FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

DEFINICIÓN Y EJECUCIÓN DEL PROCESO DE ALISTAMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN DIRECTV

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Sistemas de Computación e Informática

Profesor Guía

Ing. Franklin Bolívar Arequipa Chauca

Autor

Victor Fernando Quezada Neira

Año

2016

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”.

_____

Franklin Bolívar Arequipa Chauca
Ingeniero en Sistemas
CI. 171005055-8

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”.

_____

Victor Fernando Quezada Neira

CI. 171010658-2

AGRADECIMIENTOS

Agradezco principalmente a DIOS, su amor, paciencia, bondad y fortaleza, lograron que llegue a esta prestigiosa Universidad y pueda cumplir con uno de los objetivos que me he propuesto a lo largo de mi vida profesional.

A mis padres, Victor y Yolanda, mi hermana Diana, mis abuelitos Enrique y Laura, y todos mis tíos, por brindarme su apoyo incondicional, por enseñarme cada día que el esfuerzo y sacrificio son factores fundamentales para llegar a cumplir sueños propuestos.

DEDICATORIA

Dedico este trabajo a mis padres, Victor y Yolanda, desde pequeño me inculcaron que siempre uno puede entregar un poco más, superar lo insuperable, vencer lo invencible; y que en el momento que uno sufre alguna caída, comenzar por dar vuelta a la historia, esforzarse como el primer día y continuar por el camino del éxito.

RESUMEN

El trabajo de titulación tiene como objetivo contestar las siguientes interrogantes: ¿DIRECTV puede afrontar desafíos de Seguridad y Privacidad de la Información, como fuga de datos, robo de identidad, fraudes financieros, phishing, etc?, ¿Existe un Área de Seguridad de la Información que le permita establecer la responsabilidad y autoridad para la Gestión de Seguridad de los recursos de información en toda la Compañía?.

Como primera fase, se mantuvo reuniones con personal capacitado de los principales departamentos de la Compañía, para definir el alcance, el tiempo de duración, entregables en cada una de las fases, e identificación de los principales riesgos comprometidos con el avance y ejecución del presente trabajo de titulación.

Luego, se definió y estableció el marco de referencia para evaluar el estado actual de la Gestión de Seguridad de la Información en la Compañía.

Como segunda fase, se logró identificar las capacidades actuales de DIRECTV referente a la Gestión de Seguridad de la Información. Una vez identificadas estas capacidades, se elaboraron los diferentes planes de acción requeridos para alcanzar un nivel de madurez deseado.

Para establecer el nivel de madurez deseado, se consideró procesos y prácticas de gestión que actualmente se encontraban en la Compañía, y se evaluó la exitosa ejecución de los mismos. La metodología que se utilizó para medir el estado de madurez de la Seguridad de la Información en DIRECTV fue: “Evaluación de Riesgos de la Seguridad de la Información”, metodología desarrollada por la Empresa Deloitte.

En la segunda fase, también se definió el Marco de Gobierno y el Marco Normativo de Seguridad de la Información para DIRECTV. La definición de los marcos de seguridad descritos en el párrafo anterior, significaron un proceso de mejora continua para el Área de Seguridad de la Información y una integración en el núcleo de los procesos de negocio de la Compañía.

Finalmente, se realizó una presentación ejecutiva de alto nivel, con el principal objetivo de dar a conocer los resultados finales del Proceso de Alistamiento del Sistema de Gestión de Seguridad de la Información (SGSI) en DIRECTV.

ABSTRACT

The objective of the title work aims to answer the following questions: ¿Can DIRECTV deal with the challenges of Information Security and Privacy such as data leakage, identity theft, financial fraud, phishing, and etc?, ¿Is there an Area of Information Security that enables the company to establish responsibility and authority for the Security Management of the Company-wide information resources?.

As the first phase, meetings with trained personnel of key departments of the company were held to define the scope, duration, and deliverables of each phase, and identification of the main risks involved with the advancement and implementation of this title work.

Then, the framework to assess the current state of Management of Information Security in the Company was defined and established.

As a second phase, it was possible to identify the current capabilities of DIRECTV regarding the Management of Information Security. Having identified these capabilities, different action plans required to achieve the desired level of maturity were developed.

To establish the desired level of maturity, processes and management practices currently found in the company were considered and the successful execution of those practices were evaluated. The methodology used to measure the level of maturity of the Information Security on DIRECTV was: "Risk Assessment of Information Security," a methodology developed by the Deloitte Company.

In the second phase, the Framework of the Government and the Regulatory Framework for the Information Security of DIRECTV were also defined. The definition of the security frameworks described in the preceding paragraph meant that the process of continuous improvement for the Area of Information Security and the integration into core business processes of the Company.

Finally, a presentation of a high level was held with the main objective to present the final results of the Enlistment Process Management System Information Security (ISMS) in DIRECTV.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Introducción

Antecedentes

La mayoría de empresas públicas se encuentran en un proceso de mejoras para el área de Seguridad de la Información, basado en un plan de trabajo que surgió a partir del Acuerdo 166 para todas las entidades de la administración pública y que dependan de la función ejecutiva.

Cabe indicar que las empresas privadas del país no están obligadas a cumplir con dicho acuerdo, pero es de vital importancia el uso de la norma 27000 (familia de varios estándares) para la gestión de la Seguridad de la Información de acuerdo a los lineamientos definidos para dicha área.

El presente trabajo de titulación que tiene como tema: “Definición y Ejecución del Proceso de Alistamiento del Sistema de Gestión de Seguridad de la Información (SGSI)”, se implementará en una Compañía privada como “DIRECTV”. La norma con la cual se va a trabajar en el Marco de Evaluación para definir los controles o directrices que DIRECTV deberá implementar, es la norma ISO/IEC 27001:2013.

DIRECTV es líder de la televisión satelital en Ecuador, innovando y cambiando la historia en la forma de ver televisión. Desde el mes de Julio del año 2015, DIRECTV forma parte de la familia de AT&T, inc. Tiene como misión transformar el panorama de la comunicación mediante una combinación diversa de contenido, tecnología y servicio; convirtiendo a DIRECTV en la selección favorita del consumidor. La visión es lograr que DIRECTV sea la mejor experiencia televisiva del mundo (Directvla, s.f.).

DIRECTV cuenta con las áreas de Finanzas, RRHH, Operaciones, Ventas, Compras, etc, dentro de la estructura de su administración. Dentro del área de Operaciones, DIRECTV Ecuador ha definido un Departamento de Sistemas, en el cual se manejan las operaciones referentes a respaldos de información de los servidores de aplicaciones que interactúan con el sistema core de negocio, administración del centro de cómputo, soporte y mantenimiento a la red de la

Compañía, bases de datos y los sistemas de aplicación. El Departamento está compuesto por 16 personas, quienes brindan soporte de mesa de servicio y viabilizan la ejecución de los proyectos de sistemas.

Alcance

El alcance del presente trabajo de titulación acorde al uso de la norma ISO/IEC 27001:2013 para la gestión de la Seguridad de la Información, comprende las siguientes fases:

a) Fase I - Planear

a.1) Plan Detallado de Trabajo.- Mediante reuniones de trabajo con personal relevante de DIRECTV (TALENTO HUMANO, SISTEMAS, SEGURIDAD FÍSICA, etc), se confirmará el plan detallado de trabajo, el mismo que incluirá los siguientes puntos:

- Objetivo del plan detallado de trabajo.
- Gestión del alcance.
- Gestión de tiempos.
- Gestión de la calidad.
- Gestión del recurso humano.
- Gestión de riesgos.
- Consideraciones y expectativas.

Se generará como entregable un documento del plan detallado de trabajo.

a.2) Marco de Evaluación.- Se definirán los controles o directrices que DIRECTV deberá implementar, en base a la norma ISO/IEC 27001:2013.

Se generará como entregable un documento del marco de evaluación.

b) Fase II - Ejecutar

b.1) Diagnóstico del Estado de Gestión de Seguridad.- Esta sección contiene:

b.1.1) Plan Estratégico de Seguridad de la Información.- Con base a la actividad anterior, se realizará la identificación de las capacidades actuales de

DIRECTV referente a la gestión de Seguridad de la Información, para alcanzar un nivel de madurez deseado a corto, mediano y largo plazo, de acuerdo a los requerimientos particulares y a lo requerido por la norma ISO/IEC 27001:2013.

Una vez definido el nivel de madurez deseado en el corto, mediano y largo plazo, se deberán establecer los diferentes planes de acción requeridos para alcanzar el nivel de madurez deseado, teniendo en cuenta varios aspectos, como lo son: requisitos de la norma ISO/IEC 27001:2013, la afinidad de las tareas a ser realizadas, los recursos requeridos, los plazos de implementación, etc.

Se generará como entregable un documento del Plan Estratégico de Seguridad de la Información, el cual contendrá:

- Niveles de madurez deseados del Área a corto, mediano y largo plazo.
- Planes de acción y “roadmap” de implementación.

Adicionalmente, se generarán como entregables los siguientes documentos:

- Objetivos estratégicos del Área de Seguridad de la Información.
- Plan de concienciación a los usuarios.

b.1.2) Evaluación de los requisitos de la norma ISO/IEC 27001:2013.- Se evaluará el cumplimiento de cada uno de los requisitos de la norma ISO/IEC 27001:2013 en DIRECTV.

Se generará como entregable un documento de la evaluación de los requisitos de la norma ISO/IEC 27001:2013.

b.2) Establecimiento de Gobierno de Seguridad.- Esta sección contiene:

b.2.1) Marco de Gobierno de Seguridad de la Información.- Se establecerá un marco de gobierno de la Seguridad de la Información que permita tangibilizar los beneficios de poder contribuir con el logro de los objetivos estratégicos del negocio, incrementar la calidad del servicio, identificar riesgos de seguridad y dar cumplimiento a los requisitos de la norma ISO/IEC 27001:2013, a través de un modelo bien definido de roles y responsabilidades.

Se generarán como entregables, los siguientes documentos:

- Manual de la Función de Seguridad de la Información.
- Manual de Roles y Responsabilidades de Seguridad de la Información.
- Plan de Concienciación a los Usuarios.

b.2.2) Marco Normativo de Seguridad.- Se desarrollarán y/o adecuarán las principales políticas, procedimientos y estándares de configuración requeridos por el Área de Seguridad de la Información.

Se generará como entregable un documento por cada política. Para precautelar la información confidencial de DIRECTV se acordó con el personal de la Compañía, que las políticas y procedimientos generados como parte del Marco Normativo de Seguridad no se incluirán en el presente trabajo de titulación. En esta sección se incluirá una pequeña descripción de cada una de las políticas, manuales y procedimientos que serán desarrollados para DIRECTV.

c) Fase III - Presentar

c.1) Armado de Entregables.- Durante la ejecución de las diferentes fases, se entregarán parcialmente los documentos e informes resultantes; sin embargo, durante esta fase, se realizará el ajuste final en caso de ser necesario a satisfacción de la Compañía.

Si el caso lo amerita, se generarán como entregables los documentos e informes resultantes actualizados.

c.2) Presentación de Resultados.- Contendrá los resultados del alistamiento del SGSI, los mismos que serán socializados a la Alta Administración de DIRECTV.

Se generará como entregable una presentación ejecutiva.

Justificación

DIRECTV no cuenta con un área de Seguridad de la Información local que le permita establecer la responsabilidad y autoridad para la gestión de seguridad de los recursos de información en toda la Compañía.

DIRECTV, como la mayoría de las organizaciones del país siguen haciendo frente a los desafíos que plantean la Seguridad y Privacidad de la Información, como el robo de identidad, fugas de datos, fraudes en cuentas bancarias, phishing, y una gran cantidad de otros ataques internos y externos.

Por lo antes descrito y por un proceso de mejora continua para el área de Seguridad de la Información y una integración en el núcleo de los procesos de negocio de DIRECTV, se ha seleccionado el tema: “Definición y Ejecución del Proceso de Alistamiento del Sistema de Gestión de Seguridad de la Información (SGSI) en DIRECTV”, para el desarrollo del presente trabajo de titulación.

Objetivo General

Establecer el plan de alistamiento y la documentación requerida como base para la posterior implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

Objetivos específicos

- Definir un plan detallado de trabajo.
- Definir un marco de evaluación de los controles o directrices que DIRECTV deberá implementar.
- Definir un Plan Estratégico de Seguridad de la Información.
- Desarrollar el Marco Normativo Básico de Seguridad de la Información, esto incluirá la elaboración de la Política de Gestión de Seguridad de la Información.
- Definir un Marco de Gobierno de Seguridad de la Información.

1. Capítulo I Marco Teórico

1.1. Introducción a la Seguridad de la Información

1.1.1. Definiciones

1.1.1.1. Información

La información es un activo que, al igual que otros activos comerciales importantes, tiene un valor para el negocio de una organización y, por consiguiente debe ser adecuadamente protegida. Existen varias maneras de almacenar la información, de forma digital (por ejemplo, archivos de datos almacenados en medios electrónicos u ópticos), de forma material (por ejemplo, en papel), así como la información que se almacena indirectamente en el conocimiento de cada uno de los empleados de la organización. En la mayoría de las organizaciones, la información puede ser transmitida por diversos medios, como lo son: mensajería, comunicación electrónica o verbal. Cualquiera que sea la forma de transmitir esta información, se requiere siempre de una protección adecuada (ISO/IEC 27000:2014, 2014, p. 13).

En la actualidad, la mayoría de las empresas u organizaciones consideran a la información como el activo más significativo, esto ha conllevado a que dichas empresas u organizaciones tomen en serio los temas de seguridad de la información, para protegerla y asegurarse que no existan fugas de información hacia terceros.

1.1.1.2. Amenaza

Causa potencial de un incidente no deseado, el cual puede producir daño a un sistema u organización (ISO/IEC 27000:2014, 2014, p. 11).

1.1.1.3. Vulnerabilidad

Debilidad de un activo o un control que puede ser explotado por una o más amenazas (ISO/IEC 27000:2014, 2014, p. 12).

1.1.1.4. Riesgo

Efecto de incertidumbre sobre objetivos. En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información se pueden expresar como efecto de incertidumbre sobre los objetivos de la seguridad de la información (ISO/IEC 27000:2014, 2014, p. 8).

Se conoce al riesgo como la probabilidad de que ocurra un evento, y por consiguiente se derive en las consecuencias negativas del mismo.

1.1.1.5. Riesgo Inherente

Se considera riesgo inherente, al riesgo propio de cada organización de acuerdo a su actividad (ISO/IEC 27000:2014, 2014, p. 8).

1.1.1.6. Riesgo Residual

Es el riesgo resultante que se obtiene, luego de realizar el tratamiento a los riesgos de una organización (ISO/IEC 27000:2014, 2014, p. 8).

1.1.1.7. Identificación del Riesgo

Es el proceso que se realiza para encontrar, reconocer y describir los riesgos de una organización (ISO/IEC 27000:2014, 2014, p. 10).

1.1.1.8. Análisis del Riesgo

Es el proceso que se realiza para comprender la naturaleza del riesgo y determinar el nivel de riesgo que existe en una organización (ISO/IEC 27000:2014, 2014, p. 9).

1.1.1.9. Evaluación del Riesgo

Consiste en un proceso exhaustivo para la identificación, análisis y evaluación de los riesgos en una organización (ISO/IEC 27000:2014, 2014, p. 9).

1.1.1.10. Aceptación del Riesgo

Es cuando la organización asume un riesgo en particular. La aceptación de un riesgo puede ocurrir durante el proceso de tratamiento de los riesgos, o

también, se puede dar el caso que la organización asuma el riesgo sin existir el tratamiento de los mismos (ISO/IEC 27000:2014, 2014, p. 9).

1.1.1.11. Gestión del Riesgo

Actividades coordinadas para dirigir y controlar los riesgos en una organización (ISO/IEC 27000:2014, 2014, p. 10).

1.1.1.12. Control

Un control se define como una medida que modifica el riesgo (ISO/IEC 27000:2014, 2014, p. 2).

1.1.1.13. Objetivo de Control

El objetivo de control describe lo que se quiere lograr como resultado de la implementación de controles (ISO/IEC 27000:2014, 2014, p. 3).

1.1.1.14. Seguridad de la Información

La seguridad de la información se conoce como la preservación de la confidencialidad, integridad y disponibilidad del activo más importante en una organización (ISO/IEC 27000:2014, 2014, p. 4).

1.1.1.15. Continuidad de la Seguridad de la Información

Son los procesos y procedimientos para garantizar que las operaciones de seguridad de la información se encuentren siempre disponibles (ISO/IEC 27000:2014, 2014, p. 4).

1.1.1.16. Evento de Seguridad de la Información

Se conoce como evento de seguridad de la información a una ocurrencia identificada de un sistema, servicio o estado de la red, que indica una posible violación de la política de seguridad de la información o la falta de controles (ISO/IEC 27000:2014, 2014, p. 5).

1.1.1.17. Incidente de Seguridad de la Información

Se conoce como incidente de seguridad de la información a una serie de eventos no deseados o inesperados, los mismos que pueden comprometer las operaciones de negocio y amenazar la seguridad de la información de una organización (ISO/IEC 27000:2014, 2014, p. 5).

1.1.1.18. Gestión de Incidentes de Seguridad de la Información

Son los procesos que se utilizan para detectar, informar, evaluar, responder a, tratar con, y aprender de los incidentes de seguridad de la información que ocurran en una organización (ISO/IEC 27000:2014, 2014, p. 5).

1.1.2. Importancia de la Seguridad

1.1.2.1. Introducción

En los últimos años la seguridad de los sistemas de información se ha convertido en un elemento fundamental para el desarrollo de la sociedad, esto se debe a varios factores, entre ellos se encuentran la interconectividad y la interoperabilidad de las redes, los equipos automatizados, las aplicaciones y la tendencia cada vez más dominante de las empresas (Areitio, 2008, p. 2).

La seguridad ha sufrido un cambio en el ámbito de su utilización, en un inicio únicamente se utilizaba para preservar la información clasificada del gobierno respecto a temas diplomáticos o militares. En la actualidad la seguridad cubre varios temas de diferente índole, como lo son: transacciones financieras, acuerdos contractuales, información personal, archivos médicos y comerciales, inteligencia ambiental, negocios por internet, etc. Lo descrito anteriormente ha elevado la importancia de la seguridad, lo cual la ha convertido en una disciplina cada vez más crítica, necesaria y obligatoria para todo tipo de proyectos de sistemas de información (Areitio, 2008, p. 2).

La información de una organización siempre va a ser importante. Las empresas u organizaciones se respaldan a partir de la información que operan, si los datos manejados en dichas empresas u organizaciones no cuentan con los tres

elementos fundamentales de la seguridad de la información (confidencialidad, integridad y disponibilidad), no se asegura que esta información sea válida y confiable.

Adicionalmente, la mayoría de las empresas u organizaciones no se enfocan en temas de protección y cuidado a la información, por cuestiones de costos. Sin embargo, la inseguridad tiene un costo aún mayor, y en muchas ocasiones esto deriva en pérdidas económicas, la imagen o reputación alterada de la organización, y en casos más extremos, la inseguridad tiene como resultado la pérdida de clientes o proveedores estratégicos, y, hasta multas y sanciones a los empleados de dichas empresas u organizaciones.

1.1.2.2. Actividades implicadas en la Seguridad

Todo el personal relacionado con los sistemas de información en una organización, debe tomar en cuenta las actividades de seguridad que se ejecutan dentro de la misma, a continuación se muestra cada una de estas actividades:

- Desarrolladores de aplicaciones.
- Fabricantes de productos.
- Integradores de información en las diferentes aplicaciones de la organización.
- Compradores.
- Organizaciones de la evaluación de la seguridad.
- Administradores de sistemas y de seguridad.
- Terceras partes confiables. Por ejemplo, autoridades de certificación.
- Consultores u organizaciones de servicios. Por ejemplo, *outsourcing* de la gestión de la seguridad.

A continuación, se muestran los niveles básicos de seguridad utilizados en una organización:

Tabla 1. Niveles de Seguridad

Nivel	Especificación
Aplicación	- Es lo que ve el usuario. - Es el nivel más complejo y el menos fiable. - La mayor parte de los fraudes ocurren aquí.
Middleware	- Implicados los sistemas de gestión de bases de datos y la manipulación del software.
Sistema Operativo	- Se trata de la gestión de ficheros y las comunicaciones.
Hardware	- Es el nivel menos complejo y el más fiable. - Características de seguridad en las **CPU** y en el hardware de gestión de memoria (por ejemplo, para evitar desbordamientos de buffer o pila).

Tomado de Areitio, 2008, p. 5.

1.1.3. Elementos de Seguridad de la Información

1.1.3.1. Confidencialidad

La confidencialidad es la propiedad de la seguridad de la información que asegura el acceso a la información, únicamente a personas o sistemas que cuenten con la debida autorización. Por ejemplo, una transacción de tarjeta de crédito en internet, primeramente el número de tarjeta de crédito se transmite desde el comprador al comerciante y desde el comerciante a una red de procesamiento de transacciones. El sistema aplica la propiedad de "confidencialidad" mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Cuando alguien no autorizado obtiene el número de la tarjeta, se ha producido una violación de la confidencialidad (González, 2014, pp. 165-166).

Dentro de una organización, existe información que es considerada extremadamente valiosa, por lo cual, dicha información debe contar con un mayor grado de confidencialidad, para lograr este objetivo, se deben aplicar mayores niveles de seguridad a la estructura tecnológica y humana, y llegar a proteger de manera adecuada la información sensible de una empresa u organización.

Existen varias formas que se presentan durante la pérdida de la confidencialidad de la información, entre las principales, se encuentran: pérdida de un computador portátil con información valiosa de una empresa u organización, permitir que se pueda visualizar información confidencial en los computadores personales de los empleados, por no bloquear las pantallas de los monitores cuando abandonan su puesto de trabajo, la publicación de información privada, etc. Todos los casos expuestos pueden llegar a convertirse en una violación de la confidencialidad de la información de una empresa u organización.

1.1.3.2. Integridad

La integridad es la propiedad de la seguridad de la información que busca mantener con exactitud la información tal cual fue generada, desde su creación hasta su destrucción. Cuando un empleado, programa o proceso modifica o elimina los datos relevantes que son parte de la información de una organización, se deriva en la violación de integridad (González, 2014, p. 166).

Conseguir la integridad en la información de una organización, es asegurarse que únicamente personal autorizado pueda realizar modificaciones a nivel de forma y contenido de la información, así como los ambientes en los cuales la información puede ser almacenada.

1.1.3.3. Disponibilidad

La disponibilidad es la propiedad de la seguridad de la información que asegura que la información siempre se encuentre a disposición de personal autorizado que accede a ella, en el momento y en el medio que se requiere (González, 2014, pp. 167).

En la actualidad, las empresas o negocios, para el control y administración de la seguridad de la información, cuentan con la ayuda de sistemas de gestión, los cuales permiten conocer, administrar y minimizar los posibles riesgos que atenten contra la seguridad de la información de dichas empresas o negocios (González, 2014, pp. 167).

En los últimos años, las empresas u organizaciones, se han sentido respaldadas para los temas de control, administración y seguimiento de la seguridad de la información. Esto se debe a la inclusión de sistemas de gestión, los cuales permiten la reducción de posibles riesgos que afectan la seguridad de cada uno de los procesos que contienen la información de dichas empresas u organizaciones.

La disponibilidad de la información debe asegurar de manera continua el acceso a los sistemas informáticos. Para cumplir con esta propiedad de la seguridad de la información, se debe garantizar que los aplicativos se encuentren siempre funcionando, para que los usuarios puedan acceder a los datos en el momento que ellos lo requieran.

1.1.4. Áreas de Proceso de la Seguridad de la Información

1.1.4.1. Riesgos

El proceso de gestión de riesgos es el encargado de identificar y priorizar los peligros congénitos al desarrollo de un producto, sistema u organización. La gestión del riesgo es el proceso que se encarga de identificar y cuantificar la probabilidad de que se produzcan amenazas, con el objetivo de establecer un nivel aceptable del riesgo para la organización. La identificación de problemas antes de que aparezcan, se conoce en el mundo de la seguridad de la información como Valoración de Riesgos (Areitio, 2008, pp. 7-8).

Las empresas u organizaciones utilizan un proceso de gestión de riesgos. Como primer paso se identifica las capacidades actuales en lo que se refiere a seguridad de la información. Luego, el objetivo es contar con una visión general sobre lo que tiene que ejecutarse para la mitigación de los riesgos identificados. Como siguiente paso, se realiza la evaluación de los controles que se deben implementar a corto, mediano y largo plazo. Finalmente, esta fase concluye con el análisis respectivo, para validar si las decisiones tomadas fueron las correctas.

Existen medidas, controles o contramedidas para mitigar los riesgos de una organización. Estos controles dependiendo de las circunstancias, pueden actuar contra la amenaza, vulnerabilidad, el impacto o contra el propio riesgo. No es recomendable mitigar todos los riesgos de forma completa, debido, en la mayoría de los casos a los elevados costos económicos, y a las incertidumbres asociadas que se presentan (Areitio, 2008, pp. 7-8).

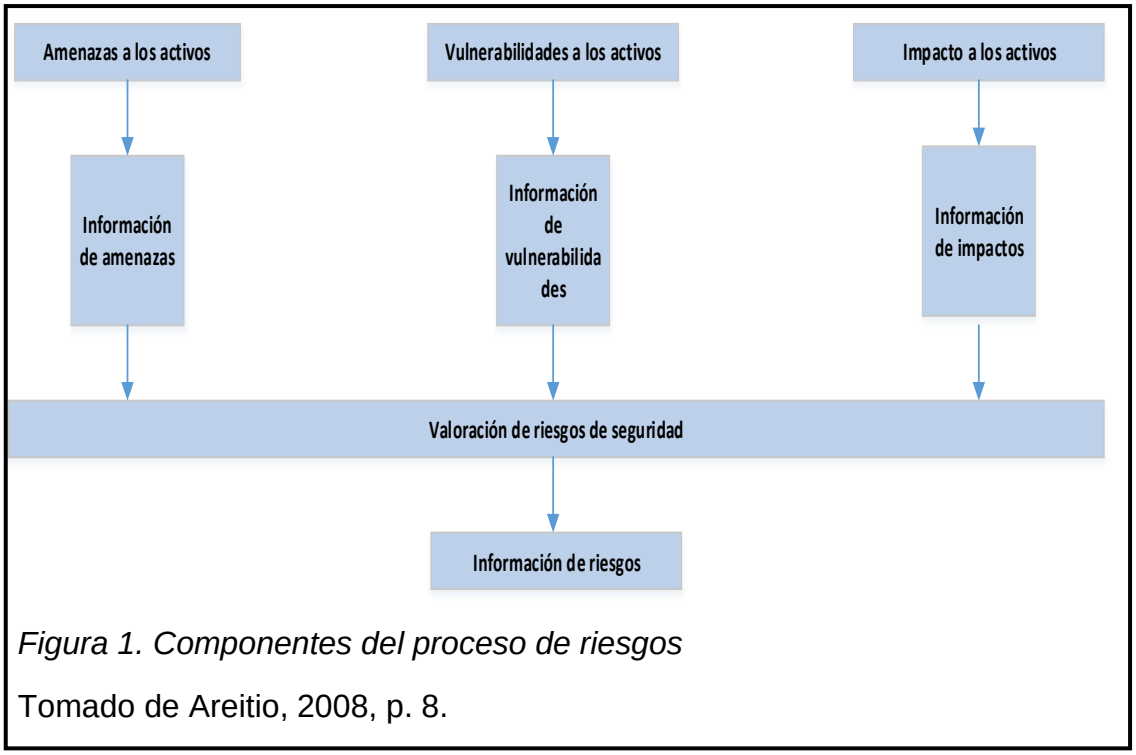


Figura 1. Componentes del proceso de riesgos

Tomado de Areitio, 2008, p. 8.

