ISO/IEC 27002, dicha revisión debería abordar: la naturaleza cambiante de las operaciones en una organización de salud, nueva legislación o requisitos de control, recomendaciones de las asociaciones de profesionales de la salud, casos médicos legales sometidos a prueba en los tribunales, etc. |

| | | | |
|---|---|---|---|
| **6. Aspectos organizativos de la seguridad de la información.** | **7.3 Organización de la seguridad de la información.** | | |
| | 7.3.1 General. | Nuevo Control | Hace referencia sobre la responsabilidad que tiene la organización de salud sobre la seguridad de la información personal de salud y otros datos protegidos relacionados con la salud, haciendo hincapié en la necesidad de una infraestructura de gestión de seguridad de información explícita y robusta. Especialmente para las organizaciones de salud que dependen de servicios proporcionados por terceros. |
| 6.1 Organización interna. | 7.3.2 Organización interna. | | |
| 6.1.1 Compromiso de gerencia con la seguridad de la información. | 7.3.2.1 Compromiso de la administración con la seguridad de la información, la coordinación de seguridad de la información y la asignación de responsabilidades de seguridad de la información. | > | **Control**<br>La aplicación de este control de seguridad es obligatoria en la asistencia sanitaria, debiendo implementar:<br>• 7.3.2.1, Literal a y b)<br>Definir y asignar claramente las responsabilidades de seguridad de la información, como también La necesidad de tener un Foro de Gestión de la Seguridad de la Información (ISMF) en sitio o Como mínimo, una persona responsable de la seguridad de la información de salud.<br>• El ISMF se reunirá mensualmente o casi cada mes.<br>• En cada reunión se producirá una declaración de alcance formal que define los límites de la actividad de cumplimiento en términos de personas, procesos, lugares, plataformas y aplicaciones.<br>**Guía de implementación**<br>Además de la orientación dada por ISO/IEC 27002, es importante señalar la naturaleza de la organización de salud al ser responsables y custodios de la información personal de salud. La rendición de cuentas y la coordinación sólo pueden mantenerse a largo plazo si la organización cuenta con una infraestructura explícita de gestión de la seguridad de la información.<br>El acceso a la información por parte de los pacientes, la presentación de informes dentro de la estructura organizativa y la entrega oportuna de información se establecen como resultados requeridos de la estructura organizativa adoptada (organización de seguridad interna). Se indica que el oficial de seguridad debe ser responsable de recopilar, publicar y comentar los informes recibidos por los miembros del foro. |
| 6.1.2 Coordinación de la seguridad de la información. | | | |
| 6.1.3 Asignación de las responsabilidades de la seguridad de la información. | | | |
| 6.1.4 Proceso de autorización de recursos para el tratamiento de la información. | 7.3.2.2 Proceso de autorización de recursos para el tratamiento de la información. | Igual (=) | |

| | | | |
|---|---|---|---|
| 6.1.5 Acuerdos de confidencialidad. | 7.3.2.3 Acuerdos de confidencialidad. | > | **Control**<br>• La aplicación de este control de seguridad es obligatoria en la asistencia sanitaria.<br>• Se requieren acuerdos de confidencialidad aplicables a todo el personal que acceda a la información de salud y que especifique la naturaleza confidencial de la información.<br>**Guía de implementación**<br>Debe incluirse la referencia a las penas aplicables al personal en caso de incumplimiento. |
| 6.1.6 Contacto con las autoridades.<br>6.1.7 Contacto con grupos de interés especial.<br>6.1.8 Revisión independiente de la seguridad de la información. | 7.3.2.4 Contacto con las autoridades, contacto con grupos de intereses especiales y revisión independiente de la seguridad de la información. | Igual (=) | |
| 6.2 Grupos o personas externas. | 7.3.3 Grupos o personas externas. | | |
| 6.2.1 Identificación de los riesgos derivados del acceso de terceros. | 7.3.3.1 Identificación de los riesgos derivados del acceso de terceros. | > | **Control**<br>La aplicación de este control de seguridad es obligatoria en la asistencia sanitaria.<br>**Guía de implementación**<br>Se hace hincapié en la importancia de proteger los derechos de los pacientes, cuando participan partes externas. Se menciona que la jurisdicción que rige el tema de la atención se aplicará, incluso si la parte externa se rige por una jurisdicción diferente. |
| 6.2.2 Tratamiento de la seguridad en la relación con los clientes. | 7.3.3.2 Tratamiento de la seguridad en la relación con los clientes. | Igual (=) | |
| 6.2.3. Tratamiento de la seguridad en contratos con terceros. | 7.3.3.3 Tratamiento de la seguridad en contratos con terceros. | > | **Control**<br>• La aplicación de este control de seguridad es obligatoria en la asistencia sanitaria.<br>• 7.3.3.3 (Literal a-h)<br>Se especifican los requisitos de seguridad que deben ser cubiertos en un contrato formal entre la organización sanitaria y el tercero.<br>Ejemplo: El acuerdo para la representación del tercero en reuniones y grupos de trabajo de organizaciones sanitarias apropiadas;<br>**Guía de implementación**<br>Cuando el flujo de información de salud personal cruza fronteras jurisdiccionales, la ISO 22857 debe servir como una directiva. |
| **7. Gestión de Activos** | **7.4 Gestión de Activos.** | | |
| 7.1 Responsabilidad sobre los activos. | 7.4.1 Responsabilidad sobre los activos de información de salud. | | |

| | | | |
|---|---|---|---|
| 7.1.1. Inventario de activos.<br><br>7.1.2. Propiedad de los activos.<br><br>7.1.3. Acuerdos sobre el uso aceptable de los activos. | | > | **Control**<br>Además de seguir la orientación dada por ISO / IEC 27002, las organizaciones que procesan información personal de salud deben: designar un custodio de los activos de información de salud, contabilizar los activos de información de salud.<br>**Guía de implementación**<br>• Se requieren reglas para mantener el valor de los activos.<br>Ejemplo: El valor de una base de datos de medicamentos;<br>• Los dispositivos médicos que registran o reportan datos pueden requerir consideraciones de seguridad especiales en relación con el entorno en el que operan y con las emisiones electromagnéticas que ocurren durante su operación. Tales dispositivos deben ser identificados de manera única. |
| 7.2 Clasificación de la información | 7.4.2 Clasificación de información de salud. | | |
| 7.2.1 Directrices de Clasificación. | 7.4.2.1 Directrices de Clasificación. | > | **Control**<br>Toda la información de salud personal debe clasificarse uniformemente como confidencial (Ejemplo: Esta información nunca dejará de ser sensible).<br>**Guía de implementación**<br>• 7.4.2.1 (Literal a-c)<br>• Se explican las características únicas de los activos de información en la asistencia sanitaria. Ejemplo: La confidencialidad de la información personal sobre la salud suele ser en gran parte subjetiva, dependiente del contexto y su confidencialidad puede cambiar durante toda la vida del registro de salud de un individuo (por ejemplo, cambiando las actitudes de la sociedad).<br>• Deben identificarse los registros de sujetos de cuidado que pueden estar en alto riesgo de acceso por parte de aquellos que no tienen necesidad de saber. La criticidad de la información, los procesos, los dispositivos informáticos, el software, las ubicaciones y el personal (en relación con la prestación de asistencia sanitaria en curso) también deben clasificarse mediante una evaluación del riesgo. |
| 7.2.2 Etiquetado y manejo de la información. | 7.4.2.2 Etiquetado y manejo de la información. | > | **Control**<br>Los sistemas de información de salud están obligados a informar a los usuarios de la confidencialidad de la información de salud personal, a la que se puede acceder desde el sistema y la salida impresa debe ser etiquetada como confidencial cuando contenga información de salud personal.<br>**Guía de implementación**<br>Los requerimientos adicionales en la declaración de control se re expresan. |
| **8. Seguridad ligada a los Recursos Humanos** | **7.5. Seguridad ligada a los Recursos Humanos** | | |
| 8.1 Antes del empleo. | 7.5.1 Antes del empleo. | | |

| | | | |
|---|---|---|---|
| 8.1.1. Roles y responsabilidades. | 7.5.1.1 Roles y responsabilidades. | > | **Guía de implementación**<br>Toda participación en el procesamiento de la información personal de salud debe documentarse en las descripciones de los funcionarios pertinentes.<br>Se debe prestar especial atención a las funciones y responsabilidades del personal temporal o de corto plazo, tales como estudiantes, pasantes, etc. |
| 8.1.2. Investigación de antecedentes. | 7.5.1.2 Investigación de antecedentes (Screening). | > | **Control:**<br>Como mínimo, se debe verificar la identidad, dirección actual y empleo previo del personal, contratistas y voluntarios en el momento de las solicitudes de empleo.<br>**Guía de implementación:**<br>Se hace hincapié en la importancia de saber cómo y dónde ponerse en contacto con el personal profesional de la salud.<br>Otras formas de verificación; Ejemplo: por organismos profesionales e instituciones académicas. |
| 8.1.3. Términos y condiciones de la relación laboral. | 7.5.1.3 Términos y condiciones de la relación laboral. | > | **Guía de implementación**<br>Todas las organizaciones que procesan información personal de salud deben incluir en los términos y condiciones de empleo de los empleados que procesan o procesarán información personal de salud una declaración sobre la responsabilidad del empleado por la seguridad de la información.<br>Los términos y condiciones de empleo deben:<br>a) incluir la referencia a las penas que sean posibles cuando se identifique el incumplimiento de la política de seguridad de la información;<br>b) velar por que las condiciones relativas a la confidencialidad de la información personal sobre la salud sobrevivan al término del empleo a perpetuidad. |
| 8.2 Durante el empleo. | 7.5.2 Durante el empleo. | | |
| 8.2.1. Responsabilidades de la Dirección. | 7.5.2.1 Responsabilidades de la Dirección. | > | **Guía de implementación**<br>Se destaca el énfasis especial que se debe poner en las preocupaciones de los pacientes, que no desean que su información personal de salud sea atendida por trabajadores de salud que son vecinos, colegas o parientes. Tales preocupaciones a menudo representan un gran porcentaje de quejas de aquellos con temores sobre la confidencialidad de su información de salud personal. |
| 8.2.2. Conocimiento, educación y capacitación en seguridad de la información. | 7.5.2.2 Conocimiento, educación y capacitación en seguridad de la información. | > | **Control**<br>• La aplicación de este control de seguridad es obligatoria en la asistencia sanitaria.<br>• La educación y capacitación en seguridad de la información debe ser proporcionada en la inducción a todos los empleados y, cuando sea relevante, a contratistas, investigadores, estudiantes y voluntarios que procesan información personal de salud |

| | | | |
|---|---|---|---|
| 8.2.3. Procedimiento disciplinario. | 7.5.2.3 Procedimiento disciplinario. | > | **Guía de implementación**<br>Los procesos disciplinarios de las organizaciones de salud con respecto a los incumplimientos de la seguridad de la información deben seguir los procedimientos que se reflejan en la política y por lo tanto conocidos por el (los) sujeto (s) del proceso disciplinario. Además de cumplir con las leyes aplicables, dichos procesos deben cumplir con los acuerdos alcanzados entre los profesionales de la salud y los organismos profesionales de la salud. |
| 8.3 Finalización del empleo o cambio del puesto de trabajo. | 7.5.3 Finalización del empleo o cambio del puesto de trabajo. | | |
| 8.3.1. Responsabilidad de finalización del empleo o cambio.<br>8.3.2. Devolución de los activos. | 7.5.3.1 Responsabilidades de terminación y devolución de activos. | > | **Guía de implementación**<br>Es importante señalar que en la asistencia sanitaria, muchos tipos de personal, por ejemplo, médicos y enfermeras, comúnmente progresan a través de programas de capacitación y otras "rotaciones" donde sus derechos de acceso pueden cambiar fundamentalmente. Para garantizar la terminación de los derechos anteriores que ya no son necesarios para su función, |
| 8.3.3. Cancelación de los permisos de acceso. | 7.5.3.2 Cancelación de los permisos de acceso. | > | **Control**<br>La aplicación de este control de seguridad es obligatoria en la asistencia sanitaria. La terminación de los privilegios de acceso debe hacerse tan pronto como sea posible (ejemplo: no necesariamente a la terminación de los servicios).<br>**Guía de implementación**<br>• Es importante tener en cuenta los muchos ejemplos de asistencia sanitaria de estudiantes y pasantes que han conservado sus privilegios de acceso después de cesar sus prácticas, etc. Especialmente en hospitales grandes, un gran número de empleados temporales normalmente tendrán acceso a corto plazo a información de salud personal.<br>• La terminación de los derechos de acceso de ese personal debe ser manejada cuidadosamente. Al mismo tiempo, en la asistencia sanitaria, muchas transacciones se llevan a cabo bien después del tiempo de la atención (por ejemplo, la firma de transcripciones médicas).<br>• Las organizaciones de salud deben considerar seriamente la terminación inmediata de los derechos de acceso después de la entrega de un aviso de dimisión, aviso de despido, etc., donde se percibe un mayor riesgo de la continuación de dicho acceso. |
| **9. Seguridad Física y del Entorno.** | **7.6 Seguridad Física y del Entorno.** | | |
| 9.1 Áreas seguras. | 7.6.1 Áreas seguras. | | |

| | | | |
|---|---|---|---|
| 9.1.1. Perímetro de seguridad física. | 7.6.1.1. Perímetro de seguridad física. | > | **Control**<br>Las áreas seguras (designadas por los perímetros de seguridad) deben estar protegidas por controles de entrada apropiados para asegurar que sólo el personal autorizado tenga acceso.<br>**Guía de implementación**<br>• Es importante reconocer que en muchos entornos de salud, la instancia de los perímetros de seguridad es especialmente difícil. Muchas áreas operacionales están permeadas (desinfectado) por temas de cuidado. De hecho, quizá no haya otro sector industrial en el que el público tenga un acceso más amplio a las áreas operativas que a la atención sanitaria. Se debe mantener un entorno seguro que preserve la seguridad física y la seguridad de los pacientes, así como de los datos y sistemas que puedan ser accesibles dentro de ese entorno.<br>• A diferencia de los clientes de otros sectores industriales, los clientes en la asistencia sanitaria a menudo son incapaces de proporcionar físicamente para su propia seguridad personal. Las medidas de seguridad física para la información deben ser coordinadas con medidas físicas de seguridad y seguridad para los sujetos de cuidado. Las organizaciones sanitarias tienen el deber de proteger ambos. |
| 9.1.2. Controles físicos de entrada.<br>9.1.3. Seguridad de oficinas, despachos y recursos.<br>9.1.4. Protección contra amenazas externas y de origen ambiental.<br>9.1.5. Trabajo en áreas seguras. | 7.6.1.2 Controles de entrada física; Asegurar oficinas, habitaciones e instalaciones; Protección contra las amenazas externas y ambientales; Trabajando en áreas seguras. | > | **Guía de implementación**<br>Las organizaciones que procesan información de salud personal deben tomar medidas razonables para asegurar que el público esté tan cerca del equipo de TI (servidores, dispositivos de almacenamiento, terminales y pantallas) como las restricciones físicas y los procesos clínicos que demandan. |
| 9.1.6. Áreas de acceso público, entrega y descarga | 7.6.1.3 Áreas de acceso público, entrega y descarga | > | **Guía de implementación**<br>Las áreas físicas en la asistencia sanitaria donde la información de salud se recopila a través de la entrevista y que contienen sistemas donde los datos se ven en la pantalla deben someterse a escrutinio adicional.<br>Ejemplo: en las salas de emergencia, los compañeros o parientes podrían estar expuestos a cantidades significativas de información sensible verbal y visual sobre otros temas de atención. Para asegurar que se mantenga la privacidad de los sujetos de cuidado, la asistencia sanitaria a menudo requiere que los avisos se coloquen en ascensores, en las puertas detrás de las cuales se puedan realizar entrevistas y en otras áreas. Tales notificaciones sirven como un recordatorio para reducir la discusión de casos de pacientes en áreas públicas. |
| 9.2 Seguridad de los equipos. | 7.6.2 Seguridad de los equipos. | | |

| | | | |
|---|---|---|---|
| 9.2.1. Ubicación y protección del equipo. | 7.6.2.1 Ubicación y protección del equipo. | > | **Guía de implementación**<br>Las organizaciones que procesan información de salud personal deben situar cualquier estación de trabajo que permita el acceso a la información personal de salud de una manera que evite la visualización no deseada o el acceso por parte de los sujetos de atención y el público.<br>Los dispositivos médicos que registran o informan los datos también pueden requerir consideraciones especiales de seguridad en relación con el entorno en el que operan y con las emisiones electromagnéticas que se producen durante su funcionamiento.<br>Las organizaciones de salud, especialmente los hospitales, deben asegurarse de que las directrices de ubicación y protección de equipos informáticos minimizan la exposición a dichas emisiones. |
| 9.2.2. Servicios públicos de soporte.<br>9.2.3. Seguridad del cableado.<br>9.2.4. Mantenimiento de equipos. | 7.6.2.2 Soporte de servicios públicos, seguridad de cableado y mantenimiento de equipos. | > | Guía de implementación<br>Además de seguir la orientación dada por ISO/IEC 27002, las organizaciones de salud deberían considerar seriamente el blindaje de la red y otros cables en áreas con altas emisiones de dispositivos médicos. |
| 9.2.5 Seguridad de equipos fuera de los locales de la Organización. | 7.6.2.3 Seguridad de equipos fuera de los locales de la Organización. | > | **Control**<br>Las organizaciones que procesan información de salud personal deberán asegurar que cualquier uso, fuera de sus instalaciones, de dispositivos médicos que registran o reportan datos ha sido autorizado. Esto debe incluir el equipo usado por los trabajadores remotos, incluso cuando este uso es perpetuo (ejemplo: cuando forma una característica central del rol del empleado, como para el personal de ambulancias, terapeutas, etc.) |
| 9.2.6. Seguridad en la reutilización o eliminación de equipos. | 7.6.2.4 Seguridad en la reutilización o eliminación de equipos. | > | **Control**<br>Las organizaciones que procesan aplicaciones de información de salud deberán sobrescribir de forma segura o destruir todos los medios que contengan software de aplicación de información de salud o información de salud personal cuando ya no se requiera el uso del material. |
| 9.2.7. Retirada de materiales propiedad de la empresa. | 7.6.2.5 Retirada de materiales propiedad de la empresa. | > | Las organizaciones que provean o usan equipo, datos o software para apoyar una aplicación médica que contenga información personal de salud no permitirán que dicho equipo, datos o software sean removidos del sitio o reubicados dentro de él sin la autorización de la organización. |
| **10. Gestión de Comunicaciones y Operaciones.** | **7.7 Gestión de Comunicaciones y Operaciones.** | | |
| 10.1. Procedimientos y responsabilidades de operación. | 7.7.1 Procedimientos y responsabilidades de operación. | | |

| | | | |
|---|---|---|---|
| 10.1.1. Documentación de los procedimientos operativos. | 7.7.1.1 Documentación de los procedimientos operativos. | Igual (=) | |
| 10.1.2. Gestión de cambios. | 7.7.1.2 Gestión de cambios. | > | **Control**<br>La organización que procesa la información de salud personal deberá, mediante un proceso formal y estructurado de control de cambios, controlar los cambios en las instalaciones de procesamiento de información y los sistemas que procesan la información personal de salud, para asegurar el control apropiado de las aplicaciones y sistemas del host y la continuidad del cuidado del paciente.<br>**Guía de implementación**<br>Es importante señalar que los cambios inadecuados, inadecuadamente probados o incorrectos en el procesamiento de la información personal de salud pueden tener consecuencias desastrosas para el cuidado y la seguridad del paciente. El proceso de cambio debe registrar y evaluar explícitamente los riesgos del cambio. |
| 10.1.3. Segregación de tareas. | 7.7.1.3 Segregación de tareas. | > | **Guía de implementación**<br>Las organizaciones que procesan información personal de salud deben, siempre que sea posible, separar los deberes y las áreas de responsabilidad, a fin de reducir las oportunidades de modificación no autorizada o mal uso de la información personal sobre la salud.<br>Las organizaciones que procesan información de salud personal deben asegurarse de que los sistemas de TI empleados, contengan funcionalidades de aplicación que impongan la aprobación de los procesos clínicos por parte de los diferentes médicos encargados de las funciones, cuando sea necesario. |
| 10.1.4. Separación de los recursos de desarrollo, prueba y operación. | 7.7.1.4 Separación de los recursos de desarrollo, prueba y operación. | > | **Control**<br>Las organizaciones que procesan la información de salud personal separarán (física o virtualmente) los entornos de desarrollo y de prueba, de los sistemas de información sanitaria operativos que procesan dicha información. Las reglas para la migración de software desde el desarrollo hasta el estado operacional deben ser definidas y documentadas por la organización que aloja las aplicaciones afectadas. |
| 10.2. Gestión de la provisión de servicios por terceros | 7.7.2 Gestión de la provisión de servicios por terceros. | | |
| 10.2.1. Provisión de servicios. | | > | **Guía de implementación**<br>Con el fin de simplificar la administración de servicios de terceros, se recomienda el uso de un acuerdo formal que especifique el conjunto mínimo de controles a implementar. |
| 10.2.2. Supervisión y revisión de los servicios prestados por terceros. | | | |
| 10.2.3. Gestión del cambio en los servicios prestados por terceros. | | | |

| | | | |
|---|---|---|---|
| 10.3. Planificación y aceptación del sistema. | 7.7.3 Planificación y aceptación del sistema. | | |
| 10.3.1. Gestión de capacidades. | 7.7.3.1 Gestión de capacidades. | Igual (=) | |
| 10.3.2. Aceptación del sistema. | 7.7.3.2 Aceptación del sistema. | > | **Control**<br>Las organizaciones que procesan información de salud personal establecerán los criterios de aceptación de los nuevos sistemas de información, actualizaciones y nuevas versiones planificadas. Deberán realizar pruebas adecuadas del sistema antes de su aceptación.<br>**Guía de implementación**<br>La extensión y el rigor de esas pruebas deben escalarse a un nivel consistente con los riesgos identificados del cambio. Véase también 7.7.1.2. |
| 10.4 Protección contra software malicioso y código móvil. | 7.7.4 Protección contra software malicioso y código móvil. | | |
| 10.4.1. Controles contra software malicioso. | 7.7.4.1 Controles contra software malicioso. | > | **Control**<br>Las organizaciones que procesan información de salud personal deben implementar controles apropiados de prevención, detección y respuesta para protegerse contra software malintencionado y se debe implementar una capacitación apropiada de concientización del usuario (medico y administrativo). |
| 10.4.2. Medidas y controles contra códigos móviles (cliente). | 7.7.4.2 Medidas y controles contra códigos móviles (cliente). | Igual (=) | |
| 10.5. Copias de seguridad. | 7.7.5 Copia de seguridad de la información de salud. | | |
| 10.5.1. Copias de seguridad de la información. | | > | **Control**<br>Las organizaciones que procesan información de salud personal respaldarán toda la información de salud personal y la almacenarán en un ambiente físicamente seguro para asegurar su futura disponibilidad.<br>Para proteger su confidencialidad, la información de salud personal debe ser respaldada en un formato cifrado. |
| 10.6. Gestión de la seguridad de las redes. | 7.7.6 Gestión de la seguridad de las redes. | | |
| 10.6.1. Controles de red. | 7.7.6.1 Controles de red. | Igual (=) | |
| 10.6.2. Seguridad en los servicios de red. | 7.7.6.2 Seguridad en los servicios de red. | > | **Guía de implementación**<br>Además de seguir la orientación dada por ISO/IEC 27002, las organizaciones que procesan información personal de salud deben considerar cuidadosamente qué impacto tendrá la pérdida de disponibilidad de servicio de red en la práctica clínica. Véase también 7.11. |
| 10.7. Manipulación de los soportes. | 7.7.7 Manipulación de los soportes. | | |

| | | | |
|---|---|---|---|
| 10.7.1. Gestión de soportes extraíbles. | 7.7.7.1 Gestión de medios informáticos extraíbles. | > | **Guía de implementación**<br>Además de seguir la guía dada por ISO/IEC 27002, las organizaciones que procesan información personal de salud deben asegurarse de que toda la información personal sobre salud almacenada en medios extraíbles sea:<br>a) cifrado mientras sus medios están en tránsito o<br>b) protegidos del robo mientras sus medios están en tránsito. |
| 10.7.2. Retirada de soportes. | 7.7.7.2 Retirada de soportes. | > | **Control**<br>Además de las indicaciones dadas por ISO/IEC 27002, toda la información personal de salud se sobrescribirá de forma segura o bien los medios de comunicación serán destruidos cuando ya no sean necesarios para su uso.<br>**Guía de implementación**<br>La eliminación inadecuada de los medios sigue siendo una fuente de graves violaciones de la confidencialidad del paciente. Es especialmente importante tener en cuenta que este control debe aplicarse antes de la reparación o eliminación de cualquier equipo asociado. Este requisito también se aplica a los dispositivos médicos que registran o informan los datos. |
| 10.7.3. Procedimientos de manipulación de la información. | 7.7.7.3 Procedimientos de manipulación de la información. | > | **Control**<br>Además de la orientación dada por ISO/IEC 27002, los medios que contienen información personal de salud deben estar físicamente protegidos o bien tienen sus datos cifrados. Se vigilará el estado y la ubicación de los medios que contengan información de salud personal no cifrada. |
| 10.7.4. Seguridad de la documentación del sistema. | 7.7.7.4 Seguridad de la documentación del sistema. | Igual (=) | |
| 10.8. Intercambio de información. | 7.7.8 Intercambio de información. | | |
| 10.8.1. Políticas y procedimientos de intercambio de información. | 7.7.8.1 Políticas y procedimientos de intercambio de información sanitaria y acuerdos de intercambio. | > | **Guía de implementación**<br>Además de la orientación dada por ISO/IEC 27002, se puede encontrar orientación específica sobre las políticas de intercambio de información sanitaria en ISO 22857. Aunque esa Norma Internacional hace referencia explícita al flujo transfronterizo de información personal de salud (donde las fronteras en este contexto representan jurisdicciones sanitarias, No necesariamente fronteras nacionales), gran parte de su asesoramiento se puede adaptar, cuando sea necesario, para tratar el intercambio de datos de una organización a otra.<br>Las organizaciones velarán por que la seguridad de dichos intercambios de información sea objeto de un desarrollo de políticas y de una auditoría del cumplimiento (véase 7.12).<br>La seguridad de los intercambios de información puede ser muy asistida por el uso de acuerdos de intercambio de información que especifiquen el conjunto mínimo de controles a implementar. |
| 10.8.2 Acuerdos de intercambio. | | | |
| 10.8.3 Soportes físicos en tránsito. | 7.7.8.2 Soportes físicos en tránsito. | Igual (=) | |