1.1.4.2. Ingeniería

El proceso de ingeniería de seguridad se desarrolla junto con otras disciplinas de la ingeniería, con el fin de determinar e implementar soluciones a los problemas presentados por amenazas y peligros. Las fases del proceso de ingeniería de seguridad son: concepto, diseño, implementación, verificación, despliegue, operación, mantenimiento y eliminación (Areitio, 2008, pp. 8-9).

El proceso de ingeniería de seguridad durante las etapas del ciclo de vida de un sistema, es el encargado de validar que los riesgos identificados sean considerados, analizados y alineados con los productos y aplicaciones de la organización. El proceso de ingeniería de seguridad es considerado fundamental dentro de los procesos de la seguridad de la información, debido a

que este proceso participa en la validación de las funcionalidades de cada uno de los sistemas, verificando de una manera óptima la seguridad de los mismos cuando se encuentran operando.

Durante el proceso de ingeniería de seguridad se ha definido una fase denominada “creación de soluciones”, la cual se basa en la identificación de posibles alternativas a los problemas de seguridad detallados durante procesos anteriores, luego se realiza un análisis y evaluación de los mismos, y finalmente, se establece la solución más óptima y la cual satisfaga las debilidades de seguridad en los problemas identificados.

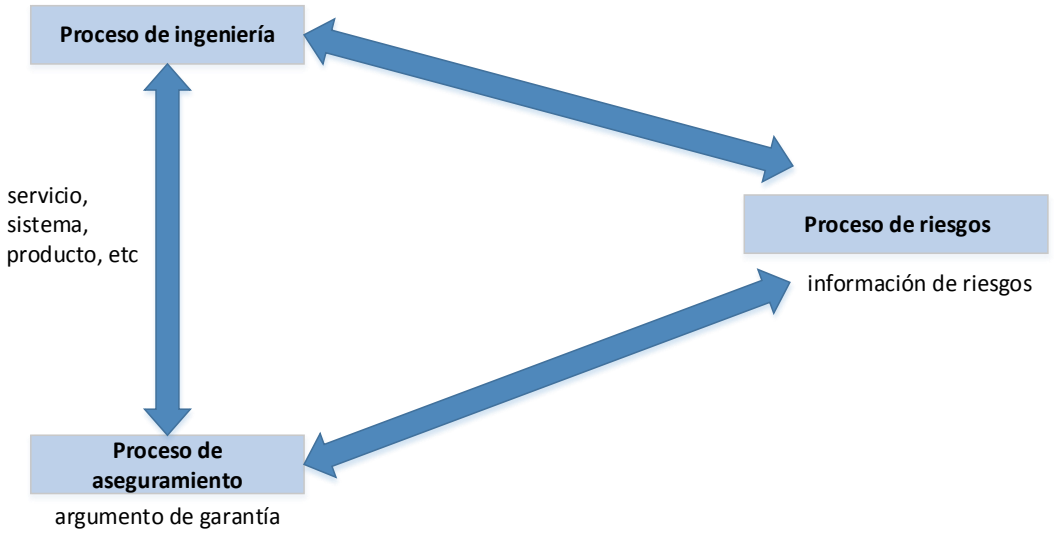


Figura 2. Áreas de proceso de la seguridad

Tomado de Areitio, 2008, p. 9.

1.1.4.3. Aseguramiento

El proceso de aseguramiento en una organización se define como el grado de confianza que satisface los requisitos de seguridad (Areitio, 2008, pp. 9-10).

Para el cumplimiento de los requerimientos de seguridad, es importante recalcar que todo sistema maduro de gestión de seguridad, garantiza la repetición continua de los resultados durante los procesos de ingeniería. Es decir, los controles implementados por una organización, no deberán ser creados cada vez que exista la manifestación de una amenaza.

Este proceso no es el encargado de implementar controles adicionales a la gestión del cálculo de riesgos de seguridad. Sin embargo, una de sus principales cualidades es proveer procedimientos estratégicos para reducir riesgos anticipados, que se generan por la implementación de controles.

Un proceso de aseguramiento es exitoso, siempre y cuando, los controles funcionen, tal y como fueron definidos desde un principio.

1.2. Normativas en Seguridad

1.2.1. Introducción a los estándares de seguridad de la información

A continuación se puede visualizar los tres modelos prioritarios con respecto a la gestión de la seguridad de la información en una organización:

- Familia ISO/IEC 27000: es un conjunto de estándares ya publicados o en fase de desarrollo, que proporcionan un marco de gestión de seguridad de la información.
- COBIT: es un marco de control que busca la gestión de procesos relacionados con tecnologías de información y su integración con el negocio.
- ITIL: es un marco de servicios donde se recopilan las mejores prácticas para la gestión de servicios relacionados con tecnologías de información.

COBIT como ITIL no son estándares, son marcos de trabajo (*frameworks*), que proveen mejores prácticas para la gestión de lo relacionado con tecnologías de información. Se integran perfectamente con la Norma ISO/IEC 27000 (familia de varios estándares), ya que igualmente se encuentran concebidos sobre el ciclo de mejora continua PDCA (Planificar-Hacer-Verificar-Actuar), y se pueden mapear entre sí.

1.2.2. Introducción a la familia ISO/IEC 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) (CCIA, s.f.).

A continuación se muestra la figura 1.3, en la cual se puede visualizar las relaciones entre la familia de normas ISO/IEC 27000:

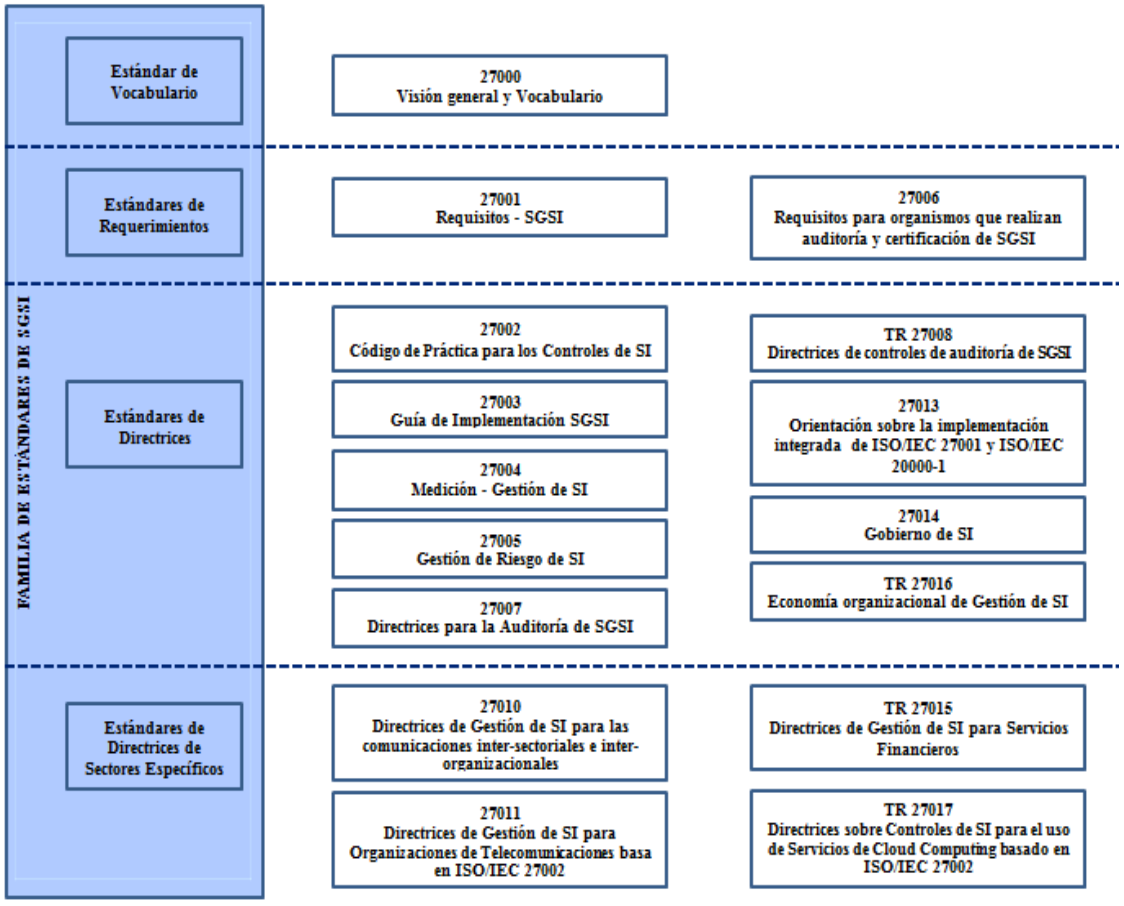


Figura 3. Normas ISO/IEC 27000

Tomado de ISO/IEC 27000:2014, 2014, p. 20.

1.2.2.1. ISO/IEC 27000

Esta norma contempla todos los aspectos fundamentales de un sistema de gestión de seguridad de la información (Datateca, s.f.).

Adicionalmente, en la presente norma se define el vocabulario estándar utilizado en la familia ISO/IEC 27000 (CCIA, s.f.).

La tercera edición de esta norma fue publicada el 15 de enero de 2014.

1.2.2.2. ISO/IEC 27001

Esta norma específica los requisitos a cumplir para la implementación de un sistema de gestión de seguridad de la información, certificable acorde a la familia de normas ISO/IEC 27000 (CCIA, s.f.).

El objetivo fundamental de esta norma es definir cómo es el sistema de gestión de seguridad de la información, cómo se gestiona y cuáles son las responsabilidades de los participantes (CCIA, s.f.).

La segunda edición de esta norma fue publicada el 01 de octubre de 2013.

1.2.2.3. ISO/IEC 27002

Esta norma no certificable, es un código de buenas prácticas que describe los objetivos de control y controles recomendables en los aspectos de seguridad de la información (Datateca, s.f.).

La norma ISO/IEC 27002 contiene recomendaciones sobre las medidas a seguir para asegurar los sistemas de información de las empresas u organizaciones. Esta norma describe los objetivos de control, que no son más que los aspectos que se deben analizar para garantizar la seguridad de la información en una organización, y especifica los controles para implementarlos, que no son más que las medidas que se deben tomar (CCIA, s.f.).

La última edición de esta norma fue publicada en el año 2013.

1.2.2.4. ISO/IEC 27003

La norma ISO/IEC 27003 tiene como objetivo el describir todos los aspectos necesarios para el diseño e implementación de un sistema de gestión de seguridad de la información de acuerdo a la norma certificable ISO/IEC 27001 (Datateca, s.f.).

La primera edición de esta norma fue publicada el 01 de febrero de 2010.

1.2.2.5. ISO/IEC 27004

La norma ISO/IEC 27004 es la encargada de especificar las métricas y las técnicas de medida aplicables, para determinar la eficacia de un sistema de gestión de seguridad de la información y de los controles relacionados (CCIA, s.f.).

La primera edición de esta norma fue publicada el 15 de diciembre de 2009.

1.2.2.6. ISO/IEC 27005

La norma ISO/IEC 27005 tiene el objetivo de proporcionar las pautas necesarias para la gestión del riesgo en la seguridad de la información. Esta norma es una guía fundamental para el éxito de la seguridad de la información en una organización, basada en un enfoque de gestión de riesgos (Datateca, s.f.).

La segunda edición de esta norma fue publicada el 01 de junio de 2011.

1.2.2.7. ISO/IEC 27006

La norma ISO/IEC 27006 específica los requisitos que deben cumplir las organizaciones que son las encargadas de emitir certificaciones ISO/IEC 27001 (CCIA, s.f.).

La segunda edición de esta norma fue publicada el 01 de diciembre de 2011.

1.2.2.8. ISO/IEC 27007

La norma ISO/IEC 27007 es una guía para las auditorías de los sistemas de gestión de seguridad de la información (Datateca, s.f.).

La primera edición de esta norma fue publicada el 14 de noviembre de 2011.

1.2.3. Norma ISO/IEC 27001

1.2.3.1. Definición

La norma ISO/IEC 27001 es la encargada de especificar los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGSI, documentado dentro del contexto global de los riesgos de negocio de una empresa (CCIA, s.f.).

Esta norma adopta el modelo PDCA (Planificar-Hacer-Verificar-Actuar), más conocido como ciclo de Deming y es utilizado para todos los procesos de una empresa u organización (CCIA, s.f.).

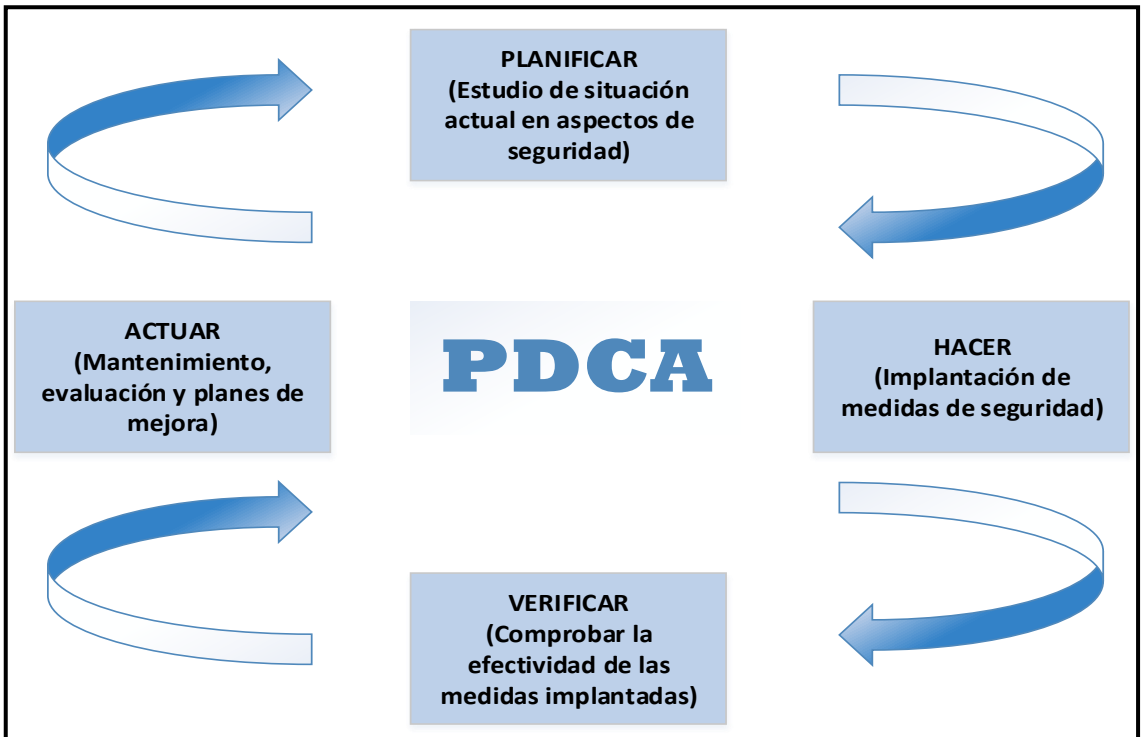


Figura 4. Ciclo de Deming

Tomado de Datateca, s.f.

A continuación se detalla cada una de las fases utilizadas en el modelo de mejora continua PDCA (ciclo de Deming):

Fase Planificación (*Plan*) [establecer el SGSI]: Esta primera fase es la encargada del análisis y recopilación de la información inicial, se realiza una identificación de la mejora que va a tener una empresa u organización referente a la gestión de seguridad de la información. Adicionalmente, en este paso se debe definir los objetivos que se desean cumplir, y se da inicio a la planificación de las actividades que van a ser implementadas en la siguiente fase.

Fase Ejecución (*Do*) [implementar y gestionar el SGSI]: Esta fase contempla la ejecución de las actividades que se definieron en la fase anterior. Es fundamental que los resultados de esta fase se encuentren debidamente documentados.

Fase Seguimiento (*Check*) [monitorizar y revisar el SGSI]: La idea de esta fase es la comparación de lo que se obtuvo frente a lo que se planteó en la fase de planeación.

Fase Mejora (*Act*) [mantener y mejorar el SGSI]: Para alcanzar la mejora continua del SGSI se debe realizar un análisis exhaustivo de las siguientes actividades: revisiones por parte de personal interno de la empresa u organización, lecciones aprendidas, los objetivos que se definieron en la fase de planeación; para luego realizar todos los ajustes que sean necesarios y dar cumplimiento con este fin.

1.2.3.2. Historia ISO/IEC 27001 - ISO/IEC 27002

A continuación se detalla una reseña del origen e historia de las normas ISO/IEC 27001 - ISO/IEC 27002:

BS-7799-1: La primera entidad de normalización a nivel mundial y una de las más antiguas (*British Standards Institution*) publicó en el año de 1995 la norma (BS-7799-1), y el objetivo de esta norma era brindar un conjunto de buenas prácticas referente a la gestión de la seguridad de la información para empresas británicas. La norma BS-7799-1, únicamente proporcionaba una

serie de recomendaciones, sin embargo, esta norma no establecía una certificación alguna, ni los mecanismos para lograrla (ISO27000, s.f.).

BS-7799-2: La segunda parte de la norma BS-7799 se publicó en el año de 1998, esta norma ya contaba con los requisitos para la implementación de un sistema de gestión de seguridad de la información certificable. Tanto la norma BS-7799-1, como la BS-7799-2 fueron revisadas en el año de 1999 (ISO27000, s.f.).

ISO 17799: En el año 2000 la Organización Internacional para la Estandarización (ISO) tomó la norma BS-7799-1 y dio lugar a la norma ISO 17799. Durante esta transición no existió algún cambio significativo (ISO27000, s.f.).

BS-7799-2:2002: En el año 2002 se publica una nueva versión de la norma BS-7799-2, con el principal objetivo de acreditar a empresas u organizaciones por medio de una entidad certificadora en Reino Unido y en otros países (ISO27000, s.f.).

ISO 27001:2005: En el año 2005 la Organización Internacional para la Estandarización (ISO), basándose en la norma BS-7799-2:2002, publicó el estándar internacional certificable ISO/IEC 27001:2005 (ISO27000, s.f.).

ISO 27002:2005: El 01 de julio del 2007, la norma ISO 17799 se renombra y pasa a ser la norma ISO 27002:2005 (ISO27000, s.f.).

A continuación se muestra la figura 1.5, en la cual se puede visualizar la cronología de la norma ISO 27001:

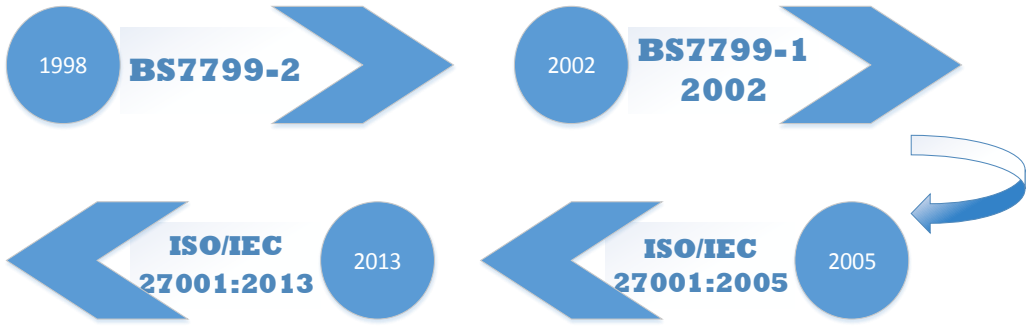


Figura 5. Cronología de la norma ISO/IEC 27001

Tomado de Magazcitum, s.f.

A continuación se muestra la figura 1.6, en la cual se puede visualizar la cronología de la norma ISO 27002:

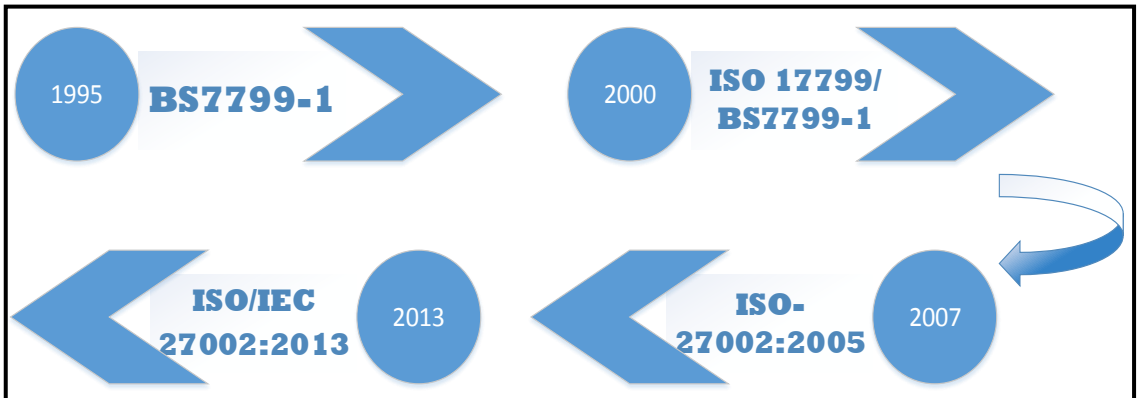


Figura 6. Cronología de la norma ISO/IEC 27002

Tomado de Magazcitum, s.f.

1.2.4. Norma ISO/IEC 27001:2103

1.2.4.1. Definición

La norma ISO/IEC 27001:2013 ha sido desarrollada con base en el anexo SL de ISO/IEC del "Suplemento Consolidado de las Directivas ISO/IEC" (anteriormente publicado como "Guía ISO:83"), el objetivo principal de esta norma es proporcionar un formato y un conjunto de lineamientos a seguir para el desarrollo documental de un sistema de gestión de seguridad de la información. Esta norma alinea bajo una misma estructura todos los documentos relacionados con los sistemas de gestión de seguridad de la información, para evitar los problemas de integración con otros marcos de referencia (Magazcitum, s.f.).

1.2.4.2. Diferencias Claves en relación a la Norma ISO/IEC 27001:2005

A continuación se detalla las diferencias fundamentales de la norma ISO/IEC 27001:2013 con respecto a la norma ISO/IEC 27001:2005:

La nueva norma se encuentra redactada en conformidad con el Anexo SL (Eficienciagerencial, s.f.).

La norma lSO/IEC 27002 ya no es una normativa de referencia (Eficienciagerencial, s.f.).

De la norma ISO/IEC 27001:2013, se eliminaron las definiciones para colocarlas en la norma ISO/IEC 27000 (Eficienciagerencial, s.f.).

Existieron cambios en la terminología. Por ejemplo, en la norma ISO/IEC 27001:2005 se utilizaba el término: Política del SGSI, en la norma ISO/IEC 27001:2013 se utiliza el término: Política de SI (Eficienciagerencial, s.f.).

Se realizó una revisión de los requisitos para el compromiso de la Alta Dirección, en la norma ISO/IEC 27001:2013 se encuentran en la Cláusula de Liderazgo (Eficienciagerencial, s.f.).

Los requerimientos de la evaluación de riesgos son más generales en la norma ISO/IEC 27001:2013, y se alinean con la norma ISO/IEC 31000, norma internacional para la gestión del riesgo (Eficienciagerencial, s.f.).

La norma ISO/IEC 27001:2013 se elaboró con mayor énfasis en el establecimiento de los objetivos, el seguimiento del desempeño y las métricas correspondientes (Eficienciagerencial, s.f.).

1.2.4.3. Estructura de la Norma ISO/IEC 27001:2013

A continuación se detalla una pequeña descripción de cada una de las secciones de la norma ISO/IEC 27001:2013:

Introducción: Uno de los cambios más significativos de la norma ISO/IEC 27001:2013 fue la eliminación de la sección “Enfoque del proceso” que contenía la norma ISO/IEC 27001:2005, en donde se describía el modelo PDCA (Planificar-Hacer-Verificar-Actuar). Adicionalmente, otro cambio fundamental fue la alineación con el Anexo SL de la ISO/IEC, sección 1 (Magazcitum, s.f.).

En esta nueva versión de la norma ISO/IEC 27001, se trabajó en el orden de la presentación de los requerimientos, como valor agregado se definió que el orden en el cual se encuentran los requisitos de la norma, no representa la

importancia de cada uno de ellos, y tampoco el orden en el cual se deben implementar.

Alcance: Esta sección define que para la implementación del sistema de gestión de seguridad de la información, se deba cumplir con cada uno de los requerimientos establecidos, los cuales se encuentran detallados desde el capítulo 4 al capítulo 10 de la norma ISO/IEC 27001:2013.

A diferencia de la versión anterior, la sección de “Alcance” en la norma ISO/IEC 27001:2013, es mucho más corta.

Referencias normativas: El estándar ISO/IEC 27002 ya no es una referencia normativa para el estándar ISO/IEC 27001:2013, sin embargo, es considerado necesario en el desarrollo de la declaración de aplicabilidad (*SOA*, por sus siglas en inglés) (Magazcitum, s.f.).

Términos y definiciones: La sección “términos y definiciones” que anteriormente se encontraba en la norma ISO/IEC 27001:2005, se colocó en la sección 3 de la norma ISO/IEC 27000 “Información General y Vocabulario”.

Es algo muy importante recalcar, que los términos y definiciones deben estar establecidos en la norma ISO/IEC 27000. En el caso que algún término no se encuentre definido en la norma ISO/IEC 27000, se debe utilizar el significado del Diccionario Inglés *Oxford*.

Contexto de la organización: El principal objetivo de esta sección es identificar los problemas externos e internos que rodean a una empresa u organización:

Establece los requisitos para la definición del contexto del sistema de gestión de seguridad de la información, sin importar el tipo de organización y su alcance (Magazcitum, s.f.).

Se ha incluido un nuevo concepto (las partes interesadas), como un elemento primordial para la definición del alcance del sistema de gestión de seguridad de la información (Magazcitum, s.f.).

Identificación y definición de las necesidades de las partes interesadas con relación a la seguridad de la información, y sus expectativas respecto al sistema de gestión de seguridad de la información (Magazcitum, s.f.).

En la norma ISO/IEC 27001:2013, “Contexto de la organización”, es una nueva sección que incluye dos temas relevantes: todo tipo de acción que se puede prevenir ante un problema o incidente, y la definición y pasos a seguir para establecer el contexto de un sistema de gestión de seguridad de la información.

Liderazgo: La sección de liderazgo es la encargada de establecer los compromisos por parte de la Alta Dirección para los temas de seguridad de la información. Adicionalmente, la gestión y cada una de las responsabilidades de la Alta Dirección, deben ser definidas en esta sección.

La Alta Dirección debe participar en un sistema de gestión de seguridad de la información con liderazgo y un compromiso ímpetu. La Alta Dirección tiene como una de sus principales responsabilidades, la definición de la política de seguridad de la información en una empresa u organización. Para lo cual, la norma ISO/IEC 27001:2013 tiene como fin, el especificar las características y propiedades que la política debe contener.

Planeación: En esta sección se definen y establecen los planes requeridos para el logro de los objetivos detallados al inicio de la implementación del Sistema de Gestión de Seguridad de la Información.

El proceso de evaluación de riesgos ha sufrido varios cambios, los cuales se muestran a continuación:

El proceso para la evaluación de riesgos ya no se encuentra enfocado en los activos, las vulnerabilidades y las amenazas (Magazcitum, s.f.).

El actual proceso para la evaluación de riesgos tiene como objetivo principal, la identificación de los riesgos asociados con la pérdida de la confidencialidad, integridad y disponibilidad de la información (Magazcitum, s.f.).

El nivel de riesgo se determina con base en la probabilidad de ocurrencia del riesgo y las consecuencias generadas (impacto), si el riesgo se materializa (Magazcitum, s.f.).

Soporte: En esta sección se establecen los requerimientos específicos de soporte, que son los que aportan a los requerimientos iniciales de cada una de las fases de la implementación de un sistema de gestión de seguridad de la información. En esta sección de la nueva versión de la norma ISO/IEC 27001, se puede visualizar una nueva definición “información documentada”, la cual sustituye a los términos “documentos” y “registros”.

Esta sección contempla un requisito indispensable que las empresas u organizaciones deben cumplir. Para poder establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información, las empresas u organizaciones se encuentran en la obligación de definir internamente los recursos necesarios para que puedan ser utilizados. De tal forma, la definición y establecimiento de los recursos necesarios, cubre todas las necesidades de los recursos que van a interactuar en un sistema de gestión de seguridad de la información.

Operación: Esta sección es la encargada de definir y establecer los requerimientos específicos para la medición del funcionamiento de un Sistema de Gestión de Seguridad de la Información, las metas y logros de la Alta Dirección en relación a temas de seguridad y la respectiva retroalimentación sobre estas.

El objetivo de esta sección es establecer un plan por parte de las empresas u organizaciones, para la administración y control de las operaciones y requerimientos de seguridad. Para lo cual, se deben ejecutar evaluaciones de riesgos por medio de intervalos periódicos y a través de aplicaciones o sistemas previamente analizados y seleccionados.

Evaluación del Desempeño: Esta sección se centra en la identificación y medición de cómo un sistema de gestión de seguridad de la información se está desempeñando y el nivel de efectividad alcanzado. Para lo cual, las

auditorías internas y las revisiones del Sistema de Gestión de Seguridad de la Información, siguen siendo las más apropiadas.

Para las revisiones del Sistema de Gestión de Seguridad de la Información, se debe tomar en cuenta la gestión y el estado de los planes de acción que se definieron en la fase “nivel de madurez”, con el objetivo de resolver las no conformidades identificadas. Adicionalmente, esta fase es la encargada de establecer “quién” y “cuando” debe ejecutar este tipo de evaluaciones.

Mejora: En esta sección se debe identificar las no conformidades encontradas, producto de la implementación del sistema de gestión de seguridad de la información, las cuales son consideradas como un elemento primordial dentro del proceso de mejora. Cuando se hayan identificado las no conformidades, el siguiente paso es la contabilización de las mismas, para luego realizar el proceso de comparación con las acciones correctivas implementadas, estableciendo que las acciones correctivas se ejecuten con éxito y no existan repeticiones.

A continuación se detallan las actividades que una empresa u organización debe realizar ante la presencia de no conformidades:

En el momento de que una empresa u organización identifique cualquier no conformidad, es primordial que se definan medidas para el control, análisis y corrección de cada una de ellas.

Durante la implementación del sistema de gestión de seguridad de la información (SGSI), se van a identificar no conformidades, las mismas que deben ser evaluadas, evitando que no se repitan o se ejecuten en otras áreas, mediante la implementación de acciones correctivas.

La mejora continua es considerada como un requisito básico de toda norma ISO/IEC en relación al desarrollo e implementación de un sistema de gestión de seguridad de la información.

A continuación se muestra todas las secciones de la estructura de la norma ISO/IEC 27001:2013:

Figura 7. Estructura de la Norma ISO/IEC 27001:2013

Tomado de Magazcitum, s.f.

A continuación se muestra el diagrama de relación de la reorganización de las secciones de la norma ISO/IEC 27001:2005 a la norma ISO/IEC 27001:2013:

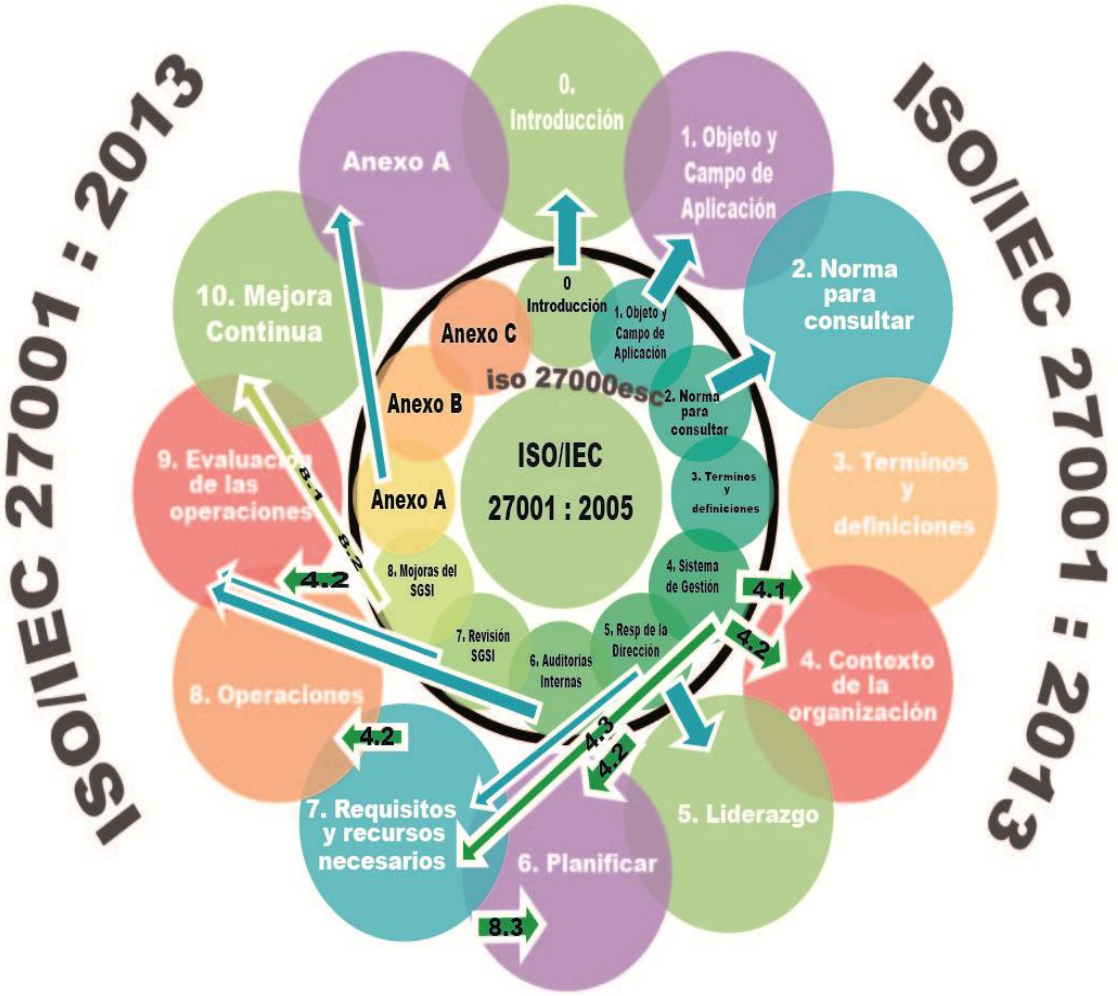


Figura 8. ISO/IEC 27001:2005 vs ISO/IEC 27001:2013

Tomado de ISO27000, s.f.

Anexo A: El título del Anexo A en esta nueva versión se conoce como: Objetivos de control y controles de referencia. Esta sección establece que los objetivos de control y los controles proceden directamente de la norma ISO/IEC 27002:2013, y que el Anexo A es utilizado en el contexto de la cláusula 6.1.3 (Tratamiento de los riesgos de seguridad de la información) de la norma ISO/IEC 27001:2013 (Bsigroup, s.f.).

Durante la revisión de la norma ISO/IEC 27002, se ha reducido el número de controles, de 133 controles a 114 controles, y el número de cláusulas ha sido expandido de 11 a 14. La mayoría de controles son idénticos o muy similares; algunos se han fusionado; algunos han sido eliminados y otros son nuevos (Bsigroup, s.f.).

A continuación se detalla el número de dominios que cuenta el Anexo A de la norma ISO/IEC 27001:2013:

Figura 9. Dominios Anexo "A" de la norma ISO/IEC 27001:2013

Tomado de Magazcitum, s.f.

A continuación se detalla la lista de controles que ya no forman parte de la norma ISO/IEC 27001:2013:

Tabla 2. Controles ausentes de la norma ISO/IEC 27001:2013

Control	**Descripción**	**Cambia por**	**Incluye los controles de la ISO 27001:2005**
A.6.1.1	Compromiso de la dirección en la seguridad de la información	Roles de la seguridad de la información y sus responsabilidades	A.6.1.3 y A.8.1.1
A.6.1.2	Coordinación de seguridad de la información	Contacto con autoridades	A.6.1.6
A.6.1.4	Proceso de autorización para medios de procesamiento de la información	Seguridad de la información en la gestión de proyectos	
A.6.2.1	Identificación de riesgos relacionados con partes externas	Política de dispositivo móvil	A.11.7.1
A.6.2.2	Tratamiento de la seguridad cuando negociamos con clientes	Teletrabajo	A.11.7.2
A.10.2.1	Entrega de servicios		
A.10.7.4	Seguridad de la documentación del sistema		
A.10.8.5	Sistemas de información de negocios		
A.10.10.2	Monitoreo del uso del sistema		

Control	Descripción	Cambia por	Incluye los controles de la ISO 27001:2005
A.10.10.5	Ingresos fallidos al sistema		
A.11.4.2	Autenticación de usuarios para conexiones externas		
A.11.4.3	Identificación de equipos en red		
A.11.4.4	Protección de puertos de diagnóstico y configuración remota		
A.11.4.6	Control de conexión a las redes		
A.11.6.2	Aislamiento de sistemas relevantes		
A.12.2.1	Validación de los datos de entrada	Controles contra malware	A.10.4.1
A.12.2.2	Control de procesamiento interno		
A.12.2.3	Autenticación de mensajes		
A.12.2.4	Validación de datos de salida		
A.12.5.4	Fuga de información		
A.15.1.5	Protección del uso inadecuado de los recursos de procesamiento de la información		

Control	Descripción	Cambia por	Incluye los controles de la ISO 27001:2005
A.15.3.2	Protección de las herramientas de auditoría de sistemas de información		

Tomado de Magazcitum, s.f.

A continuación se detalla la lista de los nuevos controles propuestos para la norma ISO/IEC 27001:2013:

Tabla 3. Nuevos controles de la norma ISO/IEC 27001:2013

Control	Descripción	Absorbe los controles de la ISO 27001:2005
A.6.1.5	Seguridad de la información en la gestión de proyectos	
A.12.6.2	Restricciones en la instalación de software	
A.14.2.1	Política de desarrollo seguro	
A.14.2.5	Principios de ingeniería de sistemas seguros	
A.14.2.6	Entorno de desarrollo seguro	
A.14.2.8	Sistema de prueba de seguridad	
A.15.1.1	Política de seguridad de la información	A.6.2.3

Control	Descripción	Absorbe los controles de la ISO 27001:2005
	en las relaciones con los proveedores	
A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	
A.16.1.5	Respuesta a incidentes de seguridad de la información	
A.17.1.2	Implementar la continuidad de la seguridad de la información	
A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	

Tomado de Magazcitum, s.f.

1.2.5. Norma ISO/IEC 27002

1.2.5.1. Definición

La norma ISO/IEC 27002 es un conjunto de recomendaciones respecto a las medidas que una empresa u organización debe seguir para que los sistemas de información funcionen a cabalidad. Su objetivo principal es la definición de los aspectos prácticos/operativos para la implementación de un sistema de gestión de seguridad de la información (CCIA, s.f.).

En una empresa u organización, para poder establecer los objetivos de seguridad, se debe analizar los puntos más relevantes e importantes que hacen que un sistema informático sea seguro. La norma ISO/IEC 27002 presenta los controles necesarios que ayudarán a la empresa u organización, definir los objetivos de seguridad óptimos referente a la implementación de un sistema de gestión de seguridad de la información.

1.2.6. Norma ISO/IEC 27002:2013

1.2.6.1. Definición

La norma ISO/IEC 27002:2013 cuenta con un número menor de controles, respecto a su versión anterior. La razón de esta reducción se debe, a que existían algunos controles que se encontraban obsoletos y otros que eran muy específicos. Adicionalmente, en la nueva versión de la norma ISO/IEC 27002, se puede notar una mayor claridad en la definición de las políticas de control (CCIA, s.f.).

1.2.6.2. Diferencias Claves en relación a la Norma ISO/IEC 27002:2005

A continuación se detalla las diferencias fundamentales de la norma ISO/IEC 27002:2013 con respecto a la norma ISO/IEC 27002:2005:

Tabla 4. Diferencias entre las normas ISO/IEC 27002:2005 y 27002:2013

ISO/IEC 27002:2005	ISO/IEC 27002:2013
11 Cláusulas de controles de seguridad de la información	14 Cláusulas de controles de seguridad de la información
39 Categorías de control	35 Categorías de control
133 Controles	111 Controles
21 Controles borrados	14 Nuevos controles
NA	Cerca de 20 controles fuertemente revisados
NA	Más de 30 controles actualizados
NA	Varios controles fusionados

Tomado de CCIA, s.f.

1.2.6.3. Estructura de la Norma ISO/IEC 27002:2013

La norma ISO/IEC 27002:2013 cuenta con 14 capítulos (del 5 al 18), los cuales corresponden a las 14 secciones que forman parte de la nueva versión de esta norma. A diferencia de la norma ISO/IEC 27002:2005, esta norma cuenta con cuatro secciones de carácter técnico, una sección respecto a temas físicos, y nueve secciones sobre temas de gestión.

A continuación se lista cada una de las secciones de la norma ISO/IEC 27002:2013:

- Políticas de seguridad de la información.
- Organización de la seguridad de la Información.
- Seguridad de los recursos humanos.
- Gestión de activos.
- Control de acceso.
- Criptografía.
- Seguridad física y del entorno.
- Seguridad de las operaciones.

- Seguridad de las comunicaciones.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Relación con proveedores.
- Gestión de incidentes de seguridad de la información.
- Aspectos de seguridad de la información para la gestión de la continuidad del negocio.
- Cumplimiento.

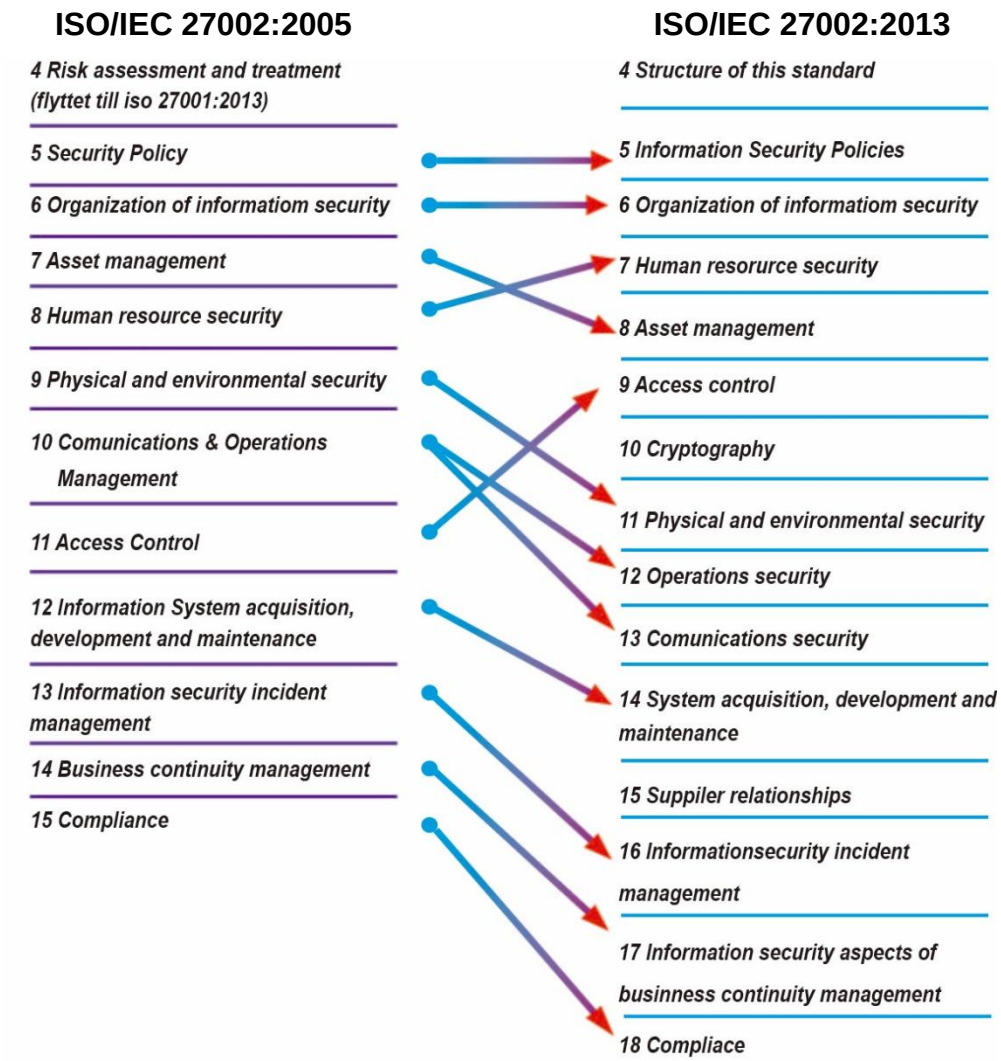


Figura 10. ISO/IEC 27002:2005 vs Norma ISO/IEC 27002:2013

Tomado de Neupart, s.f.

A continuación se detalla la lista de los controles eliminados y los nuevos controles de la norma ISO/IEC 27002:2013:

Tabla 5. Controles de la norma ISO/IEC 27002:2013

Controles eliminados	Controles nuevos
6 .1.2 Coordinador de seguridad de la información	6.1.5 Seguridad de la información en la gestión de proyectos
10.4.2 Control de código móvil	12.6.2 Restricciones en la instalación de software
11.4.2 Autenticación de usuarios en las conexiones externas	14.2.5 Principios en Ingeniería de seguridad de los sistemas
11.4.4 Diagnostico remoto y protección de la configuración de los puertos	14.2.8 Prueba de la seguridad de los sistemas
11.4.6 Control de las conexiones de las redes	17.1.2 Implementar la continuidad de la seguridad de la información
12.2.2 Control en el procesamiento interno	15.1.3 Tecnología de información y comunicación en la cadena de suministro

Tomado de CCIA, s.f.

1.3. Sistema de Gestión de la Seguridad de la Información (SGSI)

1.3.1. Definición de un SGSI

“SGSI es la abreviatura que se utiliza para referirse a un sistema de gestión de la seguridad de la información. ISMS es el concepto equivalente en el idioma inglés, siglas que corresponden a: Information Security Management System” (ISO27000, s.f.).

Un sistema de gestión de seguridad de la información, es un enfoque sistemático con el fin de establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una empresa u organización en relación con los objetivos de negocio de la misma.

Un sistema de gestión de seguridad de la información, se encuentra compuesto por políticas, procedimientos, guías, recursos y actividades asociadas, las

cuales son gestionadas por una empresa u organización con el propósito de proteger su activo más importante, la información.

1.3.2. Beneficios de un SGSI

A continuación se detalla los principales beneficios que una empresa obtendrá al momento de implementar un sistema de gestión de seguridad de la información (SGSI):

- Un análisis de riesgos, la idea fundamental de realizar este análisis es lograr la identificación de amenazas, vulnerabilidades e impactos que rodean las actividades de negocio de una empresa u organización.

- La existencia y aplicación de una mejora continua en la gestión de la seguridad de la información.

- El poder contar con procedimientos y procesos para la continuidad y disponibilidad de las operaciones de una empresa u organización.

- La existencia de una disminución de los costos que generan los incidentes de seguridad de la información.

- Establecer un grado de confianza con los clientes y *partners*.

- Obtener réditos en lo que se refiere al valor comercial de una empresa u organización, así como, ganar méritos con los clientes por una mejora de la imagen de dicha empresa u organización.

- Contar con un compromiso por parte de la Alta Dirección para los temas de gestión de seguridad de la información.

- Prevenir y detectar incidentes de seguridad de la información.

- Una evaluación continua de la seguridad de la información, con el objetivo de implementar cambios, según se los requiera.

1.3.3. Implementación de un SGSI

Para que la implementación de un sistema de gestión de seguridad de la información (SGSI) sea exitosa, se debe considerar lo siguiente:

- Definir el alcance y la planificación del sistema de gestión de seguridad de la información.

- La Alta Dirección de la empresa u organización debe comprometerse con el proyecto del sistema de gestión de seguridad de la información (SGSI) y aportar con total apoyo desde inicio a fin, para que la implementación de un SGSI sea exitosa y cumpla con las expectativas del negocio.

- Establecer el nivel de seguridad deseado, para lo cual se debe analizar y tomar en cuenta el tamaño y la complejidad de la empresa u organización.

1.3.4. Proceso de Implementación de un SGSI

Para definir y establecer la implementación de un sistema de gestión de seguridad de la información (SGSI) en una empresa u organización, se debe adoptar el modelo de mejora continua PDCA (Planificar-Hacer-Verificar-Actuar).

El modelo de mejora continua PDCA, es el encargado de definir el diseño e implementación de un sistema de gestión de seguridad de la información (SGSI), establecer revisiones periódicas y continuas para lograr una mejora del sistema, y gestionar en conjunto con la empresa u organización, la utilización de instrumentos oportunos para la medición y control de la mejora del SGSI implementado.

La idea fundamental de un sistema de gestión de seguridad de la información (SGSI), es la identificación de los objetivos y alcance del mismo, y los procesos de negocio críticos para la empresa u organización.

En la figura 1.5, se puede visualizar cada una de las fases utilizadas en el modelo de mejora continua PDCA (Planificar-Hacer-Verificar-Actuar).

1.3.5. Establecer, monitorear, mantener y mejorar un SGSI

1.3.5.1. Información General

Para establecer, monitorear, mantener y mejorar un sistema de gestión de seguridad de la información, una empresa u organización debe tomar en cuenta lo siguiente:

- Primeramente la identificación de los activos de información, y los requerimientos de seguridad asociados a los activos identificados.

- Evaluación y tratamiento de los riesgos de seguridad de la información.

- Para la gestión de riesgos inaceptables, se debe analizar, seleccionar y aplicar los controles necesarios para tratar dichos riesgos.

- Un sistema de gestión de seguridad de la información comprende un constante monitoreo, mantenimiento y mejora, de la eficacia de los controles asociados a los activos de información de una empresa u organización.

1.3.5.2. Identificación de los requisitos de Seguridad de la Información

Dentro de la estrategia de negocio y los objetivos generales de una empresa u organización, los requisitos de seguridad de la información pueden ser identificados a través de la comprensión de los siguientes puntos:

- Los activos de información identificados y el valor de cada uno de ellos.

- Las necesidades por parte del negocio para el procesamiento, almacenamiento y comunicación de la información.

- Requerimientos legales, regulatorios y contractuales.

1.3.5.3. Evaluación de los riesgos de Seguridad de la Información

El proceso de la gestión de riesgos de seguridad de la información en una empresa u organización, debe contar con un método de evaluación y tratamiento de riesgos adecuado, que puede incluir desde una estimación de

costos y beneficios, requerimientos legales, hasta las inquietudes o dudas de los grupos de interés (*stakeholders*).

Los métodos de evaluación de riesgos son los encargados de identificar, cuantificar y priorizar los riesgos contra los criterios de aceptación de riesgos y los objetivos relevantes para una empresa u organización. Los resultados deben guiar y determinar la acción de gestión adecuada y las prioridades de la gestión de riesgos de seguridad de la información, para la implementación de los controles seleccionados y de esta manera proteger a la empresa u organización de dichos riesgos.

Los métodos de evaluación de riesgos deben ejecutarse periódicamente, con el objetivo de enfrentar los cambios en los requerimientos de seguridad de la información y en la situación del riesgo, por ejemplo, en los activos, amenazas, vulnerabilidades, impactos, evaluación de riesgos, y cuando se produzcan cambios significativos. Para obtener resultados comparables y reproducibles, la evaluación de los riesgos se la debe realizar de una manera metódica y ordenada.

La norma ISO/IEC 27005 es la encargada de proporcionar una guía completa para la gestión de riesgos de seguridad de la información, incluido el asesoramiento sobre la evaluación de riesgos, tratamiento de riesgos, aceptación del riesgo, reportes de riesgos, monitoreo y revisión de riesgos.

1.3.5.4. Tratamiento de los riesgos de Seguridad de la Información

Para el tratamiento de los riesgos de seguridad de la información en una empresa u organización, se debe tomar en cuenta lo siguiente:

- La correcta aplicación de los controles adecuados para reducir los riesgos identificados.

- De una manera objetiva, aceptar los riesgos, siempre y cuando cumplan con claridad las políticas y procedimientos de aceptación de riesgos, definidos por la empresa u organización.