| | | | |
|---|---|---|---|
| 10.8.4 Mensajería electrónica. | 7.7.8.2 Mensajería electrónica. | > | **Guía de implementación**<br>Las organizaciones que transmiten información personal de salud por medio de mensajes electrónicos deben tomar medidas para garantizar su confidencialidad e integridad. Es importante señalar que la seguridad del correo electrónico y los mensajes instantáneos que contienen información personal sobre la salud pueden incluir procedimientos para el personal de salud que no pueden imponerse a los sujetos de atención y al público.<br>El correo electrónico entre profesionales de la salud que contenga información personal de salud debe ser cifrado en tránsito. Uno de los enfoques es el uso de certificados digitales. Consulte la bibliografía para obtener una lista de normas relacionadas con el uso de certificados digitales en entornos de salud.<br>Véase también 7.12.2.2 para una discusión del consentimiento previo a la comunicación fuera de la organización. |
| 10.8.5. Sistemas de información empresariales. | 7.7.8.4 Sistemas de información sanitaria. | Igual (=) | |
| 10.9. Servicios de comercio electrónico. | 7.7.9 Servicios electrónicos de información sanitaria. | | |
| 10.9.1. Seguridad en comercio electrónico. | 7.7.9.1 Comercio electrónico y transacciones en línea. | > | **Guía de implementación**<br>Además de la orientación dada por ISO/IEC 27002, es importante tener en cuenta el cuidado que se debe tener en determinar si los datos involucrados en el comercio electrónico y las transacciones en línea contienen información personal de salud. Si lo hacen, esta información debe ser adecuadamente protegida. De especial preocupación en el cuidado de la salud son los datos relacionados con la facturación, reclamaciones médicas, líneas de facturación, requisiciones y otros datos de comercio electrónico a partir de los cuales se puede derivar información de salud personal. |
| 10.9.2. Seguridad en transacciones en línea. | | | |
| 10.9.3. Seguridad en información pública disponible. | 7.7.9.2 Información de salud pública disponible. | > | **Control**<br>• Se debe archivar la información de salud pública (distinta de la información de salud personal).<br>• La integridad de la información de salud pública debe ser protegida para evitar modificaciones no autorizadas.<br>• Debe indicarse la fuente (autoría) de la información de salud disponible públicamente y su integridad debe ser protegida. |
| 10.10. Monitorización. | 7.7.10 Monitorización. | | |
| | 7.7.10.1 General. | Nuevo Control | De todos los requisitos de seguridad que protegen la información personal de salud, entre los más importantes son los relacionados con la auditoría y la autenticación. Esto garantiza la responsabilidad de los sujetos de atención que confían su información a los sistemas de registro de salud electrónicos y también proporcionan un fuerte incentivo para que los usuarios de dichos sistemas se ajusten a las políticas sobre el uso aceptable de estos sistemas. Una auditoría y registro eficaces pueden ayudar a descubrir el uso indebido de los sistemas de información de salud o de información personal de salud. Estos procesos también pueden ayudar a las organizaciones y los sujetos de atención a obtener reparación contra los usuarios que abusan de sus privilegios de acceso. |

| | | | |
|---|---|---|---|
| 10.10.1. Registros de auditoría. | 7.7.10.2 Registros de auditoría. | > | **Guía de implementación**<br>Además de seguir la guía dada por ISO/IEC 27002, los sistemas de información de salud que procesan información de salud personal deben crear un registro de auditoría seguro, para cada vez que un usuario acceda, cree, actualice o archiva información de salud personal a través del sistema. El registro de auditoría debe identificar de forma única al usuario, identificar de forma única al paciente, identificar la función realizada por el usuario (creación de registros, acceso, actualización, etc.) y anotar la hora y la fecha en la que el usuario utilizo el sistema.<br>Los sistemas de mensajería utilizados para transmitir mensajes que contienen información de salud personal deben mantener un registro de las transmisiones de mensajes (tal registro debe contener la hora, fecha, origen y destino del mensaje, pero no su contenido).<br>La organización debe evaluar y determinar cuidadosamente el período de retención de estos registros de auditoría, con especial referencia a las normas profesionales, para permitir que se lleven a cabo investigaciones cuando sea necesario y para demostrar la existencia de uso indebido cuando sea necesario. |
| 10.10.2. Supervisión del uso del sistema. | 7.7.10.3 Supervisión del uso del sistema. | > | Guía de implementación<br>Además de seguir la orientación dada por ISO/IEC 27002, el sistema de registro de auditoría del sistema de información de salud debe estar operativo en todo momento, mientras que el sistema de información de salud que se está auditando está disponible para su uso.<br>Los sistemas de información sanitaria que contengan información personal sobre la salud deberían contar con módulos para analizar registros y pistas de auditoría que:<br>a) permita la identificación de todos los usuarios del sistema que hayan accedido o modificado un determinado expediente de la atención médica durante un período de tiempo determinado;<br>b) permita la identificación de todos los pacientes cuyos registros hayan sido accesados o modificados por un usuario del sistema durante un período de tiempo determinado. |
| 10.10.3. Protección de la información de los registros. | 7.7.10.4 Protección de la información de los registros. | > | Control<br>Los registros de auditoría deben ser seguros y protegidos contra manipulaciones. El acceso a las herramientas de auditoría del sistema y las pistas de auditoría se protegerán para evitar el uso indebido o el compromiso.<br>Guía de implementación<br>Además de la orientación dada por la ISO/IEC 27002, es importante señalar que la integridad probatoria de los registros de auditoría puede desempeñar un papel esencial en investigaciones de forenses, investigaciones sobre negligencia médica y otros procedimientos judiciales o cuasi judiciales. |
| 10.10.4. Registros de administración y operación. | 7.7.10.5 Registros de administración y operación. | Igual (=) | |
| 10.10.5. Registro de fallos. | 7.7.10.6 Registro de fallos. | Igual (=) | |

| | | | |
|---|---|---|---|
| 10.10.6. Sincronización de reloj. | 7.7.10.7 Sincronización de reloj. | > | **Control**<br>La aplicación de este control de seguridad es obligatoria en la asistencia sanitaria.<br>Los sistemas de información de salud que apoyan las actividades de cuidado compartido de tiempo crítico DEBERÁ proporcionar sincronización de tiempo para apoyar el rastreo y la reconstitución de las líneas de tiempo de la actividad.<br>**Guía de implementación**<br>Además de la orientación dada por la ISO/IEC 27002, es importante señalar que el momento de los eventos registrados electrónicamente en la información personal de salud y en los registros de auditoría puede desempeñar un papel esencial en procesos tales como investigaciones de forenses, investigaciones sobre negligencia médica, Y otros procedimientos judiciales o cuasi-judiciales donde es esencial determinar con precisión una secuencia clínica de eventos. |
| **11. Control de Accesos.** | **7.8 Control de Accesos.** | | |
| 11.1 Requisitos de negocio para control de acceso. | 7.8.1 Requisitos para el control de acceso en salud. | | |
| | 7.8.1.1 Generalidades. | Nuevo Control | **Control**<br>Las organizaciones que procesen información personal de salud controlarán el acceso a dicha información. En general, los usuarios de los sistemas de información de salud sólo deben tener acceso a la información personal de salud, cuando:<br>a) cuando exista una relación sanitaria entre el usuario y el sujeto de los datos (el sujeto de la atención cuya información personal de salud se accede);<br>b) cuando el usuario esté llevando a cabo una actividad en nombre del interesado;<br>c) cuando se necesiten datos específicos para apoyar esta actividad. |
| 11.1.1 Política de control de acceso. | 7.8.1.2 Política de control de acceso. | > | **Control**<br>Las organizaciones que procesen información de salud personal tendrán una política de control de acceso que rige el acceso a estos datos.<br>La política de la organización en materia de control de acceso, se debe establecerse sobre la base de funciones predefinidas con las autoridades asociadas a dicha función.<br>**Guía de implementación**<br>Además de la orientación dada por la ISO/IEC 27002, es importante señalar que, para que la entrega de atención sanitaria no se demore o no se cumpla, existen requisitos más estrictos de lo habitual para una política y procesos pocos claros (por ejemplo: Reglas de control de acceso "normales" en situaciones de emergencia).<br>Se alienta a las organizaciones de salud a que consideren la implementación de una solución de gestión de acceso y identificación ya estandarizada, que permita ser y una herramienta de apoyo adicional y reducción de los costos de administración.. Además, esto soportará procesos de acceso de seguridad de nivel superior, como el acceso basado en tarjetas inteligentes y la capacidad de "inicio de sesión único". |

| | | | |
|---|---|---|---|
| 11.2 Gestión de acceso de usuario. | 7.8.2 Gestión de acceso de usuario. | | |
| 11.2.1 Registro de usuario. | 7.8.2.1 Registro de usuario. | > | **Control**<br>El acceso a los sistemas de información de salud que procesan información de salud personal estará sujeto a un proceso formal de registro de usuarios. Los procedimientos de registro de usuarios garantizarán que el nivel de autenticación requerido de la identidad de usuario reclamada sea coherente con el nivel de acceso que estará disponible para el usuario.<br>Los detalles del registro del usuario serán revisados periódicamente para asegurar que sean completos, precisos y que todavía se requiera el acceso.<br>**Guía de implementación**<br>Además de la orientación dada por ISO/IEC 27002, es importante entender que la tarea de identificar y registrar usuarios de sistemas de información de salud incluye todo lo siguiente:<br>a) la captura precisa de la identidad de un usuario (por ejemplo, Joan Smith, nacida el 26 de marzo de 1982, actualmente residente en una dirección específica);<br>b) la captura exacta, después de la verificación, de las credenciales profesionales duraderas de un usuario (por ejemplo, la Dra. Joan Smith, cardióloga) y / o cargo (por ejemplo, Susana Jones, Recepcionista Médica);<br>c) la asignación de un identificador de usuario inequívoco. |
| 11.2.2 Gestión de privilegios. | 7.8.2.2 Gestión de privilegios. | > | **Guía de implementación**<br>En la discusión que sigue, se especifican varias estrategias de control de acceso que pueden ayudar significativamente a garantizar la confidencialidad e integridad de la información personal sobre la salud. Estos son:<br>a) el control de acceso basado en roles, que se basa en las credenciales profesionales y los títulos de trabajo de los usuarios establecidos durante el registro para restringir los privilegios de acceso de los usuarios a aquellos requeridos para cumplir una o más funciones bien definidas;<br>b) control de acceso basado en grupos de trabajo, que depende de la asignación de usuarios a grupos de trabajo (tales como equipos clínicos) para determinar a qué registros pueden acceder;<br>c) el control de acceso discrecional, que permite a los usuarios de sistemas de información sanitaria que tienen una relación legítima con un sujeto de la información personal de salud (por ejemplo, un médico de cabecera) dar acceso a otros usuarios que no tienen una relación previamente establecida con ese sujeto (Por ejemplo, un especialista). |
| 11.2.3 Gestión de contraseñas de usuario. | 7.8.2.3 Gestión de contraseñas de usuario. | Igual (=) | |

| | | | |
|---|---|---|---|
| 11.2.4 Revisión de los derechos de acceso de los usuarios. | 7.8.2.4 Revisión de los derechos de acceso de los usuarios. | > | **Guía de implementación**<br>Además de la orientación dada por ISO/IEC 27002, se debe prestar especial atención a los usuarios que razonablemente se espera que proporcionen atención medica de emergencia, ya que pueden necesitar acceso a la información personal de salud en situaciones de emergencia , en donde un sujeto de la atención puede no tener acceso. |
| 11.3. Responsabilidades del usuario. | 7.8.3 Responsabilidades del usuario. | | |
| 11.3.1. Uso de contraseña. | | > | **Guía de implementación**<br>Además de seguir la orientación dada por la ISO/IEC 27002, las organizaciones que procesan la información de salud deben, determinar las responsabilidades de los usuarios, respetar los derechos y las responsabilidades éticas de los profesionales de la salud, según lo acordado en la ley y aceptado por los miembros de los organismos profesionales de salud. |
| 11.3.2. Equipo informático de usuario desatendido. | | | |
| 11.3.3. Política de puesto de trabajo despejado y pantalla limpia. | | | |
| 11.4. Control de acceso a la red. | 7.8.4 Control de acceso a la red y control de acceso al sistema operativo. | | |
| 11.4.1. Política de uso de los servicios de red | | Igual (=) | |
| 11.4.2. Autenticación de usuario para conexiones externas. | | | |
| 11.4.3. Identificación de los equipos en las redes | | | |
| 11.4.4. Protección a puertos de diagnóstico remoto. | | | |
| 11.4.5. Segregación de las redes. | | | |
| 11.4.6. Control de la conexión a la red. | | | |
| 11.4.7. Control de encaminamiento (routing) de red. | | | |
| 11.5. Control de acceso al sistema operativo. | | | |
| 11.5.1. Procedimientos seguros de inicio de sesión. | | | |

| | | | |
|---|---|---|---|
| 11.5.2. Identificación y autenticación de usuario. | | Igual (=) | |
| 11.5.3. Sistema de gestión de contraseñas. | | | |
| 11.5.4. Uso de los servicios del sistema. | | | |
| 11.5.5. Desconexión automática de sesión. | | | |
| 11.5.6. Limitación del tiempo de conexión. | | | |
| 11.6. Control de acceso a las aplicaciones y a la información. | 7.8.5 Control de acceso a las aplicaciones y a la información. | | |
| 11.6.1. Restricción de acceso a la información. | 7.8.5.1 Restricción de acceso a la información. | > | **Control**<br>Los sistemas de información sanitaria que procesen información de salud personal deberán autenticar a los usuarios y deberán hacerlo mediante autenticación que incluya al menos dos factores.<br>**Guía de implementación**<br>Además de la orientación dada por la ISO/IEC 27002, se debe considerar especialmente las medidas técnicas mediante las cuales un paciente es autenticado de manera segura cuando se accede a toda o parte de su propia información (en los sistemas de información de salud que permiten tal acceso). Debe hacerse igualmente hincapié en la facilidad de uso de tales medidas, especialmente para los sujetos con discapacidades de atención, y en las disposiciones para el acceso de los tomadores de decisiones sustitutos. |
| 11.6.2. Aislamiento de sistemas sensibles. | 7.8.5.2 Aislamiento de sistemas sensibles. | Igual (=) | |
| 11.7. Informática móvil y tele trabajo. | 7.8.6 Informática móvil y tele trabajo. | | |
| 11.7.1. Ordenadores portátiles y comunicaciones móviles. | 7.8.6.1. Informática móvil y comunicaciones. | > | **Guía de implementación**<br>Además de seguir la orientación dada por ISO/IEC 27002, las organizaciones que procesan información personal de salud deben:<br>a) evaluar específicamente los riesgos involucrados en la informática móvil de salud;<br>b) preparar una política sobre las precauciones que deben tomarse al utilizar dispositivos informáticos móviles, incluidos los dispositivos inalámbricos;<br>c) exigir a sus usuarios móviles que sigan esta política. |

| | | | |
|---|---|---|---|
| 11.7.2. Tele trabajo. | 7.8.6.2 Tele trabajo. | > | **Guía de implementación**<br>Además de seguir la orientación dada por ISO/IEC 27002, las organizaciones que procesan información personal de salud deben:<br>a) preparar una política sobre las precauciones que deben tomarse en el teletrabajo;<br>b) asegurar que los usuarios de teletrabajo de los sistemas de información sanitaria cumplan con esta política. Algunas jurisdicciones nacionales (por ejemplo, en Alemania) ya han impuesto restricciones al teletrabajo por parte de los profesionales de la salud.<br>c) Se enfatiza la importancia de considerar los aspectos éticos y legales en el diseño y despliegue de sistemas de información sanitaria que se pueden utilizar para el teletrabajo desde la perspectiva de que en el sector de la salud el teletrabajo pueda cruzar fronteras jurisdiccionales. Ejemplo Los médicos ya rutinariamente envían por correo electrónico imágenes médicas, etc. a través de los límites para obtener opiniones de especialistas. |
| **12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.** | **7.9. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.** | | |
| 12.1. Requisitos de seguridad de los sistemas de información. | 7.9.1 Requisitos de seguridad de los sistemas de información. | | |
| 12.1.1. Análisis y especificación de los requisitos de seguridad. | | Igual (=) | |
| 12.2. Tratamiento correcto en las aplicaciones. | 7.9.2 Tratamiento correcto en las aplicaciones. | | |
| | 7.9.2.1 Identificación única de sujetos de atención (pacientes). | Nuevo Control | **Control**<br>Los sistemas de información de salud que procesan información de salud personal deberán:<br>a) asegurar que cada paciente pueda ser identificado de manera única dentro del sistema;<br>b) ser capaz de fusionar registros duplicados o múltiples si se determina que múltiples registros para el mismo sujeto de cuidado, han sido creados sin intención o durante una emergencia médica.<br>**Guía de implementación**<br>La prestación de atención de emergencia y otras situaciones en las que la identificación adecuada de los pacientes no puede haber sido posible inevitablemente crear instancias de múltiples registros para el mismo paciente. Debe existir cierta capacidad dentro de cada sistema de información de salud para combinar múltiples instancias de registros de pacientes en un solo registro. Dicha fusión requiere el mayor cuidado y, por lo tanto, no sólo necesitará personal capacitado en dicha fusión, sino que también puede requerir herramientas técnicas para facilitar la integración de la información de los registros originales en un todo unificado. |

| | | | |
|---|---|---|---|
| 12.2.1. Validación de los datos de entrada. | 7.9.2.2 Validación de los datos de entrada. | Igual (=) | |
| 12.2.2. Control del procesamiento interno. | 7.9.2.3 Control del procesamiento interno. | Igual (=) | |
| 12.2.3. Integridad de mensajes. | 7.9.2.4 Integridad de mensajes. | Igual (=) | |
| 12.2.4. Validación de los datos de salida. | 7.9.2.5 Validación de los datos de salida. | > | **Control**<br>Los sistemas de información de salud que procesan información de salud personal, proporcionarán información de identificación del paciente para ayudar a los profesionales de la salud a confirmar que el registro de salud electrónico recuperado coincide con el tema de la atención bajo tratamiento.<br>**Guía de implementación**<br>Además de la orientación dada por ISO/IEC 27002, algunos factores importantes adicionales deben ser considerados. Antes de depender de la información personal de salud proporcionada por un sistema de información de salud, los profesionales de la salud deben mostrar suficiente información para asegurarse de que el tema de la atención que están tratando coincide con la información recuperada. Emparejar un paciente bajo tratamiento con un registro existente puede ser una tarea no trivial. Algunos sistemas mejoran la seguridad al incluir la identificación fotográfica con cada uno de los registros de la atención. Tales mejoras pueden crear problemas de privacidad, ya que potencialmente permiten la captura implícita de características faciales como la raza que no se incluyen como campos de datos.<br>Se debe ejercer gran cuidado en el diseño de sistemas de información de salud para asegurar que los profesionales de la salud puedan confiar en el sistema para proporcionar la información necesaria para confirmar que cada registro recuperado coincide con el individuo bajo tratamiento. |
| 12.3. Controles criptográficos. | 7.9.3 Controles criptográficos. | | |
| 12.3.1. Política de uso de los controles criptográficos. | 7.9.3.1 Política sobre el uso de los controles criptográficos y la gestión de claves | > | **Guía de implementación**<br>Además de las orientaciones dadas por ISO/IEC 27002, en la ISO 17090-3 se pueden encontrar guías sobre políticas para la emisión y uso de certificados digitales en salud y en la gestión de claves. |
| 12.3.2. Gestión de claves | 7.9.3.2 Gestión de claves | Igual (=) | |
| 12.4. Seguridad de los ficheros del sistema. | 7.9.4 Seguridad de los ficheros del sistema. | | |
| 12.4.1. Control del software en explotación. | 7.9.4.1. Control del software en explotación. | Igual (=) | |

| | | | |
|---|---|---|---|
| 12.4.2. Protección de los datos de prueba del sistema. | 7.9.4.2. Protección de los datos de prueba del sistema. | > | **Guía de implementación**<br>Además de seguir la orientación dada por ISO/IEC 27002, las organizaciones que procesan información personal de salud no deben usar información personal de salud personal como datos de prueba. |
| 12.4.3. Control de acceso al código fuente de los programas. | 7.9.4.3. Control de acceso al código fuente de los programas. | Igual (=) | |
| **12.5. Seguridad en los procesos de desarrollo y soporte.** | **7.9.5 Seguridad en procesos de desarrollo y soporte, y gestión de la vulnerabilidad técnica.** | | |
| 12.5.1. Procedimientos de control de cambios. | | Igual (=) | |
| 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. | | | |
| 12.5.3. Restricciones a los cambios en los paquetes de software. | | | |
| 12.5.4. Fugas de información. | | | |
| 12.5.5. Externalización del desarrollo de software | | | |
| 12.6. Gestión de las vulnerabilidades técnicas. | | | |
| 12.6.1. Control de las vulnerabilidades técnicas. | | | |
| **13. Gestión de Incidentes en la Seguridad de la Información** | **7.10 Gestión de Incidentes en la Seguridad de la Información** | | |
| 13.1 Notificación de eventos y puntos débiles de seguridad de la información. | 7.10.1 Notificación de eventos y puntos débiles de seguridad de la información. | | |

| | | | |
|---|---|---|---|
| 13.1.1. Notificación de los eventos de seguridad de la información.<br><br>13.1.2. Notificación de puntos débiles de seguridad. | | > | **Guía de implementación**<br>Además de seguir las directrices dadas por ISO/IEC 27002, las organizaciones que procesan información de salud personal deben establecer responsabilidades y procedimientos de gestión de incidentes de seguridad con el fin de:<br>a) garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad;<br>b) velar por que exista una vía eficaz de escalamiento de los incidentes de modo que los planes de gestión de la crisis y de continuidad empresarial puedan invocarse en las circunstancias adecuadas y en el momento oportuno;<br>c) recoger y conservar datos relacionados con los incidentes, tales como pistas de auditoría, registros y otras pruebas.<br>Los incidentes de seguridad de la información incluyen la corrupción o divulgación no intencional de información de salud personal o la pérdida de disponibilidad de sistemas de información de salud, donde dicha pérdida afecta negativamente la atención del paciente o contribuye a eventos clínicos adversos. |
| 13.2. Gestión de incidentes y mejoras en la seguridad de la información. | 7.10.2 Gestión de incidentes y mejoras en la seguridad de la información. | | |
| 13.2.1. Identificación de responsabilidades y procedimientos. | 7.10.2.1 Identificación de responsabilidades y procedimientos. | Igual (=) | |
| 13.2.2. Aprendizaje de los incidentes de seguridad de la información. | 7.10.2.2 Aprendizaje de los incidentes de seguridad de la información. | Igual (=) | |
| 13.2.3. Recopilación de evidencias. | 7.10.2.3 Recogida de pruebas. | > | **Guía de implementación**<br>Además de seguir la orientación dada por ISO/IEC 27002, las organizaciones que procesan información personal de salud pueden tener que considerar las implicaciones de la recopilación de evidencia con el propósito de establecer negligencia médica. |
| **14. Gestión de Continuidad del Negocio.** | **7.11 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio.** | | |

| | | | |
|---|---|---|---|
| 14.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio. | | > | **Guía de implementación**<br>Debido a los rigurosos requisitos de disponibilidad en la asistencia sanitaria, se debe realizar una importante inversión en términos de tecnología y de capacitación.<br>La planificación de la continuidad del negocio debe integrarse adecuadamente con los planes de la organización para manejar fallas de energía, implementar el control de infecciones y manejar otras emergencias clínicas.<br>Planificación de la gestión de la continuidad del negocio: debe incluir la planificación de la gestión de la crisis sanitaria, ya que los incidentes principales suelen dar lugar a escasez de personal que limita la capacidad de aplicar con éxito los planes de gestión de la continuidad. Ejemplo de brote de SARS (Síndrome respiratorio agudo y grave).<br>Con el fin de garantizar un bajo riesgo y mejorar la concienciación de los usuarios (personal), se recomienda utilizar un enfoque "programático" para probar los planes. Las pruebas deben basarse unas sobre otras, pasando de las pruebas de escritorio, a las pruebas modulares a la síntesis de tiempos de recuperación probable y finalmente a los ensayos completos. |
| 14.1.1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio. | | | |
| 14.1.2. Continuidad del negocio y evaluación de riesgos. | | | |
| 14.1.3. Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información. | | | |
| 14.1.4. Marco de referencia para la planificación de la continuidad del negocio. | | | |
| 14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad. | | | |
| **15. Conformidad** | **7.12 Conformidad** | | |
| | 7.12.1 General | Nuevo Control | **Guía de implementación**<br>Debe implementarse un programa de auditoría de cumplimiento que aborde todo el ciclo de operaciones. Dicho programa no sólo debe identificar áreas problemáticas sino también revisar los resultados y decidir actualizaciones del SGSI.<br>Se sugiere un ciclo de 12 meses a 18 meses para los programas de auditoría de las organizaciones de salud, durante el cual deben cubrirse todos los elementos de la Norma, todas las áreas de riesgo y todos los controles implementados.<br>Se recomienda que el ISMF (la auditoría del SGSI) establezca un marco de auditoría de cumplimiento gradual con auto-auditoría por parte de los operadores y gestores del proceso en la capa inferior y auditorías en las capas posteriores (por ejemplo, auditoría interna). |
| 15.1. Cumplimiento de los requisitos legales. | 7.12.2 Cumplimiento de los requisitos legales. | | |

| | | | |
|---|---|---|---|
| 15.1.1. Identificación de la legislación aplicable.<br>15.1.2. Derechos de propiedad intelectual (DPI).<br>15.1.3. Protección de los documentos de la organización. | 7.12.2.1 Identificación de la legislación aplicable, derechos de propiedad intelectual (DPI) y protección de los documentos de la organización. | Igual (=) | |
| 15.1.4. Protección de datos y privacidad de la información de carácter personal.<br>15.1.5. Prevención del uso indebido de recursos de tratamiento de la información.<br>15.1.6. Regulación de los controles criptográficos. | 7.12.2.2. Protección de datos y privacidad de la información personal.<br>7.12.2.3 Prevención del uso indebido de recursos de tratamiento de la información y Regulación de los controles criptográficos. | > | **Control**<br>Además de seguir la orientación dada por ISO/IEC 27002, las organizaciones que procesan información personal de salud deben manejar el consentimiento informativo de los pacientes.<br>Siempre que sea posible, se debe obtener el consentimiento informativo de los pacientes antes de que la información personal de salud sea enviada por correo electrónico, por fax o comunicada por conversación telefónica, o de otra forma divulgada a las partes externas a la organización sanitaria.<br>**Guía de implementación**<br>Ejemplo (requisito legal para obtener el consentimiento), Recomendación del Consejo de Europa, R (97) 5 Sobre la protección de datos médicos, Consejo de Europa, Estrasburgo, 12 de febrero de 1997 |
| 15.2. Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico. | 7.12.3 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico. | | |
| 15.2.1. Cumplimiento de las políticas y normas de seguridad.<br>15.2.2. Comprobación del cumplimiento técnico. | | > | **Guía de implementación**<br>Se presta especial atención al cumplimiento a los efectos de la interoperabilidad técnica, ya que los sistemas de información sanitaria a gran escala suelen consistir en muchos sistemas interoperables. |
| 15.3. Consideraciones sobre las auditorías de los sistemas de información. | 7.12.4 Consideraciones de la auditoría de los sistemas de información en un entorno sanitario. | | |
| 15.3.1. Controles de auditoría de los sistemas de información.<br>15.3.2. Protección de las herramientas de auditoría de los sistemas de información. | | Igual (=) | |