- Analizar la posibilidad de compartir los riesgos que se encuentran asociados a otras partes, por ejemplo, empresas externas, aseguradoras o proveedores de servicio.

1.3.5.5. Selección e implementación de controles

Los controles son los encargados de asegurar que los riesgos identificados se reduzcan a un nivel aceptable. Para lo cual se debe tener en cuenta lo siguiente:

- Los requerimientos y restricciones de la legislación y reglamentación nacional e internacional.

- Objetivos de la empresa u organización.

- Requisitos operativos y limitaciones.

- La necesidad de equilibrar la inversión en la implementación de los controles contra la pérdida que pueda derivarse de los incidentes de seguridad de la información.

1.3.5.6. Monitorear, mantener y mejorar la eficacia del SGSI

Para mantener y mejorar un sistema de gestión de seguridad de la información, las empresas u organizaciones son las encargadas de evaluar el desempeño del sistema contra sus políticas, procedimientos y objetivos.

Cuando se realiza la revisión de un sistema de gestión de seguridad de la información (SGSI), el principal objetivo es comprobar que el sistema de gestión cuente con controles específicos para el tratamiento de riesgos, los cuales deben encontrarse definidos dentro del alcance del SGSI.

Es muy valioso las actividades de monitoreo, mantenimiento y mejora de un SGSI, ya que a partir de los registros de los eventos monitoreados, se puede evidenciar la verificación y trazabilidad de las acciones correctivas, preventivas y de mejora.

1.3.5.7. Mejora Continua

A continuación se detallan las siguientes acciones de mejora:

- Analizar y evaluar la situación actual, con el objetivo de identificar áreas de mejora.

- Definir y establecer los objetivos para la mejora del SGSI.

- Para lograr los objetivos propuestos de la mejora continua del SGSI, se debe analizar, identificar, evaluar e implementar las posibles soluciones.

- Para poder determinar el cumplimiento de los objetivos de mejora, se debe realizar una medición, verificación, análisis y evaluación de los resultados obtenidos.

- Cuando existan cambios que se deban aplicar al SGSI, es primordial que primeramente se formalicen dichos cambios.

2. Capítulo II Metodología

2.1. Método Científico

2.1.1. Metodología Deductiva

El principal material que se utilizó en el presente trabajo de titulación, fue la norma ISO/IEC 27001:2013. Cabe indicar que es una norma internacional, y que será de gran ayuda para DIRECTV, en el momento que la Compañía decida certificar su Sistema de Gestión de la Seguridad de la información.

Se seleccionó la metodología deductiva, debido a que el presente trabajo de titulación fue de lo general a lo particular, de lo complejo a lo simple. Por lo cual, se hizo énfasis en la norma ISO/IEC 27001:2013, esta norma fue la referencia inicial, para luego definir el marco de evaluación del estado actual de la Gestión de la Seguridad de la Información en DIRECTV.

El objetivo principal del método deductivo es partir de datos generales válidos, y así poder deducir varias suposiciones, es decir; iniciar con verdades que se encuentran establecidas como principios generales, para proceder con la aplicación de estos puntos en casos individuales y evidenciar la validez de cada uno. La definición de un marco de evaluación para determinar el nivel de madurez de la seguridad de la información en DIRECTV es muy importante, puesto que está estrechamente relacionado con el objetivo que se persigue a través del presente trabajo de titulación. Esta definición permitirá que cualquier lector o nuevo interesado en el proyecto, pueda visualizar claramente cuál es el punto de referencia desde donde partió el mismo, y permitirá continuamente monitorear el nivel de avance de proyectos o iniciativas relacionadas con la Seguridad de la Información en DIRECTV.

La metodología deductiva se aplicará en el capítulo “3. Desarrollo del Proyecto”, del presente trabajo de titulación.

2.2. Método Técnico

2.2.1. Metodología Evaluación de Riesgos de la Seguridad de la Información

2.2.1.1. Introducción

La metodología “Evaluación de Riesgos de la Seguridad de la Información” (Deloitte, 2008), se encuentra estructurada para soportar dos objetivos primarios de la seguridad de la información:

- Identificar y mitigar los riesgos de la seguridad de la información en una organización.
- Evaluar un sistema de gestión de la seguridad de la información en una organización.

El objetivo “evaluar un sistema de gestión de la seguridad de la información en una organización”, incluye los pasos necesarios de trabajo y tareas claves para el desarrollo del tema “Definición y Ejecución del Proceso de Alistamiento del Sistema de Gestión de Seguridad de la Información (SGSI) en DIRECTV”, en el presente trabajo de titulación.

2.2.2. Metodología Evaluación del Sistema

2.2.2.1. Introducción

La metodología “Evaluación del Sistema” se ha diseñado para evaluar un sistema de gestión de la seguridad de la información en una organización (Deloitte, 2008, p. 44).

2.2.2.2. Definiciones

Para entender la metodología “Evaluación del Sistema”, se debe tener claro ciertos términos, los cuales son primordiales para el proceso de evaluación.

Estos términos pueden encontrarse definidos de diferentes maneras. En el presente trabajo de titulación, en el capítulo “1. Marco Teórico”, se encuentran detalladas algunas definiciones con respecto a la introducción de la seguridad

de la información. La mayoría de estos términos son utilizados en esta metodología, por lo cual, para mayor detalle de los términos utilizados en la metodología “Evaluación del Sistema”, referirse al capítulo “1. Marco Teórico”, la sección de “1.1.1 Definiciones” que se encuentra dentro del punto “1.1 Introducción a la Seguridad de la Información”.

2.2.2.3. Proceso de Evaluación del Sistema

El proceso de evaluación del sistema se encuentra compuesto por tres actividades básicas:

- Planear
- Ejecutar
- Presentar

A continuación se detalla el diagrama de proceso de la metodología “Evaluación del Sistema”, utilizada en el presente trabajo de titulación:

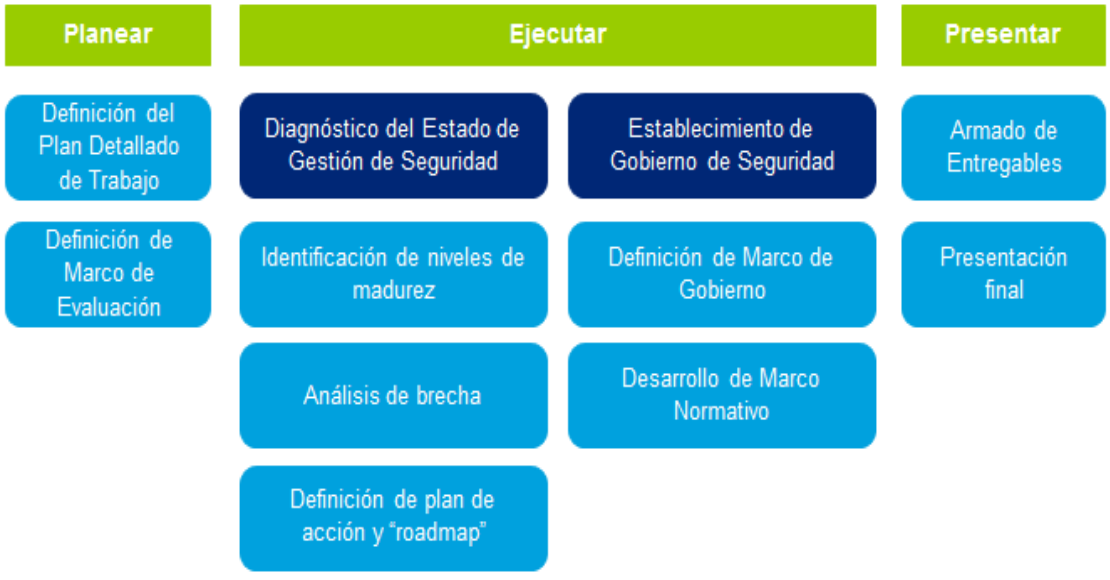


Figura 11. Diagrama de Proceso - Metodología “Evaluación del Sistema”

Tomado de Deloitte, 2008, p. 45.

1) Planear

Definición del Plan Detallado de Trabajo.- Identificar y definir el plan detallado del proyecto, el cronograma de reuniones de relevamiento con personal clave y el formato de los entregables a generar.

Adicionalmente definir el esquema de gerenciamiento del proyecto, formato de los reportes de avance y frecuencia de las reuniones de seguimiento.

Definición del Marco de Evaluación.- Definir el marco de referencia contra el cual se debe realizar la evaluación del estado actual de la gestión de la seguridad de la información en la organización.

2) Ejecutar

Diagnóstico del Estado de Gestión de Seguridad

Identificación de Niveles de Madurez y Análisis de Brecha.- Identificar las capacidades actuales del área de seguridad de la información para alcanzar un nivel de madurez determinado a corto, mediano y largo plazo.

Considerar criterios que permitan evaluar el estado actual de la seguridad en dominios y sub-dominios para definir planes de acción específicos basados en estos criterios.

Definición del Plan de Acción y "Roadmap".- Establecer las diferentes iniciativas o proyectos de seguridad requeridos para alcanzar el nivel de madurez deseado.

Establecimiento de Gobierno de Seguridad

Definición del Marco de Gobierno.- Establecer un marco de gobierno de la seguridad de la información.

Definición del Marco Normativo.- Desarrollar y/o adecuar las principales políticas, procedimientos y estándares de configuración requeridos por el área de seguridad de la información.

3) Presentar

Armado de Entregables.- Durante la ejecución de las diferentes tareas, entregar parcialmente los documentos e informes resultantes; sin embargo, durante esta fase, realizar el ajuste final en caso de ser necesario a satisfacción de la Compañía.

Presentación de Resultados.- Dar a conocer a la alta administración de la Compañía, los principales resultados del alistamiento del SGSI.

A continuación se detalla el diagrama de flujo sobre la metodología “Evaluación del Sistema”, utilizada en el presente trabajo de titulación:

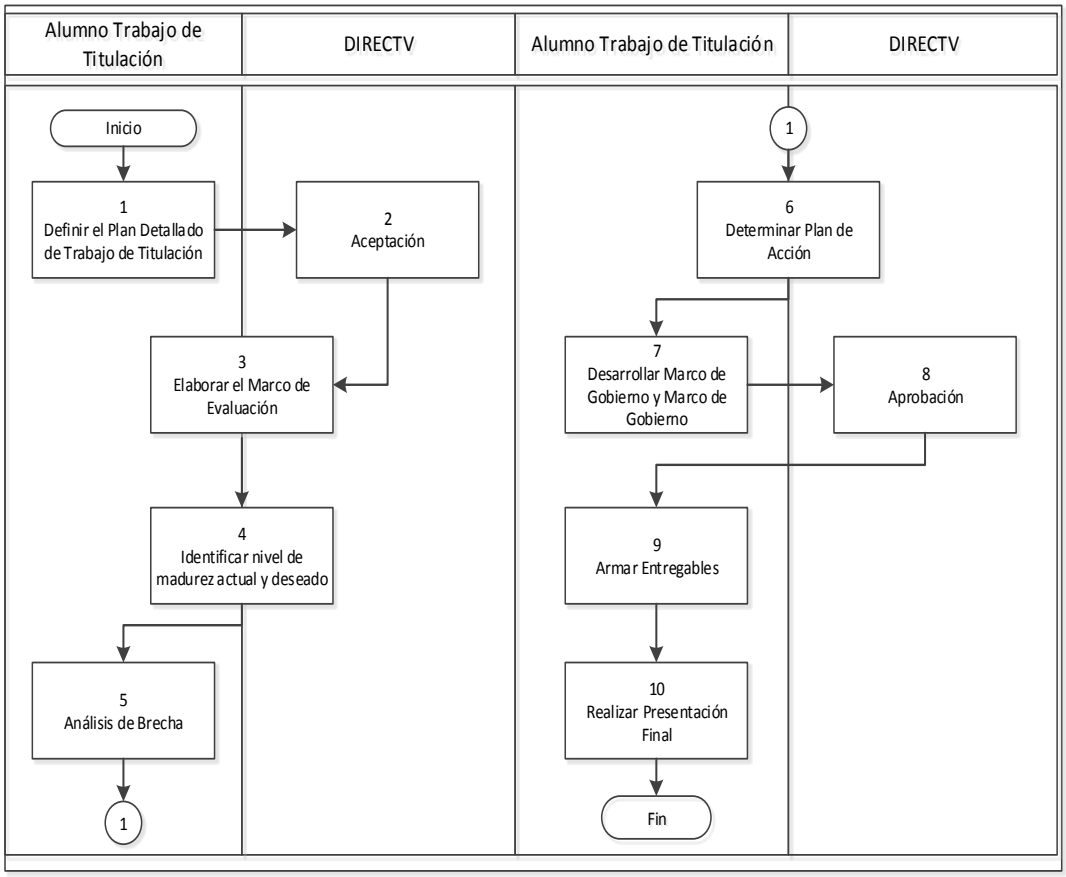


Figura 12. Diagrama de Flujo - Metodología “Evaluación del Sistema”

Tomado de Deloitte, 2008, p. 52.

2.2.2.4. Método de Evaluación del Sistema

Para establecer el nivel de madurez de un sistema de seguridad de la información, se deben considerar los procesos y prácticas de gestión que actualmente se encuentran en la Compañía, y evaluar la exitosa ejecución de los mismos. El objetivo de una estrategia e implementación "roadmap", es llegar a una madurez aceptable del sistema.

En este caso, la evaluación del sistema de seguridad de la información es esencialmente una evaluación "*Gap*"; es decir, se debe contemplar las siguientes preguntas: "¿Tienen estas capacidades?" y "¿Se están ejecutando exitosamente?".

A continuación se detalla la escala de evaluación, con el fin de medir el estado de madurez de la seguridad de la información en la organización. La escala contiene 6 rangos de evaluación (0-5):

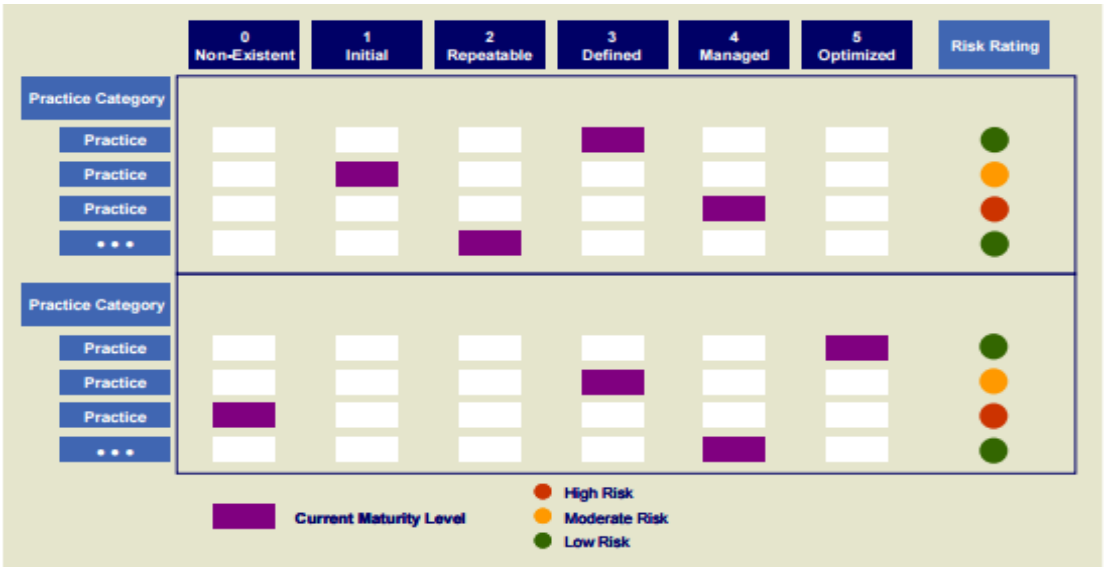


Figura 13. Nivel de Madurez

Tomado de Deloitte, 2008, p. 46.

Non-Existent (No Existe).- No existen directrices o no se encuentra evidencia de su existencia.

Initial (Inicial).- Las directrices no se encuentran estructuradas. Únicamente existen enfoques de forma individual.

Repeatable (Repetible).- Las directrices se basan en un enfoque similar de actividades, las cuales son ejecutadas por diferentes personas que desarrollan la misma tarea.

Defined (Definido).- Las directrices se encuentran estandarizadas, documentadas y comunicadas. Se cuenta con un entrenamiento disponible por cada una, sin embargo, no se aplica en forma obligatoria.

Managed (Administrado).- Las directrices se monitorean y se miden. Existe una identificación de acciones de mejora, sin embargo, estas se aplican irregularmente.

Optimized (Optimizado).- Las directrices se basan en las buenas prácticas de seguridad. Se cuenta con la evidencia de una constante mejora continua. Adicionalmente, existe la ejecución de acciones preventivas y correctivas y la respectiva medición de la eficacia de su correcta aplicación.

3. Capítulo III Desarrollo del Proyecto

3.1. Fase de Planeación

3.1.1. Plan Detallado de Trabajo

3.1.1.1. Objetivo del Plan Detallado de Trabajo

Definir y establecer un marco de referencia para la Alta Administración, con el objetivo de apoyar a Directv Ecuador, (en adelante "DIRECTV"), en el alistamiento del sistema de gestión de seguridad de la información (en adelante "SGSI"), con el fin de:

- Brindar el entendimiento de lo que el presente trabajo de titulación desea lograr para DIRECTV.

- Presentar las definiciones y lineamientos para la ejecución del alistamiento del SGSI en DIRECTV.

3.1.1.2. Gestión del Alcance

El alcance del alistamiento del SGSI consiste en establecer los lineamientos generales de gestión para la Seguridad de la Información en DIRECTV.

3.1.1.3. Matriz de Entregables

Los entregables de la definición y ejecución del proceso de alistamiento del SGSI, de acuerdo con las etapas del mismo, son los siguientes:

Tabla 6. Entregables - Alistamiento del SGSI

Fase	Entregable
Fase I - Planear	**Plan detallado de trabajo** Este documento contiene: • Entendimiento del trabajo de titulación. • Entregables del trabajo de titulación. • Plan de trabajo. • Cronograma del trabajo de titulación. • Equipo del trabajo de titulación, roles y responsabilidades.

Fase	Entregable
	• Consideraciones y expectativas.
	Marco de evaluación Contiene el marco de referencia contra el cual se realizará la evaluación del estado actual de la gestión de seguridad de la información en DIRECTV.
Fase II - Ejecutar / Diagnóstico del Estado de Gestión de Seguridad	**Plan estratégico de seguridad de la información** Contiene el análisis de brecha entre las capacidades actuales de la gestión de seguridad de la información en DIRECTV respecto a lo requerido por la norma ISO/IEC 27001:2013. Se compone de: • Niveles de madurez deseados del área a corto, mediano y largo plazo. • Planes de acción y “roadmap” de implementación. • Objetivos estratégicos del área de seguridad de la información. • Plan de concienciación a los usuarios. **Evaluación de los requisitos de la norma ISO/IEC 27001:2013** Contiene la validación del cumplimiento de cada uno de los requisitos de la norma ISO/IEC 27001:2013 en DIRECTV.
Fase II - Ejecutar / Establecimiento de Gobierno de Seguridad	**Documento de Marco de Gobierno** Contiene el establecimiento del marco de gobierno de seguridad de la información, incluye: • Un organigrama funcional del departamento de seguridad de la información y TI. • Definición detallada de roles y funciones del área. • Estructura o mapa del marco normativo de seguridad de DIRECTV. • Plan de entrenamiento a funcionarios del

Fase	Entregable
	área de seguridad de la información.
	Políticas y Procedimientos Incluye el desarrollo y/o adecuación de las principales políticas, procedimientos y estándares de configuración requeridos por el área de seguridad de la información, contempla: ***Políticas:*** • Política de Seguridad de la Información. • Política de Gestión de Activos de Información. • Metodología de Análisis de Riesgos. • Política de Gestión de Acceso a Información. • Política de Administración de Seguridad de Red. • Política de Protección y Revisión de las Pistas de Auditoría. • Política de Administración de Respaldos. • Política de Monitoreo de Recursos de los Servicios y Sistemas Informáticos. • Política de Gestión de Software. • Política de Monitoreo de Niveles de Servicio de Incidentes de Seguridad. ***Procedimientos:*** • Procedimiento de Administración de Usuarios. • Procedimiento de Utilización de Cuentas de Máximos Privilegios. • Procedimiento de Control de Acceso Físico y Ambiental del Centro de Cómputo. • Procedimiento de Administración de Respaldos. • Procedimiento de Gestión de Incidentes de Seguridad.

Fase	Entregable
Fase III - Presentar	**Presentación ejecutiva** Contiene los resultados del alistamiento del SGSI, con el objetivo de socializar los mismos a la Alta Administración de DIRECTV.

3.1.1.4. Gestión de Tiempos

La duración del presente trabajo de titulación es de 120 (ciento veinte) días, para realizar el proyecto de alistamiento del sistema de gestión de seguridad de la información (SGSI) en DIRECTV.

A continuación se presenta el cronograma general de actividades del alistamiento del SGSI en DIRECTV:

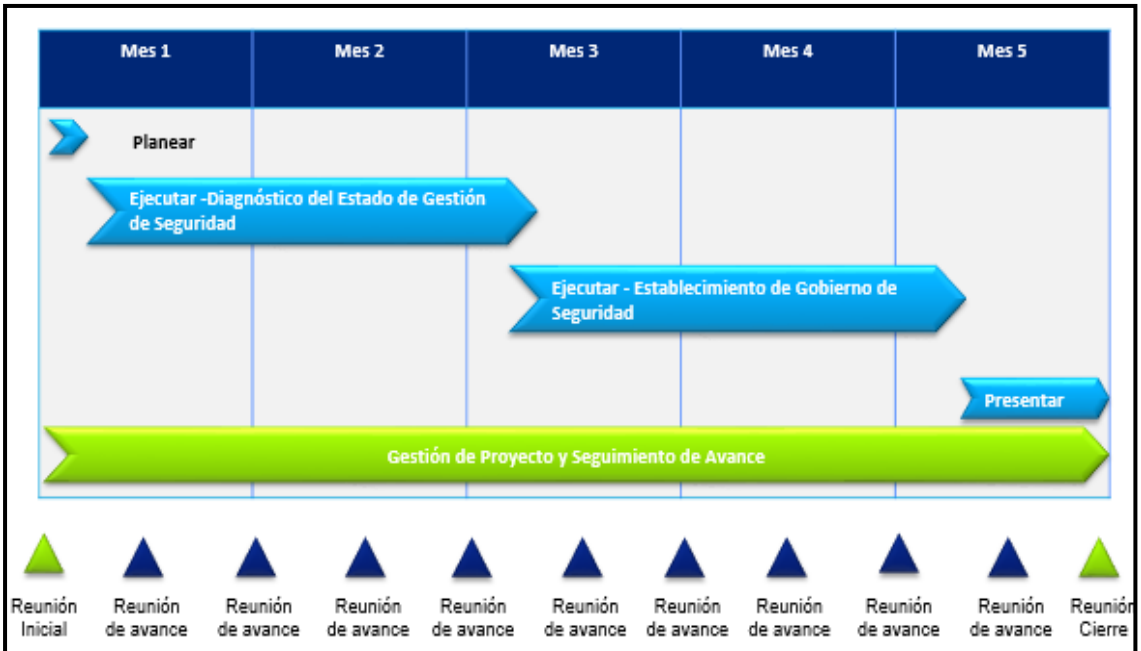


Figura 14. Cronograma de Actividades - Alistamiento del SGSI.

3.1.1.5. Control de Calidad

El proceso de control de calidad se enfoca en la identificación del cumplimiento de expectativas de los entregables del alistamiento del SGSI (ver sección 2.1.1.3). Los responsables de esta actividad son el tutor del trabajo de titulación designado por la Universidad de las Américas UDLA, y el estudiante responsable del trabajo de titulación, quienes son los encargados de validar los

entregables finales en conjunto con el Administrador de Seguridad de la Información de DIRECTV.

Para facilidad de revisión de los entregables, se ha seleccionado la siguiente nomenclatura en el nombre del archivo:

PLA Alistamiento ISO27001 2013 - Plan Detallado de Trabajo 2015 06 15 v1, donde el nombre se encuentra conformado por los siguientes elementos:

PLA: se refiere a la fase del ciclo de vida del alistamiento del SGSI, las fases son:

- PLA, Planificación.

- EJE, Ejecución.

- CIE, Cierre.

Alistamiento ISO27001 2013: es la denominación del proyecto de alistamiento del SGSI.

Plan Detallado de Trabajo: es el nombre del entregable.

2015 06 15: es la última fecha de revisión del entregable, siguiendo el formato AAAA MM DD (A: año, M: mes, D: día).

v1: es la versión del documento luego de las revisiones de DIRECTV y el estudiante del trabajo de titulación. El número será reemplazado por la palabra Final, cuando el entregable corresponda a la versión aprobada por el Administrador de Seguridad de la Información de DIRECTV.

3.1.1.6. Gestión de Riesgos

Identifica de forma general los riesgos que pueden impactar en el avance y ejecución del alistamiento del SGSI; así como también los planes de acción a ejecutar para disminuir la probabilidad de la ocurrencia de tales eventos de riesgo. Esta actividad de administración de riesgos debe realizarse durante toda la ejecución del alistamiento del SGSI.

A continuación se detalla los riesgos y cada uno de los planes de acción que pueden intervenir en la ejecución del presente alistamiento del SGSI en DIRECTV:

Tabla 7. Gestión de Riesgos - Alistamiento del SGSI

Riesgo	Plan de Acción
Falta de tiempo de la administración.	- Definir las tareas críticas y acuerdos con DIRECTV. - Planear las entrevistas necesarias con la mayor antelación posible.
Toma de decisiones inoportuna.	- Gestionar reuniones de avances quincenales y emergentes, con el objetivo de informar a la Gerencia de Infraestructura y Operaciones IT, los temas que no se han resuelto.
Inapropiada asignación de personal responsable para la aprobación de los entregables del trabajo de titulación.	- Cumplir con los tiempos acordados para la generación y aprobación de los entregables definidos en la sección 2.3.
Falta de compromiso de los recursos requeridos para cumplir con las tareas del trabajo de titulación.	- Establecer una gestión adecuada de los recursos e información necesaria para el desarrollo del trabajo de titulación.
Falta de seguimiento al desarrollo de actividades.	- Validar las responsabilidades del personal de DIRECTV. - Elaborar presentaciones puntuales sobre el avance del proyecto, dirigido a la Gerencia de Infraestructura y Operaciones IT.

Riesgo	Plan de Acción
Información desactualizada.	- Verificar que la información utilizada durante el proyecto, se encuentre vigente y esté alineada con los procesos que se ejecutan actualmente en DIRECTV.