# Anexo 3: Combinación entre COBIT 5, ISO/IEC 27002:2005 e ISO 27799:2008

| COBIT 5 | | | | ISO/IEC 27002:2005 | ISO 27799:2008 | Mapeo |
|---|---|---|---|---|---|---|
| Evaluar, Orientar y Supervisar (EDM) | EDM01 | Asegurar el establecimiento y mantenimiento del marco de gobierno. | • EDM01.01 Evaluar el sistema de gobierno. | | | |
| | | | • EDM01.02 Orientar el sistema de gobierno. | **6.1 Organización interna:**<br>• 6.1.1 Compromiso de gerencia con la seguridad de la información. | **7.3.2 Organización interna:**<br>• 7.3.2.1 Compromiso de la administración con la seguridad de la información, la coordinación de seguridad de la información y la asignación de responsabilidades de seguridad de la información.<br>7.3.3 Grupos o personas externas: | P |
| | | | • EDM01.03 Supervisar el sistema de gobierno. | | | |
| | EDM03 | Asegurar la optimización del riesgo. | • EDM03.01 Evaluar la gestión de riesgos. | **14.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio:**<br>• 14.1.2 Continuidad del negocio y evaluación de riesgos. | **7.11 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio:** | P |
| | | | • EDM03.02 Orientar la gestión de riesgos. | | | |
| | | | • EDM03.03 Supervisar la gestión de riesgos. | | | |
| | EDM05 | Asegurar la transparencia hacia las partes interesadas. | • EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas. | | | |
| | | | • EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes. | **6.1 Organización interna:**<br>• 6.1.6 Contacto con las autoridades.<br>• 6.1.7 Contacto con grupos de interés especial. | **7.3.2 Organización interna:**<br>• 7.3.2.4 Contacto con las autoridades, contacto con grupos de intereses especiales y revisión independiente de la seguridad de la información. | P |
| | | | • EDM05.03 Supervisar la comunicación con las partes interesadas. | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Alinear, Planificar y Organizar (APO) | APO01 | Gestionar el Marco de Gestión de TI. | • APO01.01 Definir la estructura organizativa. | | | |
| | | | • APO01.02 Establecer roles y responsabilidades. | **6.1 Organización interna:**<br>• 6.1.3 Asignación de las responsabilidades de la seguridad de la información.<br>**8.2 Durante el empleo:**<br>• 8.2.1. Responsabilidades de la Dirección.<br>**7.1 Responsabilidad sobre los activos:**<br>• 7.1.3. Acuerdos sobre el uso aceptable de los activos.<br>**13.2. Gestión de incidentes y mejoras en la seguridad de la información:**<br>• 13.2.1. Identificación de responsabilidades y procedimientos. | **7.3.2 Organización interna:**<br>• 6.1.3 Asignación de las responsabilidades de la seguridad de la información.<br>**7.5.2 Durante el empleo:**<br>• 7.5.2.1 Responsabilidades de la Dirección.<br>**7.1 Responsabilidad sobre los activos:**<br>• 7.1.3. Acuerdos sobre el uso aceptable de los activos.<br>**13.2. Gestión de incidentes y mejoras en la seguridad de la información:**<br>• 13.2.1. Identificación de responsabilidades y procedimientos. | **P** |
| | | | • APO01.03 Mantener los elementos catalizadores del sistema de gestión. | | | |
| | | | • APO01.04 Comunicar los objetivos y la dirección de gestión. | | | |
| | | | • APO01.05 Optimizar la ubicación de la función de TI. | | | |
| | | | • APO01.06 Definir la propiedad de la información (datos) y del sistema. | **7.1 Responsabilidad sobre los activos:**<br>• 7.1.1. Inventario de activos.<br>• 7.1.2. Propiedad de los activos.<br>• 7.1.3. Acuerdos sobre el uso aceptable de los activos.<br>**7.2 Clasificación de la información:**<br>• 7.2.1 Directrices de Clasificación. | **7.4.1 Responsabilidad sobre los activos de información de salud:**<br>**7.4.2 Clasificación de información de salud:**<br>• 7.4.2.1 Directrices de Clasificación. | **C** |
| | | | • APO01.07 Gestionar la mejora continua delos procesos. | | | |
| | | | • APO01.08 Mantener el cumplimiento con las políticas y procedimientos. | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Alinear, Planificar y Organizar (APO) | APO07 | Gestionar los Recursos Humanos. | • APO07.01 Mantener la dotación de personal suficiente y adecuado. | **8.1 Antes del empleo:**<br>• 8.1.1. Roles y responsabilidades.<br>• 8.1.2. Investigación de antecedentes.<br>• 8.1.3. Términos y condiciones de la relación laboral. | **7.5.1 Antes del empleo:**<br>• 7.5.1.1 Roles y responsabilidades.<br>• 7.5.1.2 Investigación de antecedentes (Screening).<br>• 7.5.1.3 Términos y condiciones de la relación laboral. | **P** |
| | | | • APO07.02 Identificar personal clave de TI. | **8.3 Finalización del empleo o cambio del puesto de trabajo:**<br>• 8.3.1. Responsabilidad de finalización del empleo o cambio.<br>• 8.3.2. Devolución de los activos.<br>• 8.3.3. Cancelación de los permisos de acceso. | **7.5.3 Finalización del empleo o cambio del puesto de trabajo:**<br>• 7.5.3.1 Responsabilidades de terminación y devolución de activos.<br>• 7.5.3.2 Cancelación de los permisos de acceso. | **P** |
| | | | • APO07.03 Mantener las habilidades y competencias del personal. | | | |
| | | | • APO07.04 Evaluar el desempeño laboral de los empleados. | **8.2 Durante el empleo:**<br>• 8.2.3. Procedimiento disciplinario. | **7.5.2.1 Responsabilidades de la Dirección:**<br>• 7.5.2.3 Procedimiento disciplinario. | **P** |
| | | | • APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio. | | | |
| | | | • APO07.06 Gestionar el personal contratado. | | | |
| | APO09 | Gestionar los Acuerdos de Servicios. | • APO09.01 Identificar servicios TI. | | | |
| | | | • APO09.02 Catalogar servicios basados en TI. | | | |
| | | | • APO09.03 Definir y preparar acuerdos de servicio. | | | |
| | | | • APO09.04 Supervisar e informar de los niveles de servicio. | | | |
| | | | • APO09.05 Revisar acuerdos de servicio y contratos. | **10.2. Gestión de la provisión de servicios por terceros:**<br>• 10.2.1 Provisión de servicios.<br>• 10.2.2. Supervisión y revisión de los servicios prestados por terceros.<br>• 10.2.3. Gestión del cambio en los servicios prestados por terceros. | **7.7.2 Gestión de la provisión de servicios por terceros:** | **P** |

| | | | | | | |
|---|---|---|---|---|---|---|
| Alinear, Planificar y Organizar (APO) | APO13 | Gestionar la Seguridad. | • APO13.01 Establecer y mantener un SGSI. | **6.1 Organización interna:**<br>• 6.1.1 Compromiso de gerencia con la seguridad de la información.<br>• 6.1.2 Coordinación de la seguridad de la información. | **7.3.2 Organización interna:**<br>• 7.3.2.1 Compromiso de la administración con la seguridad de la información, la coordinación de seguridad de la información y la asignación de responsabilidades de seguridad de la información. | **C** |
| | | | • APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información. | **5.1. Política de seguridad de la información:**<br>• 5.1.1 Documento de la Política de Seguridad de la Información.<br>**6.1 Organización interna:**<br>• 6.1.2 Coordinación de la seguridad de la información.<br>• 6.1.5 Acuerdos de confidencialidad.<br>**11.1 Requisitos de negocio para control de acceso:**<br>• 11.1.1 Política de control de acceso.<br>**11.7. Informática móvil y tele trabajo:**<br>• 11.7.1. Ordenadores portátiles y comunicaciones móviles.<br>• 11.7.2. Tele trabajo. | **7.2 Política de Seguridad de la Información:**<br>• 7.2.1 Documento de la Política de Seguridad de la Información.<br>**7.3.2 Organización interna:**<br>• 7.3.2.1 Compromiso de la administración con la seguridad de la información, la coordinación de seguridad de la información y la asignación de responsabilidades de seguridad de la información.<br>• 7.3.2.3 Acuerdos de confidencialidad.<br>**7.8.1 Requisitos para el control de acceso en salud:**<br>• 7.8.1.2 Política de control de acceso.<br>**7.8.6 Informática móvil y tele trabajo:**<br>• 7.8.6.1. Informática móvil y comunicaciones.<br>• 7.8.6.2 Tele trabajo. | **C** |
| | | | • APO13.03 Supervisar y revisar el SGSI. | **5.1. Política de seguridad de la información:**<br>• 5.1.2 Revisión de la política de seguridad de la información.<br>**15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico:**<br>• 15.2.1 Cumplimiento de las políticas y normas de seguridad.<br>• 15.2.2 Comprobación del cumplimiento técnico. | **7.2 Política de Seguridad de la Información:**<br>• 7.2.2 Revisión del documento de política de seguridad de la información.<br>**7.12.3 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico:** | **C** |
| Construir, Adquirir e Implementar | BAI02 | Gestionar la Definición de Requisitos. | • BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio. | | | |
| | | | • BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas. | **10.3. Planificación y aceptación del sistema:**<br>• 10.3.2 Aceptación del sistema. | **7.7.3 Planificación y aceptación del sistema:**<br>• 7.7.3.2 Aceptación del sistema. | P |
| | | | • BAI02.03 Gestionar los riesgos de los requerimientos. | **10.1. Procedimientos y responsabilidades de operación:**<br>• 10.1.1. Documentación de los procedimientos operativos.<br>**11.6. Control de acceso a las aplicaciones y a la información:**<br>• 11.6.2. Aislamiento de sistemas sensibles.<br>**12.1. Requisitos de seguridad de los sistemas de información:**<br>• 12.1.1 Análisis y especificación de requisitos de seguridad. | **7.7.1 Procedimientos y responsabilidades de operación:**<br>• 7.7.1.1 Documentación de los procedimientos operativos.<br>**7.8.5 Control de acceso a las aplicaciones y a la información:**<br>• 7.8.5.2 Aislamiento de sistemas sensibles.<br>**7.9.1 Requisitos de seguridad de los sistemas de información:** | P |

| | | | | | | |
|---|---|---|---|---|---|---|
| | BAI02 | | • BAI02.04 Obtener la aprobación de los requerimientos y soluciones. | | | |
| Construir, Adquirir e Implementar (BAI) | BAI03 | Gestionar la Identificación y la Construcción de Soluciones. | • BAI03.01 Diseñar soluciones de alto nivel. | | | |
| | | | • BAI03.02 Diseñar los componentes detallados de la solución. | | | |
| | | | • BAI03.03 Desarrollar los componentes de la solución. | **12.1. Requisitos de seguridad de los sistemas de información:**<br>• 12.1.1 Análisis y especificación de requisitos de seguridad. | **7.9.1 Requisitos de seguridad de los sistemas de información:** | P |
| | | | • BAI03.04 Obtener los componentes de la solución. | | | |
| | | | • BAI03.05 Construir soluciones. | **10.10. Monitorización:**<br>• 10.10.1. Registros de auditoría.<br>**12.5. Seguridad en los procesos de desarrollo y soporte:**<br>• 12.5.1. Procedimientos de control de cambios. | **7.7.10 Monitorización:**<br>7.7.10.2 Registros de auditoría.<br>**7.9.5 Seguridad en procesos de desarrollo y soporte, y gestión de la vulnerabilidad técnica:** | P |
| | | | • BAI03.06 Realizar controles de calidad. | | | |
| | | | • BAI03.07 Preparar pruebas de la solución. | **10.1. Procedimientos y responsabilidades de operación:**<br>10.1.4. Separación de los recursos de desarrollo, prueba y operación. | **7.7.1 Procedimientos y responsabilidades de operación:**<br>• 7.7.1.4 Separación de los recursos de desarrollo, prueba y operación. | P |
| | | | • BAI03.08 Ejecutar pruebas de la solución. | **10.1. Procedimientos y responsabilidades de operación:**<br>10.1.4. Separación de los recursos de desarrollo, prueba y operación. | **7.7.1 Procedimientos y responsabilidades de operación:**<br>• 7.7.1.4 Separación de los recursos de desarrollo, prueba y operación. | P |
| | | | • BAI03.09 Gestionar cambios a los requerimientos. | **12.5. Seguridad en los procesos de desarrollo y soporte:**<br>• 12.5.1. Procedimientos de control de cambios. | **7.9.5 Seguridad en procesos de desarrollo y soporte, y gestión de la vulnerabilidad técnica:** | P |
| | | | • BAI03.10 Mantener soluciones. | **9.1 Áreas seguras:**<br>9.1.5. Trabajo en áreas seguras.<br>**9.2 Seguridad de los equipos:**<br>9.2.4. Mantenimiento de equipos.<br>**12.4. Seguridad de los ficheros del sistema:**<br>12.4.2. Protección de los datos de prueba del sistema.<br>**12.5. Seguridad en los procesos de desarrollo y soporte:**<br>12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.<br>**12.6. Gestión de las vulnerabilidades técnicas:**<br>12.6.1. Control de las vulnerabilidades técnicas. | **7.6.1 Áreas seguras:**<br>• 7.6.1.2 Controles de entrada física; Asegurar oficinas, habitaciones e instalaciones; Protección contra las amenazas externas y ambientales; Trabajando en áreas seguras.<br>**9.2 Seguridad de los equipos:**<br>• 7.6.2.2 Soporte de servicios públicos, seguridad de cableado y mantenimiento de equipos.<br>**7.9.4 Seguridad de los ficheros del sistema:**<br>• 7.9.4.2. Protección de los datos de prueba del sistema.<br>**7.9.5 Seguridad en procesos de desarrollo y soporte, y gestión de la vulnerabilidad técnica:** | P |

| | | | | | | |
|---|---|---|---|---|---|---|
| | BAI03 | | • BAI03.11 Definir los servicios TI y mantener el catálogo de servicios. | | | |
| Construir, Adquirir e Implementar (BAI) | BAI04 | Gestionar la Disponibilidad y Capacidad. | • BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia. | **Gestión de Comunicaciones y Operaciones:**<br>• 10.3.1. Gestión de capacidades. | **7.7.3 Planificación y aceptación del sistema:**<br>• 7.7.3.1 Gestión de capacidades. | P |
| | | | • BAI04.02 Evaluar el impacto en el negocio. | **Gestión de Comunicaciones y Operaciones:**<br>• 10.3.1. Gestión de capacidades. | **7.7.3 Planificación y aceptación del sistema:**<br>• 7.7.3.1 Gestión de capacidades. | P |
| | | | • BAI04.03 Planificar requisitos de servicio nuevos o modificados. | **Gestión de Comunicaciones y Operaciones:**<br>• 10.3.1. Gestión de capacidades. | **7.7.3 Planificación y aceptación del sistema:**<br>• 7.7.3.1 Gestión de capacidades. | P |
| | | | • BAI04.04 Supervisar y revisar la disponibilidad y la capacidad. | | | |
| | | | • BAI04.05 Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad. | | | |
| | BAI06 | Gestionar los Cambios. | • BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio. | **10.1. Procedimientos y responsabilidades de operación:**<br>• 10.1.2 Gestión de cambios.<br>**11.5. Control de acceso al sistema operativo:**<br>• 11.5.4. Uso de los servicios del sistema.<br>**12.5. Seguridad en los procesos de desarrollo y soporte:**<br>• 12.5.1 Procedimientos de control de cambios.<br>• 12.5.3. Restricciones a los cambios en los paquetes de software.<br>**12.6. Gestión de las vulnerabilidades técnicas:**<br>• 12.6.1 Control de las vulnerabilidades técnicas. | **7.7.1 Procedimientos y responsabilidades de operación:**<br>• 7.7.1.2 Gestión de cambios.<br>**7.8.4 Control de acceso a la red y control de acceso al sistema operativo:**<br>**7.9.5 Seguridad en procesos de desarrollo y soporte, y gestión de la vulnerabilidad técnica:** | P |
| | | | • BAI06.02 Gestionar cambios de emergencia. | | | |
| | | | • BAI06.03 Hacer seguimiento e informar de cambios de estado. | | | |
| | | | • BAI06.04 Cerrar y documentar los cambios. | | | |
| | BAI07 | Gestionar la Aceptación del Cambio y de la Transición. | • BAI07.01 Establecer un plan de implementación. | **12.5. Seguridad en los procesos de desarrollo y soporte:**<br>• 12.5.1. Procedimientos de control de cambios.<br>**8.2 Durante el empleo:**<br>• 8.2.2. Conocimiento, educación y capacitación en seguridad de la información. | **7.9.5 Seguridad en procesos de desarrollo y soporte, y gestión de la vulnerabilidad técnica:**<br>**7.5.2 Durante el empleo:**<br>• 7.5.2.2 Conocimiento, educación y capacitación en seguridad de la información. | P |
| | | | • BAI07.02 Planificar la conversión de procesos de negocio, sistemas y datos. | | | |
| | | | • BAI07.03 Planificar pruebas de aceptación. | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Construir, Adquirir e Implementar (BAI) | BAI07 | Gestionar la Aceptación del Cambio y de la Transición. | • BAI07.04 Establecer un entorno de pruebas. | **6.1 Organización interna:**<br>• 6.1.4 Proceso de autorización de recursos para el tratamiento de la información.<br>**9.1 Áreas seguras:**<br>• 9.1.6. Áreas de acceso público, entrega y carga.<br>**10.1. Procedimientos y responsabilidades de operación:**<br>• 10.1.4. Separación de los recursos de desarrollo, prueba y operación.<br>**12.4. Seguridad de los ficheros del sistema:**<br>• 12.4.2. Protección de los datos de prueba del sistema.<br>• 12.4.3. Control de acceso al código fuente de los programas. | **7.3.2 Organización interna:**<br>• 7.3.2.2 Proceso de autorización de recursos para el tratamiento de la información.<br>**7.6.1 Áreas seguras:**<br>• 7.6.1.3 Áreas de acceso público, entrega y descarga.<br>**7.7.1 Procedimientos y responsabilidades de operación:**<br>• 7.7.1.4 Separación de los recursos de desarrollo, prueba y operación.<br>**7.9.3 Controles criptográficos:**<br>• 7.9.4.2. Protección de los datos de prueba del sistema.<br>• 7.9.4.3. Control de acceso al código fuente de los programas. | P |
| | | | • BAI07.05 Ejecutar pruebas de aceptación. | **12.5. Seguridad en los procesos de desarrollo y soporte:**<br>• 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.<br>**10.3. Planificación y aceptación del sistema:**<br>• 10.3.2 Aceptación del sistema. | **7.9.5 Seguridad en procesos de desarrollo y soporte, y gestión de la vulnerabilidad técnica:**<br>**7.7.3 Planificación y aceptación del sistema:**<br>• 7.7.3.2 Aceptación del sistema. | P |
| | | | • BAI07.06 Pasar a producción y gestionar los lanzamientos. | | | |
| | | | • BAI07.07 Proporcionar soporte en producción desde el primer momento. | | | |
| | | | • BAI07.08 Ejecutar una revisión post implantación. | | | |
| | BAI08 | Gestionar el Conocimiento. | • BAI08.01 Cultivar y facilitar una cultura de intercambio de conocimientos. | | | |
| | | | • BAI08.02 Identificar y clasificar las fuentes de información. | | | |
| | | | • BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento. | **10.1. Procedimientos y responsabilidades de operación:**<br>• 10.1.1. Documentación de los procedimientos operativos.<br>**10.3. Planificación y aceptación del sistema:**<br>• 10.3.2 Aceptación del sistema.<br>**10.7. Manipulación de los soportes:**<br>• 10.7.4. Seguridad de la documentación del sistema. | **7.7.1 Procedimientos y responsabilidades de operación:**<br>• 7.7.1.1 Documentación de los procedimientos operativos.<br>**7.7.3 Planificación y aceptación del sistema:**<br>• 7.7.3.2 Aceptación del sistema.<br>**7.7.7 Manipulación de los soportes:**<br>• 7.7.7.4 Seguridad de la documentación del sistema. | P |

| | | | | | | |
|---|---|---|---|---|---|---|
| Construir, Adquirir e Implementar (BAI) | BAI08 | Gestionar el Conocimiento. | • BAI08.04 Utilizar y compartir el conocimiento. | **13.2. Gestión de incidentes y mejoras en la seguridad de la información:**<br>• 13.2.2. Aprendizaje de los incidentes de seguridad de la información. | **7.10.2 Gestión de incidentes y mejoras en la seguridad de la información:**<br>• 7.10.2.2 Aprendizaje de los incidentes de seguridad de la información. | P |
| | | | • BAI08.05 Evaluar y retirar la información. | | | |
| | BAI09 | Gestionar los Activos. | • BAI09.01 Identificar y registrar activos actuales. | **7.1 Responsabilidad sobre los activos:**<br>• 7.1.1 Inventario de activos.<br>• 7.1.2 Propiedad de los activos.<br>**11.4. Control de acceso a la red:**<br>• 11.4.3. Identificación de los equipos en las redes. | **7.4.1 Responsabilidad sobre los activos de información de salud:**<br>**7.8.4 Control de acceso a la red y control de acceso al sistema operativo:** | P |
| | | | • BAI09.02 Gestionar activos críticos. | **10.7. Manipulación de los soportes:**<br>• 10.7.4. Seguridad de la documentación del sistema.<br>**12.4. Seguridad de los ficheros del sistema:**<br>• 12.4.1 Control del software en explotación.<br>• 12.4.2 Protección de los datos de prueba del sistema.<br>**12.5. Seguridad en los procesos de desarrollo y soporte:**<br>• 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.<br>• 12.5.3. Restricciones a los cambios en los paquetes de software.<br>**12.6. Gestión de las vulnerabilidades técnicas:**<br>• 12.6.1 Control de las vulnerabilidades técnicas.<br>**15.1. Cumplimiento de los requisitos legales:**<br>• 15.1.5. Prevención del uso indebido de recursos de tratamiento de la información. | **7.7.7 Manipulación de los soportes:**<br>• 7.7.7.4 Seguridad de la documentación del sistema.<br>**7.9.4 Seguridad de los ficheros del sistema:**<br>• 7.9.4.1. Control del software en explotación.<br>• 7.9.4.2. Protección de los datos de prueba del sistema.<br>**7.9.5 Seguridad en procesos de desarrollo y soporte, y gestión de la vulnerabilidad técnica:**<br>**7.12.2 Cumplimiento de los requisitos legales:**<br>• 7.12.2.3 Prevención del uso indebido de recursos de tratamiento de la información y Regulación de los controles criptográficos. | P |
| | | | • BAI09.03 Gestionar el ciclo de vida de los activos. | **7.2 Clasificación de la información:**<br>• 7.2.2 Etiquetado y manejo de la información.<br>**7.1.1. Inventario de activos:**<br>• 7.1.3. Acuerdos sobre el uso aceptable de los activos.<br>**8.3 Finalización del empleo o cambio del puesto de trabajo:**<br>• 8.3.2. Devolución de los activos | **7.4.2 Clasificación de información de salud:**<br>• 7.4.2.2 Etiquetado y manejo de la información.<br>**7.4.1 Responsabilidad sobre los activos de información de salud:**<br>**7.5.3 Finalización del empleo o cambio del puesto de trabajo:**<br>• 7.5.3.1 Responsabilidades de terminación y devolución de activos. | P |
| | | | • BAI09.04 Optimizar el coste de los activos. | | | |
| | | | • BAI09.05 Administrar licencias. | **15.1. Cumplimiento de los requisitos legales:**<br>• 15.1.2. Derechos de propiedad intelectual (DPI). | **7.12.2 Cumplimiento de los requisitos legales:**<br>• 7.12.2.1 Identificación de la legislación aplicable, derechos de propiedad intelectual (DPI) y protección de los documentos de la organización. | P |

| | | | | | | |
|---|---|---|---|---|---|---|
| Construir, Adquirir e Implementar (BAI) | BAI10 | Gestionar la Configuración. | • BAI10.01 Establecer y mantener un modelo de configuración. | | | |
| | | | • BAI10.02 Establecer y mantener un repositorio de configuración y una base de referencia. | | | |
| | | | • BAI10.03 Mantener y controlar los elementos de configuración. | **12.4. Seguridad de los ficheros del sistema:**<br>• 12.4.1. Control del software en explotación.<br>• 12.4.2 Protección de los datos de prueba del sistema.<br>**12.5. Seguridad en los procesos de desarrollo y soporte:**<br>• 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.<br>• 12.5.3. Restricciones a los cambios en los paquetes de software.<br>**12.6. Gestión de las vulnerabilidades técnicas:**<br>• 12.6.1. Control de las vulnerabilidades técnicas.<br>**15.1. Cumplimiento de los requisitos legales:**<br>• 15.1.5. Prevención del uso indebido de recursos de tratamiento de la información. | **7.9.4 Seguridad de los ficheros del sistema:**<br>• 7.9.4.1. Control del software en explotación.<br>• 7.9.4.2. Protección de los datos de prueba del sistema.<br>**7.9.5 Seguridad en procesos de desarrollo y soporte, y gestión de la vulnerabilidad técnica:**<br>**7.12.2 Cumplimiento de los requisitos legales:**<br>• 7.12.2.3 Prevención del uso indebido de recursos de tratamiento de la información y Regulación de los controles criptográficos. | P |
| | | | • BAI10.04 Generar informes de estado y configuración. | | | |
| | | | • BAI10.05 Verificar y revisar la integridad del repositorio de configuración. | **7.1 Responsabilidad sobre los activos:**<br>• 7.1.1 Inventario de activos.<br>• 7.1.2 Propiedad de los activos.<br>**7.2 Clasificación de la información:**<br>• 7.2.2 Etiquetado y manejo de la información.<br>**10.7. Manipulación de los soportes:**<br>• 10.7.4. Seguridad de la documentación del sistema.<br>**11.4. Control de acceso a la red:**<br>• 11.4.3 Identificación de los equipos en las redes. | **7.4.1 Responsabilidad sobre los activos de información de salud:**<br>**7.4.2 Clasificación de información de salud:**<br>• 7.4.2.2 Etiquetado y manejo de la información.<br>**7.7.7 Manipulación de los soportes:**<br>• 7.7.7.4 Seguridad de la documentación del sistema.<br>**7.8.4 Control de acceso a la red y control de acceso al sistema operativo:** | P |

| | | | | | | |
|---|---|---|---|---|---|---|
| Entrega, Servicio y Soporte (DSS) | DSS01 | Gestionar las Operaciones. | • DSS01.01 Ejecutar procedimientos operativos | **10.1. Procedimientos y responsabilidades de operación:**<br>• 10.1.1. Documentación de los procedimientos operativos. | **7.7.1 Procedimientos y responsabilidades de operación:**<br>• 7.7.1.1 Documentación de los procedimientos operativos. | E |
| | | | • DSS01.02 Gestionar servicios externalizados de TI | **6.2 Grupos o personas externas:**<br>• 6.2.3. Tratamiento de la seguridad en contratos con terceros.<br>**10.2. Gestión de la provisión de servicios por terceros:**<br>• 10.2.2. Supervisión y revisión de los servicios prestados por terceros. | **7.3.3 Grupos o personas externas:**<br>• 7.3.3.3 Tratamiento de la seguridad en contratos con terceros.<br>**7.7.2 Gestión de la provisión de servicios por terceros:** | P |
| | | | • DSS01.03 Supervisar la infraestructura de TI | **13.1 Notificación de eventos y puntos débiles de seguridad de la información:**<br>• 13.1.1. Notificación de los eventos de seguridad de la información**.** | **7.10.1 Notificación de eventos y puntos débiles de seguridad de la información:** | P |
| | | | • DSS01.04 Gestionar el entorno | **6.1 Organización interna:**<br>• 6.1.6 Contacto con las autoridades.<br>**11.7. Informática móvil y tele trabajo:**<br>• 11.7.1. Ordenadores portátiles y comunicaciones móviles.<br>**9.1 Áreas seguras:**<br>• 9.1.4. Protección contra amenazas externas y de origen ambiental.<br>• 9.1.5. Trabajo en áreas seguras.<br>**9.2 Seguridad de los equipos:**<br>• 9.2.1. Ubicación y protección del equipo.<br>• 9.2.5 Seguridad de equipos fuera de los locales de la Organización. | **7.3.2 Organización interna:**<br>• 7.3.2.4 Contacto con las autoridades, contacto con grupos de intereses especiales y revisión independiente de la seguridad de la información.<br>**7.8.6 Informática móvil y tele trabajo:**<br>• 7.8.6.1. Informática móvil y comunicaciones.<br>**7.6.1 Áreas seguras:**<br>• 7.6.1.2 Controles de entrada física; Asegurar oficinas, habitaciones e instalaciones; Protección contra las amenazas externas y ambientales; Trabajando en áreas seguras.<br>**9.2 Seguridad de los equipos:**<br>• 7.6.2.1 Ubicación y protección del equipo.<br>• 7.6.2.3 Seguridad de equipos fuera de los locales de la Organización. | P |
| | | | • DSS01.05 Gestionar las instalaciones | **9.1 Áreas seguras:**<br>• 9.1.1. Perímetro de seguridad física.<br>• 9.1.3. Seguridad de oficinas, despachos y recursos.<br>• 9.1.6. Áreas de acceso público, entrega y descarga.<br>**9.2 Seguridad de los equipos**<br>• 9.2.2. Servicios públicos de soporte.<br>• 9.2.3. Seguridad del cableado.<br>• 9.2.4. Mantenimiento de equipos. | **7.6.1 Áreas seguras:**<br>• 7.6.1.1. Perímetro de seguridad física.<br>• 7.6.1.2 Controles de entrada física; Asegurar oficinas, habitaciones e instalaciones; Protección contra las amenazas externas y ambientales; Trabajando en áreas seguras.<br>• 7.6.1.3 Áreas de acceso público, entrega y descarga.<br>**9.2 Seguridad de los equipos:**<br>• 7.6.2.2 Soporte de servicios públicos, seguridad de cableado y mantenimiento de equipos. | P |

| | | | | | | |
|---|---|---|---|---|---|---|
| Entrega, Servicio y Soporte (DSS) | DSS02 | Gestionar las Peticiones y los Incidentes del Servicio. | • DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio. | **13.1 Notificación de eventos y puntos débiles de seguridad de la información:**<br>• 13.1.1. Notificación de los eventos de seguridad de la información.<br>• 13.1.2. Notificación de puntos débiles de seguridad. | **7.10.1 Notificación de eventos y puntos débiles de seguridad de la información:** | P |
| | | | • DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes. | **13.1 Notificación de eventos y puntos débiles de seguridad de la información:**<br>• 13.1.2. Notificación de puntos débiles de seguridad. | **7.10.1 Notificación de eventos y puntos débiles de seguridad de la información:** | P |
| | | | • DSS02.03 Verificar, aprobar y resolver peticiones de servicio. | | | |
| | | | • DSS02.04 Investigar, diagnosticar y localizar incidentes. | **13.2. Gestión de incidentes y mejoras en la seguridad de la información.**<br>• 13.2.1. Identificación de responsabilidades y procedimientos.<br>• 13.2.3. Recopilación de evidencias. | **7.10.2 Gestión de incidentes y mejoras en la seguridad de la información:**<br>• 7.10.2.1 Identificación de responsabilidades y procedimientos.<br>• 7.10.2.3 Recogida de pruebas. | P |
| | | | • DSS02.05 Resolver y recuperarse de incidentes. | **13.2. Gestión de incidentes y mejoras en la seguridad de la información.**<br>• 13.2.1. Identificación de responsabilidades y procedimientos.<br>• 13.2.3. Recopilación de evidencias. | **7.10.2 Gestión de incidentes y mejoras en la seguridad de la información:**<br>• 7.10.2.1 Identificación de responsabilidades y procedimientos.<br>• 7.10.2.3 Recogida de pruebas. | P |
| | | | • DSS02.06 Cerrar peticiones de servicio e incidentes. | | | |
| | | | • DSS02.07 Seguir el estado y emitir informes. | | | |
| | DSS03 | Gestionar los Problemas. | • DSS03.01 Identificar y clasificar problemas. | | | |
| | | | • DSS03.02 Investigar y diagnosticar problemas. | | | |
| | | | • DSS03.03 Levantar errores conocidos. | | | |
| | | | • DSS03.04 Resolver y cerrar problemas. | | | |
| | | | • DSS03.05 Realizar una gestión de problemas proactiva. | **13.2. Gestión de incidentes y mejoras en la seguridad de la información:**<br>• 13.2.2. Aprendizaje de los incidentes de seguridad de la información. | **7.10.2 Gestión de incidentes y mejoras en la seguridad de la información:**<br>• 7.10.2.2 Aprendizaje de los incidentes de seguridad de la información. | P |

| | | | | | | |
|---|---|---|---|---|---|---|
| Entrega, Servicio y Soporte (DSS) | DSS04 | Gestionar la Continuidad. | • DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance. | **14.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio:**<br>• 14.1.1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio. | **7.11 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio:** | P |
| | | | • DSS04.02 Mantener una estrategia de continuidad. | **14.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio:**<br>• 14.1.2. Continuidad del negocio y evaluación de riesgos.<br>**6.1 Organización interna:**<br>• 6.1.6 Contacto con las autoridades.<br>• 6.1.7 Contacto con grupos de interés especial. | **7.11 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio:**<br>**7.3.2 Organización interna:**<br>• 7.3.2.4 Contacto con las autoridades, contacto con grupos de intereses especiales y revisión independiente de la seguridad de la información. | P |
| | | | • DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio. | **14.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio:**<br>• 14.1.3. Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información. | **7.11 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio:** | P |
| | | | • DSS04.04 Ejercitar, probar y revisar el plan de continuidad. | **14.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio:**<br>• 14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad. | **7.11 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio:** | P |
| | | | • DSS04.05 Revisar, mantener y mejorar el plan de continuidad. | **14.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio:**<br>• 14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad. | **7.11 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio:** | P |
| | | | • DSS04.06 Proporcionar formación en el plan de continuidad. | **14.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio:**<br>• 14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad. | **7.11 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio:** | P |
| | | | • DSS04.07 Gestionar acuerdos de respaldo. | **10.5. Copias de seguridad:**<br>• 10.5.1. Copias de seguridad de la información. | **7.7.5 Copia de seguridad de la información de salud:** | P |
| | | | • DSS04.08 Ejecutar revisiones post reanudación. | **14.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio:**<br>• 14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad. | **7.11 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio:** | P |
| | DSS05 | Gestionar los Servicios de Seguridad. | • DSS05.01 Proteger contra software malicioso (malware). | **6.1 Organización interna:**<br>• 6.1.7 Contacto con grupos de interés especial.<br>**7.1 Responsabilidad sobre los activos:**<br>• 7.1.3. Acuerdos sobre el uso aceptable de los activos.<br>**10.4 Protección contra software malicioso y código móvil:**<br>• 10.4.1. Controles contra software malicioso.<br>• 10.4.2. Medidas y controles contra códigos móviles (cliente). | **7.3.2 Organización interna:**<br>• 7.3.2.4 Contacto con las autoridades, contacto con grupos de intereses especiales y revisión independiente de la seguridad de la información.<br>**7.4.1 Responsabilidad sobre los activos de información de salud:**<br>**7.7.4 Protección contra software malicioso y código móvil:**<br>• 7.7.4.1 Controles contra software malicioso.<br>• 7.7.4.2 Medidas y controles contra códigos móviles (cliente). | E |

| | | | | | | |
|---|---|---|---|---|---|---|
| Entrega, Servicio y Soporte (DSS) | DSS05 | Gestionar los Servicios de Seguridad. | • DSS05.02 Gestionar la seguridad de la red y las conexiones. | **6.2 Grupos o personas externas:**<br>• 6.2.1 Identificación de los riesgos derivados del acceso de terceros.<br>**10.6. Gestión de la seguridad de las redes:**<br>• 10.6.1. Controles de red.<br>• 10.6.2. Seguridad en los servicios de red.<br>**11.4. Control de acceso a la red:**<br>• 11.4.1. Política de uso de los servicios de red.<br>• 11.4.2. Autenticación de usuario para conexiones externas.<br>• 11.4.3. Identificación de los equipos en las redes.<br>• 11.4.4. Protección a puertos de diagnóstico remoto.<br>• 11.4.5. Segregación de las redes.<br>• 11.4.6. Control de la conexión a la red.<br>• 11.4.7. Control de encaminamiento (routing) de red.<br>**11.6. Control de acceso a las aplicaciones y a la información:**<br>• 11.6.2. Aislamiento de sistemas sensibles. | **7.3.3 Grupos o personas externas:**<br>• 7.3.3.1 Identificación de los riesgos derivados del acceso de terceros.<br>**7.7.6 Gestión de la seguridad de las redes:**<br>• 7.7.6.1 Controles de red.<br>• 7.7.6.2 Seguridad en los servicios de red.<br>**7.8.4 Control de acceso a la red y control de acceso al sistema operativo:**<br>**7.8.5 Control de acceso a las aplicaciones y a la información:**<br>• 7.8.5.2 Aislamiento de sistemas sensibles. | E |
| | | | • DSS05.03 Gestionar la seguridad de los puestos de usuario final. | **11.7. Informática móvil y tele trabajo:**<br>• 11.7.1. Ordenadores portátiles y comunicaciones móviles.<br>**10.8. Intercambio de información:**<br>• 10.8.4 Mensajería electrónica.<br>**12.2. Tratamiento correcto en las aplicaciones:**<br>• 12.2.3. Integridad de mensajes.<br>**12.3. Controles criptográficos:**<br>• 12.3.1. Política de uso de los controles criptográficos.<br>• 12.3.2. Gestión de claves.<br>**15.1. Cumplimiento de los requisitos legales:**<br>• 15.1.6. Regulación de los controles criptográficos. | **7.8.6 Informática móvil y tele trabajo:**<br>• 7.8.6.1. Informática móvil y comunicaciones.<br>**7.7.8 Intercambio de información:**<br>• 7.7.8.2 Mensajería electrónica.<br>**7.9.2 Tratamiento correcto en las aplicaciones**:<br>• 7.9.2.4 Integridad de mensajes.<br>**7.9.3 Controles criptográficos:**<br>• 7.9.3.1 Política sobre el uso de los controles criptográficos y la gestión de claves.<br>• 7.9.3.2 Gestión de claves.<br>**7.12.2 Cumplimiento de los requisitos legales:**<br>• 7.12.2.3 Prevención del uso indebido de recursos de tratamiento de la información y Regulación de los controles criptográficos. | E |
| | | | • DSS05.04 Gestionar la identidad del usuario y el acceso lógico. | **6.2 Grupos o personas externas:**<br>• 6.2.1 Identificación de los riesgos derivados del acceso de terceros.<br>• 6.2.2 Tratamiento de la seguridad en la relación con los clientes.<br>**8.3 Finalización del empleo o cambio del puesto de trabajo:**<br>• 8.3.1. Responsabilidad de finalización del empleo o cambio.<br>• 8.3.3. Cancelación de los permisos de acceso. | **7.3.3 Grupos o personas externas:**<br>• 7.3.3.1 Identificación de los riesgos derivados del acceso de terceros.<br>• 7.3.3.2 Tratamiento de la seguridad en la relación con los clientes.<br>**7.5.3 Finalización del empleo o cambio del puesto de trabajo:**<br>• 7.5.3.1 Responsabilidades de terminación y devolución de activos.<br>• 7.5.3.2 Cancelación de los permisos de acceso. | E |

| | | | | | | |
|---|---|---|---|---|---|---|
| Entrega, Servicio y Soporte (DSS) | DSS05 | Gestionar los Servicios de Seguridad. | • DSS05.04 Gestionar la identidad del usuario y el acceso lógico. | **11.1 Requisitos de negocio para control de acceso:**<br>• 11.1.1 Política de control de acceso.<br>**11.2 Gestión de acceso de usuario:**<br>• 11.2.1 Registro de usuario.<br>• 11.2.2 Gestión de privilegios.<br>• 11.2.4 Revisión de los derechos de acceso de los usuarios. | **7.8.1 Requisitos para el control de acceso en salud:**<br>• 7.8.1.2 Política de control de acceso.<br>**7.8.2 Gestión de acceso de usuario:**<br>• 7.8.2.1 Registro de usuario. | E |
| | | | • DSS05.05 Gestionar el acceso físico a los activos de TI. | **6.1 Organización interna:**<br>• 6.1.4 Proceso de autorización de recursos para el tratamiento de la información.<br>**9.1 Áreas seguras:**<br>• 9.1.6. Áreas de acceso público, entrega y descarga.<br>**9.2 Seguridad de los equipos:**<br>• 9.2.1. Ubicación y protección del equipo.<br>• 9.2.3. Seguridad del cableado.<br>**10.6. Gestión de la seguridad de las redes:**<br>• 10.6.2. Seguridad en los servicios de red.<br>**10.7. Manipulación de los soportes:**<br>• 10.7.4. Seguridad de la documentación del sistema.<br>**10.10. Monitorización:**<br>• 10.10.1. Registros de auditoría.<br>• 10.10.3. Protección de la información de los registros.<br>• 10.10.4. Registros de administración y operación.<br>• 10.10.5. Registro de fallos.<br>• 10.10.6. Sincronización de reloj.<br>**11.3. Responsabilidades del usuario:**<br>• 11.3.2. Equipo informático de usuario desatendido.<br>• 11.3.3. Política de puesto de trabajo despejado y pantalla limpia. | **7.3 Organización de la seguridad de la información:**<br>• 7.3.2.2 Proceso de autorización de recursos para el tratamiento de la información.<br>**7.6.1 Áreas seguras:**<br>• 7.6.1.3 Áreas de acceso público, entrega y descarga.<br>**7.6.2 Seguridad de los equipos:**<br>• 7.6.2.1 Ubicación y protección del equipo.<br>• 7.6.2.2 Soporte de servicios públicos, seguridad de cableado y mantenimiento de equipos.<br>**7.7.6 Gestión de la seguridad de las redes:**<br>• 7.7.6.2 Seguridad en los servicios de red.<br>**7.7.7 Manipulación de los soportes:**<br>• 7.7.7.4 Seguridad de la documentación del sistema.<br>**7.7.10 Monitorización:**<br>• 7.7.10.2 Registros de auditoría.<br>• 7.7.10.4 Protección de la información de los registros.<br>• 7.7.10.5 Registros de administración y operación.<br>• 7.7.10.6 Registro de fallos.<br>• 7.7.10.7 Sincronización de reloj.<br>**7.8.3 Responsabilidades del usuario:** | E |
| | | | | **11.4. Control de acceso a la red:**<br>• 11.4.3. Identificación de los equipos en las redes.<br>• 11.4.4. Protección a puertos de diagnóstico remoto.<br>**11.5. Control de acceso al sistema operativo:**<br>• 11.5.1. Procedimientos seguros de inicio de sesión.<br>• 11.5.4. Uso de los servicios del sistema.<br>• 11.5.5. Desconexión automática de sesión.<br>• 11.5.6. Limitación del tiempo de conexión.<br>**11.7. Informática móvil y tele trabajo:**<br>• 11.7.1. Ordenadores portátiles y comunicaciones móviles.<br>• 11.7.2. Tele trabajo. | **7.8.4 Control de acceso a la red y control de acceso al sistema operativo:**<br>**7.8.6 Informática móvil y tele trabajo:**<br>• 7.8.6.1. Informática móvil y comunicaciones.<br>• 7.8.6.2 Tele trabajo. | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Entrega, Servicio y Soporte (DSS) | DSS05 | Gestionar los Servicios de Seguridad. | • DSS05.05 Gestionar el acceso físico a los activos de TI. | **13.1 Notificación de eventos y puntos débiles de seguridad de la información:**<br>• 13.1.2. Notificación de puntos débiles de seguridad.<br>**15.2. Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico:**<br>• 15.2.2. Comprobación del cumplimiento técnico.<br>**15.3. Consideraciones sobre las auditorías de los sistemas de información:**<br>• 15.3.2. Protección de las herramientas de auditoría de los sistemas de información. | **7.10.1 Notificación de eventos y puntos débiles de seguridad de la información:**<br>**7.12.3 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico:**<br>**7.12.4 Consideraciones de la auditoría de los sistemas de información en un entorno sanitario:** | E |
| | | | • DSS05.06 Gestionar documentos sensibles y dispositivos de salida. | **10.7. Manipulación de los soportes:**<br>• 10.7.1. Gestión de soportes extraíbles.<br>• 10.7.2. Retirada de soportes.<br>• 10.7.3. Procedimientos de manipulación de la información. | **7.7.7 Manipulación de los soportes:**<br>• 7.7.7.1 Gestión de medios informáticos extraíbles.<br>• 7.7.7.2 Retirada de soportes.<br>• 7.7.7.3 Procedimientos de manipulación de la información. | E |
| | | | • DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad. | **10.10. Monitorización:**<br>• 10.10.2. Supervisión del uso del sistema.<br>• 10.10.3. Protección de la información de los registros<br>• 10.10.4. Registros de administración y operación.<br>**11.6. Control de acceso a las aplicaciones y a la información:**<br>• 11.6.1. Restricción de acceso a la información.<br>**13.1 Notificación de eventos y puntos débiles de seguridad de la información:**<br>• 13.1.2. Notificación de puntos débiles de seguridad.<br>**15.2. Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico:**<br>• 15.2.2. Comprobación del cumplimiento técnico. | **7.7.10 Monitorización:**<br>• 7.7.10.3 Supervisión del uso del sistema.<br>• 7.7.10.4 Protección de la información de los registros.<br>• 7.7.10.5 Registros de administración y operación.<br>**7.8.5 Control de acceso a las aplicaciones y a la información:**<br>• 7.8.5.1 Restricción de acceso a la información.<br>**7.10.1 Notificación de eventos y puntos débiles de seguridad de la información:**<br>**7.12.3 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico:** | E |
| | DSS06 | Gestionar los Controles de los Procesos del Negocio. | • DSS06.01 Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos. | | | |
| | | | • DSS06.02 Controlar el procesamiento de la información. | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Entrega, Servicio y Soporte (DSS) | DSS06 | Gestionar los Controles de los Procesos del Negocio. | • DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización. | **8.2 Durante el empleo:**<br>• 8.2.1 Responsabilidades de la dirección.<br>**6.1 Organización interna:**<br>• 6.1.3 Asignación de las responsabilidades de la seguridad de la información<br>**10.1. Procedimientos y responsabilidades de operación:**<br>• 10.1.3 Segregación de tareas.<br>• 10.1.4. Separación de los recursos de desarrollo, prueba y operación.<br>**12.4. Seguridad de los ficheros del sistema:**<br>• 12.4.3. Control de acceso al código fuente de los programas. | **7.5.2 Durante el empleo:**<br>• 7.5.2.1 Responsabilidades de la Dirección.<br>**7.3.2 Organización interna:**<br>• 7.3.2.1 Compromiso de la administración con la seguridad de la información, la coordinación de seguridad de la información y la asignación de responsabilidades de seguridad de la información.<br>**7.7.1 Procedimientos y responsabilidades de operación:**<br>• 7.7.1.3 Segregación de tareas.<br>• 7.7.1.4 Separación de los recursos de desarrollo, prueba y operación.<br>**7.9.4 Seguridad de los ficheros del sistema:**<br>• 7.9.4.3. Control de acceso al código fuente de los programas. | P |
| | | | • DSS06.04 Gestionar errores y excepciones. | | | |
| | | | • DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información. | **10.10. Monitorización:**<br>• 10.10.1. Registros de auditoría.<br>**12.5. Seguridad en los procesos de desarrollo y soporte:**<br>• 12.5.1. Procedimientos de control de cambios. | **7.7.10 Monitorización:**<br>• 7.7.10.2 Registros de auditoría.<br>**7.9.5 Seguridad en procesos de desarrollo y soporte, y gestión de la vulnerabilidad técnica:** | P |
| | | | • DSS06.06 Asegurar los activos de información. | **7.1 Responsabilidad sobre los activos:**<br>• 7.1.3. Acuerdos sobre el uso aceptable de los activos.<br>**7.2 Clasificación de la información:**<br>• 7.2.1 Directrices de Clasificación.<br>**10.5. Copias de seguridad:**<br>• 10.5.1 Copias de seguridad de la información.<br>**10.6. Gestión de la seguridad de las redes:**<br>• 10.6.1 Controles de red.<br>**10.7. Manipulación de los soportes:**<br>• 10.7.3. Procedimientos de manipulación de la información.<br>**10.8. Intercambio de información:**<br>• 10.8.3 Soportes físicos en tránsito.<br>• 10.8.4 Mensajería electrónica.<br>**12.4. Seguridad de los ficheros del sistema:**<br>• 12.4.2. Protección de los datos de prueba del sistema. | **7.4.1 Responsabilidad sobre los activos de información de salud:**<br>**7.4.2 Clasificación de información de salud:**<br>• 7.4.2.1 Directrices de Clasificación.<br>**7.7.5 Copia de seguridad de la información de salud:**<br>**7.7.6 Gestión de la seguridad de las redes:**<br>• 7.7.6.1 Controles de red.<br>**7.7.7 Manipulación de los soportes:**<br>• 7.7.7.3 Procedimientos de manipulación de la información.<br>**7.7.8 Intercambio de información:**<br>• 7.7.8.2 Soportes físicos en tránsito.<br>• 7.7.8.2 Mensajería electrónica.<br>**7.9.4 Seguridad de los ficheros del sistema:**<br>• 7.9.4.2. Protección de los datos de prueba del sistema. | P |