En el ***Anexo 1*** se encuentra el documento “PLA Alistamiento ISO27001 2013 - Plan Detallado de Trabajo 2015 06 15 vFinal”, donde se puede visualizar el plan de trabajo que se va a utilizar en el alistamiento del SGSI en DIRECTV.

3.1.2. Marco de Evaluación

3.1.2.1. Objetivo del Marco de Evaluación

Definir un marco de referencia, contra el cuál se realizó la evaluación del estado actual de la gestión de la seguridad de la información en DIRECTV, como parte del alistamiento del sistema de gestión de seguridad de la información (SGSI).

3.1.2.2. Importancia del Marco de Evaluación

La definición de un marco de evaluación para determinar el nivel de madurez de la seguridad de la información en DIRECTV, es muy importante, puesto que está estrechamente relacionado con el objetivo que se persigue a través del alistamiento del SGSI. Esta definición permitirá que cualquier lector o persona interesada en el proyecto, pueda visualizar claramente cuál es el punto de referencia desde donde partió el proyecto. Adicionalmente, permitirá un monitoreo continuo del nivel de avance de proyectos o iniciativas relacionadas con la seguridad de la información en DIRECTV.

En el momento que DIRECTV decida certificar su sistema de gestión de seguridad de la información, este documento será un buen punto de partida para la reproducción de una *Declaración de Aplicabilidad*, en la cual se resumen los controles implementados y no implementados, así como las justificaciones para ambos casos.

3.1.2.3. Definición del Marco de Evaluación

Acorde al uso de la norma ISO/IEC 27001:2013, se considera que la etapa inicial consiste en establecer los lineamientos generales del SGSI, para su posterior implementación. Incluyendo como primera fase la realización de:

- Plan detallado de trabajo.

- Definición de los controles o directrices que DIRECTV deberá implementar.

- Niveles de madurez deseados.

- Planes de acción u hojas de ruta, acorde a los criterios definidos en conjunto.

- Los entregables como políticas, normas y procedimientos en base a lo requerido por la norma ISO/IEC 27001:2013.

Para cumplir con las actividades descritas, se definió un Marco de Evaluación de Seguridad de la Información. Este documento se convirtió en un insumo importante para la realización de las mismas.

En el **Anexo 2** se encuentra el documento “PLA Alistamiento ISO27001 2013 - Marco de Evaluación 2015 06 15 vFinal”, donde se puede visualizar el marco de evaluación establecido para el alistamiento del SGSI en DIRECTV.

3.2. Fase de Ejecución - Diagnóstico del Estado de Gestión de Seguridad

3.2.1. Plan Estratégico de Seguridad de la Información

3.2.1.1. Objetivo del Plan Estratégico

El Plan Estratégico de Seguridad de la Información contiene las diferentes actividades realizadas para el establecimiento del estado de gestión de seguridad de la información en DIRECTV, considerando el marco de evaluación definido en el punto *3.1.2 Marco de Evaluación*, y además, la identificación del nivel de madurez futuro que la Compañía pretende alcanzar,

mediante la definición de planes de acción, iniciativas o proyectos de seguridad con su respectiva ruta de implementación.

3.2.1.2. Niveles de madurez deseados del Área a corto, mediano y largo plazo

Niveles de madurez actual

Para medir el estado de madurez actual de la seguridad de la información en DIRECTV, se utilizó la escala de evaluación de la metodología “Evaluación de Riesgos de la Seguridad de la Información” (Deloitte, 2008, p. 46). La escala contiene 6 rangos de evaluación (0-5) y 3 rangos de alineación con el marco de evaluación. Para mayor detalle de la metodología utilizada, se puede visualizar la Figura 13. Nivel de Madurez.

Los 3 rangos de alineación con el marco de evaluación que se utilizó durante el alistamiento del SGSI, corresponden a:

Tabla 8. Rangos de Alineación - Niveles de Madurez Actual

Color	**Alineación**
Rojo	Baja
Amarillo	Media
Verde	Alta

Considerando las directrices por subdominio establecidas en el marco de evaluación definido en el punto *3.1.2 Marco de Evaluación*, y la escala de evaluación, se evaluó las directrices o controles en reuniones mantenidas con personal de DIRECTV.

Una vez realizada la evaluación, se consolidó las respuestas y se obtuvo un valor promedio por subdominio, que corresponde a la sumatoria de todos los valores por directriz. Estos valores fueron validados con cada uno de los responsables de DIRECTV, para obtener su aprobación correspondiente.

Considerando los promedios obtenidos por subdominio, se estableció la alineación de estos valores con el marco de evaluación.

En el **Anexo 3** se encuentra el documento “EJE Alistamiento ISO27001 2013 - Plan Estratégico de Seguridad de la Información 2015 06 22 vFinal”, en el punto *1.2.1 Niveles de madurez actual* se puede visualizar una tabla que muestra el promedio de evaluación obtenido por subdominio de la situación actual referente a la gestión de seguridad de la información en DIRECTV, y su alineación con el marco de evaluación.

Niveles de madurez futuro

Para determinar el nivel de madurez futuro de cada directriz del marco de evaluación definido en el punto *3.1.2 Marco de Evaluación*, se realizó diversas reuniones con personal de DIRECTV, estableciendo el nivel futuro y el plazo dentro del cual se alcanzará dicho nivel.

Los plazos establecidos se detallan a continuación:

Tabla 9. Plazos Establecidos - Niveles de Madurez Futuro

Plazo	**Fecha límite**
Corto	Hasta Febrero de 2016
Mediano	Hasta Mayo de 2016
Largo	Hasta Noviembre 2016

En el **Anexo 3** se encuentra el documento “EJE Alistamiento ISO27001 2013 - Plan Estratégico de Seguridad de la Información 2015 06 22 vFinal”, en el punto *1.2.2 Niveles de madurez futuro* se puede visualizar una tabla que muestra el nivel de madurez futuro por cada subdominio.

3.2.1.3. Planes de Acción

Posterior al establecimiento del nivel de madurez futuro, se definió las principales acciones a ejecutar por cada subdominio. Estas acciones fueron categorizadas utilizando dos escalas (brecha y nivel de esfuerzo).

Brecha, considera el número de saltos para alcanzar el nivel futuro. La siguiente tabla muestra los rangos definidos para esta escala:

Tabla 10. Brecha - Planes de Acción

Brecha	**No. de saltos para alcanzar Nivel Futuro**
Alta	De 4 a 5
Media	De 2 a 3
Baja	1

Nivel de Esfuerzo, se refiere al nivel de esfuerzo involucrado para llevar adelante los planes de acción. En el presente alistamiento del SGSI en DIRECTV, se realizó la medición en base a 3 elementos claves: tiempo, personas y costo. La siguiente tabla muestra los rangos definidos para esta escala:

Tabla 11. Nivel de Esfuerzo - Planes de Acción

	Nivel de esfuerzo			
Criterio	*Bajo*	*Medio*	*Alto*	
Tiempo	De 1 a 3 meses	De 4 a 6 meses	Mayor a 6 meses	
Personas	1-2 personas / áreas	3-6 personas / áreas	Más de 6 personas / áreas	
Costo	Hasta $20K	De $20K a $50K	Más de $50K	Sólo esfuerzo interno

Adicionalmente, se estableció el plazo para la ejecución de los planes de acción, considerando la siguiente tabla:

Tabla 12. Plazo - Planes de Acción

Plazo	Tiempo en meses
Corto	3 meses
Mediano	6 meses
Largo	12 meses

En el **Anexo 4** se encuentra el documento “Planes de Acción”, donde se puede visualizar todos los planes de acción identificados por cada subdominio.

3.2.1.4. Hoja de Ruta (Roadmap) de Implementación

Se realizó una revisión de todos los planes de acción y se agruparon aquellos que tenían un enfoque de aplicabilidad común para determinar iniciativas macro.

Las iniciativas de agrupación son:

Tabla 13. Iniciativas

#	Iniciativas
1	Definición, formalización y aprobación del marco normativo de seguridad de la información (políticas, procedimientos, reglamentos, manuales, etc).
2	Implantación de controles.
3	Aplicación de enfoques de mejora continua.
4	Sensibilización del personal.

3.2.1.5. Ficha Técnica de Iniciativas

Todas las iniciativas propuestas para el alistamiento del SGSI en DIRECTV se encuentran dentro de la hoja de ruta (roadmap) de implementación.

En el **Anexo 3** se encuentra el documento “EJE Alistamiento ISO27001 2013 - Plan Estratégico de Seguridad de la Información 2015 06 22 vFinal”, en el punto *3.1 Ficha técnica de iniciativas* se puede visualizar cada una de las

iniciativas definidas para el alistamiento del SGSI en DIRECTV. En cada una de estas iniciativas se encuentra establecido su objetivo principal, actividades a ejecutarse, dominios asociados y un resumen con los valores de las dos escalas utilizadas para la categorización de los planes de acción. Adicionalmente, se puede visualizar la duración del tiempo estimado para que DIRECTV pueda cumplir con las iniciativas propuestas.

A continuación se detalla el cronograma tentativo de ejecución de las iniciativas macro definidas para DIRECTV:

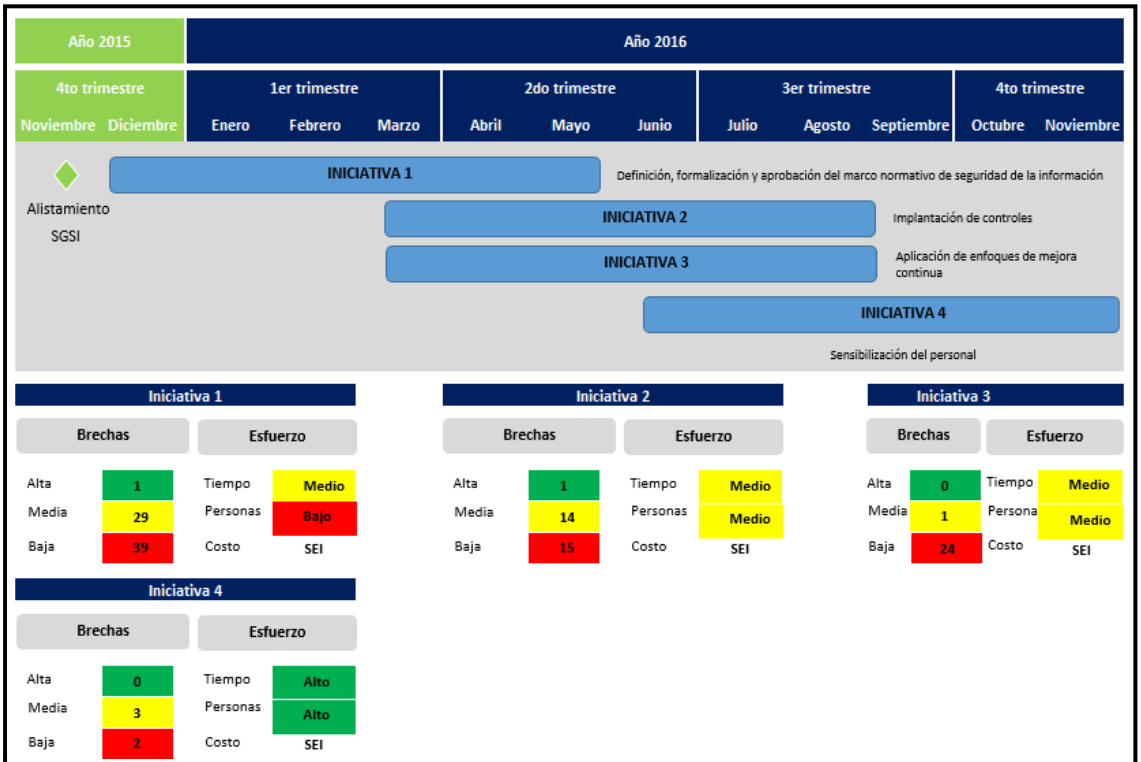


Figura 15. Cronograma Tentativo de Ejecución de las Iniciativas.

En el **Anexo 5** se encuentra el documento “Hoja de Ruta de Implementación”, donde se encuentran las iniciativas propuestas con el detalle de los planes de acción, agrupados de acuerdo a un enfoque de aplicabilidad común.

3.2.1.6. Objetivos Estratégicos del Área de Seguridad de la Información

En alineación con los objetivos estratégicos que persigue DIRECTV y los objetivos de Seguridad de la Información, se han definido lineamientos con relación a la función de Seguridad de la Información dentro de la Compañía.

En el **Anexo 6** se encuentra el documento “Manual de la Función de Seguridad de la Información”, en el punto *6.1 Objetivos Estratégicos de Seguridad de la Información* se puede visualizar los lineamientos específicos respecto a la Seguridad de la Información dentro de DIRECTV.

3.2.1.7. Plan de Concienciación a los Usuarios

Con base a las necesidades de aprendizaje requeridas por el personal de DIRECTV en temas de Seguridad de la Información, se han definido los siguientes aspectos para planificar y llevar a cabo sesiones de concientización y capacitación en la Compañía:

- Audiencias (empleados de DIRECTV), a las cuales se orientó las sesiones de concientización y capacitación.

- Contenido, listado de temas de acuerdo a las audiencias definidas.

- Tiempos, duración de las sesiones.

En el **Anexo 7** se encuentra el documento “Plan de Concienciación a los Usuarios”, donde se puede visualizar los aspectos relevantes respecto a la Seguridad de la Información, para llevar a cabo sesiones de concientización y capacitación en DIRECTV.

3.2.2. Evaluación de los Requisitos de la Norma ISO/IEC 27001:2013

3.2.2.1. Objetivo

Definir un check-list de verificación para corroborar el cumplimiento de los requisitos de la norma ISO/IEC 27001:2013 en DIRECTV.

3.2.2.2. Trabajo Realizado

La elaboración del check-list de verificación durante la evaluación de los requisitos de la norma ISO/IEC 27001:2013, contempló la siguiente actividad:

- Check-list de cumplimiento para cada requisito de la norma ISO/IEC 27001:2013.

3.2.2.3. Metodología

Como parte de la metodología aplicada para elaborar el check-list de verificación, se realizó la siguiente actividad:

- Se tomó en cuenta cada uno de los requisitos, el estado (cumple/no cumple) y observaciones al respecto.

3.2.2.4. Check-list de Evaluación de los Requisitos de la Norma ISO/IEC 27001:2013

En el **Anexo 8** se encuentra el documento “Check-list Requisitos Alistamiento SGSI”, donde se puede visualizar el estado (cumple/no cumple) de cada uno de los requisitos de la norma ISO/IEC 27001:2013 en DIRECTV.

3.3. Fase de Ejecución - Establecimiento de Gobierno de Seguridad

3.3.1. Marco de Gobierno

3.3.1.1. Objetivo

Establecer los elementos y lineamientos del Marco de Gobierno de Seguridad de la Información para la gestión de dicha función en DIRECTV, acorde con las necesidades empresariales y requerimientos regulatorios aplicables a la Compañía.

3.3.1.2. Organigrama Funcional del Departamento de SI

La posición de la función de seguridad de la información dentro de DIRECTV, es clave para la consecución de los objetivos estratégicos de seguridad de la información definidos para dicha Compañía. Existen dos (2) elementos a considerar cuando se habla de la posición de dicha área:

- Departamento o área a la cual pertenece.

- Nivel de profundidad en la Compañía.

El departamento o área a la cual pertenece la función de Seguridad de la Información es muy importante, puesto que su ámbito de acción es amplio,

abarcando temas relacionados con Recursos Humanos hasta Cumplimiento Regulatorio. No existe una buena práctica con respecto a la ubicación óptima de dicha función dentro de una Compañía, pero con base al principio de segregación de funciones, el área de Seguridad de la Información en DIRECTV no debería pertenecer a los departamentos de Tecnología de la Información, ni Auditoría Interna.

Con respecto al nivel de profundidad dentro de la Compañía, dado que la función de Seguridad de la Información deberá abarcar el tratamiento de temas relacionados con todas las áreas de la Compañía, no es recomendable relegarla en la estructura organizacional, más bien considerar ubicarla en un punto visible con el nivel de empoderamiento adecuado para su gestión.

En el **Anexo 6** se encuentra el documento “Manual de la Función de Seguridad de la Información”, en el punto *6.3.1 Posición de la función de Seguridad de la Información dentro de DIRECTV* se puede visualizar dos (2) modelos para ubicar la función de seguridad de la información en el organigrama de DIRECTV.

3.3.1.3. Definición Detallada de Roles y Funciones

Como parte de los mecanismos de gestión y control de la Compañía, se han establecido responsabilidades respecto a la gestión de la seguridad de la información en DIRECTV. Se han definido responsabilidades de acuerdo a los siguientes roles:

- Departamento de Seguridad.

- Oficial de Seguridad de la Información.

- Encargado de Seguridad en el Departamento de Tecnología.

- Dueño de la Información.

- Custodio de la Información.

- Usuario Final.

En el **Anexo 9** se encuentra el documento “Manual de Roles y Responsabilidades de Seguridad de la Información”, donde se puede visualizar el detalle de las responsabilidades para cada rol respecto a la gestión de la seguridad de la información en DIRECTV.

3.3.1.4. Plan de Entrenamiento

Los empleados del departamento de Seguridad de la Información de DIRECTV, deberán contar con un plan de entrenamiento orientado a dar cumplimiento a las funciones y responsabilidades de cada uno de sus cargos, así como los temas relacionados con la ejecución de sus actividades diarias.

El plan de entrenamiento para los empleados del departamento de Seguridad de la Información de DIRECTV, deberá cubrir de forma general los siguientes temas:

- Gestión por procesos.

- Gestión de riesgos de Seguridad de la Información.

- Diseño e implementación de Sistemas de Gestión de Seguridad de la Información (SGSI).

- Administración de la Continuidad del Negocio.

- Legislación de Seguridad de la Información local.

En el **Anexo 7** se encuentra el documento “Plan de Concienciación a los Usuarios”, en el punto *6. Plan de Entrenamiento para Empleados del Departamento de Seguridad de la Información* se puede visualizar el temario sugerido para el plan de entrenamiento a los funcionarios del área de Seguridad de la Información de DIRECTV.

3.3.2. Marco Normativo de Seguridad

3.3.2.1. Desarrollo del Marco Normativo

Se realizó la evaluación de las políticas, reglamentos, manuales, procedimientos e instructivos, que se encuentran actualmente implementados en DIRECTV. Se llegó a la conclusión que existen ciertos documentos requeridos por el área de Seguridad de la Información que no se encuentran documentados, aprobados ni difundidos a todo el personal de la Compañía. Por tal motivo, y para cumplir con el Marco Normativo de Seguridad, se desarrolló las políticas y procedimientos que faltaban, con base a la realidad y objetivos futuros de DIRECTV.

A continuación se encuentran los documentos que abarcan el Marco Normativo de Seguridad para DIRECTV, relacionados con cada uno de los dominios de control de la norma ISO/IEC 27001:2013:

Tabla 14. Marco Normativo DIRECTV

Dominio de Control	Marco Normativo
1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	- Política de Seguridad de la Información.
2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	- Política de Seguridad de la Información. - Manual de la Función de Seguridad de la Información. - Plan de Concienciación a Usuarios. - Manual de Roles y Responsabilidades de Seguridad de la Información.
3. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	- Plan de Concienciación a Usuarios.

Dominio de Control	Marco Normativo
4. GESTIÓN DE ACTIVOS	- Política de Gestión de Activos de Información. - Metodología de Análisis de Riesgos.
5. CONTROL DE ACCESO	- Política de Gestión de Acceso a Información. - Metodología de Análisis de Riesgos. - Política de Administración de Seguridad de Red. - Política de Protección y Revisión de Pistas de Auditoría. - Procedimiento de Administración de Usuarios. - Procedimiento de Utilización de Cuentas de Máximos Privilegios.
6. CRIPTOGRAFÍA	NA
7. SEGURIDAD FISICA Y DEL ENTORNO	Procedimiento de Control de Acceso Físico y Ambiental del Centro de Cómputo.
8. SEGURIDAD DE LAS OPERACIONES	- Política de Administración de Respaldos. - Procedimiento de Administración de Respaldos.
9. SEGURIDAD DE LAS COMUNICACIONES	- Política de Administración de Seguridad de Red. - Política de Protección y Revisión de Pistas de Auditoría. - Política de Monitoreo de Recursos de los Servicios y Sistemas

Dominio de Control	Marco Normativo
	Informáticos.
10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	- Política de Gestión de Software.
11. RELACIÓN CON PROVEEDORES	NA
12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	- Política de Monitoreo de Niveles de Servicio de Incidentes de Seguridad. - Procedimiento de Gestión de Incidentes de Seguridad.
13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	- Metodología de Análisis de Riesgos.
14. CUMPLIMIENTO	NA

3.3.2.2. Descripción de los documentos del Marco Normativo

A continuación se detalla una pequeña descripción de cada una de las políticas, manuales y procedimientos que fueron desarrollados para DIRECTV, con el objetivo de cumplir con el Marco Normativo de Seguridad en dicha Compañía:

Política de Seguridad de la Información

Se refiere a la definición de los lineamientos específicos, relacionados con la gestión y administración de la Seguridad de la Información en DIRECTV.

Se encuentran cada uno de los pasos que se debe seguir, para asegurar el cumplimiento de los tres elementos fundamentales de la Seguridad de la Información (confidencialidad, integridad y disponibilidad).

Adicionalmente, los lineamientos y controles para prevenir o responder a amenazas respecto a temas de seguridad de la información, se encuentran claramente detallados en la política de Seguridad de la Información establecida para DIRECTV.

Política de Gestión de Activos de Información

Se refiere a la definición de los lineamientos específicos que se deben considerar, en la identificación y uso aceptable de los activos de información de DIRECTV.

Se encuentran definidos los niveles de seguridad para el reguardo de los activos de información en la Compañía.

Adicionalmente, los lineamientos y controles sobre el uso de los activos de información de la Compañía por personal externo (auditores, consultores, contratistas, entre otros) y las terceras partes (proveedores, clientes, entre otros), se encuentran claramente detallados en la política de Gestión de Activos de Información establecida para DIRECTV.

Metodología de Análisis de Riesgos

Analizar los riesgos de seguridad de los activos de información en DIRECTV. De igual manera, se encuentran definidas las medidas de tratamiento necesarias para mantener los riesgos en niveles aceptables.

Identificar los atributos estratégicos de la Compañía, para lo cual se utiliza tres elementos estratégicos (visión, misión y planes estratégicos). Dichos atributos son utilizados para la calificación del impacto de pérdidas de confidencialidad, integridad y disponibilidad sufridas por los activos de información de DIRECTV.

Contiene la definición y uso de las siguientes escalas:

- *Escala de clasificación de impacto*.- Contiene los diferentes niveles que deberán utilizarse para calificar cualitativamente las pérdidas de confidencialidad, integridad y confidencialidad de los activos de información.

- *Escala de probabilidad o vulnerabilidad*.- Contiene los niveles que deberán utilizarse para determinar la probabilidad de ocurrencia de que una amenaza explote una vulnerabilidad de un activo de información, basado en los niveles de controles implementados.

- *Nivel de aceptación de riesgos*.- Corresponde al nivel que se define cuando un riesgo es inaceptable y cuando es aceptable.

Se encuentran definidos los lineamientos de seguridad para la identificación de los activos de información de los procesos de negocio de DIRECTV.

Adicionalmente, en lo que se refiere a la “Clasificación de Activos de Información”, esta metodología contiene cada uno de los pasos a seguir para determinar el nivel de impacto cualitativo que tendría para la Compañía, la pérdida de cualquiera de los elementos fundamentales de la seguridad de la información (confidencialidad, integridad y disponibilidad).

Contiene lineamientos específicos de seguridad de la información para los siguientes procesos:

- Determinación de los activos críticos de información.

- Identificación del universo de amenazas y vulnerabilidades.

- Determinación de la probabilidad de ocurrencias de amenazas.

- Determinación de la probabilidad de ocurrencia de los riesgos.

- Análisis y evaluación de riesgos.

- Definición de tratamiento de riesgos.

Política de Gestión de Acceso a Información

Describe cada una de las actividades a ejecutarse, respecto al control del acceso a la información. El acceso de los usuarios a cada uno de las aplicaciones, software de sistemas, recursos, servicios y redes de comunicaciones de DIRECTV, de acuerdo con los requisitos de la Compañía.

El acceso a la información se debe controlar con base en las buenas prácticas de seguridad de la información y de la Compañía. Esta política cuenta con los lineamientos de seguridad específicos para cumplir con lo antes descrito.

Política de Administración de Seguridad de Red

Se refiere a la definición de los lineamientos específicos, relacionados con la gestión y administración de seguridad de la red de datos de DIRECTV.

Contiene los controles de seguridad de la información que se deben aplicar en la red de DIRECTV, con el objetivo de protegerla de accesos no autorizados.

Política de Protección y Revisión de Pistas de Auditoría

Se refiere a los procedimientos establecidos para la revisión y análisis del contenido de pistas de auditoría generadas en los recursos informáticos de DIRECTV.

Contiene una descripción de las principales actividades que deben ser consideradas para ser registradas, en todos los recursos informáticos digitales críticos de DIRECTV.

Con respecto al almacenamiento de pistas de auditoría, se detalla los pasos, para que las pistas de auditoría sean almacenadas de manera correcta y segura, de acuerdo a los procedimientos establecidos por DIRECTV.

Contiene lineamientos de seguridad definidos para el proceso de revisión de las mismas. Finalmente, se detalla las actividades que se deben seguir, respecto a los reportes de los resultados producto de la revisión, y, los siguientes pasos en el caso que se identifique un incidente de seguridad.

Procedimiento de Administración de Usuarios

Describe las principales actividades, con respecto a la creación, modificación y eliminación de los usuarios, con acceso a los sistemas de aplicación, software de sistemas y red de DIRECTV.

Contiene los lineamientos específicos de seguridad de la información para las siguientes actividades:

- Creación de cuentas.

- Modificación de cuentas.

- Eliminación de cuentas.

- Revisión periódica de los derechos de acceso de los usuarios.

- Indicadores de cada proceso (Creación, modificación y eliminación de cuentas de usuarios).

Procedimiento de Utilización de Cuentas de Máximos Privilegios

Describe las principales actividades para el uso de usuarios de “Máximos Privilegios”, con acceso a los sistemas de aplicación y software de sistemas en DIRECTV.

Contiene los lineamientos específicos de seguridad de la información para las siguientes actividades:

- Definición de cuentas de máximos privilegios.

- Generación y almacenamiento de contraseñas ensobradas.

- Utilización de cuentas de máximos privilegios.

- Indicadores del procedimiento de utilización de cuentas de máximos privilegios.

Procedimiento de Control de Acceso Físico y Ambiental del Centro de Cómputo

Se refiere a la definición de los lineamientos de seguridad que se deben considerar en el centro de cómputo de la Compañía, tales como, medidas de prevención para evitar el acceso físico no autorizado, el daño o la interferencia a las instalaciones donde se procesa información de DIRECTV.

Cuenta con lineamientos de seguridad para las siguientes actividades:

- Acceso al centro de cómputo por personal de la Compañía.

- Acceso de visitantes al centro de cómputo.

- Revisión de los accesos al centro de cómputo.

- Seguridad ambiental en el centro de cómputo.

Política de Administración de Respaldos

Se establecen lineamientos y normas a seguir para la gestión de respaldos, con el objetivo de salvaguardar la información de DIRECTV, de cualquier riesgo de pérdida, eliminación o corrupción; y garantizar su disponibilidad al momento que se la requiera.

Cuenta con lineamientos de seguridad para los siguientes procesos:

- Información a respaldar.

- Tipos de respaldos.

- Periodicidad de respaldos.

- Medios de respaldo.

- Rotación de medios de respaldo.

- Revisión de legibilidad de respaldos.

- Almacenamiento y transporte de copias de respaldos.

- Recuperación de copias de respaldos.

- Eliminación de copias de respaldos.

Procedimiento de Administración de Respaldos

Describe las principales actividades para la obtención, administración y recuperación de respaldos, con el objetivo de salvaguardar la información de DIRECTV, de cualquier riesgo de pérdida, eliminación o corrupción; y garantizar su disponibilidad al momento que se la requiera.

Describe las actividades a ejecutarse respecto a la información que se va a respaldar. También, se ha establecido los tipos de respaldos que se van a obtener, considerando criterios o buenas prácticas de seguridad, tales como, importancia de la información, la capacidad de almacenamiento, el tiempo disponible para realizarlos y el tiempo necesario para recuperarlos.

Cuenta con la descripción de cada una de las actividades descritas a continuación:

- Periodicidad de respaldos.

- Medios de respaldo.

- Rotación de medios de respaldo.

- Revisión de legibilidad de respaldos.

- Almacenamiento y transporte de copias de respaldos.

- Recuperación de copias de respaldos.

- Eliminación de copias de respaldos.

Política de Monitoreo de Recursos de los Servicios y Sistemas Informáticos

Se refiere a la definición de lineamientos de seguridad que se deben considerar, para el monitoreo del uso de los recursos de los servicios y sistemas informáticos; y el registro y manejo de fallas en los mismos, con el

objetivo de efectuar una planeación de requerimientos de recursos, asegurando el correcto desempeño de los sistemas y servicios en DIRECTV.

Cuenta con las actividades a ejecutarse para el monitoreo técnico de los recursos de los sistemas de información.

Adicionalmente, cuenta con las actividades que se deben seguir, respecto a las alertas e informes que se deben presentar, producto de los monitoreos efectuados.

Política de Gestión de Software

Detalla las diferentes directrices o lineamientos que los funcionarios de DIRECTV deberán ejecutar para la correcta gestión de software, administrando de forma adecuada la seguridad que se requiere en las actividades a efectuar en dicha gestión, tanto para software de sistemas como aplicaciones.

Cuenta con lineamientos de seguridad para los siguientes procesos:

- Adquisición de software.

- Mantenimiento de aplicaciones.

- Actualización de software de sistemas.

- Licenciamiento.

Política de Monitoreo de Niveles de Servicio de Incidentes de Seguridad

Describe los controles que se deben implementar, para realizar un adecuado monitoreo de la gestión de prestación de servicios por parte del personal de mesa de servicios y terceras partes relacionadas de DIRECTV, con respecto a incidentes de seguridad de la información.

Cuenta con lineamientos de seguridad para los siguientes procesos:

- Prestación de servicios por terceras partes.

- Prestación de servicios por parte de la mesa de servicios de DIRECTV.

Procedimiento de Gestión de Incidentes de Seguridad

Describe las principales actividades para gestionar el tratamiento y mitigación de incidentes de seguridad de la información en DIRECTV.

Cuenta con la descripción de cada una de las actividades descritas a continuación:

- Reporte de incidentes de seguridad.

- Registro de incidentes de seguridad.

- Categorías de incidentes.

- Priorización de incidentes.

- Atención de los incidentes de seguridad.

3.4. Fase de Presentación

3.4.1. Armado de Entregables

Luego de revisar los documentos e informes resultantes en conjunto con personal de DIRECTV, se llegó a la conclusión que los documentos generados en cada una de las fases anteriores, corresponden a los entregables finales del proyecto de alistamiento del SGSI en DIRECTV.

3.4.2. Presentación de Resultados

3.4.2.1. Objetivo

Socializar los resultados finales del alistamiento del SGSI a la Alta Administración de DIRECTV. Los resultados fueron comunicados por medio de una presentación ejecutiva.

3.4.2.2. Departamentos Involucrados

A continuación se detalla el departamento y cargo del personal involucrado durante el alistamiento del SGSI en DIRECTV:

Tabla 15. Personal de DIRECTV - Alistamiento SGSI

Departamento	Cargo
Procesos y Control Interno.	Jefe de Control Interno. Coordinador de Procesos. Analista de Control Interno.
Seguridad de la Información.	Oficial de Seguridad de la Información. Coordinador de Seguridad de la Información. Arquitecto de Seguridad. Administrador de Seguridad de la Información. Operador de Seguridad.
Compensaciones y Beneficios.	Gerente de Gestión Humana.
Finanzas.	Contador General.
Infraestructura.	Jefe de Infraestructura.
Desarrollo.	Gerente de Desarrollo y Proyectos. Jefe de Desarrollo y Proyectos.
Departamento Jurídico.	Abogado.

3.4.2.3. Fortalezas y Oportunidades de Mejora

A continuación se detalla las fortalezas y oportunidades de mejora, como resultado del alistamiento del SGSI en DIRECTV:

Fortalezas

- Apoyo fundamental por parte de la Dirección de TI en la consecución del alistamiento del SGSI en DIRECTV.

- Alta colaboración del personal de DIRECTV que gestionó el proyecto.

- Buena disposición por parte del personal entrevistado de los distintos departamentos.

- Entrega de información a tiempo durante las reuniones.

- Alta involucración de personal de DIRECTV, durante la revisión de las políticas y procedimientos relacionados con la seguridad de la información.

Oportunidades de Mejora

- Mejora en los tiempos acordados para las actividades definidas dentro del alistamiento del SGSI en DIRECTV.

3.4.2.4. Resultados Obtenidos

A continuación se detalla los resultados finales, producto del alistamiento del SGSI en DIRECTV:

Resultado 1.- Política de Seguridad de la Información.

En el punto "*3.3.2.2 Descripción de los documentos del Marco Normativo",* se encuentra la descripción de la "Política de Seguridad de la Información".

Resultado 2.- Plan Estratégico de Seguridad de la Información. Contiene:

- Niveles de madurez deseados del Área a corto, mediano y largo plazo.

- Planes de acción y "roadmap" de implementación.

- Objetivos estratégicos del área de Seguridad de la Información.

- Plan de concienciación a los usuarios.

En el **Anexo 3** se encuentra el documento "EJE Alistamiento ISO27001 2013 - Plan Estratégico de Seguridad de la Información 2015 06 22 vFinal", en el punto *1.2.1 Niveles de madurez actual* se puede visualizar una tabla que muestra el promedio de evaluación obtenido por subdominio de la situación actual referente a la gestión de seguridad de la información en DIRECTV, y su alineación con el marco de evaluación.

En el **Anexo 3** se encuentra el documento “EJE Alistamiento ISO27001 2013 - Plan Estratégico de Seguridad de la Información 2015 06 22 vFinal”, en el punto *1.2.2 Niveles de madurez futuro* se puede visualizar una tabla que muestra el nivel de madurez futuro por cada subdominio.

En el **Anexo 4** se encuentra el documento “Planes de Acción”, donde se puede visualizar todos los planes de acción identificados por cada subdominio.

En el **Anexo 3** se encuentra el documento “EJE Alistamiento ISO27001 2013 - Plan Estratégico de Seguridad de la Información 2015 06 22 vFinal”, en el punto *3.1 Ficha técnica de iniciativas* se puede visualizar cada una de las iniciativas definidas para el alistamiento del SGSI en DIRECTV. En cada una de estas iniciativas se encuentra establecido su objetivo principal, actividades a ejecutarse, dominios asociados y un resumen con los valores de las dos escalas utilizadas para la categorización de los planes de acción. Adicionalmente, se puede visualizar la duración del tiempo estimado para que DIRECTV pueda cumplir con las iniciativas propuestas.

En el **Anexo 5** se encuentra el documento “Hoja de Ruta de Implementación”, donde se encuentran las iniciativas propuestas con el detalle de los planes de acción, agrupados de acuerdo a un enfoque de aplicabilidad común.

En el **Anexo 6** se encuentra el documento “Manual de la Función de Seguridad de la Información”, en el punto *6.1 Objetivos Estratégicos de Seguridad de la Información* se puede visualizar los lineamientos específicos respecto a la Seguridad de la Información dentro de DIRECTV.

En el **Anexo 7** se encuentra el documento “Plan de Concienciación a los Usuarios”, donde se puede visualizar los aspectos relevantes respecto a la Seguridad de la Información, para llevar a cabo sesiones de concientización y capacitación en DIRECTV.

Resultado 3.- Marco de Gobierno de Seguridad de la Información. Contiene:

- Organigrama Funcional del Departamento de Seguridad de la Información y TI.

- Definición Detallada de Roles y Funciones del Departamento.

- Plan de Entrenamiento para Empleados del Departamento de Seguridad de la Información.

En el **Anexo 6** se encuentra el documento “Manual de la Función de Seguridad de la Información”, en el punto *6.3.1 Posición de la función de Seguridad de la Información dentro de DIRECTV* se puede visualizar dos (2) modelos para ubicar la función de seguridad de la información en el organigrama de DIRECTV.

En el **Anexo 9** se encuentra el documento “Manual de Roles y Responsabilidades de Seguridad de la Información”, donde se puede visualizar el detalle de las responsabilidades para cada rol respecto a la gestión de la seguridad de la información en DIRECTV.

En el **Anexo 7** se encuentra el documento “Plan de Concienciación a los Usuarios”, en el punto *6. Plan de Entrenamiento para Empleados del Departamento de Seguridad de la Información* se puede visualizar el temario sugerido para el plan de entrenamiento a los funcionarios del área de Seguridad de la Información de DIRECTV.

Resultado 4.- Marco Normativo de Seguridad de la Información.

Contiene las políticas y procedimientos desarrollados como parte del trabajo de titulación, debido a que ciertos documentos requeridos por el área de Seguridad de la Información no se encontraban documentados, aprobados ni difundidos a todo el personal de la Compañía.

En el punto “*3.3.2.2 Descripción de los documentos del Marco Normativo”,* se encuentra la descripción de las políticas y procedimientos desarrollados como parte del trabajo de titulación.

Finalmente, en el **Anexo 10** se encuentra la presentación ejecutiva, con el objetivo de socializar los resultados finales del trabajo de titulación a la Alta Administración de DIRECTV.

Adicionalmente, en el **Anexo 11** se encuentra una Carta de Conformidad por parte de DIRECTV. En la cual se detalla que se realizó la identificación de las capacidades actuales de la Compañía referente a la Gestión de Seguridad de la Información. Producto del trabajo realizado se generaron entregables en cada una de las fases del proyecto, los cuales fueron entregados a personal responsable, de acuerdo a lo establecido al inicio del trabajo de titulación, desarrollado e implementado en DIRECTV.

4. Conclusiones y Recomendaciones

4.1. Conclusiones

- El estudio realizado concluyó con la definición de un conjunto de actividades, documentos generados y estrategias de seguridad que forman parte del alistamiento de un Sistema de Gestión de Seguridad de la Información para DIRECTV.

- La elaboración de un plan de trabajo en el inicio del proyecto, significó una iniciativa de gestión para todas las fases del mismo. Se brindó el entendimiento necesario para que la Compañía conozca a detalle cuales serían los resultados producto del desarrollo del proyecto. Adicionalmente, se elaboró un conjunto de definiciones y lineamientos que fueron de vital importancia durante la ejecución del alistamiento del SGSI en DIRECTV.

- El material utilizado para la ejecución de este proyecto fue la norma ISO/IEC 27001:2013. En base a esta norma se definió los controles o directrices que DIRECTV deberá implementar. Adicionalmente, se utilizó la metodología “Evaluación de Riesgos de la Seguridad de la Información”, que fue desarrollada por la empresa Deloitte.
  La definición y ejecución del proceso de alistamiento del SGSI en la Compañía, es considerado como el primer paso para una posterior implementación de este sistema, y la obtención de la certificación internacional. El estudio realizado en DIRECTV, permitirá a la Compañía tomar ventaja competitiva del resto de empresas del sector.

- En DIRECTV Ecuador únicamente existe una persona para los temas relacionados con la seguridad de la información, la gestión de esta disciplina se la realiza desde la regional de la Compañía. Esto significa

que DIRECTV a nivel local no cuenta con un área para la gestión de la seguridad de la información.

- A pesar que en DIRECTV Ecuador únicamente cuentan con una persona para los temas relacionados con la seguridad de la información, se consideró los diferentes procesos y prácticas de gestión de seguridad que actualmente se encuentran en la Compañía, y se evaluó la exitosa ejecución de los mismos. Producto de esta evaluación, se identificó que DIRECTV se encuentra en un nivel 2 (dos), lo cual significa que las directrices de seguridad se encuentran estructuradas y son ejecutadas por diferentes personas que desarrollan la misma tarea.

- Se realizó la evaluación de las políticas, reglamentos, manuales, procedimientos e instructivos, formalizados en DIRECTV. Se concluyó que ciertos documentos no se encontraban documentados, aprobados ni difundidos a todo el personal de la Compañía. Por tal motivo, y para cumplir con el Marco Normativo de Seguridad, se desarrolló las políticas y procedimientos que faltaban, con base a la realidad y objetivos futuros de DIRECTV.

- El estudio realizado tuvo como fin la definición y ejecución del proceso de alistamiento del Sistema de Gestión de Seguridad de la Información (SGSI) en DIRECTV. Sin embargo, la Compañía tiene que tomar en cuenta que un proyecto de ésta índole, como es la implementación de un SGSI, implica los siguientes factores:

    - La integración de los diferentes procesos de la Compañía.
    - Adquisición de nuevos sistemas informáticos.
    - Contratación de personal para el Departamento local de Seguridad de la Información.
    - Conocimiento y compromiso por parte de la Gerencia General.

4.2. Recomendaciones

- Trabajar en la posterior implementación del Sistema de Gestión de Seguridad de la Información para DIRECTV.

- Utilizar como línea base el plan detallado de trabajo, para la administración, gestión e implementación del SGSI en DIRECTV.

- Verificar la correcta implementación de los controles o directrices que fueron definidos en el proceso de alistamiento con base a la norma ISO/IEC 27001:2013.

- Desarrollar una estrategia de seguridad de la información a nivel local, y promover la creación de un Área de Seguridad para la gestión local de la seguridad de la información en la Compañía.

- Realizar una revisión continua de los procesos y prácticas de gestión de seguridad que fueron identificados en el alistamiento del SGSI, y verificar si el nivel de madurez se mantiene o ha sufrido mejoras, por lo menos una vez al año.

- Evaluar que las políticas, reglamentos, manuales, procedimientos e instructivos que forman parte de DIRECTV, se encuentren aplicadas a los diferentes procesos de la Compañía.

- Definir el alcance, tiempo estimado, gestión de la calidad, riesgos a considerar, personal involucrado, costos adicionales, expectativas de la Compañía; factores fundamentales que intervienen en la implementación de un Sistema de Seguridad de la Información (SGSI) en DIRECTV.

Referencias

Areitio, J. (2008). Seguridad de la Información. Madrid, España: Learning Paraninfo, S.A. [versión electrónica]. Recuperado el 25 de mayo de 2015 de https://books.google.es/books?id=_z2GcBD3deYC&printsec=frontcover&dq=Seguridad+de+la+Informaci%C3%B3n&hl=en&sa=X&ved=0CD8Q6AEwAmoVChMI7Nnr8rq-xwIVSNkeCh2IowDf#v=onepage&q&f=false

Bsigroup. (s.f.). Pasando de ISO/IEC 27001:2005 a ISO/IEC 27001:2013. Recuperado el 03 de agosto de 2015 de http://www.bsigroup.com/LocalFiles/es-MX/ISO%20IEC%2027001/Gu%C3%ADa%20de%20Transici%C3%B3n_ISO27001.pdf

CCIA. (s.f.). Legislación y normas ISO 27000. Recuperado el 08 de junio de 2015 de http://ccia.ei.uvigo.es/docencia/SSI/normas-leyes.pdf

Datateca. (s.f.). Ciclo PDCA (Edward Deming). Recuperado el 08 de junio de 2015 de http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

Datateca. (s.f.). Familia de las normas ISO/IEC 27000. Recuperado el 08 de junio de 2015 de http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/22__leccin_7_familia_de_las_normas_isoiec_27000.html

Deloitte. (2008). Metodología Evaluación de Riesgos de la Seguridad de la Información

Directvla. (s.f.). DIRECTV te cambia la vida. Recuperado el 01 de octubre de 2015 de http://www.directvla.com/#item-two

Eficienciagerencial. (s.f.). Nuevo Estándar en Sistemas de Gestión de Seguridad de la Información ISO/IEC 27001:2013. Recuperado el 27 de julio de 2015 de http://eficienciagerencial.com/tienda/temario/nuevo_sgsi_2013.pdf

González, A. (2014). Seguridad de la Información. Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica, 160-173. Recuperado el 25 de mayo de 2015 de https://books.google.es/books?id=xKkYBgAAQBAJ&pg=PA100&dq=Seguridad+de+la+Informaci%C3%B3n&hl=en&sa=X&ved=0CFMQ6AEwBWoVChMI7Nnr8rq-xwIVSNkeCh2IowDf#v=onepage&q&f=false

ISO27000. (s.f.). ISO 27000. Recuperado el 08 de junio de 2015 de http://www.iso27000.es/iso27000.html

ISO27000. (s.f.). SGSI. Recuperado el 03 de agosto de 2015 de http://www.iso27000.es/sgsi.html

ISO/IEC 27000:2014, Information technology - Security techniques - Information security management systems - Overview and vocabulary. (2014). Geneva, Switzerland: ISO copyright office

Magazcitum. (s.f.). ISO-27001: ¿Qué es y para qué sirve?. Recuperado el 27 de julio del 2015 de http://www.magazcitum.com.mx/?p=1574#.VhHF2vl_Okp

Magazcitum. (s.f.). ISO-27001:2013 ¿Qué hay de nuevo?. Recuperado el 27 de julio de 2015 de http://www.magazcitum.com.mx/?p=2397#.VeXD4_l_Okp

Neupart. ISO 27001:Konvertering til ISO 27002:2013. Recuperado el 03 de agosto de 2015 de http://www.neupart.dk/temaer/iso-27001/konvertering-til-iso-270022013

ANEXOS

Anexo 1. PLA Alistamiento ISO27001 2013 - Plan Detallado de Trabajo 2015 06 15 vFinal

DEFINICIÓN Y EJECUCIÓN DEL PROCESO DE ALISTAMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN DIRECTV.

Plan Detallado de Trabajo

Fase: I - Planear

Versión Final

Fecha: 15/06/2015

1. Objetivo del Plan Detallado de Trabajo

Establecer un marco de referencia para la gerencia y la persona que trabaje en el proyecto de titulación para apoyar a Directv Ecuador, (en adelante "DIRECTV"), en el alistamiento del sistema de gestión de seguridad de la información (ISO/IEC 27001:2013), con el fin de:

- Brindar el entendimiento de lo que el trabajo de titulación desea lograr para DIRECTV.
- Presentar las definiciones y lineamientos que guiarán la ejecución del trabajo de titulación.

Este documento incluye la definición de los siguientes aspectos relacionados con el proyecto:

- Gestión del Alcance.
- Gestión de Tiempos.
- Gestión de la Calidad.
- Gestión del Recurso Humano.
- Gestión de Riesgos.
- Consideraciones / Expectativas.

2. Gestión del Alcance

2.1 Entendimiento del Proyecto

2.1.1 Objetivo General

El objetivo general del trabajo de titulación de acuerdo a lo establecido en el anteproyecto es: *Establecer el plan de alistamiento y la documentación requerida como base para la posterior implementación del Sistema de Gestión de Seguridad de la Información (SGSI).*

2.1.2 Objetivos Específicos

A continuación se detallan los objetivos específicos del trabajo de titulación:

- Definir un plan detallado de trabajo.
- Definir un marco de evaluación.
- Definir un plan estratégico de seguridad de la información.
- Desarrollar el marco normativo básico de seguridad de la información, esto incluirá la elaboración de la política de gestión de seguridad de la información.
- Definir un marco de gobierno de seguridad de la información.

2.2 Alcance

El alcance del presente trabajo de titulación acorde al uso de la norma ISO/IEC 27001:2013 consiste en establecer los lineamientos generales del SGSI para su posterior implementación.

2.3 Matriz de Entregables

Los entregables del trabajo de titulación, de acuerdo con las etapas del mismo, son los siguientes:

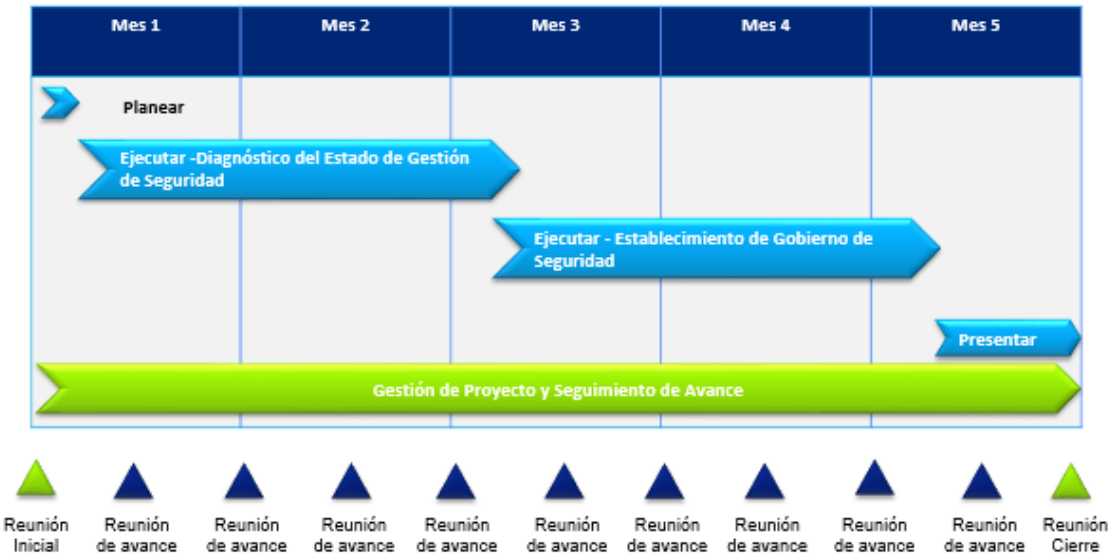
Fase	Entregable
Fase I - Planear	**Plan detallado de trabajo (Project charter)** Este documento contiene: • Entendimiento del trabajo de titulación. • Entregables del trabajo de titulación. • Plan de trabajo. • Cronograma del trabajo de titulación. • Equipo del trabajo de titulación, roles y responsabilidades. • Consideraciones y expectativas.
	Marco de evaluación Contiene el marco de referencia contra el cual se realizará la evaluación del estado actual de la gestión de seguridad de la información en DIRECTV.
Fase II - Ejecutar / Diagnóstico del Estado de Gestión de Seguridad	**Plan estratégico de seguridad de la información** Contiene el análisis de brecha entre las capacidades actuales de la gestión de seguridad de la información en DIRECTV respecto a lo requerido por la norma ISO/IEC 27001:2013. Los siguientes puntos forman parte del plan estratégico definido para DIRECTV: • Niveles de madurez deseados del área a corto, mediano y largo plazo. • Planes de acción y “roadmap” de implementación. • Objetivos estratégicos del área de seguridad de la información. • Plan de concienciación a los usuarios. **Evaluación de los requisitos de la norma ISO/IEC 27001:2013** Contiene la validación del cumplimiento de cada uno de los requisitos de la norma ISO/IEC 27001:2013 en DIRECTV.
Fase II - Ejecutar / Establecimiento de Gobierno de Seguridad	**Documento de Marco de Gobierno** Contiene el establecimiento del marco de gobierno de seguridad de la información, incluye: • Un organigrama funcional del departamento de

Fase	Entregable
	seguridad de la información y TI. • Definición detallada de roles y funciones del área. • Estructura o mapa del marco normativo de seguridad de DIRECTV. • Plan de entrenamiento a funcionarios del área de seguridad de la información.
	Políticas y Procedimientos Incluye el desarrollo y/o adecuación de las principales políticas y procedimientos requeridos por el área de seguridad de la información, contempla: ***Políticas:*** • Política de Seguridad de la Información. • Política de Gestión de Activos de Información. • Metodología de Análisis de Riesgos. • Política de Gestión de Acceso a Información. • Política de Administración de Seguridad de Red. • Política de Protección y Revisión de las Pistas de Auditoría. • Política de Administración de Respaldos. • Política de Monitoreo de Recursos de los Servicios y Sistemas Informáticos. • Política de Gestión de Software. • Política de Monitoreo de Niveles de Servicio de Incidentes de Seguridad. ***Procedimientos:*** • Procedimiento de Administración de Usuarios. • Procedimiento de Utilización de Cuentas de Máximos Privilegios. • Procedimiento de Control de Acceso Físico y Ambiental del Centro de Cómputo. • Procedimiento de Administración de Respaldos. • Procedimiento de Gestión de Incidentes de Seguridad.
Fase III - Presentar	**Armado de Entregables** Contiene los documentos e informes resultantes. En el caso de realizar algún ajuste sobre dichos documentos, actualizar y dar a conocer los informes finales del trabajo de titulación. **Presentación ejecutiva** Contiene los resultados del trabajo de titulación, con el fin de socializar a la Alta Administración de DIRECTV.