| | | | | | | |
|---|---|---|---|---|---|---|
| Supervisar, Evaluar y Valorar (MEA) | MEA01 | Supervisar, Evaluar y Valorar el Rendimiento y Conformidad. | • MEA01.01 Establecer un enfoque de la supervisión. | | | |
| | | | • MEA01.02 Establecer los objetivos de cumplimiento y rendimiento. | | | |
| | | | • MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento. | **10.10. Monitorización:**<br>• 10.10.2. Supervisión del uso del sistema.<br>**5.1. Política de seguridad de la información:**<br>• 5.1.2 Revisión de la política de seguridad de la información<br>**6.1 Organización interna:**<br>• 6.1.8 Revisión independiente de la seguridad de la información. | **7.7.10 Monitorización:**<br>• 7.7.10.3 Supervisión del uso del sistema.<br>**7.2 Política de Seguridad de la Información:**<br>• 7.2.2 Revisión del documento de política de seguridad de la información.<br>**7.3.2 Organización interna:**<br>• 7.3.2.4 Contacto con las autoridades, contacto con grupos de intereses especiales y revisión independiente de la seguridad de la información. | P |
| | | | • MEA01.04 Analizar e informar sobre el rendimiento. | | | |
| | | | • MEA01.05 Asegurar la implantación de medidas correctivas. | | | |
| | MEA02 | Supervisar, Evaluar y Valorar el Sistemas de Control Interno. | • MEA02.01 Supervisar el control interno. | **5.1. Política de seguridad de la información:**<br>• 5.1.2 Revisión de la política de seguridad de la información.<br>• 5.1.1 Documento de la Política de Seguridad de la Información.<br>**15.2. Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico:**<br>• 15.2.1 Cumplimiento de políticas y normas de seguridad. | **7.2 Política de Seguridad de la Información:**<br>• 7.2.1 Documento de la Política de Seguridad de la Información.<br>• 7.2.2 Revisión del documento de política de seguridad de la información.<br>**7.12.3 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico:** | P |
| | | | • MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio. | **6.1 Organización interna:**<br>• 6.1.8 Revisión independiente de la seguridad de la información.<br>**15.3. Consideraciones sobre las auditorías de los sistemas de información:**<br>• 15.3.1 Controles de auditoría de los sistemas de información.<br>**10.10. Monitorización:**<br>• 10.10.4 Registros de administración y operación. | **7.3.2 Organización interna:**<br>• 7.3.2.4 Contacto con las autoridades, contacto con grupos de intereses especiales y revisión independiente de la seguridad de la información.<br>**7.12.4 Consideraciones de la auditoría de los sistemas de información en un entorno sanitario:**<br>**7.7.10 Monitorización:**<br>• 7.7.10.5 Registros de administración y operación. | P |
| | | | • MEA02.03 Realizar autoevaluaciones de control. | **15.2. Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico:**<br>• 15.2.2 Comprobación del cumplimiento técnico. | **7.12.3 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico:** | P |
| | | | • MEA02.04 Identificar y comunicar las deficiencias de control. | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Supervisar, Evaluar y Valorar (MEA) | MEA02 | Supervisar, Evaluar y Valorar el Sistemas de Control Interno. | • MEA02.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados. | **15.2. Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico:**<br>• 15.2.1 Cumplimiento de políticas y normas de seguridad.<br>**6.2 Grupos o personas externas:**<br>• 6.2.3. Tratamiento de la seguridad en contratos con terceros.<br>**10.2. Gestión de la provisión de servicios por terceros:**<br>• 10.2.2. Supervisión y revisión de los servicios prestados por terceros.<br>**10.10. Monitorización:**<br>• 10.10.2 Supervisión del uso del sistema. | **7.12.3 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico:**<br>**7.3.3 Grupos o personas externas:**<br>• 7.3.3.3 Tratamiento de la seguridad en contratos con terceros.<br>**7.7.2 Gestión de la provisión de servicios por terceros:**<br>**7.7.10 Monitorización:**<br>• 7.7.10.3 Supervisión del uso del sistema. | P |
| | | | • MEA02.06 Planificar iniciativas de aseguramiento. | | | |
| | | | • MEA02.07 Estudiar las iniciativas de aseguramiento. | | | |
| | | | • MEA02.08 Ejecutar las iniciativas de aseguramiento. | | | |
| | MEA03 | Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos. | • MEA03.01 Identificar requisitos externos de cumplimiento. | **15.1. Cumplimiento de los requisitos legales:**<br>• 15.1.1 Identificación de la legislación aplicable. | **7.12 Conformidad:**<br>• 7.12.2.1 Identificación de la legislación aplicable, derechos de propiedad intelectual (DPI) y protección de los documentos de la organización. | P |
| | | | • MEA03.02 Optimizar la respuesta a requisitos externos. | **15.1. Cumplimiento de los requisitos legales:**<br>• 15.1.2 Derechos de propiedad intelectual (DPI).<br>• 15.1.4. Protección de datos y privacidad de la información de carácter personal. | **7.12.2 Cumplimiento de los requisitos legales:**<br>• 7.12.2.1 Identificación de la legislación aplicable, derechos de propiedad intelectual (DPI) y protección de los documentos de la organización.<br>• 7.12.2.2. Protección de datos y privacidad de la información personal. | P |
| | | | • MEA03.03 Confirmar el cumplimiento de requisitos externos. | **15.1. Cumplimiento de los requisitos legales:**<br>• 15.1.4. Protección de datos y privacidad de la información de carácter personal.<br>• 15.1.6. Regulación de los controles criptográficos. | **7.12.2 Cumplimiento de los requisitos legales:**<br>• 7.12.2.2. Protección de datos y privacidad de la información personal.<br>• 7.12.2.3 Prevención del uso indebido de recursos de tratamiento de la información y Regulación de los controles criptográficos. | P |
| | | | • MEA03.04 Obtener garantía de cumplimiento de requisitos externos. | **6.1 Organización interna:**<br>• 6.1.6 Contacto con las autoridades.<br>**15.1. Cumplimiento de los requisitos legales:**<br>• 15.1.4. Protección de datos y privacidad de la información de carácter personal.<br>• 15.1.6. Regulación de los controles criptográficos. | **7.3.2.3 Acuerdos de confidencialidad:**<br>• 7.3.2.4 Contacto con las autoridades, contacto con grupos de intereses especiales y revisión independiente de la seguridad de la información.<br>**7.12.2 Cumplimiento de los requisitos legales:**<br>• 7.12.2.2. Protección de datos y privacidad de la información personal.<br>• 7.12.2.3 Prevención del uso indebido de recursos de tratamiento de la información y Regulación de los controles criptográficos. | P |

# Anexo 4: Plantillas de documentos

## 1. Acta de Constitución del Proyecto

| Nombre del Proyecto | Siglas del Proyecto |
|---|---|
| | |

| Descripción del proyecto: ¿qué, quién, cómo, cuándo y dónde? |
|---|
| |
| Definición del producto del proyecto: descripción del producto, servicio o capacidad a generar. |
| |
| Definición de requisitos del proyecto: descripción de requerimientos funcionales, no funcionales, de calidad, etc., del proyecto/producto. |
| |
| Objetivos del proyecto: metas hacia las cuales se debe dirigir el trabajo del proyecto en términos de la triple restricción. |

| Concepto | Objetivos |
|---|---|
| 1. Alcance | |
| 2. Tiempo | |
| 3. Costo | |

| Finalidad del proyecto: fin último, propósito general, u objetivo de nivel superior por el cual se ejecuta el Proyecto. Enlace con programas, portafolios, o estrategias de la organización. |
|---|
| |
| Justificación del proyecto: motivos, razones, o argumentos que justifican la ejecución del Proyecto. |
| |

| Designación del Director del Proyecto. | | |
|---|---|---|
| Nombre: | | Niveles de autoridad: |
| Reporta a: | | |
| Supervisa a: | | |

| Principales amenazas del Proyecto (riesgos negativos). |
|---|
| |
| Principales oportunidades del Proyecto (riesgos positivos). |
| |

| Sponsor que autoriza el Proyecto. | | | |
|---|---|---|---|
| Nombre: | Empresa / Organización: | Cargo: | Fecha: |
| | | | |

## 2. Plan de Gestión del Cronograma

| Nombre del Proyecto | Siglas del Proyecto |
|---|---|
| | |
| Definir el cronograma del Proyecto: | |
| | |

## 3. Plan de Gestión de los Recursos Humanos

| Nombre del Proyecto | Siglas del Proyecto |
|---|---|
| | |
| Organigrama del Proyecto: especificar el organigrama del proyecto. | |
| | |
| Roles y responsabilidades: especificar la matriz de asignaciones de responsabilidades. | |
| | |
| Capacitación, entrenamiento, tutoría requerido: | |
| | |
| Cumplimiento de regulaciones, pactos, y políticas: | |
| | |

## 4. Plan de Gestión de los Costos

| Nombre del Proyecto | Siglas del Proyecto |
|---|---|
| | |
| Consideraciones: | |
| | |
| Costos de implementación del Proyecto | |
| | |

## 5. Plan de Gestión de las Comunicaciones

| Nombre del Proyecto | Siglas del Proyecto |
|---|---|
| | |
| Procedimiento para tratar polémicas: defina el procedimiento para procesar y resolver las polémicas, especificando la forma de capturarlas y registrarlas, el modo en que se abordará su tratamiento y resolución. | |
| | |
| Guías para eventos de comunicación: defina guía para reuniones, conferencias, correo electrónico, etc. | |
| | |

## 6. Plan de Gestión de los Riesgos

| Nombre del Proyecto | Siglas del Proyecto |
|---|---|
| | |
| Identificación y descripción de las posibles amenazas que podrían afectar a la ejecución del Proyecto. | |
| | |
| Análisis cualitativo los riesgos | |
| | |
| Plan de Contingencia. | |
| | |

## 7. Acta de Cierre del Proyecto

| Nombre del Proyecto | Siglas del Proyecto |
|---|---|
| | |
| Descripción de entregables concluidos: | |
| | |
| Declaración de la aceptación formal: | |
| | |
| Observaciones adicionales: | |
| | |
| Plan de Contingencia: | |
| | |
| Aceptado por: | |
| Nombre del cliente, sponsor u otro funcionario. | Fecha: |
| | |

## Anexo 5: Encuesta de evaluación de procesos

Se detallan las preguntas de la encuesta que nos permita identificar el estado actual de los procesos.

1. **EDM01 - Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno.**

a) ¿En qué nivel existe en el Hospital un modelo óptimo en toma de decisiones para TI?

b) ¿En qué nivel se han definido, asignado y aceptado los roles y responsabilidades, para los responsables de la gestión del negocio y de las TI en el Hospital?

c) ¿En qué nivel se supervisa que esté operando de forma efectiva, el sistema de gobierno y los mecanismos implementados (incluyendo estructuras, principios y procesos) en el Hospital?

2. **APO01 - Gestionar el Marco de Gestión de TI**

a) ¿En qué nivel se han definido e implantado de manera eficaz las políticas relativas a TI en el Hospital que permita cumplir los requisitos del Gobierno Corporativo?

b) ¿En qué nivel usted tiene conocimiento de las políticas relativas a TI y de cómo deberían implementarse en el Hospital?

3. **APO07 - Gestionar los Recursos Humanos**

a) ¿En qué nivel la estructura organizacional del Hospital y las relaciones de TI son flexibles y dan respuesta ágil a las necesidades del negocio y de TI?

b) ¿En qué nivel los recursos humanos del Hospital son gestionados eficaz y eficientemente?

4. **APO09 - Gestionar los Acuerdos de Servicios**

a) ¿En qué nivel los procesos agregadores de valor del Hospital tienen ya definido su Acuerdo de Nivel de Servicio (SLA)?

b) ¿En qué nivel los servicios provistos por TI cumplen con las expectativas y necesidades del negocio?

c) ¿En qué nivel los servicios provistos por TI alcanzan su objetivo?

5. **APO12 - Gestionar los Riesgos**

a) ¿En qué nivel usted considera que el riesgo relacionado con TI está identificado, analizado, gestionado y reportado dentro de los procesos del Hospital?

b) ¿En qué nivel se realiza un análisis de riesgos e informes del perfil de riesgos para la Gerencia del Hospital?

c) ¿En qué nivel las acciones de gestión para los riesgos significativos de TI están gestionadas y bajo control?

d) ¿En qué nivel las acciones diseñadas para gestionar los riesgos de TI, han sido implementadas y ejecutadas en el Hospital?

6. **APO13 - Gestionar la Seguridad**

a) ¿En qué nivel se encuentran definidos y comunicados los roles y las responsabilidades de la gestión de la Seguridad de la Información en el Hospital?

b) ¿En qué nivel usted considera que las soluciones de seguridad y prácticas de gestión actuales del Hospital, son apropiadas y óptimas para gestionar los riesgos identificados de seguridad de información?

c) ¿En qué nivel usted considera que las soluciones de Seguridad de la Información ofrecidas por TI, están implementadas y operadas de forma consistente en todo el Hospital?

7. **BAI02 - Gestionar la Definición de Requisitos**

a) ¿En qué nivel los requerimientos funcionales y técnicos de los procesos agregadores de valor reflejan las necesidades y expectativas del Hospital?

b) ¿En qué nivel las soluciones de TI satisfacen los requerimientos funcionales y técnicos de la Gerencia del Hospital?

c) ¿En qué nivel el riesgo asociado con los requerimientos funcionales y técnicos ha sido tomado en cuenta en la solución propuesta?

d) ¿En qué nivel los requerimientos y soluciones propuestas por TI cumplen con los objetivos del Hospital?

8. **DSS04 - Gestionar la Continuidad**

a) ¿En qué nivel los de servicios de TI cumplen con los niveles de servicio mínimos requeridos?
b) ¿Qué nivel de resiliencia (capacidad para recuperarse de una interrupción significativa) considera usted que se encuentran los servicios de TI críticos del Hospital?
c) ¿Entre la escala propuesta, con qué frecuencia usted considera que se realiza pruebas de continuidad a un servicio de TI?
d) ¿En qué nivel se consideran los requisitos del negocio actuales, dentro de los procedimientos y actividades que permiten mantener la disponibilidad de un servicio ante una interrupción significativa?
e) ¿En qué nivel se desarrolla las competencias y habilidades de las partes interesadas, para el proceso de mantener la disponibilidad de un servicio ante un evento de interrupción significativa?

**9. DSS05 - Gestionar los Servicios de Seguridad**

a) ¿En qué nivel la seguridad de las redes y las comunicaciones cumple con las necesidades del negocio?
b) ¿En qué nivel la información procesada, almacenada y transmitida en los dispositivos de usuario final está protegida?
c) ¿En qué nivel los usuarios de TI del Hospital, están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio?
d) ¿En qué nivel se han implantado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida en el Hospital?
e) ¿En qué nivel la información electrónica del Hospital tiene las medidas de seguridad apropiadas mientras es almacenada, transmitida o destruida?

# Anexo 6: Evaluación del Nivel de Capacidad de los Procesos del Hospital General Docente de Calderón

| EDM01 - Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Propósito:** | Proporcionar un enfoque consistente, integrado y alineado con el alcance del gobierno de la empresa. Para garantizar que las decisiones relativas a TI se han adoptado en línea con las estrategias y objetivos de la empresa, garantizando la supervisión de los procesos de manera efectiva y transparentemente, el cumplimiento con los requerimientos regulatorios y legales y que se han alcanzado los requerimientos de gobierno de los miembros del Consejo de Administración. | | | | | | | | |
| **Nivel** | **Evaluar si los siguientes resultados son alcanzados** | **Criterios** | **Los criterios se cumplen S/N** | **Comentarios** | **N (%)** | **P (%)** | **L (%)** | **F (%)** | **Valor (%)** |
| Nivel 0 Incompleto | El proceso no está implantado o no alcanza sus objetivos. | En este nivel, hay poca o ninguna evidencia de cualquier logro o del propósito del proceso. | | El proceso se encuentra definido. | | | | | 0 |
| Nivel 1 Realizado | PA 1.1 Rendimiento del proceso - El proceso implementado alcanza su propósito de proceso. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | EDM01-01 Modelo estratégico de toma de decisiones para que las TI sean efectivas y estén alineadas con el entorno externo e interno de la empresa y los requerimientos de las partes interesadas. | N | Existen encuestas del nivel de satisfacción de las partes interesadas por la gestión de TI dentro del hospital, pero las mismas no son realizadas y revisadas con la frecuencia requerida. | | 19 | | | 20 |
| | | EDM01-02 Garantizar que el sistema de gobierno para TI está incorporado al gobierno corporativo. | N | Existe el registros de casos de no cumplimiento de las directrices de comportamiento ético y no profesional. | | 20 | | | |
| | | EDM01-03 Obtener garantías de que el sistema de gobierno para TI está operando de manera efectiva. | N | Existe informes de buenas practicas de TI, al comité de gestión y gerencia del Hospital. | | 21 | | | |
| Nivel 2 Gestionado | PA 2.1 Gestión de rendimiento - Una medida del nivel de gestión del proceso. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | a) Los objetivos para el desempeño del proceso se identifican.<br>b) El rendimiento del proceso está planificado y monitoreado.<br>c) El Rendimiento del proceso se ajusta para cumplir con los planes.<br>d) Las responsabilidades y autoridades para la realización del procedimiento están definidos, asignados y comunicados.<br>e) Los recursos e información necesaria para realizar el proceso se identifican, son puestas a disposición, y son asignados y utilizados.<br>f) Las interfaces entre las partes involucradas son manejadas para garantizar la efectiva comunicación y una clara asignación de responsabilidades. | N | | 0 | | | | 0 |
| | PA 2.2 Gestión del producto de trabajo - Medida del grado en que los productos del proceso son gestionados. apropiadamente. Los productos de trabajo (o salidas del proceso) se definen y controlan. | Como resultado de la plena realización este atributo se obtiene: | | | | | | | |
| | | a) Los requisitos para los productos de trabajo del proceso se definen.<br>b) Los requisitos para la documentación y el control de los productos de trabajo se definen.<br>c) Los productos de trabajo son adecuadamente identificados, documentados y controlados.<br>d) Los productos de trabajo se revisan de acuerdo con lo planificado y se ajustan según sea necesario para satisfacer los requisitos. | N | | 0 | | | | 0 |
| Nivel 3 Establecido | PA 3.1 Definición del proceso - Una medida del grado en que se mantiene un proceso estándar para apoyar el despliegue del proceso definido. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | a) Un proceso estándar, incluyendo guías de adaptación adecuadas, es definido tanto que describe los elementos fundamentales que deben ser incorporados en un proceso definido.<br>b) Se determina la secuencia y la interacción del proceso estándar con otros procesos.<br>c) Competencias requeridas y las funciones para llevar a cabo un proceso se identifican como parte del proceso estándar.<br>d) La infraestructura necesaria y ambiente de trabajo para la realización de un proceso se identifican como parte del proceso estándar.<br>e) Se determinan los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso. | N | | 0 | | | | 0 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Nivel 3 Establecido | PA 3.2 Despliegue del proceso - Una medida en que el proceso estándar se implementa eficazmente como un proceso definido para lograr sus resultados del proceso | Como resultado de la plena realización de este atributo:<br>a) Un proceso definido es implementado basado en un apropiadamente seleccionado y adaptado proceso estándar.<br>b) Roles, responsabilidades y autoridades requeridas para llevar a cabo el proceso definido son asignados y comunicados<br>c) El personal que realiza la definición del proceso es competente sobre las bases de educación, formación y experiencia.<br>d) Los recursos necesarios y la información necesaria para realizar el de finido el proceso se hacen disponibles, asignados y utilizado.<br>e) La infraestructura requerida y el ambiente de trabajo para llevar a cabo el definido proceso se ponen a disposición, y son manejados y mantenidos.<br>f) Los datos apropiados son recogidos y analizados como base para la comprensión del comportamiento, y para demostrar la idoneidad y la eficacia del proceso, y para evaluar dónde se puede realizar la mejora continua del proceso. | N | | 0 | | | | 0 |
| Nivel 4 Predecible | PA 4.1 Medición de procesos - Una medida del grado en que los resultados de medición se utilizan para asegurar que el rendimiento del proceso apoya el logro de los objetivos de rendimiento de los procesos pertinentes en apoyo de los objetivos de negocio definidos. | Como resultado de la plena realización de este atributo:<br>Como resultado de la plena realización de este atributo:<br>a) Información sobre el proceso necesario para apoyar a los objetivos empresariales definidos relevantes son establecidos.<br>b) Objetivos de medición de proceso son derivado de las necesidades de información de proceso.<br>c) Los objetivos cuantitativos para el proceso de actuación en apoyo de la correspondiente se establecen los objetivos de negocio.<br>d) Las medidas y la frecuencia de la medición se identifican y se definen de acuerdo con objetivos y medición de procesos objetivos cuantitativos para el proceso de rendimiento.<br>e) Los resultados de la medición son recogidos, analizados y reportados para supervisar la medida en que los objetivos cuantitativos de rendimiento de los procesos se cumplan.<br>f) Los resultados de medición se utilizan para caracterizar el rendimiento del proceso. | N | | 0 | | | | 0 |
| | PA 4.2 Control de procesos - Una medida de la medida en que el proceso es gestionado cuantitativamente para producir un proceso que es estable, capaz y predecible dentro de límites definidos. | Como resultado de la plena realización de este atributo:<br>a) Técnicas de análisis y control son determinada y aplicada en su caso.<br>b) Se establecen límites de control de la variación para el rendimiento normal de proceso.<br>c) Los datos de medición se analizan para determinar causas especiales de variación.<br>d) Se tomen las medidas correctivas para hacer frente a causas especiales de variación.<br>e) Los límites de control se restablecen (como es necesario) después de la acción correctiva. | N | | 0 | | | | 0 |
| Nivel 5 Optimizado | PA 5.1 Innovación del proceso - Una medida del grado en que los cambios en el proceso son identificados a partir del análisis de las causas comunes de variación en el rendimiento, ya partir de las investigaciones de enfoques innovadores para la definición e implementación del proceso. | Como resultado de la plena realización de este atributo:<br>a) Objetivos de mejora de procesos para el proceso que se definen compatible con los objetivos de negocio relevantes.<br>b) Los datos apropiados se analizan para identificar causas comunes de las variaciones en el proceso de rendimiento.<br>c) Los datos apropiados se analizan para identificar oportunidades para las mejores prácticas e innovación.<br>d) Oportunidades de mejora derivados de nuevas tecnologías y conceptos de proceso se identifican.<br>e) Una estrategia de implementación es establecido para lograr el proceso objetivos de mejora. | N | | 0 | | | | 0 |
| | PA 5.2 Proceso Optimizado - Una medida del grado en que los cambios en la definición, gestión y ejecución del resultado del proceso de impacto efectivo que logre los objetivos de mejora de procesos pertinentes. | Como resultado de la plena realización de este atributo:<br>a) Impacto de los cambios propuestos es evaluado contra los objetivos del proceso definido y el proceso estándar.<br>b) La aplicación de todos los cambios acordados es manejado para asegurar ninguna interrupción en el rendimiento del proceso entendido y actuado.<br>c) La eficacia de los cambios en los procesos se evalúa basándose en el rendimiento real en contra de los requisitos de los productos definidos y los objetivos del proceso para determinar si los resultados son comunes o causas especiales. | N | | 0 | | | | 0 |