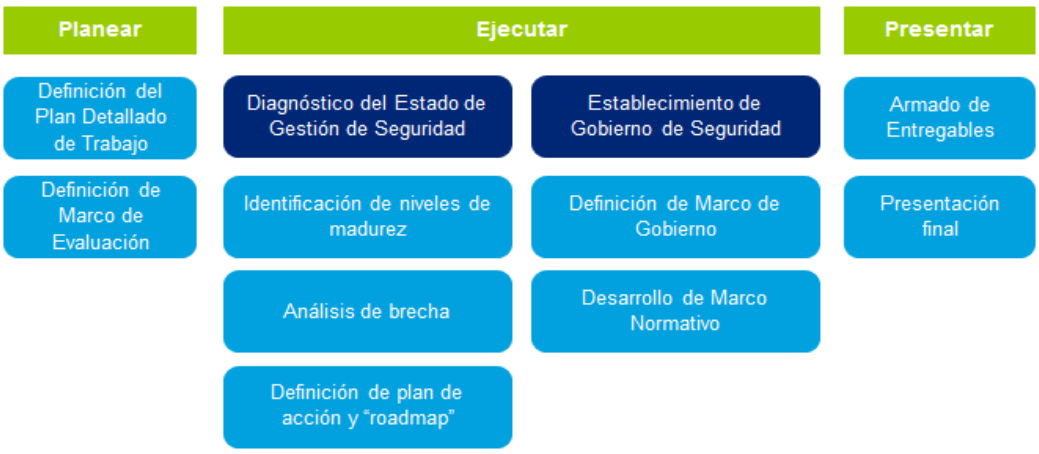
3. Gestión de Tiempos

La duración del trabajo de titulación es de 120 (ciento veinte) días a partir de la aprobación de DIRECTV, para poder realizar el proyecto de alistamiento del sistema de gestión de seguridad de la información (SGSI) en dicha Compañía.

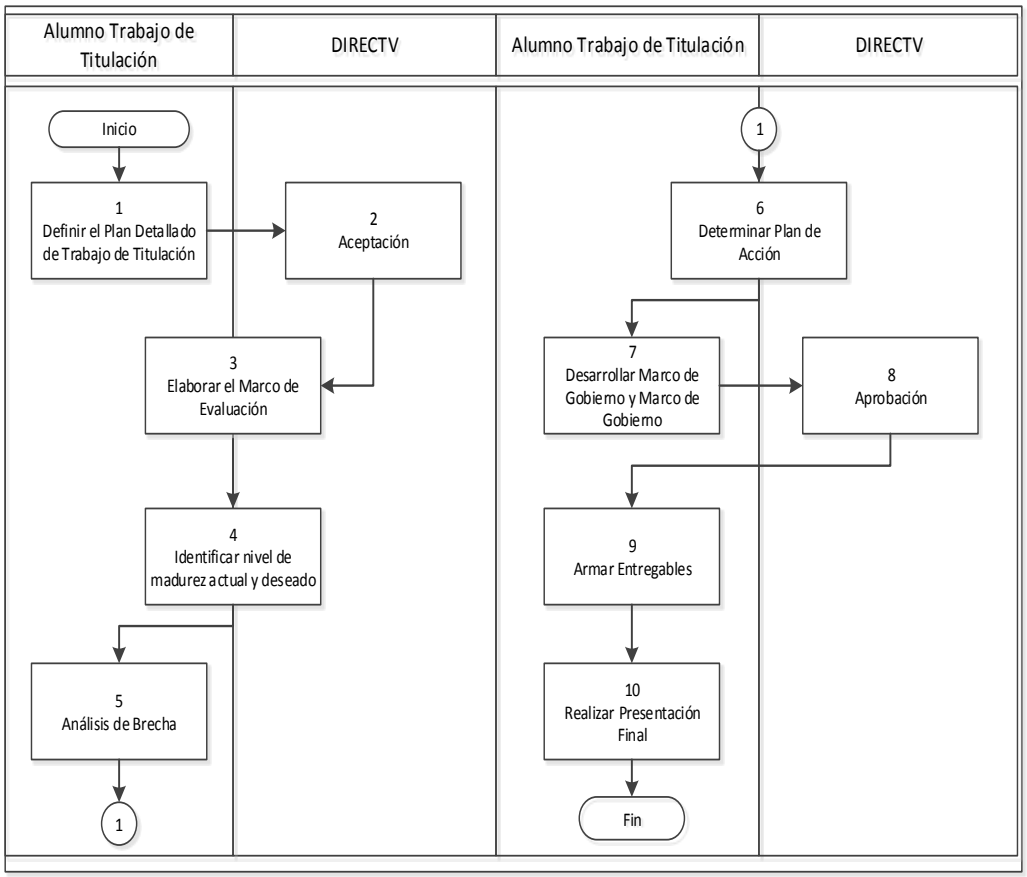
A continuación se presenta el cronograma general de actividades a ejecutarse en el presente trabajo de titulación:



A continuación se presenta el gráfico sobre la metodología a utilizar en el trabajo de titulación:



A continuación se presenta el diagrama de flujo sobre la metodología a utilizar en el trabajo de titulación:



Adicionalmente, se incluye el cronograma con fechas de inicio y fin por cada capítulo:

Trabajo de Titulación	120 days	Mon 18/05/15	Fri 30/10/15
Inicio	0 days	Mon 18/05/15	Mon 18/05/15
Capítulo I (Marco Teórico - Introducción a la Seguridad de la Información - Normativas en Seguridad - SGSI)	15 days	Mon 18/05/15	Fri 05/06/15
Capítulo I Concluido	0 days	Fri 05/06/15	Fri 05/06/15
Capítulo II (Metodología - Fase de Planeación - Fase de Ejecución - Fase de Presentación)	80 days	Mon 08/06/15	Fri 25/09/15
Capítulo II Concluido	0 days	Fri 25/09/15	Fri 25/09/15
Capítulo III (Gestión de Proyecto y Seguimiento de Avance - Fase de Seguimiento - Entregables)	15 days	Mon 28/09/15	Fri 16/10/15
Capítulo III Concluido	0 days	Fri 16/10/15	Fri 16/10/15
Capítulo IV (Conclusiones y Recomendaciones)	8 days	Mon 19/10/15	Wed 28/10/15
Capítulo IV Concluido	0 days	Wed 28/10/15	Wed 28/10/15
Capítulo V (Referencias)	1 day	Thu 29/10/15	Thu 29/10/15
Capitulo V Concluido	0 days	Thu 29/10/15	Thu 29/10/15
Capítulo VI (Anexos)	1 day	Fri 30/10/15	Fri 30/10/15
Capitulo VI Concluido	0 days	Fri 30/10/15	Fri 30/10/15

4. Gestión de la Calidad

Los entregables que se generarán, y que se detallan en la sección 2.3 Matriz de Entregables, serán revisados previamente a su entrega a DIRECTV por el tutor del trabajo de titulación designado por la Universidad de las Américas UDLA. Posteriormente, estos deberán ser revisados y aprobados por DIRECTV de forma previa a su entrega formal.

4.1 Aseguramiento de Calidad

El proceso de aseguramiento de calidad tiene como objetivo mejorar el proceso de ejecución del trabajo de titulación para evitar que los entregables no contengan errores o no cumplan con las expectativas de DIRECTV. Las actividades a realizar están listadas en la sección 5.1.2 y son parte de las funciones del Administrador de Seguridad de la Información de DIRECTV y el estudiante responsable del trabajo de titulación.

La periodicidad del proceso de aseguramiento de calidad con DIRECTV será quincenal en el cual se informará el avance del proyecto y los asuntos pendientes.

4.2 Control de Calidad

El proceso de control de calidad se enfoca en la identificación del cumplimiento de expectativas de los entregables del trabajo de titulación (ver sección 2.3). Los responsables de esta actividad serán el tutor del trabajo de titulación designado por la Universidad de las Américas UDLA y el estudiante responsable del trabajo de titulación, quienes serán responsables por validar los entregables finales en conjunto con el Administrador de Seguridad de la Información de DIRECTV.

Para facilidad de revisión de los entregables, se asignará la siguiente nomenclatura en el nombre del archivo:

PLA Alistamiento ISO27001 2013 - Plan del Trabajo de Titulación 2015 06 15 v1

Donde el nombre está conformado por los siguientes elementos:

PLA: se refiere a la fase del ciclo de vida del trabajo de titulación, las fases son:

- PLA, Planificación.
- EJE, Ejecución.
- CIE, Cierre.

Alistamiento ISO27001 2013: es la denominación del trabajo de titulación.

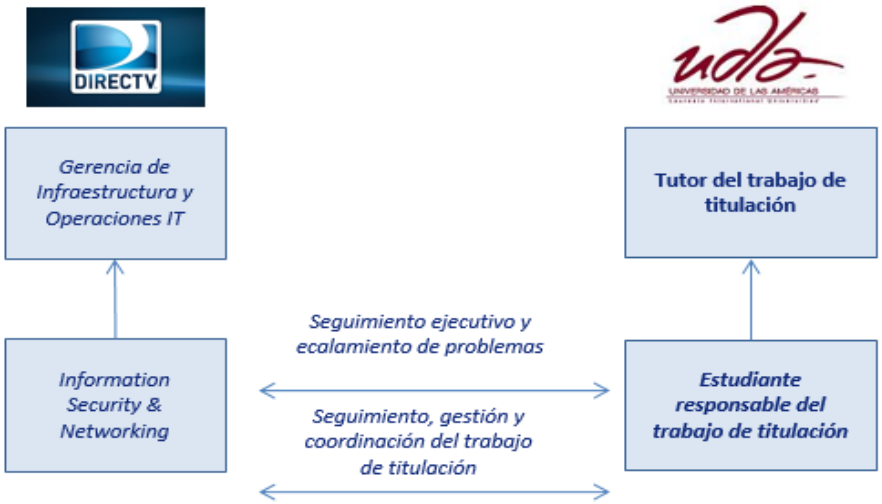
Plan de trabajo: es el nombre del entregable.

2014 04 30: es la última fecha de revisión del entregable, se colocará siguiendo el formato AAAA MM DD (A: año, M: mes, D: día).

v4: es la versión del documento luego de las revisiones de DIRECTV y el estudiante del trabajo de titulación. El número será reemplazado por la palabra Final cuando el entregable sea la versión aprobada por el Administrador de Seguridad de la Información de DIRECTV.

5. Gestión del Recurso Humano

A continuación se presenta la estructura del equipo de trabajo para el proyecto de titulación:



5.1 Roles y Responsabilidades

A continuación se presenta los roles y responsabilidades del equipo de trabajo del proyecto de titulación integrado por el estudiante responsable del proyecto y los funcionarios de DIRECTV que con su apoyo contribuirán al desarrollo del proyecto.

5.1.1 Gerencia del Proyecto

- Gerente de Infraestructura y Operaciones IT - DIRECTV

DIRECTV proveerá un Gerente de Infraestructura y Operaciones IT, él tendrá la responsabilidad de dar seguimiento al trabajo de titulación, resolver rápidamente los asuntos pendientes de DIRECTV y comunicar el estado del proyecto a la Dirección IT.

Sus funciones principales son:

- Promover la integración entre los diferentes equipos.
- Liderar la ejecución del trabajo de titulación.
- Gestionar internamente el escalamiento de temas críticos que necesiten de una definición por parte de DIRECTV.

5.1.2 Grupo de Apoyo - DIRECTV

Estará conformado por el Administrador de Seguridad de la Información. Su compromiso con el trabajo de titulación es de vital importancia para el logro de los objetivos.

- Administrador de Seguridad de la Información

Será la persona que hará cumplir con las estipulaciones específicas que constan en el trabajo de titulación, ejercerá las siguientes funciones:

- Vigilar permanentemente la ejecución del proyecto.
- Mantener una coordinación cercana con el Gerente de Infraestructura y Operaciones IT de DIRECTV, a fin de identificar el desempeño y cumplimiento del trabajo de titulación propuesto por el estudiante de la Universidad de las Américas UDLA.

5.1.3 Grupo de Apoyo - Estudiante Trabajo de Titulación

- Estudiante responsable del trabajo de titulación

Tendrá a cargo la definición y ejecución del proceso de alistamiento del Sistema de Gestión de Seguridad de la Información (SGSI) en DIRECTV.

Dentro de sus funciones como parte del trabajo de titulación, se encuentran:

- Asistir a las reuniones establecidas.
- Proponer soluciones eficientes de trabajo.
- Desarrollar las tareas asignadas en el plan de trabajo.
- Informar al tutor del trabajo de titulación cualquier problema o dificultad en la ejecución de tareas en forma oportuna para que las acciones requeridas sean implementadas.

6. Gestión de Riesgos

La siguiente sección identifica de forma general los riesgos que pueden impactar en el avance y ejecución del trabajo de titulación; así como también los planes de acción a ejecutar para disminuir la probabilidad de la ocurrencia de tales eventos de riesgo. Esta actividad de administración de riesgos debe realizarse durante toda la ejecución del trabajo de titulación.

Riesgo	Plan de Acción
Falta de tiempo de la administración.	- Definir las tareas críticas y acuerdos con DIRECTV. - Planear las entrevistas necesarias con la mayor antelación posible.

Riesgo	Plan de Acción
Toma de decisiones inoportuna.	- Gestionar reuniones de avances quincenales y emergentes, con el objetivo de informar a la Gerencia de Infraestructura y Operaciones IT, los temas que no se han resuelto.
Inapropiada asignación de personal responsable para la aprobación de los entregables del trabajo de titulación.	- Cumplir con los tiempos acordados para la generación y aprobación de los entregables definidos en la sección 2.3.
Falta de compromiso de los recursos requeridos para cumplir con las tareas del trabajo de titulación.	- Establecer una gestión adecuada de los recursos e información necesaria para el desarrollo del trabajo de titulación.
Falta de seguimiento al desarrollo de actividades.	- Validar las responsabilidades del personal de DIRECTV. - Elaborar presentaciones puntuales sobre el avance del proyecto, dirigido a la Gerencia de Infraestructura y Operaciones IT.
Información desactualizada.	- Verificar que la información utilizada durante el proyecto, se encuentre vigente y esté alineada con los procesos que se ejecutan actualmente en DIRECTV.

7. Consideraciones / Expectativas

- El presente trabajo de titulación cubre la primera fase para la posterior implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

- El trabajo de titulación incluye lineamientos establecidos con respecto a la gestión de la seguridad de la información. La implementación del resultado final del alistamiento del SGSI, es responsabilidad de DIRECTV.

- DIRECTV debe proveer al estudiante responsable del trabajo de titulación, toda la información que sea requerida para desarrollar adecuadamente los objetivos del proyecto.

- Igualmente, DIRECTV debe ser el encargado de gestionar el apoyo completo del personal de la Compañía durante la ejecución del alistamiento del SGSI.

- El estudiante responsable del trabajo de titulación mantendrá absoluta confidencialidad de la información suministrada por DIRECTV como parte del desarrollo del proyecto.

Anexo 2. PLA Alistamiento ISO27001 2013 - Marco de Evaluación 2015 06 15 vFinal

DEFINICIÓN Y EJECUCIÓN DEL PROCESO DE ALISTAMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN DIRECTV.

Marco de Evaluación de Seguridad de la Información

Fase: I - Planear

Versión Final

Fecha: 15/06/2015

1. Objetivo

Definir el marco de referencia contra el cual se realizó la evaluación del estado actual de la Gestión de la Seguridad de la Información en Directv Ecuador, (en adelante “DIRECTV”), como parte del trabajo de titulación de alistamiento del sistema de gestión de seguridad de la información.

2. Marco de Evaluación

La definición de un marco de evaluación para determinar el nivel de madurez de la seguridad de la información en DIRECTV es muy importante, puesto que está estrechamente relacionado con el objetivo que se persigue a través del presente trabajo de titulación. Esta definición permitirá que cualquier lector o nuevo interesado en el proyecto, pueda visualizar claramente cuál es el ***punto de referencia*** desde donde partió el proyecto y permitirá continuamente monitorear el nivel de avance de proyectos o iniciativas relacionadas con la Seguridad de la Información en DIRECTV.

Adicionalmente y en el momento que DIRECTV decida certificar su Sistema de Gestión de Seguridad de la Información (en adelante “SGSI”), este documento será un buen punto de partida para la reproducción de una Declaración de Aplicabilidad, en la cual se resumen los controles implementados y no implementados, así como las justificaciones para ambos casos.

2.1 Marco de Evaluación de Seguridad de la Información para DIRECTV

Acorde al uso de la norma ISO/IEC 27001:2013, se considera que la etapa inicial consiste en establecer los lineamientos generales del SGSI para su posterior implementación. Incluyendo como primera fase la realización de:

- Plan detallado de trabajo para cumplir lo acordado con DIRECTV.
- Definición de los controles o directrices que DIRECTV deberá implementar.
- Niveles de madurez deseados.
- Planes de acción u hojas de ruta, acorde a los criterios definidos en conjunto.
- Los entregables como políticas, normas y procedimientos en base a lo requerido por la norma ISO/IEC 27001:2013.

Para cumplir con las actividades descritas, se definió un Marco de Evaluación de Seguridad de la Información, que es un insumo importante para la realización de las mismas.

A continuación el marco de referencia o evaluación que se consideró en el alistamiento del SGSI en DIRECTV:

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	1.1 Políticas para la seguridad de la información	a) Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	SI
	1.2 Revisión de las políticas para la seguridad de la información	a) Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	SI
2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	2.1 Roles y responsabilidades en seguridad de la información	a) Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.	SI
	2.2 Segregación de tareas	a) Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.	SI
	2.3 Contacto con las autoridades	a) Deben mantenerse los contactos apropiados con las autoridades pertinentes.	SI
	2.4 Contacto con grupo de interés especial	a) Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializadas en seguridad.	SI
	2.5 Seguridad de la información en la gestión de proyectos	a) La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
	2.6 Política de dispositivos móviles	a) Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.	SI
	2.7 Teletrabajo	a) Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.	
3. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	3.1 Investigación de antecedentes	a) La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normas y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.	SI
	3.2 Términos y condiciones del empleo	a) Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones de su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.	SI
	3.3 Responsabilidades de gestión	a) La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.	SI
	3.4 Concienciación, educación y capacitación en seguridad de la	a) Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
	información		
	3.5 Proceso disciplinario	a) Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.	SI
	3.6 Responsabilidades ante la finalización o cambio	a) Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir.	SI
4. GESTIÓN DE ACTIVOS	4.1 Inventario de activos	a) Los activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.	SI
	4.2 Propiedad de los activos	a) Todos los activos que figuran en el inventario deben tener un propietario.	SI
	4.3 Uso aceptable de los activos	a) Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.	SI
	4.4 Devolución de activos	a) Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
	4.5 Clasificación de la información	a) La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.	SI
	4.6 Etiquetado de la información	a) Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.	SI
	4.7 Manipulado de la información	a) Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.	SI
	4.8 Gestión de soportes extraíbles	a) Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.	SI
	4.9 Eliminación de soportes	a) Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.	SI
	4.10 Soportes físicos en tránsito	a) Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.	SI
5. CONTROL DE ACCESO	5.1 Política de control de acceso	a) Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	SI
	5.2 Acceso a las redes y a los servicios de red	a) Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
	5.3 Registro y baja de usuario	a) Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.	SI
	5.4 Provisión de acceso de usuario	a) Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.	SI
	5.5 Gestión de privilegios de acceso	a) La asignación y el uso de privilegios de acceso debe estar restringida y controlada.	SI
	5.6 Gestión de la información secreta de autenticación de los usuarios	a) La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.	SI
	5.7 Revisión de los derechos de acceso de usuario	a) Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.	SI
	5.8 Retirada o reasignación de los derechos de acceso	a) Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.	SI
	5.9 Uso de la información secreta de	a) Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
	autenticación		
	5.10 Restricción del acceso a la información	a) Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.	SI
	5.11 Procedimientos seguros de inicio de sesión	a) Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.	SI
	5.12 Sistema de gestión de contraseñas	a) Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.	SI
	5.13 Uso de utilidades con privilegios del sistema	a) Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.	SI
	5.14 Control de acceso al código fuente de los programas	a) Se debe restringir el acceso al código fuente de los programas.	SI
6. CRIPTOGRAFÍA	6.1 Política de uso de los	a) Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
	controles criptográficos		
	6.2 Gestión de claves	a) Se debe desarrollar e implementar una política de sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.	SI
7. SEGURIDAD FISICA Y DEL ENTORNO	7.1 Perímetro de seguridad física	a) Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.	SI
	7.2 Controles físicos de entrada	a) Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.	SI
	7.3 Seguridad de oficinas, despachos y recursos	a) Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.	SI
	7.4 Protección contra las amenazas externas y ambientales	a) Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.	SI
	7.5 El trabajo en áreas seguras	a) Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
	7.6 Áreas de carga y descarga	a) Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.	SI
	7.7 Emplazamiento y protección de equipos	a) Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.	SI
	7.8 Instalaciones de suministro	a) Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.	SI
	7.9 Seguridad del cableado	a) El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.	SI
	7.10 Mantenimiento de los equipos	a) Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.	SI
	7.11 Retirada de materiales propiedad de la empresa	a) Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.	SI
	7.12 Seguridad de los equipos fuera de las instalaciones	a) Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
	7.13 Reutilización o eliminación segura de equipos	a) Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.	SI
	7.14 Equipo de usuario desatendido	a) Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.	SI
	7.15 Política de puesto de trabajo despejado y pantalla limpia	a) Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
8. SEGURIDAD DE LAS OPERACIONES	8.1 Documentación de procedimientos de operación	a) Deben documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.	SI
	8.2 Gestión de cambios	a) Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de información deben ser controlados.	SI
	8.3 Gestión de capacidades	a) Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	SI
	8.4 Separación de los recursos de desarrollo, prueba y operación	a) Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.	SI
	8.5 Controles contra el código malicioso	a) Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.	SI
	8.6 Copias de seguridad de la información	a) Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.	SI
	8.7 Registro de eventos	a) Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
	8.8 Protección de la información de registro	a) Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.	SI
	8.9 Registros de administración y operación	a) Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.	SI
	8.10 Sincronización del reloj	a) Los relojes de todos los sistemas de tratamiento de información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente precisa y acordada de tiempo.	SI
	8.11 Instalación del software en uso	a) Se deben implementar procedimientos para controlar la instalación del software en uso.	SI
	8.12 Gestión de las vulnerabilidades técnicas	a) Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.	SI
	8.13 Restricción en la instalación de software	a) Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.	SI
	8.14 Controles de auditoría de sistemas de información	a) Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.	SI
9. SEGURIDAD DE LAS	9.1 Controles de red	a) Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
COMUNICACIONES	9.2 Seguridad de los servicios de red	a) Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.	SI
	9.3 Segregación en redes	a) Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.	SI
	9.4 Políticas y procedimientos de intercambio de información	a) Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.	SI
	9.5 Acuerdos de intercambio de información	a) Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.	SI
	9.6 Mensajería electrónica	a) La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.	SI
	9.7 Acuerdos de confidencialidad o no revelación	a) Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación.	SI
10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE	10.1 Análisis de requisitos y especificaciones de seguridad de la	a) Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
LOS SISTEMAS DE INFORMACIÓN	información		
	10.2 Asegurar los servicios de aplicaciones en redes públicas	a) La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizada.	SI
	10.3 Protección de las transacciones de servicios de aplicaciones	a) La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizado.	SI
	10.4 Política de desarrollo seguro	a) Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.	SI
	10.5 Procedimiento de control de cambios en sistemas	a) La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios.	SI
	10.6 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	a) Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
	10.7 Restricciones a los cambios en los paquetes de software	a) Se deben restringir las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.	SI
	10.8 Principios de ingeniería de sistemas seguros	a) Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.	SI
	10.9 Entorno de desarrollo seguro	a) Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.	SI
	10.10 Externalización del desarrollo de software	a) El desarrollo de software realizado por empresas externas debe ser supervisado y controlado por la organización.	SI
	10.11 Pruebas funcionales de seguridad de sistemas	a) Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.	SI
	10.12 Pruebas de aceptación de sistemas	a) Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.	SI
	10.13 Protección de los datos de prueba	a) Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
11. RELACIÓN CON PROVEEDORES	11.1 Política de seguridad de la información en las relaciones con los proveedores	a) Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben acordarse con el proveedor y quedar documentados.	SI
	11.2 Requisitos de seguridad en contratos con terceros	a) Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura IT.	SI
	11.3 Cadena de suministro de tecnología de la información y de las comunicaciones	a) Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.	SI
	11.4 Control y revisión de la provisión de servicios del proveedor	a) Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor	SI
	11.5 Gestión de cambios en la provisión del servicio del proveedor	a) Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los riesgos.	SI
12. GESTIÓN DE INCIDENTES DE	12.1 Responsabilidades y	a) Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
SEGURIDAD DE LA INFORMACIÓN	procedimientos	seguridad de la información.	
	12.2 Notificación de los eventos de seguridad de la información	a) Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.	SI
	12.3 Notificación de puntos débiles de la seguridad	a) Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.	SI
	12.4 Evaluación y decisión sobre los eventos de seguridad de Información	a) Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.	SI
	12.5 Respuesta a incidentes de seguridad de la información	a) Los incidentes de seguridad de la información deben contar con una respuesta de acuerdo con los procedimientos documentados.	SI
	12.6 Aprendizaje de los incidentes de seguridad de la información	a) El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.	SI
	12.7 Recopilación de evidencias	a) La organización debe definir y aplicar procedimientos para la identificación, recopilación, adquisición y preservación de información que puede servir de	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
		evidencia.	
13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	13.1 Planificación de la continuidad de la seguridad de la información	a) La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	SI
	13.2 Implementar la continuidad de la seguridad de la información	a) La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.	SI
	13.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	a) La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.	SI
	13.4 Disponibilidad de los recursos de tratamiento de la información	a) Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
14. CUMPLIMIENTO	14.1 Identificación de la legislación aplicable y de los requisitos contractuales	a) Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deben definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.	SI
	14.2 Derechos de propiedad intelectual (DPI)	a) Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	SI
	14.3 Protección de los registros de la organización	a) Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.	SI
	14.4 Protección y privacidad de la información de carácter personal	a) Se debe garantizar la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.	SI
	14.5 Regulación de los controles criptográficos	a) Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.	SI

Dominio del Control	Subdominio	Directriz	Control que se considerará prioritario en esta primera fase
	14.6 Revisión independiente de la seguridad de la información	a) El enfoque de la organización para la gestión de seguridad de la información y su implantación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.	SI
	14.7 Cumplimiento de las políticas y normas de seguridad	a) Los directivos deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable	SI
	14.8 Comprobación del cumplimiento técnico	a) Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.	SI

Anexo 3. EJE Alistamiento ISO27001 2013 - Plan Estratégico de Seguridad de la Información 2015 06 22 vFinal

DEFINICIÓN Y EJECUCIÓN DEL PROCESO DE ALISTAMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN DIRECTV.

Plan Estratégico de Seguridad de la Información

Fase: II - Ejecutar

Versión Final

Fecha: 22/06/2015

Plan estratégico de Seguridad de la Información

El presente documento incluye las diferentes actividades realizadas para el establecimiento del estado de gestión de Seguridad de la Información en DIRECTV, considerando el Marco de Evaluación definido en la Fase de Planeación, y además la identificación del nivel de madurez futuro que la empresa pretende alcanzar, mediante la definición de planes de acción, iniciativas o proyectos de seguridad con su respectiva ruta de implementación, los cuales son de gran ayuda para lograr alcanzar el nivel requerido.