| APO01 - Gestionar el Marco de Gestión de TI | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Propósito:** | Proveer un enfoque de gestión consistente para permitir que los requerimientos de gobierno de la empresa sean conocidos, cubriendo procesos de gestión, estructuras organizacionales, roles y responsabilidades, actividades seguras y repetibles, habilidades y competencias. | | | | | | | | |
| **Nivel** | **Evaluar si los siguientes resultados son** | **Criterios** | **Los criterios se cumplen S/N** | **Comentarios** | **N (%)** | **P (%)** | **L (%)** | **F (%)** | **Valor (%)** |
| Nivel 0 Incompleto | El proceso no está implantado o no alcanza sus objetivos. | En este nivel, hay poca o ninguna evidencia de cualquier logro o del propósito del proceso. | N | | | | | | 0 |
| Nivel 1 Realizado | PA 1.1 Rendimiento del proceso - El proceso implementado alcanza su propósito de proceso. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | APO01-01 Se ha definido y se mantiene un conjunto eficaz de políticas. | N | Existe cierta documentación con políticas y buenas practicas internas de cada área de gestión del hospital, sin embargo no están actualizados e implementados en su totalidad. | | 30 | | | 31 |
| | | APO01-02 Todos tienen conocimiento de las políticas y de cómo deberían implementarse. | N | Se realizan sesiones de formación o sensibilización exclusivas para el personal que se encuentra dentro de cada área de gestión. | | 32 | | | |
| Nivel 2 Gestionado | PA 2.1 Gestión de rendimiento - Una medida del nivel de gestión del proceso. | Como resultado de la plena realización de este atributo:<br>a) Los objetivos para el desempeño del proceso se identifican.<br>b) El rendimiento del proceso está planificado y monitoreado.<br>c) El Rendimiento del proceso se ajusta para cumplir con los planes.<br>d) Las responsabilidades y autoridades para la realización del procedimiento están definidos, asignados y comunicados.<br>e) Los recursos e información necesaria para realizar el proceso se identifican, son puestas a disposición, y son asignados y utilizados.<br>f) Las interfaces entre las partes involucradas son manejadas para garantizar la efectiva comunicación y una clara asignación de responsabilidades. | N | | | | | | 0 |
| | PA 2.2 Gestión del producto de trabajo - Medida del grado en que los productos del proceso son gestionados. apropiadamente. Los productos (o salidas del proceso) se definen y controlan. | Como resultado de la plena realización este atributo se obtiene:<br>a) Los requisitos para los productos de trabajo del proceso se definen.<br>b) Los requisitos para la documentación y el control de los productos de trabajo se definen.<br>c) Los productos de trabajo son adecuadamente identificados, documentados y controlados.<br>d) Los productos de trabajo se revisan de acuerdo con lo planificado y se ajustan según sea necesario para satisfacer los requisitos. | N | | | | | | 0 |
| Nivel 3 Establecido | PA 3.1 Definición del proceso - Una medida del grado en que se mantiene un proceso estándar para apoyar el despliegue del proceso definido. | Como resultado de la plena realización de este atributo:<br>a) Un proceso estándar, incluyendo guías de adaptación adecuadas, es definido tanto que describe los elementos fundamentales que deben ser incorporados en un proceso definido.<br>b) Se determina la secuencia y la interacción del proceso estándar con otros procesos.<br>c) Competencias requeridas y las funciones para llevar a cabo un proceso se identifican como parte del proceso estándar.<br>d) La infraestructura necesaria y ambiente de trabajo para la realización de un proceso se identifican como parte del proceso estándar.<br>e) Se determinan los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso. | N | | | | | | 0 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Nivel 3 Establecido | PA 3.2 Despliegue del proceso - Una medida en que el proceso estándar se implementa eficazmente como un proceso definido para lograr sus resultados del proceso | Como resultado de la plena realización de este atributo:<br>a) Un proceso definido es implementado basado en un apropiadamente seleccionado y adaptado proceso estándar.<br>b) Roles, responsabilidades y autoridades requeridas para llevar a cabo el proceso definido son asignados y comunicados<br>c) El personal que realiza la definición del proceso es competente sobre las bases de educación, formación y experiencia.<br>d) Los recursos necesarios y la información necesaria para realizar el de finido el proceso se hacen disponibles, asignados y utilizado.<br>e) La infraestructura requerida y el ambiente de trabajo para llevar a cabo el definido proceso se ponen a disposición, y son manejados y mantenidos.<br>f) Los datos apropiados son recogidos y analizados como base para la comprensión del comportamiento, y para demostrar la idoneidad y la eficacia del proceso, y para evaluar dónde se puede realizar la mejora continua del proceso. | N | | | | | | 0 |
| Nivel 4 Predecible | PA 4.1 Medición de procesos - Una medida del grado en que los resultados de medición se utilizan para asegurar que el rendimiento del proceso apoya el logro de los objetivos de rendimiento de los procesos pertinentes en apoyo de los objetivos de negocio definidos. | Como resultado de la plena realización de este atributo:<br>Como resultado de la plena realización de este atributo:<br>a) Información sobre el proceso necesario para apoyar a los objetivos empresariales definidos relevantes son establecidos.<br>b) Objetivos de medición de proceso son derivado de las necesidades de información de proceso.<br>c) Los objetivos cuantitativos para el proceso de actuación en apoyo de la correspondiente se establecen los objetivos de negocio.<br>d) Las medidas y la frecuencia de la medición se identifican y se definen de acuerdo con objetivos y medición de procesos objetivos cuantitativos para el proceso de rendimiento.<br>e) Los resultados de la medición son recogidos, analizados y reportados para supervisar la medida en que los objetivos cuantitativos de rendimiento de los procesos se cumplan.<br>f) Los resultados de medición se utilizan para caracterizar el rendimiento del proceso. | N | | | | | | 0 |
| | PA 4.2 Control de procesos - Una medida de la medida en que el proceso es gestionado cuantitativamente para producir un proceso que es estable, capaz y predecible dentro de límites definidos. | Como resultado de la plena realización de este atributo:<br>a) Técnicas de análisis y control son determinada y aplicada en su caso.<br>b) Se establecen límites de control de la variación para el rendimiento normal de proceso.<br>c) Los datos de medición se analizan para determinar causas especiales de variación.<br>d) Se tomen las medidas correctivas para hacer frente a causas especiales de variación.<br>e) Los límites de control se restablecen (como es necesario) después de la acción correctiva. | N | | | | | | 0 |
| Nivel 5 Optimizado | PA 5.1 Innovación del proceso - Una medida del grado en que los cambios en el proceso son identificados a partir del análisis de las causas comunes de variación en el rendimiento, ya partir de las investigaciones de enfoques innovadores para la definición e implementación del proceso. | Como resultado de la plena realización de este atributo:<br>a) Objetivos de mejora de procesos para el proceso que se definen compatible con los objetivos de negocio relevantes.<br>b) Los datos apropiados se analizan para identificar causas comunes de las variaciones en el proceso de rendimiento.<br>c) Los datos apropiados se analizan para identificar oportunidades para las mejores prácticas e innovación.<br>d) Oportunidades de mejora derivados de nuevas tecnologías y conceptos de proceso se identifican.<br>e) Una estrategia de implementación es establecido para lograr el proceso objetivos de mejora. | N | | | | | | 0 |
| | PA 5.2 Proceso Optimizado - Una medida del grado en que los cambios en la definición, gestión y ejecución del resultado del proceso de impacto efectivo que logre los objetivos de mejora de procesos pertinentes. | Como resultado de la plena realización de este atributo:<br>a) Impacto de los cambios propuestos es evaluado contra los objetivos del proceso definido y el proceso estándar.<br>b) La aplicación de todos los cambios acordados es manejado para asegurar ninguna interrupción en el rendimiento del proceso entendido y actuado.<br>c) La eficacia de los cambios en los procesos se evalúa basándose en el rendimiento real en contra de los requisitos de los productos definidos y los objetivos del proceso para determinar si los resultados son comunes o causas especiales. | N | | | | | | 0 |

| APO07 - Gestionar los Recursos Humanos | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Propósito:** | Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa. | | | | | | | | |
| **Nivel** | **Evaluar si los siguientes resultados son** | **Criterios** | **Los criterios se cumplen S/N** | **Comentarios** | **N (%)** | **P (%)** | **L (%)** | **F (%)** | **Valor (%)** |
| Nivel 0 Incompleto | El proceso no está implantado o no alcanza sus objetivos. | En este nivel, hay poca o ninguna evidencia de cualquier logro o del propósito del proceso. | N | | | | | | 0 |
| Nivel 1 Realizado | PA 1.1 Rendimiento del proceso - El proceso implementado alcanza su propósito de proceso. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | APO07-01 La estructura organizacional y las relaciones de TI son flexibles y dan respuesta ágil. | N | Existe una referencia de catálogo de servicios que provee TI al hospital y registros de incidentes que no pudieron resolverse dentro de las estructuras de gestión y se escalaron a las estructuras de gobierno | | 34 | | | 36 |
| | | APO 07-02 Los recursos humanos son gestionados eficaz y eficientemente. | N | Existe registros y estadísticas de la alta rotación de personal médico y administrativo del hospital. | | 38 | | | |
| Nivel 2 Gestionado | PA 2.1 Gestión de rendimiento - Una medida del nivel de gestión del proceso. | Como resultado de la plena realización de este atributo:<br>a) Los objetivos para el desempeño del proceso se identifican.<br>b) El rendimiento del proceso está planificado y monitoreado.<br>c) El Rendimiento del proceso se ajusta para cumplir con los planes.<br>d) Las responsabilidades y autoridades para la realización del procedimiento están definidos, asignados y comunicados.<br>e) Los recursos e información necesaria para realizar el proceso se identifican, son puestas a disposición, y son asignados y utilizados.<br>f) Las interfaces entre las partes involucradas son manejadas para garantizar la efectiva comunicación y una clara asignación de responsabilidades. | N | | | | | | 0 |
| | PA 2.2 Gestión del producto de trabajo - Medida del grado en que los productos del proceso son gestionados. apropiadamente. Los productos (o salidas del proceso) se definen y controlan. | Como resultado de la plena realización este atributo se obtiene:<br>a) Los requisitos para los productos de trabajo del proceso se definen.<br>b) Los requisitos para la documentación y el control de los productos de trabajo se definen.<br>c) Los productos de trabajo son adecuadamente identificados, documentados y controlados.<br>d) Los productos de trabajo se revisan de acuerdo con lo planificado y se ajustan según sea necesario para satisfacer los requisitos. | N | | | | | | 0 |
| Nivel 3 Establecido | PA 3.1 Definición del proceso - Una medida del grado en que se mantiene un proceso estándar para apoyar el despliegue del proceso definido. | Como resultado de la plena realización de este atributo:<br>a) Un proceso estándar, incluyendo guías de adaptación adecuadas, es definido tanto que describe los elementos fundamentales que deben ser incorporados en un proceso definido.<br>b) Se determina la secuencia y la interacción del proceso estándar con otros procesos.<br>c) Competencias requeridas y las funciones para llevar a cabo un proceso se identifican como parte del proceso estándar.<br>d) La infraestructura necesaria y ambiente de trabajo para la realización de un proceso se identifican como parte del proceso estándar.<br>e) Se determinan los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso. | N | | | | | | 0 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Nivel 3 Establecido | PA 3.2 Despliegue del proceso - Una medida en que el proceso estándar se implementa eficazmente como un proceso definido para lograr sus resultados del proceso | Como resultado de la plena realización de este atributo:<br>a) Un proceso definido es implementado basado en un apropiadamente seleccionado y adaptado proceso estándar.<br>b) Roles, responsabilidades y autoridades requeridas para llevar a cabo el proceso definido son asignados y comunicados<br>c) El personal que realiza la definición del proceso es competente sobre las bases de educación, formación y experiencia.<br>d) Los recursos necesarios y la información necesaria para realizar el de finido el proceso se hacen disponibles, asignados y utilizado.<br>e) La infraestructura requerida y el ambiente de trabajo para llevar a cabo el definido proceso se ponen a disposición, y son manejados y mantenidos.<br>f) Los datos apropiados son recogidos y analizados como base para la comprensión del comportamiento, y para demostrar la idoneidad y la eficacia del proceso, y para evaluar dónde se puede realizar la mejora continua del proceso. | N | | | | | | 0 |
| Nivel 4 Predecible | PA 4.1 Medición de procesos - Una medida del grado en que los resultados de medición se utilizan para asegurar que el rendimiento del proceso apoya el logro de los objetivos de rendimiento de los procesos pertinentes en apoyo de los objetivos de negocio definidos. | Como resultado de la plena realización de este atributo:<br>Como resultado de la plena realización de este atributo:<br>a) Información sobre el proceso necesario para apoyar a los objetivos empresariales definidos relevantes son establecidos.<br>b) Objetivos de medición de proceso son derivado de las necesidades de información de proceso.<br>c) Los objetivos cuantitativos para el proceso de actuación en apoyo de la correspondiente se establecen los objetivos de negocio.<br>d) Las medidas y la frecuencia de la medición se identifican y se definen de acuerdo con objetivos y medición de procesos objetivos cuantitativos para el proceso de rendimiento.<br>e) Los resultados de la medición son recogidos, analizados y reportados para supervisar la medida en que los objetivos cuantitativos de rendimiento de los procesos se cumplan.<br>f) Los resultados de medición se utilizan para caracterizar el rendimiento del proceso. | N | | | | | | 0 |
| | PA 4.2 Control de procesos - Una medida de la medida en que el proceso es gestionado cuantitativamente para producir un proceso que es estable, capaz y predecible dentro de límites definidos. | Como resultado de la plena realización de este atributo:<br>a) Técnicas de análisis y control son determinada y aplicada en su caso.<br>b) Se establecen límites de control de la variación para el rendimiento normal de proceso.<br>c) Los datos de medición se analizan para determinar causas especiales de variación.<br>d) Se tomen las medidas correctivas para hacer frente a causas especiales de variación.<br>e) Los límites de control se restablecen (como es necesario) después de la acción correctiva. | N | | | | | | 0 |
| Nivel 5 Optimizado | PA 5.1 Innovación del proceso - Una medida del grado en que los cambios en el proceso son identificados a partir del análisis de las causas comunes de variación en el rendimiento, ya partir de las investigaciones de enfoques innovadores para la definición e implementación del proceso. | Como resultado de la plena realización de este atributo:<br>a) Objetivos de mejora de procesos para el proceso que se definen compatible con los objetivos de negocio relevantes.<br>b) Los datos apropiados se analizan para identificar causas comunes de las variaciones en el proceso de rendimiento.<br>c) Los datos apropiados se analizan para identificar oportunidades para las mejores prácticas e innovación.<br>d) Oportunidades de mejora derivados de nuevas tecnologías y conceptos de proceso se identifican.<br>e) Una estrategia de implementación es establecido para lograr el proceso objetivos de mejora. | N | | | | | | 0 |
| | PA 5.2 Proceso Optimizado - Una medida del grado en que los cambios en la definición, gestión y ejecución del resultado del proceso de impacto efectivo que logre los objetivos de mejora de procesos pertinentes. | Como resultado de la plena realización de este atributo:<br>a) Impacto de los cambios propuestos es evaluado contra los objetivos del proceso definido y el proceso estándar.<br>b) La aplicación de todos los cambios acordados es manejado para asegurar ninguna interrupción en el rendimiento del proceso entendido y actuado.<br>c) La eficacia de los cambios en los procesos se evalúa basándose en el rendimiento real en contra de los requisitos de los productos definidos y los objetivos del proceso para determinar si los resultados son comunes o causas especiales. | N | | | | | | 0 |

| APO09 - Gestionar los Acuerdos de Servicios | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Propósito:** | Asegurar que los servicios TI y los niveles de servicio cubren las necesidades presentes y futuras de la empresa. | | | | | | | | |
| **Nivel** | **Evaluar si los siguientes resultados son** | **Criterios** | **Los criterios se cumplen S/N** | **Comentarios** | **N (%)** | **P (%)** | **L (%)** | **F (%)** | **Valor (%)** |
| Nivel 0 Incompleto | El proceso no está implantado o no alcanza sus objetivos. | En este nivel, hay poca o ninguna evidencia de cualquier logro o del propósito del proceso. | N | | | | | | 0 |
| Nivel 1 Realizado | PA 1.1 Rendimiento del proceso - El proceso implementado alcanza su propósito de proceso. | Como resultado de la plena realización de este atributo: | | | | | | | 35,66 |
| | | APO09-01 La empresa puede utilizar efectivamente los servicios de TI tal como se han definido en el catálogo. | N | Existen servicios de TI, que todavía no tienen definidos completamente los acuerdos de nivel de servicio. | | 34 | | | |
| | | APO09-02 Los acuerdos de servicios reflejan las necesidades de la empresa y las capacidades de TI. | N | Existen servicios de TI, que todavía no tienen definidos completamente los acuerdos de nivel de servicio. | | 33 | | | |
| | | APO09-03 Los servicios TI rinden como está estipulado en los acuerdos de servicio. | N | Existen informes de monitoreo de los servicios de TI, como también el registros de sanciones por incumplimiento o denegación del servicio. | | 40 | | | |
| Nivel 2 Gestionado | PA 2.1 Gestión de rendimiento - Una medida del nivel de gestión del proceso. | Como resultado de la plena realización de este atributo: | | | | | | | 0 |
| | | a) Los objetivos para el desempeño del proceso se identifican.<br>b) El rendimiento del proceso está planificado y monitoreado.<br>c) El Rendimiento del proceso se ajusta para cumplir con los planes.<br>d) Las responsabilidades y autoridades para la realización del procedimiento están definidos, asignados y comunicados.<br>e) Los recursos e información necesaria para realizar el proceso se identifican, son puestas a disposición, y son asignados y utilizados.<br>f) Las interfaces entre las partes involucradas son manejadas para garantizar la efectiva comunicación y una clara asignación de responsabilidades. | N | | | | | | | |
| | PA 2.2 Gestión del producto de trabajo - Medida del grado en que los productos del proceso son gestionados. apropiadamente. Los productos (o salidas del proceso) se definen y controlan. | Como resultado de la plena realización este atributo se obtiene: | | | | | | | 0 |
| | | a) Los requisitos para los productos de trabajo del proceso se definen.<br>b) Los requisitos para la documentación y el control de los productos de trabajo se definen.<br>c) Los productos de trabajo son adecuadamente identificados, documentados y controlados.<br>d) Los productos de trabajo se revisan de acuerdo con lo planificado y se ajustan según sea necesario para satisfacer los requisitos. | N | | | | | | | |
| Nivel 3 Establecido | PA 3.1 Definición del proceso - Una medida del grado en que se mantiene un proceso estándar para apoyar el despliegue del proceso definido. | Como resultado de la plena realización de este atributo: | | | | | | | 0 |
| | | a) Un proceso estándar, incluyendo guías de adaptación adecuadas, es definido tanto que describe los elementos fundamentales que deben ser incorporados en un proceso definido.<br>b) Se determina la secuencia y la interacción del proceso estándar con otros procesos.<br>c) Competencias requeridas y las funciones para llevar a cabo un proceso se identifican como parte del proceso estándar.<br>d) La infraestructura necesaria y ambiente de trabajo para la realización de un proceso se identifican como parte del proceso estándar.<br>e) Se determinan los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso. | N | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Nivel 3 Establecido | PA 3.2 Despliegue del proceso - Una medida en que el proceso estándar se implementa eficazmente como un proceso definido para lograr sus resultados del proceso | Como resultado de la plena realización de este atributo:<br>a) Un proceso definido es implementado basado en un apropiadamente seleccionado y adaptado proceso estándar.<br>b) Roles, responsabilidades y autoridades requeridas para llevar a cabo el proceso definido son asignados y comunicados<br>c) El personal que realiza la definición del proceso es competente sobre las bases de educación, formación y experiencia.<br>d) Los recursos necesarios y la información necesaria para realizar el de finido el proceso se hacen disponibles, asignados y utilizado.<br>e) La infraestructura requerida y el ambiente de trabajo para llevar a cabo el definido proceso se ponen a disposición, y son manejados y mantenidos.<br>f) Los datos apropiados son recogidos y analizados como base para la comprensión del comportamiento, y para demostrar la idoneidad y la eficacia del proceso, y para evaluar dónde se puede realizar la mejora continua del proceso. | N | | | | | | 0 |
| Nivel 4 Predecible | PA 4.1 Medición de procesos - Una medida del grado en que los resultados de medición se utilizan para asegurar que el rendimiento del proceso apoya el logro de los objetivos de rendimiento de los procesos pertinentes en apoyo de los objetivos de negocio definidos. | Como resultado de la plena realización de este atributo:<br>Como resultado de la plena realización de este atributo:<br>a) Información sobre el proceso necesario para apoyar a los objetivos empresariales definidos relevantes son establecidos.<br>b) Objetivos de medición de proceso son derivado de las necesidades de información de proceso.<br>c) Los objetivos cuantitativos para el proceso de actuación en apoyo de la correspondiente se establecen los objetivos de negocio.<br>d) Las medidas y la frecuencia de la medición se identifican y se definen de acuerdo con objetivos y medición de procesos objetivos cuantitativos para el proceso de rendimiento.<br>e) Los resultados de la medición son recogidos, analizados y reportados para supervisar la medida en que los objetivos cuantitativos de rendimiento de los procesos se cumplan.<br>f) Los resultados de medición se utilizan para caracterizar el rendimiento del proceso. | N | | | | | | 0 |
| | PA 4.2 Control de procesos - Una medida de la medida en que el proceso es gestionado cuantitativamente para producir un proceso que es estable, capaz y predecible dentro de límites definidos. | Como resultado de la plena realización de este atributo:<br>a) Técnicas de análisis y control son determinada y aplicada en su caso.<br>b) Se establecen límites de control de la variación para el rendimiento normal de proceso.<br>c) Los datos de medición se analizan para determinar causas especiales de variación.<br>d) Se tomen las medidas correctivas para hacer frente a causas especiales de variación.<br>e) Los límites de control se restablecen (como es necesario) después de la acción correctiva. | N | | | | | | 0 |
| Nivel 5 Optimizado | PA 5.1 Innovación del proceso - Una medida del grado en que los cambios en el proceso son identificados a partir del análisis de las causas comunes de variación en el rendimiento, ya partir de las investigaciones de enfoques innovadores para la definición e implementación del proceso. | Como resultado de la plena realización de este atributo:<br>a) Objetivos de mejora de procesos para el proceso que se definen compatible con los objetivos de negocio relevantes.<br>b) Los datos apropiados se analizan para identificar causas comunes de las variaciones en el proceso de rendimiento.<br>c) Los datos apropiados se analizan para identificar oportunidades para las mejores prácticas e innovación.<br>d) Oportunidades de mejora derivados de nuevas tecnologías y conceptos de proceso se identifican.<br>e) Una estrategia de implementación es establecido para lograr el proceso objetivos de mejora. | N | | | | | | 0 |
| | PA 5.2 Proceso Optimizado - Una medida del grado en que los cambios en la definición, gestión y ejecución del resultado del proceso de impacto efectivo que logre los objetivos de mejora de procesos pertinentes. | Como resultado de la plena realización de este atributo:<br>a) Impacto de los cambios propuestos es evaluado contra los objetivos del proceso definido y el proceso estándar.<br>b) La aplicación de todos los cambios acordados es manejado para asegurar ninguna interrupción en el rendimiento del proceso entendido y actuado.<br>c) La eficacia de los cambios en los procesos se evalúa basándose en el rendimiento real en contra de los requisitos de los productos definidos y los objetivos del proceso para determinar si los resultados son comunes o causas especiales. | N | | | | | | 0 |

| APO12 - Gestionar los Riesgos | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Propósito:** | Integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI. | | | | | | | | |
| **Nivel** | **Evaluar si los siguientes resultados son** | **Criterios** | **Los criterios se cumplen S/N** | **Comentarios** | **N (%)** | **P (%)** | **L (%)** | **F (%)** | **Valor (%)** |
| Nivel 0 Incompleto | El proceso no está implantado o no alcanza sus objetivos. | En este nivel, hay poca o ninguna evidencia de cualquier logro o del propósito del proceso. | N | | | | | | 0 |
| Nivel 1 Realizado | PA 1.1 Rendimiento del proceso - El proceso implementado alcanza su propósito de proceso. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | APO12-01 El riesgo relacionado con TI está identificado, analizado, gestionado y reportado. | N | Existe el registro de amenazas relacionadas con TI. | | 40 | | | 38,25 |
| | | APO12-02 Existe un perfil de riesgo actual y completo. | N | Se tiene documentado las amenazas relacionadas con TI actuales, que pueden afectar a los procesos agregadores de valor del Hospital. | | 36 | | | |
| | | APO12-03 Todas las acciones de gestión para los riesgos significativos están gestionadas y bajo control. | N | Existe documentación con la lista de amenazas relacionadas con TI que no han sido solucionadas o identificadas. | | 38 | | | |
| | | APO12-04 Las acciones de gestión de riesgos están efectivamente implementadas. | N | Las actividades diseñadas para la mitigación de riesgos se encuentran en definida y difundida en el Hospital. | | 39 | | | |
| Nivel 2 Gestionado | PA 2.1 Gestión de rendimiento - Una medida del nivel de gestión del proceso. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | a) Los objetivos para el desempeño del proceso se identifican.<br>b) El rendimiento del proceso está planificado y monitoreado.<br>c) El Rendimiento del proceso se ajusta para cumplir con los planes.<br>d) Las responsabilidades y autoridades para la realización del procedimiento están definidos, asignados y comunicados.<br>e) Los recursos e información necesaria para realizar el proceso se identifican, son puestas a disposición, y son asignados y utilizados.<br>f) Las interfaces entre las partes involucradas son manejadas para garantizar la efectiva comunicación y una clara asignación de responsabilidades. | N | | | | | | | 0 |
| | PA 2.2 Gestión del producto de trabajo - Medida del grado en que los productos del proceso son gestionados. apropiadamente. Los productos (o salidas del proceso) se definen y controlan. | Como resultado de la plena realización este atributo se obtiene: | | | | | | | |
| | | a) Los requisitos para los productos de trabajo del proceso se definen.<br>b) Los requisitos para la documentación y el control de los productos de trabajo se definen.<br>c) Los productos de trabajo son adecuadamente identificados, documentados y controlados.<br>d) Los productos de trabajo se revisan de acuerdo con lo planificado y se ajustan según sea necesario para satisfacer los requisitos. | N | | | | | | | 0 |
| Nivel 3 Establecido | PA 3.1 Definición del proceso - Una medida del grado en que se mantiene un proceso estándar para apoyar el despliegue del proceso definido. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | a) Un proceso estándar, incluyendo guías de adaptación adecuadas, es definido tanto que describe los elementos fundamentales que deben ser incorporados en un proceso definido.<br>b) Se determina la secuencia y la interacción del proceso estándar con otros procesos.<br>c) Competencias requeridas y las funciones para llevar a cabo un proceso se identifican como parte del proceso estándar.<br>d) La infraestructura necesaria y ambiente de trabajo para la realización de un proceso se identifican como parte del proceso estándar.<br>e) Se determinan los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso. | N | | | | | | | 0 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Nivel 3 Establecido | PA 3.2 Despliegue del proceso - Una medida en que el proceso estándar se implementa eficazmente como un proceso definido para lograr sus resultados del proceso | Como resultado de la plena realización de este atributo:<br>a) Un proceso definido es implementado basado en un apropiadamente seleccionado y adaptado proceso estándar.<br>b) Roles, responsabilidades y autoridades requeridas para llevar a cabo el proceso definido son asignados y comunicados<br>c) El personal que realiza la definición del proceso es competente sobre las bases de educación, formación y experiencia.<br>d) Los recursos necesarios y la información necesaria para realizar el de finido el proceso se hacen disponibles, asignados y utilizado.<br>e) La infraestructura requerida y el ambiente de trabajo para llevar a cabo el definido proceso se ponen a disposición, y son manejados y mantenidos.<br>f) Los datos apropiados son recogidos y analizados como base para la comprensión del comportamiento, y para demostrar la idoneidad y la eficacia del proceso, y para evaluar dónde se puede realizar la mejora continua del proceso. | N | | | | | | 0 |
| Nivel 4 Predecible | PA 4.1 Medición de procesos - Una medida del grado en que los resultados de medición se utilizan para asegurar que el rendimiento del proceso apoya el logro de los objetivos de rendimiento de los procesos pertinentes en apoyo de los objetivos de negocio definidos. | Como resultado de la plena realización de este atributo:<br>Como resultado de la plena realización de este atributo:<br>a) Información sobre el proceso necesario para apoyar a los objetivos empresariales definidos relevantes son establecidos.<br>b) Objetivos de medición de proceso son derivado de las necesidades de información de proceso.<br>c) Los objetivos cuantitativos para el proceso de actuación en apoyo de la correspondiente se establecen los objetivos de negocio.<br>d) Las medidas y la frecuencia de la medición se identifican y se definen de acuerdo con objetivos y medición de procesos objetivos cuantitativos para el proceso de rendimiento.<br>e) Los resultados de la medición son recogidos, analizados y reportados para supervisar la medida en que los objetivos cuantitativos de rendimiento de los procesos se cumplan.<br>f) Los resultados de medición se utilizan para caracterizar el rendimiento del proceso. | N | | | | | | 0 |
| | PA 4.2 Control de procesos - Una medida de la medida en que el proceso es gestionado cuantitativamente para producir un proceso que es estable, capaz y predecible dentro de límites definidos. | Como resultado de la plena realización de este atributo:<br>a) Técnicas de análisis y control son determinada y aplicada en su caso.<br>b) Se establecen límites de control de la variación para el rendimiento normal de proceso.<br>c) Los datos de medición se analizan para determinar causas especiales de variación.<br>d) Se tomen las medidas correctivas para hacer frente a causas especiales de variación.<br>e) Los límites de control se restablecen (como es necesario) después de la acción correctiva. | N | | | | | | 0 |
| Nivel 5 Optimizado | PA 5.1 Innovación del proceso - Una medida del grado en que los cambios en el proceso son identificados a partir del análisis de las causas comunes de variación en el rendimiento, ya partir de las investigaciones de enfoques innovadores para la definición e implementación del proceso. | Como resultado de la plena realización de este atributo:<br>a) Objetivos de mejora de procesos para el proceso que se definen compatible con los objetivos de negocio relevantes.<br>b) Los datos apropiados se analizan para identificar causas comunes de las variaciones en el proceso de rendimiento.<br>c) Los datos apropiados se analizan para identificar oportunidades para las mejores prácticas e innovación.<br>d) Oportunidades de mejora derivados de nuevas tecnologías y conceptos de proceso se identifican.<br>e) Una estrategia de implementación es establecido para lograr el proceso objetivos de mejora. | N | | | | | | 0 |
| | PA 5.2 Proceso Optimizado - Una medida del grado en que los cambios en la definición, gestión y ejecución del resultado del proceso de impacto efectivo que logre los objetivos de mejora de procesos pertinentes. | Como resultado de la plena realización de este atributo:<br>a) Impacto de los cambios propuestos es evaluado contra los objetivos del proceso definido y el proceso estándar.<br>b) La aplicación de todos los cambios acordados es manejado para asegurar ninguna interrupción en el rendimiento del proceso entendido y actuado.<br>c) La eficacia de los cambios en los procesos se evalúa basándose en el rendimiento real en contra de los requisitos de los productos definidos y los objetivos del proceso para determinar si los resultados son comunes o causas especiales. | N | | | | | | 0 |

| APO13 - Gestionar la Seguridad | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Propósito:** | Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa. | | | | | | | | |
| **Nivel** | **Evaluar si los siguientes resultados son** | **Criterios** | **Los criterios se cumplen S/N** | **Comentarios** | **N (%)** | **P (%)** | **L (%)** | **F (%)** | **Valor (%)** |
| Nivel 0 Incompleto | El proceso no está implantado o no alcanza sus objetivos. | En este nivel, hay poca o ninguna evidencia de cualquier logro o del propósito del proceso. | N | | | | | | 0 |
| Nivel 1 Realizado | PA 1.1 Rendimiento del proceso - El proceso implementado alcanza su propósito de proceso. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | APO13-01 Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la empresa. | N | Existe registro de incidentes relacionados con la seguridad de la información en el Hospital, como también indicar que los roles de seguridad (tareas que puede realizar el usuario y los recursos a los que tiene acceso) y los mecanismos para la respuesta inmediata a incidentes no se encuentran definidos completamente. | | 42 | | | 40,6 |
| | | APO13-02 Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad. | N | No existe implementado un Sistema de Gestión de Seguridad de la Información (SGSI) que proteja los activos de información del Hospital. | | 42 | | | |
| | | APO13-03 Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa. | N | No existe implementado un Sistema de Gestión de Seguridad de la Información (SGSI) que proteja los activos de información del Hospital. | | 38 | | | |
| Nivel 2 Gestionado | PA 2.1 Gestión de rendimiento - Una medida del nivel de gestión del proceso. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | a) Los objetivos para el desempeño del proceso se identifican.<br>b) El rendimiento del proceso está planificado y monitoreado.<br>c) El Rendimiento del proceso se ajusta para cumplir con los planes.<br>d) Las responsabilidades y autoridades para la realización del procedimiento están definidos, asignados y comunicados.<br>e) Los recursos e información necesaria para realizar el proceso se identifican, son puestas a disposición, y son asignados y utilizados.<br>f) Las interfaces entre las partes involucradas son manejadas para garantizar la efectiva comunicación y una clara asignación de responsabilidades. | N | | | | | | 0 |
| | PA 2.2 Gestión del producto de trabajo - Medida del grado en que los productos del proceso son gestionados. apropiadamente. Los productos (o salidas del proceso) se definen y controlan. | Como resultado de la plena realización este atributo se obtiene: | | | | | | | |
| | | a) Los requisitos para los productos de trabajo del proceso se definen.<br>b) Los requisitos para la documentación y el control de los productos de trabajo se definen.<br>c) Los productos de trabajo son adecuadamente identificados, documentados y controlados.<br>d) Los productos de trabajo se revisan de acuerdo con lo planificado y se ajustan según sea necesario para satisfacer los requisitos. | N | | | | | | 0 |
| Nivel 3 Establecido | PA 3.1 Definición del proceso - Una medida del grado en que se mantiene un proceso estándar para apoyar el despliegue del proceso definido. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | a) Un proceso estándar, incluyendo guías de adaptación adecuadas, es definido tanto que describe los elementos fundamentales que deben ser incorporados en un proceso definido.<br>b) Se determina la secuencia y la interacción del proceso estándar con otros procesos.<br>c) Competencias requeridas y las funciones para llevar a cabo un proceso se identifican como parte del proceso estándar.<br>d) La infraestructura necesaria y ambiente de trabajo para la realización de un proceso se identifican como parte del proceso estándar.<br>e) Se determinan los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso. | N | | | | | | 0 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Nivel 3 Establecido | PA 3.2 Despliegue del proceso - Una medida en que el proceso estándar se implementa eficazmente como un proceso definido para lograr sus resultados del proceso | Como resultado de la plena realización de este atributo:<br>a) Un proceso definido es implementado basado en un apropiadamente seleccionado y adaptado proceso estándar.<br>b) Roles, responsabilidades y autoridades requeridas para llevar a cabo el proceso definido son asignados y comunicados<br>c) El personal que realiza la definición del proceso es competente sobre las bases de educación, formación y experiencia.<br>d) Los recursos necesarios y la información necesaria para realizar el de finido el proceso se hacen disponibles, asignados y utilizado.<br>e) La infraestructura requerida y el ambiente de trabajo para llevar a cabo el definido proceso se ponen a disposición, y son manejados y mantenidos.<br>f) Los datos apropiados son recogidos y analizados como base para la comprensión del comportamiento, y para demostrar la idoneidad y la eficacia del proceso, y para evaluar dónde se puede realizar la mejora continua del proceso. | N | | | | | | 0 |
| Nivel 4 Predecible | PA 4.1 Medición de procesos - Una medida del grado en que los resultados de medición se utilizan para asegurar que el rendimiento del proceso apoya el logro de los objetivos de rendimiento de los procesos pertinentes en apoyo de los objetivos de negocio definidos. | Como resultado de la plena realización de este atributo:<br>Como resultado de la plena realización de este atributo:<br>a) Información sobre el proceso necesario para apoyar a los objetivos empresariales definidos relevantes son establecidos.<br>b) Objetivos de medición de proceso son derivado de las necesidades de información de proceso.<br>c) Los objetivos cuantitativos para el proceso de actuación en apoyo de la correspondiente se establecen los objetivos de negocio.<br>d) Las medidas y la frecuencia de la medición se identifican y se definen de acuerdo con objetivos y medición de procesos objetivos cuantitativos para el proceso de rendimiento.<br>e) Los resultados de la medición son recogidos, analizados y reportados para supervisar la medida en que los objetivos cuantitativos de rendimiento de los procesos se cumplan.<br>f) Los resultados de medición se utilizan para caracterizar el rendimiento del proceso. | N | | | | | | 0 |
| | PA 4.2 Control de procesos - Una medida de la medida en que el proceso es gestionado cuantitativamente para producir un proceso que es estable, capaz y predecible dentro de límites definidos. | Como resultado de la plena realización de este atributo:<br>a) Técnicas de análisis y control son determinada y aplicada en su caso.<br>b) Se establecen límites de control de la variación para el rendimiento normal de proceso.<br>c) Los datos de medición se analizan para determinar causas especiales de variación.<br>d) Se tomen las medidas correctivas para hacer frente a causas especiales de variación.<br>e) Los límites de control se restablecen (como es necesario) después de la acción correctiva. | N | | | | | | 0 |
| Nivel 5 Optimizado | PA 5.1 Innovación del proceso - Una medida del grado en que los cambios en el proceso son identificados a partir del análisis de las causas comunes de variación en el rendimiento, ya partir de las investigaciones de enfoques innovadores para la definición e implementación del proceso. | Como resultado de la plena realización de este atributo:<br>a) Objetivos de mejora de procesos para el proceso que se definen compatible con los objetivos de negocio relevantes.<br>b) Los datos apropiados se analizan para identificar causas comunes de las variaciones en el proceso de rendimiento.<br>c) Los datos apropiados se analizan para identificar oportunidades para las mejores prácticas e innovación.<br>d) Oportunidades de mejora derivados de nuevas tecnologías y conceptos de proceso se identifican.<br>e) Una estrategia de implementación es establecido para lograr el proceso objetivos de mejora. | N | | | | | | 0 |
| | PA 5.2 Proceso Optimizado - Una medida del grado en que los cambios en la definición, gestión y ejecución del resultado del proceso de impacto efectivo que logre los objetivos de mejora de procesos pertinentes. | Como resultado de la plena realización de este atributo:<br>a) Impacto de los cambios propuestos es evaluado contra los objetivos del proceso definido y el proceso estándar.<br>b) La aplicación de todos los cambios acordados es manejado para asegurar ninguna interrupción en el rendimiento del proceso entendido y actuado.<br>c) La eficacia de los cambios en los procesos se evalúa basándose en el rendimiento real en contra de los requisitos de los productos definidos y los objetivos del proceso para determinar si los resultados son comunes o causas especiales. | N | | | | | | 0 |

| BAI02 - Gestionar la Definición de Requisitos | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Propósito:** | Crear soluciones viables y óptimas que cumplan con las necesidades de la organización mientras minimizan el riesgo. | | | | | | | | |
| **Nivel** | **Evaluar si los siguientes resultados son** | **Criterios** | **Los criterios se cumplen S/N** | **Comentarios** | **N (%)** | **P (%)** | **L (%)** | **F (%)** | **Valor (%)** |
| Nivel 0 Incompleto | El proceso no está implantado o no alcanza sus objetivos. | En este nivel, hay poca o ninguna evidencia de cualquier logro o del propósito del proceso. | N | | | | | | 0 |
| Nivel 1 Realizado | PA 1.1 Rendimiento del proceso - El proceso implementado alcanza su propósito de proceso. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | BAI02-01 Los requerimientos funcionales y técnicos del negocio reflejan las necesidades y expectativas de la organización. | N | Existe actualmente un alto porcentaje de requerimientos repetidos al momento de diseñar y elaborar los servicios de TI para el Hospital. | | 38 | | | 38,5 |
| | | BAI02-02 La solución propuesta satisface los requerimientos funcionales, técnicos y de cumplimiento del negocio. | N | Dentro del hospital existe proceso informales para definir las características, el propósito, la dirección y el tamaño de la solución tecnológica que va a ser desarrollado o adquirido | | 37 | | | |
| | | BAI 02-03 El riesgo asociado con los requerimientos ha sido tomado en cuenta en la solución propuesta. | N | La inclusión de una sección de riesgos asociado a los requerimientos, actualmente no se encuentra dentro del proceso de elaboración de proyecto del Hospital. | | 41 | | | |
| | | BAI 02-04 Los requerimientos y soluciones propuestas cumplen con los objetivos del caso de negocio (valor esperado y costes probables). | N | Existe registros del no cumplimiento de los objetivos de negocio , con la solución propuesta e implementada. | | 38 | | | |
| Nivel 2 Gestionado | PA 2.1 Gestión de rendimiento - Una medida del nivel de gestión del proceso. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | a) Los objetivos para el desempeño del proceso se identifican.<br>b) El rendimiento del proceso está planificado y monitoreado.<br>c) El Rendimiento del proceso se ajusta para cumplir con los planes.<br>d) Las responsabilidades y autoridades para la realización del procedimiento están definidos, asignados y comunicados.<br>e) Los recursos e información necesaria para realizar el proceso se identifican, son puestas a disposición, y son asignados y utilizados.<br>f) Las interfaces entre las partes involucradas son manejadas para garantizar la efectiva comunicación y una clara asignación de responsabilidades. | N | | | | | | 0 |
| | PA 2.2 Gestión del producto de trabajo - Medida del grado en que los productos del proceso son gestionados. apropiadamente. Los productos (o salidas del proceso) se definen y controlan. | Como resultado de la plena realización este atributo se obtiene: | | | | | | | |
| | | a) Los requisitos para los productos de trabajo del proceso se definen.<br>b) Los requisitos para la documentación y el control de los productos de trabajo se definen.<br>c) Los productos de trabajo son adecuadamente identificados, documentados y controlados.<br>d) Los productos de trabajo se revisan de acuerdo con lo planificado y se ajustan según sea necesario para satisfacer los requisitos. | N | | | | | | 0 |
| Nivel 3 Establecido | PA 3.1 Definición del proceso - Una medida del grado en que se mantiene un proceso estándar para apoyar el despliegue del proceso definido. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | a) Un proceso estándar, incluyendo guías de adaptación adecuadas, es definido tanto que describe los elementos fundamentales que deben ser incorporados en un proceso definido.<br>b) Se determina la secuencia y la interacción del proceso estándar con otros procesos.<br>c) Competencias requeridas y las funciones para llevar a cabo un proceso se identifican como parte del proceso estándar.<br>d) La infraestructura necesaria y ambiente de trabajo para la realización de un proceso se identifican como parte del proceso estándar.<br>e) Se determinan los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso. | N | | | | | | 0 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Nivel 3 Establecido | PA 3.2 Despliegue del proceso - Una medida en que el proceso estándar se implementa eficazmente como un proceso definido para lograr sus resultados del proceso | Como resultado de la plena realización de este atributo:<br>a) Un proceso definido es implementado basado en un apropiadamente seleccionado y adaptado proceso estándar.<br>b) Roles, responsabilidades y autoridades requeridas para llevar a cabo el proceso definido son asignados y comunicados<br>c) El personal que realiza la definición del proceso es competente sobre las bases de educación, formación y experiencia.<br>d) Los recursos necesarios y la información necesaria para realizar el de finido el proceso se hacen disponibles, asignados y utilizado.<br>e) La infraestructura requerida y el ambiente de trabajo para llevar a cabo el definido proceso se ponen a disposición, y son manejados y mantenidos.<br>f) Los datos apropiados son recogidos y analizados como base para la comprensión del comportamiento, y para demostrar la idoneidad y la eficacia del proceso, y para evaluar dónde se puede realizar la mejora continua del proceso. | N | | | | | | 0 |
| Nivel 4 Predecible | PA 4.1 Medición de procesos - Una medida del grado en que los resultados de medición se utilizan para asegurar que el rendimiento del proceso apoya el logro de los objetivos de rendimiento de los procesos pertinentes en apoyo de los objetivos de negocio definidos. | Como resultado de la plena realización de este atributo:<br>Como resultado de la plena realización de este atributo:<br>a) Información sobre el proceso necesario para apoyar a los objetivos empresariales definidos relevantes son establecidos.<br>b) Objetivos de medición de proceso son derivado de las necesidades de información de proceso.<br>c) Los objetivos cuantitativos para el proceso de actuación en apoyo de la correspondiente se establecen los objetivos de negocio.<br>d) Las medidas y la frecuencia de la medición se identifican y se definen de acuerdo con objetivos y medición de procesos objetivos cuantitativos para el proceso de rendimiento.<br>e) Los resultados de la medición son recogidos, analizados y reportados para supervisar la medida en que los objetivos cuantitativos de rendimiento de los procesos se cumplan.<br>f) Los resultados de medición se utilizan para caracterizar el rendimiento del proceso. | N | | | | | | 0 |
| | PA 4.2 Control de procesos - Una medida de la medida en que el proceso es gestionado cuantitativamente para producir un proceso que es estable, capaz y predecible dentro de límites definidos. | Como resultado de la plena realización de este atributo:<br>a) Técnicas de análisis y control son determinada y aplicada en su caso.<br>b) Se establecen límites de control de la variación para el rendimiento normal de proceso.<br>c) Los datos de medición se analizan para determinar causas especiales de variación.<br>d) Se tomen las medidas correctivas para hacer frente a causas especiales de variación.<br>e) Los límites de control se restablecen (como es necesario) después de la acción correctiva. | N | | | | | | 0 |
| Nivel 5 Optimizado | PA 5.1 Innovación del proceso - Una medida del grado en que los cambios en el proceso son identificados a partir del análisis de las causas comunes de variación en el rendimiento, ya partir de las investigaciones de enfoques innovadores para la definición e implementación del proceso. | Como resultado de la plena realización de este atributo:<br>a) Objetivos de mejora de procesos para el proceso que se definen compatible con los objetivos de negocio relevantes.<br>b) Los datos apropiados se analizan para identificar causas comunes de las variaciones en el proceso de rendimiento.<br>c) Los datos apropiados se analizan para identificar oportunidades para las mejores prácticas e innovación.<br>d) Oportunidades de mejora derivados de nuevas tecnologías y conceptos de proceso se identifican.<br>e) Una estrategia de implementación es establecido para lograr el proceso objetivos de mejora. | N | | | | | | 0 |
| | PA 5.2 Proceso Optimizado - Una medida del grado en que los cambios en la definición, gestión y ejecución del resultado del proceso de impacto efectivo que logre los objetivos de mejora de procesos pertinentes. | Como resultado de la plena realización de este atributo:<br>a) Impacto de los cambios propuestos es evaluado contra los objetivos del proceso definido y el proceso estándar.<br>b) La aplicación de todos los cambios acordados es manejado para asegurar ninguna interrupción en el rendimiento del proceso entendido y actuado.<br>c) La eficacia de los cambios en los procesos se evalúa basándose en el rendimiento real en contra de los requisitos de los productos definidos y los objetivos del proceso para determinar si los resultados son comunes o causas especiales. | N | | | | | | 0 |

| DSS04 - Gestionar la Continuidad | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Propósito:** | Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa. | | | | | | | | |
| **Nivel** | **Evaluar si los siguientes resultados son** | **Criterios** | **Los criterios se cumplen S/N** | **Comentarios** | **N (%)** | **P (%)** | **L (%)** | **F (%)** | **Valor (%)** |
| Nivel 0 Incompleto | El proceso no está implantado o no alcanza sus objetivos. | En este nivel, hay poca o ninguna evidencia de cualquier logro o del propósito del proceso. | N | | | | | | 0 |
| Nivel 1 Realizado | PA 1.1 Rendimiento del proceso - El proceso implementado alcanza su propósito de proceso. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | DSS04-01 La información crítica para el negocio está disponible para el negocio en línea con los niveles de servicio mínimos requeridos. | N | Existen servicios de TI que en periodos frecuentes no cumplen con los niveles de servicio mínimos requeridos por el Hospital. | | 37 | | | 35,8 |
| | | DSS04-02 Los servicios críticos tienen suficiente resistencia. | N | La capacidad de los servicios de TI, para recuperarse de una interrupción significativa actualmente no es eficiente. | | 36 | | | |
| | | DSS04-03 Las pruebas de continuidad del servicio han verificado la efectividad del plan. | N | Las pruebas de continuidad a un servicio de TI dentro del Hospital, se realizan con poca frecuencia. | | 38 | | | |
| | | DSS04-04 Un plan de continuidad actualizado refleja los requisitos de negocio actuales. | N | En el hospital no se consideran los requisitos del negocio , dentro de los procedimientos y actividades que permiten mantener la disponibilidad de un servicio. | | 36 | | | |
| | | DSS04-05 Las partes interesadas internas y externas han sido formadas en el plan de continuidad. | N | Existe registros de capacitación a las partes interesadas, específicamente en el momento de implementar el servicio de TI. | | 32 | | | |
| Nivel 2 Gestionado | PA 2.1 Gestión de rendimiento - Una medida del nivel de gestión del proceso. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | a) Los objetivos para el desempeño del proceso se identifican.<br>b) El rendimiento del proceso está planificado y monitoreado.<br>c) El Rendimiento del proceso se ajusta para cumplir con los planes.<br>d) Las responsabilidades y autoridades para la realización del procedimiento están definidos, asignados y comunicados.<br>e) Los recursos e información necesaria para realizar el proceso se identifican, son puestas a disposición, y son asignados y utilizados.<br>f) Las interfaces entre las partes involucradas son manejadas para garantizar la efectiva comunicación y una clara asignación de responsabilidades. | N | | | | | | | 0 |
| | PA 2.2 Gestión del producto de trabajo - Medida del grado en que los productos del proceso son gestionados. apropiadamente. Los productos (o salidas del proceso) se definen y controlan. | Como resultado de la plena realización este atributo se obtiene: | | | | | | | |
| | | a) Los requisitos para los productos de trabajo del proceso se definen.<br>b) Los requisitos para la documentación y el control de los productos de trabajo se definen.<br>c) Los productos de trabajo son adecuadamente identificados, documentados y controlados.<br>d) Los productos de trabajo se revisan de acuerdo con lo planificado y se ajustan según sea necesario para satisfacer los requisitos. | N | | | | | | | 0 |
| Nivel 3 Establecido | PA 3.1 Definición del proceso - Una medida del grado en que se mantiene un proceso estándar para apoyar el despliegue del proceso definido. | Como resultado de la plena realización de este atributo: | | | | | | | |
| | | a) Un proceso estándar, incluyendo guías de adaptación adecuadas, es definido tanto que describe los elementos fundamentales que deben ser incorporados en un proceso definido.<br>b) Se determina la secuencia y la interacción del proceso estándar con otros procesos.<br>c) Competencias requeridas y las funciones para llevar a cabo un proceso se identifican como parte del proceso estándar.<br>d) La infraestructura necesaria y ambiente de trabajo para la realización de un proceso se identifican como parte del proceso estándar.<br>e) Se determinan los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso. | N | | | | | | | 0 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Nivel 3 Establecido | PA 3.2 Despliegue del proceso - Una medida en que el proceso estándar se implementa eficazmente como un proceso definido para lograr sus resultados del proceso | Como resultado de la plena realización de este atributo:<br>a) Un proceso definido es implementado basado en un apropiadamente seleccionado y adaptado proceso estándar.<br>b) Roles, responsabilidades y autoridades requeridas para llevar a cabo el proceso definido son asignados y comunicados<br>c) El personal que realiza la definición del proceso es competente sobre las bases de educación, formación y experiencia.<br>d) Los recursos necesarios y la información necesaria para realizar el de finido el proceso se hacen disponibles, asignados y utilizado.<br>e) La infraestructura requerida y el ambiente de trabajo para llevar a cabo el definido proceso se ponen a disposición, y son manejados y mantenidos.<br>f) Los datos apropiados son recogidos y analizados como base para la comprensión del comportamiento, y para demostrar la idoneidad y la eficacia del proceso, y para evaluar dónde se puede realizar la mejora continua del proceso. | N | | | | | | 0 |
| Nivel 4 Predecible | PA 4.1 Medición de procesos - Una medida del grado en que los resultados de medición se utilizan para asegurar que el rendimiento del proceso apoya el logro de los objetivos de rendimiento de los procesos pertinentes en apoyo de los objetivos de negocio definidos. | Como resultado de la plena realización de este atributo:<br>Como resultado de la plena realización de este atributo:<br>a) Información sobre el proceso necesario para apoyar a los objetivos empresariales definidos relevantes son establecidos.<br>b) Objetivos de medición de proceso son derivado de las necesidades de información de proceso.<br>c) Los objetivos cuantitativos para el proceso de actuación en apoyo de la correspondiente se establecen los objetivos de negocio.<br>d) Las medidas y la frecuencia de la medición se identifican y se definen de acuerdo con objetivos y medición de procesos objetivos cuantitativos para el proceso de rendimiento.<br>e) Los resultados de la medición son recogidos, analizados y reportados para supervisar la medida en que los objetivos cuantitativos de rendimiento de los procesos se cumplan.<br>f) Los resultados de medición se utilizan para caracterizar el rendimiento del proceso. | N | | | | | | 0 |
| | PA 4.2 Control de procesos - Una medida de la medida en que el proceso es gestionado cuantitativamente para producir un proceso que es estable, capaz y predecible dentro de límites definidos. | Como resultado de la plena realización de este atributo:<br>a) Técnicas de análisis y control son determinada y aplicada en su caso.<br>b) Se establecen límites de control de la variación para el rendimiento normal de proceso.<br>c) Los datos de medición se analizan para determinar causas especiales de variación.<br>d) Se tomen las medidas correctivas para hacer frente a causas especiales de variación.<br>e) Los límites de control se restablecen (como es necesario) después de la acción correctiva. | N | | | | | | 0 |
| Nivel 5 Optimizado | PA 5.1 Innovación del proceso - Una medida del grado en que los cambios en el proceso son identificados a partir del análisis de las causas comunes de variación en el rendimiento, ya partir de las investigaciones de enfoques innovadores para la definición e implementación del proceso. | Como resultado de la plena realización de este atributo:<br>a) Objetivos de mejora de procesos para el proceso que se definen compatible con los objetivos de negocio relevantes.<br>b) Los datos apropiados se analizan para identificar causas comunes de las variaciones en el proceso de rendimiento.<br>c) Los datos apropiados se analizan para identificar oportunidades para las mejores prácticas e innovación.<br>d) Oportunidades de mejora derivados de nuevas tecnologías y conceptos de proceso se identifican.<br>e) Una estrategia de implementación es establecido para lograr el proceso objetivos de mejora. | N | | | | | | 0 |
| | PA 5.2 Proceso Optimizado - Una medida del grado en que los cambios en la definición, gestión y ejecución del resultado del proceso de impacto efectivo que logre los objetivos de mejora de procesos pertinentes. | Como resultado de la plena realización de este atributo:<br>a) Impacto de los cambios propuestos es evaluado contra los objetivos del proceso definido y el proceso estándar.<br>b) La aplicación de todos los cambios acordados es manejado para asegurar ninguna interrupción en el rendimiento del proceso entendido y actuado.<br>c) La eficacia de los cambios en los procesos se evalúa basándose en el rendimiento real en contra de los requisitos de los productos definidos y los objetivos del proceso para determinar si los resultados son comunes o causas especiales. | N | | | | | | 0 |

| DSS05 - Gestionar los Servicios de Seguridad | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Propósito:** | Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información. | | | | | | | | |
| **Nivel** | **Evaluar si los siguientes resultados son** | **Criterios** | **Los criterios se cumplen S/N** | **Comentarios** | **N (%)** | **P (%)** | **L (%)** | **F (%)** | **Valor (%)** |
| Nivel 0 Incompleto | El proceso no está implantado o no alcanza sus objetivos. | En este nivel, hay poca o ninguna evidencia de cualquier logro o del propósito del proceso. | N | | | | | | 0 |
| Nivel 1 Realizado | PA 1.1 Rendimiento del proceso - El proceso implementado alcanza su propósito de proceso. | Como resultado de la plena realización de este atributo: | | | | | | | 41,4 |
| | | DSS05-01: La seguridad de las redes y las comunicaciones cumple con las necesidades del negocio. | N | Para la transmisión de la información crítica del Hospital, actualmente se aplican técnicas básicas de encriptación, apoyados mediante software libre. | | 48 | | | |
| | | DSS05-02: La información procesada, almacenada y transmitida en los dispositivos de usuario final está protegida. | N | Existe el registro de incidentes que implican a los dispositivos de usuario final del Hospital, como también la esporádica concienciación sobre la seguridad de la información. | | 41 | | | |
| | | DSS05-03: Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio. | N | El hospital no cuenta formalmente con políticas y procedimientos para el control de accesos a la información. Existe recomendaciones emitidas por el Ministerio de salud Publica. | | 43 | | | |
| | | DSS05-04: Se han implantado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida. | N | Debido a la naturaleza del negocio del hospital, actualmente se tiene definido parcialmente las medidas necesarias para proteger los activos de información, de igual manera existen recomendaciones emitidas por el Ministerio de Salud Publica. | | 41 | | | |
| | | DSS05-05: La información electrónica tiene las medidas de seguridad apropiadas mientras está almacenada, transmitida o destruida. | N | Existe documentación sobre incidentes relacionados con accesos no autorizados a los activos de información del hospital. | | 34 | | | |
| Nivel 2 Gestionado | PA 2.1 Gestión de rendimiento - Una medida del nivel de gestión del proceso. | Como resultado de la plena realización de este atributo:<br>a) Los objetivos para el desempeño del proceso se identifican.<br>b) El rendimiento del proceso está planificado y monitoreado.<br>c) El Rendimiento del proceso se ajusta para cumplir con los planes.<br>d) Las responsabilidades y autoridades para la realización del procedimiento están definidos, asignados y comunicados.<br>e) Los recursos e información necesaria para realizar el proceso se identifican, son puestas a disposición, y son asignados y utilizados.<br>f) Las interfaces entre las partes involucradas son manejadas para garantizar la efectiva comunicación y una clara asignación de responsabilidades. | N | | | | | | 0 |
| | PA 2.2 Gestión del producto de trabajo - Medida del grado en que los productos del proceso son gestionados. apropiadamente. Los productos (o salidas del proceso) se definen y controlan. | Como resultado de la plena realización este atributo se obtiene:<br>a) Los requisitos para los productos de trabajo del proceso se definen.<br>b) Los requisitos para la documentación y el control de los productos de trabajo se definen.<br>c) Los productos de trabajo son adecuadamente identificados, documentados y controlados.<br>d) Los productos de trabajo se revisan de acuerdo con lo planificado y se ajustan según sea necesario para satisfacer los requisitos. | N | | | | | | 0 |
| Nivel 3 Establecido | PA 3.1 Definición del proceso - Una medida del grado en que se mantiene un proceso estándar para apoyar el despliegue del proceso definido. | Como resultado de la plena realización de este atributo:<br>a) Un proceso estándar, incluyendo guías de adaptación adecuadas, es definido tanto que describe los elementos fundamentales que deben ser incorporados en un proceso definido.<br>b) Se determina la secuencia y la interacción del proceso estándar con otros procesos.<br>c) Competencias requeridas y las funciones para llevar a cabo un proceso se identifican como parte del proceso estándar.<br>d) La infraestructura necesaria y ambiente de trabajo para la realización de un proceso se identifican como parte del proceso estándar.<br>e) Se determinan los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso. | N | | | | | | 0 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Nivel 3 Establecido | PA 3.2 Despliegue del proceso - Una medida en que el proceso estándar se implementa eficazmente como un proceso definido para lograr sus resultados del proceso | Como resultado de la plena realización de este atributo:<br>a) Un proceso definido es implementado basado en un apropiadamente seleccionado y adaptado proceso estándar.<br>b) Roles, responsabilidades y autoridades requeridas para llevar a cabo el proceso definido son asignados y comunicados<br>c) El personal que realiza la definición del proceso es competente sobre las bases de educación, formación y experiencia.<br>d) Los recursos necesarios y la información necesaria para realizar el de finido el proceso se hacen disponibles, asignados y utilizado.<br>e) La infraestructura requerida y el ambiente de trabajo para llevar a cabo el definido proceso se ponen a disposición, y son manejados y mantenidos.<br>f) Los datos apropiados son recogidos y analizados como base para la comprensión del comportamiento, y para demostrar la idoneidad y la eficacia del proceso, y para evaluar dónde se puede realizar la mejora continua del proceso. | N | | | | | | 0 |
| Nivel 4 Predecible | PA 4.1 Medición de procesos - Una medida del grado en que los resultados de medición se utilizan para asegurar que el rendimiento del proceso apoya el logro de los objetivos de rendimiento de los procesos pertinentes en apoyo de los objetivos de negocio definidos. | Como resultado de la plena realización de este atributo:<br>Como resultado de la plena realización de este atributo:<br>a) Información sobre el proceso necesario para apoyar a los objetivos empresariales definidos relevantes son establecidos.<br>b) Objetivos de medición de proceso son derivado de las necesidades de información de proceso.<br>c) Los objetivos cuantitativos para el proceso de actuación en apoyo de la correspondiente se establecen los objetivos de negocio.<br>d) Las medidas y la frecuencia de la medición se identifican y se definen de acuerdo con objetivos y medición de procesos objetivos cuantitativos para el proceso de rendimiento.<br>e) Los resultados de la medición son recogidos, analizados y reportados para supervisar la medida en que los objetivos cuantitativos de rendimiento de los procesos se cumplan.<br>f) Los resultados de medición se utilizan para caracterizar el rendimiento del proceso. | N | | | | | | 0 |
| | PA 4.2 Control de procesos - Una medida de la medida en que el proceso es gestionado cuantitativamente para producir un proceso que es estable, capaz y predecible dentro de límites definidos. | Como resultado de la plena realización de este atributo:<br>a) Técnicas de análisis y control son determinada y aplicada en su caso.<br>b) Se establecen límites de control de la variación para el rendimiento normal de proceso.<br>c) Los datos de medición se analizan para determinar causas especiales de variación.<br>d) Se tomen las medidas correctivas para hacer frente a causas especiales de variación.<br>e) Los límites de control se restablecen (como es necesario) después de la acción correctiva. | N | | | | | | 0 |
| Nivel 5 Optimizado | PA 5.1 Innovación del proceso - Una medida del grado en que los cambios en el proceso son identificados a partir del análisis de las causas comunes de variación en el rendimiento, ya partir de las investigaciones de enfoques innovadores para la definición e implementación del proceso. | Como resultado de la plena realización de este atributo:<br>a) Objetivos de mejora de procesos para el proceso que se definen compatible con los objetivos de negocio relevantes.<br>b) Los datos apropiados se analizan para identificar causas comunes de las variaciones en el proceso de rendimiento.<br>c) Los datos apropiados se analizan para identificar oportunidades para las mejores prácticas e innovación.<br>d) Oportunidades de mejora derivados de nuevas tecnologías y conceptos de proceso se identifican.<br>e) Una estrategia de implementación es establecido para lograr el proceso objetivos de mejora. | N | | | | | | 0 |
| | PA 5.2 Proceso Optimizado - Una medida del grado en que los cambios en la definición, gestión y ejecución del resultado del proceso de impacto efectivo que logre los objetivos de mejora de procesos pertinentes. | Como resultado de la plena realización de este atributo:<br>a) Impacto de los cambios propuestos es evaluado contra los objetivos del proceso definido y el proceso estándar.<br>b) La aplicación de todos los cambios acordados es manejado para asegurar ninguna interrupción en el rendimiento del proceso entendido y actuado.<br>c) La eficacia de los cambios en los procesos se evalúa basándose en el rendimiento real en contra de los requisitos de los productos definidos y los objetivos del proceso para determinar si los resultados son comunes o causas especiales. | N | | | | | | 0 |

# Anexo 7: Registro de participantes y definición del estado deseado para los procesos del HGDC

Ministerio de Salud Pública

HOSPITAL GENERAL DOCENTE DE CALDERÓN
Tecnología de Información y Comunicaciones

| Participantes en la Evaluación de Procesos de Gobierno y Gestión de TI - GOBTISI | | | |
|---|---|---|---|
| **Área** | **Nombre** | **Puesto** | **Firma** |
| Gerencia Hospitalaria | Marco Andrés Sotomayor Paredes | Gerente Hospital General Docente Calderón - HGDC | Hospital Docente de Calderón · Ministerio de Salud Pública · Gerencia |
| Gestión Asistencial | Dorys Malena Ortiz Galarza | Médico General 8HD - HGDC | |
| Gestión de Planificación, Seguimiento y Evaluación de Gestión | Evelin Johana Esparza Proaño | Analista de Planificación, Seguimiento y evaluación de la Gestión 3 - HGDC | Ministerio de Salud Pública Hospital Docente de CALDERÓN Planificación, Seguimiento y Evaluación |
| Gestión de Asesoría Jurídica | Erika Gabriela Arguello Urbina | Analista de Asesoría Jurídica 2-HGDC | Firma 24 MAR 2017 RECIBIDO |
| Gestión de Calidad | Edison Wilmer Ipiales Celín | Analista de Calidad 3 | |
| Gestión de Talento Humano | Ángela María Villamil Carlín | Analista de Talento Humano 2 - HGDC | |
| Gestión Financiera | María Elena Barahona Chica | Analista Financiera 2 - HGDC | Ministerio de Salud Pública Hospital Docente de CALDERÓN Area Financiera |
| Gestión Administrativa | María Belén Medina Villegas | Analista Administrativo 2 - HGDC | Ministerio de Salud Pública Hospital Docente de CALDERÓN 24 MAR 2017 ADQUISICIONES RECIBIDO |
| Gestión de Tecnologías de la Información y Comunicaciones | Alberto Vinicio Callay Pailiacho | Analista de Tecnologías de la Información y Comunicaciones 2 - HGDC | Ministerio de Salud Pública Hospital Docente de CALDERÓN Tecnologías de la Información y Comunicaciones |

**Observación:** Se adjunta el resumen de la evaluación realizada y el estado deseado para cada proceso priorizado del HGDC.



Calle derby y Giovanny Calles
Teléfonos: 593 (2) 3952700 Ext. 1326
www.hgdc.gob.ec

| | Preguntas | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | EDM01 | | | APO01 | | APO07 | | APO09 | | | APO12 | | | | APO13 | | | BAI02 | | | | DSS04 | | | | | DSS05 | | | | |
| Participantes de la evaluacion: | a | b | c | a | b | a | b | a | b | c | a | b | c | d | a | b | c | a | b | c | d | a | s | c | d | e | a | b | c | d | e |
| andres.sotomayor@hgdc.gob.ec | 1 | 1 | 1 | 2 | 2 | 3 | 3 | 4 | 4 | 3 | 3 | 4 | 4 | 4 | 5 | 5 | 5 | 4 | 4 | 5 | 3 | 4 | 4 | 5 | 5 | 4 | 5 | 5 | 4 | 4 | 4 |
| malena.ortiz@hgdc.gob,ec | 3 | 2 | 2 | 4 | 3 | 4 | 5 | 2 | 2 | 3 | 3 | 3 | 3 | 4 | 4 | 2 | 3 | 3 | 2 | 2 | 2 | 3 | 3 | 4 | 3 | 4 | 4 | 5 | 3 | 4 | 4 |
| evelin.esparza@hgdc.gob.ec | 2 | 2 | 3 | 3 | 4 | 4 | 3 | 3 | 2 | 3 | 4 | 3 | 2 | 2 | 2 | 3 | 3 | 3 | 4 | 3 | 3 | 4 | 3 | 3 | 4 | 2 | 4 | 5 | 6 | 3 | 3 |
| erika.arguello@hgdc.gob.ec | 1 | 2 | 2 | 2 | 2 | 3 | 3 | 4 | 4 | 3 | 3 | 3 | 5 | 5 | 5 | 4 | 2 | 5 | 3 | 4 | 4 | 3 | 3 | 4 | 4 | 4 | 5 | 4 | 4 | 5 | 2 |
| edison.ipiales@hgdc.gob.ec | 2 | 2 | 2 | 3 | 2 | 2 | 3 | 2 | 3 | 4 | 4 | 3 | 3 | 4 | 5 | 4 | 4 | 5 | 3 | 4 | 4 | 2 | 2 | 4 | 3 | 4 | 4 | 3 | 5 | 4 | 2 |
| angela.villamil@hgdc.gob.ec | 2 | 2 | 3 | 2 | 3 | 4 | 4 | 3 | 3 | 4 | 4 | 3 | 3 | 3 | 4 | 5 | 3 | 3 | 4 | 4 | 5 | 3 | 4 | 2 | 2 | 3 | 4 | 3 | 3 | 3 | 4 |
| maria.barahona@hgdc.gob.ec | 1 | 2 | 1 | 3 | 3 | 2 | 2 | 3 | 3 | 4 | 3 | 4 | 3 | 3 | 3 | 3 | 4 | 3 | 3 | 4 | 4 | 3 | 3 | 4 | 4 | 3 | 5 | 3 | 4 | 4 | 3 |
| belen.medina@hgdc.gob.ec | 2 | 2 | 1 | 4 | 3 | 4 | 5 | 5 | 2 | 5 | 6 | 3 | 5 | 5 | 5 | 6 | 4 | 5 | 3 | 6 | 2 | 5 | 3 | 4 | 4 | 2 | 5 | 4 | 4 | 5 | 3 |
| alberto.callay@hgdc.gob.ec | 3 | 3 | 4 | 4 | 7 | 5 | 6 | 5 | 7 | 7 | 6 | 6 | 6 | 5 | 5 | 6 | 6 | 3 | 7 | 5 | 7 | 6 | 7 | 4 | 3 | 3 | 7 | 5 | 6 | 5 | 6 |
| Promedio: | 1,9 | 2,0 | 2,1 | 3,0 | 3,2 | 3,4 | 3,8 | 3,4 | 3,3 | 4,0 | 4,0 | 3,6 | 3,8 | 3,9 | 4,2 | 4,2 | 3,8 | 3,8 | 3,7 | 4,1 | 3,8 | 3,7 | 3,6 | 3,8 | 3,6 | 3,2 | 4,8 | 4,1 | 4,3 | 4,1 | 3,4 |
| Promedio (Porcentaje/Pregunta): | 19 | 20 | 21 | 30 | 32 | 34 | 38 | 34 | 33 | 40 | 40 | 36 | 38 | 39 | 42 | 42 | 38 | 38 | 37 | 41 | 38 | 37 | 36 | 38 | 36 | 32 | 48 | 41 | 43 | 41 | 34 |
| Promedio (Porcentaje/Proceso): | 20,0 | | | 31,0 | | 36,0 | | 35,7 | | | 38,3 | | | | 40,6 | | | 38,5 | | | | 35,8 | | | | | 41,4 | | | | |
| Escala de calificación alcanzado | P | | | P | | P | | P | | | P | | | | P | | | P | | | | P | | | | | P | | | | |
| Nivel de capacidad alcanzado: | 0 | | | 0 | | 0 | | 0 | | | 0 | | | | 0 | | | 0 | | | | 0 | | | | | 0 | | | | |
| Nivel de capacidad deseado: | 1 | | | 1 | | 1 | | 1 | | | 1 | | | | 1 | | | 1 | | | | 1 | | | | | 1 | | | | |
| Escala de calificación deseada | L | | | L | | L | | L | | | L | | | | L | | | L | | | | L | | | | | L | | | | |
| Nivel de importancia | Muy Importante | | | Muy Importante | | Importante | | Poco importante | | | Importante | | | | Muy Importante | | | Poco importante | | | | Poco importante | | | | | Muy Importante | | | | |



Planificación, Seguimiento y Evaluación

2 MAR 2017 ADQUISICIONES RECIBIDO

Hospital Docente de Calderón · Ministerio de Salud Pública · Gerencia

Tecnologías de la Información y Comunicación TIC's

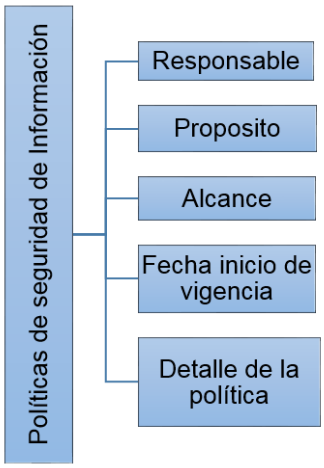
Calle derby y Giovanny Calles
Teléfono: (2) 3932700 Ext. 1326
www.hgdc.gob.ec

# Anexo 8: Políticas de Seguridad de Información del proyecto GOBTISI

Las políticas son los vehículos mediante los cuales las decisiones o instrucciones de gobierno son transmitidas a la dirección de la organización, y por esa razón son una interacción entre las decisiones de gobierno (establecer orientaciones) y gestión (ejecutar las decisiones). Para proteger los activos de información del Hospital, la formulación de políticas es un elemento imprescindible para gestionar la Seguridad de la Información en una empresa. Dicho lo anterior la política de Seguridad de la Información es un conjunto de directrices que permiten resguardar los activos de información de la organización, proporcionando además una Dirección Gerencial y apoyo a la Seguridad de la Información de acuerdo con las necesidades del Hospital y las leyes y reglamentos pertinentes a salud.

1. **Estructura de la política**

La estructura que se utilizará, para elaborar las políticas de Seguridad de la Información para el Hospital General Docente de Calderón es:




Estructura para las políticas del Hospital

2. **Políticas de seguridad de información:**

Para la elaboración de las políticas de Seguridad de la Información se utiliza la información del anexo 3 y los procesos primarios que permitirán alcanzar los objetivos estratégicos del Hospital General Docente de Calderón identificados en el ítem 4.2.2.3 del Capítulo 4. Considerando que la elaboración total de

políticas de Seguridad de la Información no se encuentra dentro del alcance de trabajo de titulación, pero para agregar un valor adicional al Modelo de Gobierno de TI propuesto y exponer la usabilidad de la información del anexo 3, se realiza la política sobre aspectos organizativos de la Seguridad de la Información.

| **Política de aspectos organizativos de la Seguridad de la Información** |
|---|
| **Responsable**: Director de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones. |
| **Propósito:** Establecer los roles y responsabilidades para la gestión y difusión de la Seguridad de la Información en la organización y garantizar el alineamiento con la estrategia y objetivos de negocio. |
| **Alcance:** Esta política se aplica a todos los recursos del Hospital y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de los recursos informáticos o información del Hospital. |
| **Fecha inicio vigencia:** Junio 2017 |
| **Detalle de la política:** |
| **a) Organización Interna:**<br>Se debería establecer una estructura de gestión para iniciar y controlar la implementación de la Seguridad de la Información dentro del Hospital. La Gerencia Hospitalaria debería aprobar la política de Seguridad de la Información, asignar las funciones de seguridad, coordinar y revisar la implementación de la seguridad en la casa de salud. Si es necesario, se recomienda establecer una fuente de asesoría especializada sobre Seguridad de la Información y ponerla a disposición del Hospital.<br>Para soportar un Gobierno de TI e iniciativas de Seguridad de la Información e incluso proyectos de Sistema de Gestión de Seguridad de Información se propone incorporar:<br>• **Comité estratégico de Seguridad de información:**<br>Entre sus funciones principales, el comité tiene:<br>▪ Revisar y proponer para la aprobación de la Gerencia Hospitalaria |

las políticas y funciones de Seguridad de la Información.

- Supervisar, investigar y monitorear los incidentes relativos a la Seguridad de la Información.
- Desarrollar y aprobar iniciativas para incrementar niveles de seguridad de información en el Hospital de acuerdo a competencias y responsabilidades asignadas a cada área.
- Evaluar y coordinar la implementación de controles de Seguridad de la Información para sistemas o servicios de TI.
- Promover difusión y apoyo de actividades relacionadas con la Seguridad de la Información y las capacitaciones.
- Revisar anualmente las políticas, de manera de asegurar su actualización.

El Comité de Seguridad de la Información será integrado por todos los responsables de todas las unidades de gestión del Hospital. El mismo contará con un Oficial de Seguridad de la Información.

- **Oficial de seguridad de información**

El oficial dentro de sus funciones tiene la supervisión de todos los aspectos inherentes a la seguridad dentro del Hospital, incluyendo el Gobierno de TI, y velar por las siguientes políticas:

- Política de Seguridad de la Información
- Política de estructura organizacional interna
- Política de recursos humanos
- Política de gestión de activos
- Política de control de accesos
- Política de seguridad física y ambiental
- Política de operaciones y comunicaciones
- Política de gestión de proveedores
- Política de gestión de incidentes de seguridad de información
- Política de continuidad de negocio
- Política de cumplimiento

b) **Roles y responsabilidades de Seguridad de la Información**

De acuerdo a los requerimientos de Seguridad de la Información y

capacidades y exigencias dentro de los procesos de negocio del Hospital, se deben proponen los roles y las nuevas responsabilidades de acuerdo a la seguridad de información según sea el caso. Se pretende garantizar:

- Confidencialidad de información: Verificar que la información puede ser accedida solo por personas autorizadas. Proteger la información crítica del Hospital.
- Integridad de Información: Verificar que los datos almacenados sean íntegros y que no exista una pérdida que genere vacíos dentro de los procesos medios y administrativos del Hospital.
- Disponibilidad de información: Garantizar que todo tipo de información crítica del Hospital se encuentre disponible o que pueda ser recuperada dentro de períodos de tiempo adecuados para minimizar el impacto en los procesos agregadores de valor del Hospital.

De acuerdo a estos tres requerimientos, se definen nuevas responsabilidades para que dentro de los procesos de negocio se vele por el cumplimiento de los tres pilares de la seguridad de información.

**c) Segregación de funciones**

El Oficial de Seguridad de la Información en conjunto con el Comité de Gestión Hospitalario y responsable de Recursos Humanos deben proponer una estructura de roles de acuerdo a los procesos de negocio del Hospital sobre el cual aplican las políticas de manera que garantice:

- Evitar redundancia de las actividades dentro de los procesos, es decir que dos personas no ejerzan un mismo rol.
- Los roles y requerimientos de seguridad son ejercidos por distintas personas de acuerdo a sus capacidades, funciones y competencias, así como sus permisos y accesos en los sistemas y a la documentación física.

**d) Seguridad frente al acceso por parte de terceros**

- **Identificación de riesgos del acceso de terceras partes**

Cuando exista la necesidad de otorgar acceso a terceras partes a información del Hospital, el oficial de seguridad de información y el propietario de la Información de que se trate, llevarán a cabo una evaluación

de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la Seguridad de la Información del Hospital.

- **Requerimientos de seguridad en contratos o acuerdos con terceros**
  - Se revisarán los contratos o acuerdos existentes o que se efectúen con terceros, teniendo cuenta la necesidad de aplicar los siguientes controles:
  - Cumplimiento de la política de Seguridad de la Información del Hospital.
  - Protección de los activos de información del Hospital.
  - Descripción de los servicios de TI disponibles en el Hospital.
  - Nivel de servicio esperado y niveles de servicio aceptables.
  - Permiso para la transferencia de personal cuando sea necesario.
  - Existencia de derechos de propiedad Intelectual.
  - Definiciones relacionadas con la protección de datos del sector salud.
  - Acuerdos de control de accesos que contemplen: Métodos de acceso permitidos y proceso de autorización de accesos.
  - Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
  - Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
- **Requerimientos de seguridad en contratos de tercerización**
  - Forma en que se cumplirán los requisitos legales aplicables.
  - Medios para garantizar que todas las partes involucradas en la

tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de Seguridad de la Información.

- Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos de información del Hospital.
- Controles físicos y lógicos que se utilizarán para restringir y limitar el acceso a la información sensible del Hospital.
- Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
- Niveles de seguridad física que se asignarán al equipamiento tercerizado.