El documento contiene las siguientes secciones:

- Niveles de madurez deseados del Área a corto, mediano y largo plazo.
- Planes de acción y "roadmap" de implementación.

1. Niveles de madurez deseados del Área a corto, mediano y largo plazo

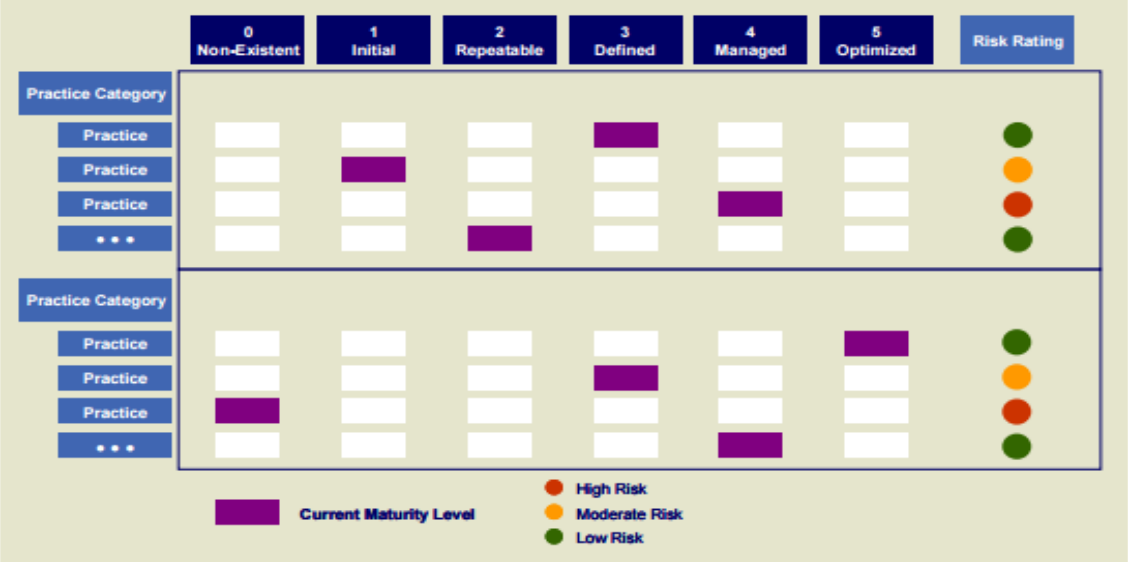
1.1 Objetivos

- Determinar el estado actual de madurez de Seguridad de la Información en DIRECTV, tomando como referencia el Marco de Evaluación.
- Establecer el nivel de madurez futuro de Seguridad de la Información a corto, mediano y largo plazo, en conjunto con las áreas responsables, de acuerdo a los requerimientos particulares de la Compañía, y además, alineándose a lo establecido en el Marco de Evaluación.
- Establecer iniciativas o proyectos de seguridad requeridos para alcanzar el nivel de madurez deseado.
- Establecer la hoja de ruta (roadmap) de implementación de los diferentes planes de acción considerando aspectos tales como brechas y nivel de esfuerzo.

1.2 Actividades realizadas

1.2.1 Niveles de madurez actual

- Se utilizó la escala de evaluación de la Metodología desarrollada por la empresa Deloitte “Evaluación de Riesgos de la Seguridad de la Información”, con el fin de medir el estado de madurez de la Seguridad de la Información en DIRECTV. La escala contiene 6 rangos de evaluación (0-5) y 3 rangos de alineación con el Marco de Evaluación. A continuación se detalla la escala de evaluación y los rangos de alineación:



Los 3 rangos de alineación con el Marco de Evaluación, corresponden a:

Color	Alineación
Rojo	Baja
Amarillo	Media
Verde	Alta

- Se solicitaron reuniones con personal responsable de cada una de las Áreas involucradas en el presente trabajo de titulación.

- Considerando las directrices por subdominio establecidas en el Marco de Evaluación y la escala de calificación, se evaluó las directrices o controles en reuniones mantenidas con personal responsable de cada una de las Áreas involucradas en el presente trabajo de titulación.

- Una vez realizada la evaluación, se consolidó las respuestas y se obtuvo un valor promedio por subdominio que corresponde a la sumatoria de todos los valores por directriz. Estos valores fueron validados con cada uno de los responsables, para obtener su aprobación correspondiente.

- Considerando los promedios obtenidos por subdominio, se estableció la alineación de estos valores con el Marco de Evaluación.

La siguiente tabla muestra el promedio de evaluación obtenido por subdominio y su alineación con el Marco de Evaluación:

Dominio	Sub-dominio	Promedio / Alineación

Dominio	Sub-dominio	Promedio / Alineación
1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	1.1 Políticas para la seguridad de la información	1.00
	1.2 Revisión de las políticas para la seguridad de la información	2.00
2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	2.1 Roles y responsabilidades en seguridad de la información	5.00
	2.2 Segregación de tareas	3.00
	2.3 Contacto con las autoridades	1.00
	2.4 Contacto con grupo de interés especial	1.00
	2.5 Seguridad de la información en la gestión de proyectos	3.00
	2.6 Política de dispositivos móviles	1.00
	2.7 Teletrabajo	1.00
3. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	3.1 Investigación de antecedentes	2.00
	3.2 Términos y condiciones del empleo	0.00
	3.3 Responsabilidades de gestión	1.00
	3.4 Concienciación, educación y capacitación en seguridad de la información	1.00
	3.5 Proceso disciplinario	0.00
	3.6 Responsabilidades ante la finalización o cambio	1.00
4. GESTIÓN DE ACTIVOS	4.1 Inventario de activos	2.00
	4.2 Propiedad de los activos	3.00
	4.3 Uso aceptable de los activos	3.00
	4.4 Devolución de activos	3.00

Dominio	Sub-dominio	Promedio / Alineación
	4.5 Clasificación de la información	0.00
	4.6 Etiquetado de la información	0.00
	4.7 Manipulado de la información	0.00
	4.8 Gestión de soportes extraíbles	0.00
	4.9 Eliminación de soportes	0.00
	4.10 Soportes físicos en tránsito	2.00
5. CONTROL DE ACCESO	5.1 Política de control de acceso	2.00
	5.2 Acceso a las redes y a los servicios de red	2.00
	5.3 Registro y baja de usuario	4.00
	5.4 Provisión de acceso de usuario	4.00
	5.5 Gestión de privilegios de acceso	2.00
	5.6 Gestión de la información secreta de autenticación de los usuarios	3.00
	5.7 Revisión de los derechos de acceso de usuario	1.00
	5.8 Retirada o reasignación de los derechos de acceso	5.00
	5.9 Uso de la información secreta de autenticación	3.00
	5.10 Restricción del acceso a la información	3.00
	5.11 Procedimientos seguros de inicio de sesión	3.00
	5.12 Sistema de gestión de contraseñas	3.00
	5.13 Uso de utilidades con privilegios del sistema	2.00

Dominio	Sub-dominio	Promedio / Alineación
	5.14 Control de acceso al código fuente de los programas	2.00
6. CRIPTOGRAFÍA	6.1 Política de uso de los controles criptográficos	5.00
	6.2 Gestión de claves	4.00
7. SEGURIDAD FISICA Y DEL ENTORNO	7.1 Perímetro de seguridad física	2.00
	7.2 Controles físicos de entrada	2.00
	7.3 Seguridad de oficinas, despachos y recursos	2.00
	7.4 Protección contra las amenazas externas y ambientales	2.00
	7.5 El trabajo en áreas seguras	2.00
	7.6 Áreas de carga y descarga	4.00
	7.7 Emplazamiento y protección de equipos	4.00
	7.8 Instalaciones de suministro	3.00
	7.9 Seguridad del cableado	3.00
	7.10 Mantenimiento de los equipos	4.00
	7.11 Retirada de materiales propiedad de la empresa	4.00
	7.12 Seguridad de los equipos fuera de las instalaciones	3.00
	7.13 Reutilización o eliminación segura de equipos	2.00
	7.14 Equipo de usuario desatendido	3.00
	7.15 Política de puesto de trabajo despejado y pantalla limpia	3.00
8. SEGURIDAD DE LAS OPERACIONES	8.1 Documentación de procedimientos de operación	2.00
	8.2 Gestión de cambios	5.00

Dominio	Sub-dominio	Promedio / Alineación
	8.3 Gestión de capacidades	0.00
	8.4 Separación de los recursos de desarrollo, prueba y operación	3.00
	8.5 Controles contra el código malicioso	4.00
	8.6 Copias de seguridad de la información	3.00
	8.7 Registro de eventos	0.00
	8.8 Protección de la información de registro	0.00
	8.9 Registros de administración y operación	2.00
	8.10 Sincronización del reloj	2.00
	8.11 Instalación del software en uso	2.00
	8.12 Gestión de las vulnerabilidades técnicas	5.00
	8.13 Restricción en la instalación de software	2.00
	8.14 Controles de auditoría de sistemas de información	2.00
9. SEGURIDAD DE LAS COMUNICACIONES	9.1 Controles de red	2.00
	9.2 Seguridad de los servicios de red	2.00
	9.3 Segregación en redes	2.00
	9.4 Políticas y procedimientos de intercambio de información	2.00
	9.5 Acuerdos de intercambio de información	2.00
	9.6 Mensajería electrónica	2.00
	9.7 Acuerdos de confidencialidad o no revelación	2.00

Dominio	Sub-dominio	Promedio / Alineación
10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	10.1 Análisis de requisitos y especificaciones de seguridad de la información	1.00
	10.2 Asegurar los servicios de aplicaciones en redes públicas	2.00
	10.3 Protección de las transacciones de servicios de aplicaciones	2.00
	10.4 Política de desarrollo seguro	2.00
	10.5 Procedimiento de control de cambios en sistemas	4.00
	10.6 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	1.00
	10.7 Restricciones a los cambios en los paquetes de software	4.00
	10.8 Principios de ingeniería de sistemas seguros	2.00
	10.9 Entorno de desarrollo seguro	0.00
	10.10 Externalización del desarrollo de software	2.00
	10.11 Pruebas funcionales de seguridad de sistemas	2.00
	10.12 Pruebas de aceptación de sistemas	2.00
	10.13 Protección de los datos de prueba	2.00
11. RELACIÓN CON PROVEEDORES	11.1 Política de seguridad de la información en las relaciones con los proveedores	2.00
	11.2 Requisitos de seguridad en contratos con terceros	2.00
	11.3 Cadena de suministro de tecnología de la información y de las comunicaciones	2.00

Dominio	Sub-dominio	Promedio / Alineación
	11.4 Control y revisión de la provisión de servicios del proveedor	2.00
	11.5 Gestión de cambios en la provisión del servicio del proveedor	2.00
12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	12.1 Responsabilidades y procedimientos	5.00
	12.2 Notificación de los eventos de seguridad de la información	5.00
	12.3 Notificación de puntos débiles de la seguridad	3.00
	12.4 Evaluación y decisión sobre los eventos de seguridad de Información	5.00
	12.5 Respuesta a incidentes de seguridad de la información	5.00
	12.6 Aprendizaje de los incidentes de seguridad de la información	1.00
	12.7 Recopilación de evidencias	1.00
13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	13.1 Planificación de la continuidad de la seguridad de la información	3.00
	13.2 Implementar la continuidad de la seguridad de la información	2.00
	13.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	0.00
	13.4 Disponibilidad de los recursos de tratamiento de la información	5.00
14. CUMPLIMIENTO	14.1 Identificación de la legislación aplicable y de los requisitos contractuales	3.00
	14.2 Derechos de propiedad intelectual (DPI)	3.00

Dominio	Sub-dominio	Promedio / Alineación
	14.3 Protección de los registros de la organización	3.00
	14.4 Protección y privacidad de la información de carácter personal	3.00
	14.5 Regulación de los controles criptográficos	3.00
	14.6 Revisión independiente de la seguridad de la información	2.00
	14.7 Cumplimiento de las políticas y normas de seguridad	0.00
	14.8 Comprobación del cumplimiento técnico	4.00

1.2.2 Niveles de madurez futuro

- Para determinar el nivel de madurez futuro de cada directriz del Marco de Evaluación, se realizó diversas reuniones con personal de DIRECTV, estableciendo el nivel futuro y el plazo dentro del cual se alcanzará dicho nivel.

Los plazos establecidos se detallan:

Plazo	Fecha límite
Corto	Hasta Febrero de 2016
Mediano	Hasta Mayo de 2016
Largo	Hasta Noviembre 2016

La siguiente tabla muestra el nivel de madurez futuro por cada subdominio:

Dominio	Sub-dominio	Nivel de madurez futuro	Plazo
1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	1.1 Políticas para la seguridad de la información	3.00	Largo Plazo

Dominio	Sub-dominio	Nivel de madurez futuro	Plazo
	1.2 Revisión de las políticas para la seguridad de la información	4.00	Mediano Plazo
2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	2.1 Roles y responsabilidades en seguridad de la información	5.00	Se Mantiene
	2.2 Segregación de tareas	5.00	Mediano Plazo
	2.3 Contacto con las autoridades	3.00	Mediano Plazo
	2.4 Contacto con grupo de interés especial	3.00	Mediano Plazo
	2.5 Seguridad de la información en la gestión de proyectos	4.00	Corto Plazo
	2.6 Política de dispositivos móviles	3.00	Largo Plazo
	2.7 Teletrabajo	3.00	Largo Plazo
3. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	3.1 Investigación de antecedentes	3.00	Mediano Plazo
	3.2 Términos y condiciones del empleo	3.00	Mediano Plazo
	3.3 Responsabilidades de gestión	3.00	Mediano Plazo
	3.4 Concienciación, educación y capacitación en seguridad de la información	3.00	Mediano Plazo
	3.5 Proceso disciplinario	2.00	Mediano Plazo

Dominio	Sub-dominio	Nivel de madurez futuro	Plazo
	3.6 Responsabilidades ante la finalización o cambio	3.00	Mediano Plazo
4. GESTIÓN DE ACTIVOS	4.1 Inventario de activos	3.00	Mediano Plazo
	4.2 Propiedad de los activos	4.00	Mediano Plazo
	4.3 Uso aceptable de los activos	4.00	Mediano Plazo
	4.4 Devolución de activos	4.00	Mediano Plazo
	4.5 Clasificación de la información	3.00	Corto Plazo
	4.6 Etiquetado de la información	3.00	Largo Plazo
	4.7 Manipulado de la información	3.00	Largo Plazo
	4.8 Gestión de soportes extraíbles	2.00	Corto Plazo
	4.9 Eliminación de soportes	2.00	Corto Plazo
	4.10 Soportes físicos en tránsito	4.00	Corto Plazo
5. CONTROL DE ACCESO	5.1 Política de control de acceso	4.00	Corto Plazo
	5.2 Acceso a las redes y a los servicios de red	4.00	Mediano Plazo
	5.3 Registro y baja de usuario	5.00	Mediano Plazo
	5.4 Provisión de acceso de usuario	4.00	Se Mantiene
	5.5 Gestión de privilegios de acceso	3.00	Largo Plazo

Dominio	Sub-dominio	Nivel de madurez futuro	Plazo
	5.6 Gestión de la información secreta de autenticación de los usuarios	4.00	Mediano Plazo
	5.7 Revisión de los derechos de acceso de usuario	2.00	Mediano Plazo
	5.8 Retirada o reasignación de los derechos de acceso	5.00	Se Mantiene
	5.9 Uso de la información secreta de autenticación	4.00	Corto Plazo
	5.10 Restricción del acceso a la información	4.00	Corto Plazo
	5.11 Procedimientos seguros de inicio de sesión	4.00	Corto Plazo
	5.12 Sistema de gestión de contraseñas	4.00	Corto Plazo
	5.13 Uso de utilidades con privilegios del sistema	4.00	Largo Plazo
	5.14 Control de acceso al código fuente de los programas	4.00	Mediano Plazo
6. CRIPTOGRAFÍA	6.1 Política de uso de los controles criptográficos	5.00	Se Mantiene
	6.2 Gestión de claves	5.00	Corto Plazo
7. SEGURIDAD FISICA Y DEL	7.1 Perímetro de seguridad física	3.00	Mediano Plazo

Dominio	Sub-dominio	Nivel de madurez futuro	Plazo
ENTORNO	7.2 Controles físicos de entrada	3.00	Mediano Plazo
	7.3 Seguridad de oficinas, despachos y recursos	3.00	Mediano Plazo
	7.4 Protección contra las amenazas externas y ambientales	3.00	Mediano Plazo
	7.5 El trabajo en áreas seguras	3.00	Largo Plazo
	7.6 Áreas de carga y descarga	5.00	Mediano Plazo
	7.7 Emplazamiento y protección de equipos	5.00	Mediano Plazo
	7.8 Instalaciones de suministro	4.00	Mediano Plazo
	7.9 Seguridad del cableado	4.00	Mediano Plazo
	7.10 Mantenimiento de los equipos	5.00	Mediano Plazo
	7.11 Retirada de materiales propiedad de la empresa	5.00	Mediano Plazo
	7.12 Seguridad de los equipos fuera de las instalaciones	4.00	Mediano Plazo
	7.13 Reutilización o eliminación segura de equipos	3.00	Mediano Plazo
	7.14 Equipo de usuario desatendido	4.00	Mediano Plazo

Dominio	Sub-dominio	Nivel de madurez futuro	Plazo
	7.15 Política de puesto de trabajo despejado y pantalla limpia	4.00	Mediano Plazo
8. SEGURIDAD DE LAS OPERACIONES	8.1 Documentación de procedimientos de operación	3.00	Largo Plazo
	8.2 Gestión de cambios	5.00	Se Mantiene
	8.3 Gestión de capacidades	4.00	Largo Plazo
	8.4 Separación de los recursos de desarrollo, prueba y operación	4.00	Mediano Plazo
	8.5 Controles contra el código malicioso	5.00	Mediano Plazo
	8.6 Copias de seguridad de la información	4.00	Mediano Plazo
	8.7 Registro de eventos	3.00	Mediano Plazo
	8.8 Protección de la información de registro	3.00	Mediano Plazo
	8.9 Registros de administración y operación	3.00	Mediano Plazo
	8.10 Sincronización del reloj	3.00	Mediano Plazo
	8.11 Instalación del software en uso	3.00	Mediano Plazo
	8.12 Gestión de las vulnerabilidades técnicas	5.00	Se Mantiene

Dominio	Sub-dominio	Nivel de madurez futuro	Plazo
	8.13 Restricción en la instalación de software	3.00	Mediano Plazo
	8.14 Controles de auditoría de sistemas de información	3.00	Mediano Plazo
9. SEGURIDAD DE LAS COMUNICACIONES	9.1 Controles de red	3.00	Mediano Plazo
	9.2 Seguridad de los servicios de red	3.00	Mediano Plazo
	9.3 Segregación en redes	3.00	Mediano Plazo
	9.4 Políticas y procedimientos de intercambio de información	3.00	Mediano Plazo
	9.5 Acuerdos de intercambio de información	3.00	Mediano Plazo
	9.6 Mensajería electrónica	3.00	Mediano Plazo
	9.7 Acuerdos de confidencialidad o no revelación	3.00	Mediano Plazo
10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	10.1 Análisis de requisitos y especificaciones de seguridad de la información	3.00	Mediano Plazo
	10.2 Asegurar los servicios de aplicaciones en redes públicas	3.00	Mediano Plazo
	10.3 Protección de las transacciones de servicios de aplicaciones	3.00	Mediano Plazo
	10.4 Política de desarrollo seguro	3.00	Mediano Plazo

Dominio	Sub-dominio	Nivel de madurez futuro	Plazo
	10.5 Procedimiento de control de cambios en sistemas	4.00	Se Mantiene
	10.6 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	3.00	Mediano Plazo
	10.7 Restricciones a los cambios en los paquetes de software	4.00	Se Mantiene
	10.8 Principios de ingeniería de sistemas seguros	3.00	Mediano Plazo
	10.9 Entorno de desarrollo seguro	3.00	Mediano Plazo
	10.10 Externalización del desarrollo de software	3.00	Mediano Plazo
	10.11 Pruebas funcionales de seguridad de sistemas	3.00	Mediano Plazo
	10.12 Pruebas de aceptación de sistemas	3.00	Mediano Plazo
	10.13 Protección de los datos de prueba	3.00	Mediano Plazo
11. RELACIÓN CON PROVEEDORES	11.1 Política de seguridad de la información en las relaciones con los proveedores	3.00	Mediano Plazo
	11.2 Requisitos de seguridad en contratos con terceros	3.00	Mediano Plazo

Dominio	Sub-dominio	Nivel de madurez futuro	Plazo
	11.3 Cadena de suministro de tecnología de la información y de las comunicaciones	3.00	Mediano Plazo
	11.4 Control y revisión de la provisión de servicios del proveedor	3.00	Mediano Plazo
	11.5 Gestión de cambios en la provisión del servicio del proveedor	3.00	Mediano Plazo
12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	12.1 Responsabilidades y procedimientos	5.00	Se Mantiene
	12.2 Notificación de los eventos de seguridad de la información	5.00	Se Mantiene
	12.3 Notificación de puntos débiles de la seguridad	4.00	Mediano Plazo
	12.4 Evaluación y decisión sobre los eventos de seguridad de Información	5.00	Se Mantiene
	12.5 Respuesta a incidentes de seguridad de la información	5.00	Se Mantiene
	12.6 Aprendizaje de los incidentes de seguridad de la información	3.00	Mediano Plazo
	12.7 Recopilación de evidencias	3.00	Mediano Plazo

Dominio	Sub-dominio	Nivel de madurez futuro	Plazo
13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	13.1 Planificación de la continuidad de la seguridad de la información	4.00	Largo Plazo
	13.2 Implementar la continuidad de la seguridad de la información	3.00	Largo Plazo
	13.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	3.00	Largo Plazo
	13.4 Disponibilidad de los recursos de tratamiento de la información	5.00	Se Mantiene
14. CUMPLIMIENTO	14.1 Identificación de la legislación aplicable y de los requisitos contractuales	4.00	Mediano Plazo
	14.2 Derechos de propiedad intelectual (DPI)	4.00	Mediano Plazo
	14.3 Protección de los registros de la organización	4.00	Mediano Plazo
	14.4 Protección y privacidad de la información de carácter personal	4.00	Mediano Plazo
	14.5 Regulación de los controles criptográficos	4.00	Mediano Plazo
	14.6 Revisión independiente de la seguridad de la información	3.00	Mediano Plazo

Dominio	Sub-dominio	Nivel de madurez futuro	Plazo
	14.7 Cumplimiento de las políticas y normas de seguridad	2.00	Mediano Plazo
	14.8 Comprobación del cumplimiento técnico	5.00	Mediano Plazo

2. Planes de Acción

- Posterior al establecimiento del nivel de madurez a alcanzar, se definieron acciones a ejecutar por subdominio.

Estas acciones fueron categorizadas utilizando dos escalas (brecha y nivel de esfuerzo).
Brecha, considera el número de saltos para alcanzar el nivel futuro, la siguiente tabla muestra los rangos definidos para esta escala:

Brecha	No. de saltos para alcanzar Nivel Futuro
Alta	De 4 a 5
Media	De 2 a 3
Baja	1

Nivel de Esfuerzo, se trata del nivel de esfuerzo involucrado para llevar adelante los planes de acción. Se medirá con base en 3 elementos claves: tiempo, personas y costo, la siguiente tabla muestra los rangos definidos para esta escala:

Criterio	Nivel de esfuerzo		
	Bajo	*Medio*	*Alto*
Tiempo	De 1 a 3 meses	De 4 a 6 meses	Mayor a 6 meses

Criterio	Nivel de esfuerzo			
	Bajo	*Medio*	*Alto*	
Personas	1-2 personas / áreas	3-6 personas / áreas	Más de 6 personas / áreas	
Costo	Hasta $20K	De $20K a $50K	Más de $50K	Sólo esfuerzo interno

- Adicionalmente se estableció el plazo para la ejecución de los planes de acción, considerando la siguiente tabla:

Plazo	Tiempo en meses
Corto	3 meses
Mediano	6 meses
Lago	12 meses

El plazo para cada plan de acción fue establecido en conjunto con los funcionarios de las diferentes áreas involucradas de DIRECTV.

3. Hoja de ruta (Roadmap) de implementación

- Se realizó una revisión de todos los planes de acción y se agruparon aquellos que tenían un enfoque de aplicabilidad común para determinar iniciativas macro.

Las iniciativas de agrupación son:

#	Iniciativas
1	Definición, formalización y aprobación del marco normativo de seguridad de la información (políticas, procedimientos, reglamentos, manuales, etc).
2	Implantación de controles.
3	Aplicación de enfoques de mejora continua.
4	Sensibilización del personal.

3.1 Ficha técnica de iniciativas

En esta sección se detallan las iniciativas propuestas.

Iniciativa 1

INICIATIVA 1			
Definición, formalización y aprobación del marco normativo de seguridad de la información (políticas, procedimientos, reglamentos, manuales, etc).			
Objetivo:			
Establecer un marco normativo mediante la definición de políticas, procedimientos, estándares y reglamentos, que permita implantar controles de seguridad de la información en DIRECTV con base en la norma ISO/IEC 27001:2013.			
Principales actividades:			
- Identificar el marco normativo necesario en DIRECTV. - Confirmar los documentos que forman parte del marco normativo y que han sido desarrollados como parte del alistamiento del SGSI en DIRECTV y desarrollar aquellos que aún estén pendientes. - Formalizar, aprobar y socializar los documentos del marco normativo con las áreas impactadas. - Incorporar dichos documentos del marco normativo a un esquema de mejora continua, que permita asegurar su correcto mantenimiento, revisión y actualización.			
Dominios Asociados:			
1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 3. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS 4. GESTIÓN DE ACTIVOS 5. CONTROL DE ACCESO 7. SEGURIDAD FISICA Y DEL ENTORNO 8. SEGURIDAD DE LAS OPERACIONES 9. SEGURIDAD DE LAS COMUNICACIONES 10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN 11. RELACIÓN CON PROVEEDORES 12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO 14. CUMPLIMIENTO			
Brechas:		**Esfuerzo de Resolución:**	
Alta	1	Tiempo	Medio
Media	29	Personas	Bajo
Baja	39	Costo	SEI

INICIATIVA 1	
Duración Estimada:	6 meses (Mayo 2016)

Iniciativa 2

INICIATIVA 2			
Implantación de controles.			
Objetivo:			
Poner en ejecución los controles documentados en los planes de acción. Establecer un período de estabilización para corroborar que dichos controles están operando tal como fueron diseñados. Modificar la documentación de controles de acuerdo a su operación tomando en cuenta los lineamientos de seguridad de la información.			
Principales actividades:			
- Implantar los controles documentados en los planes de acción. - Socializar con los impactados el funcionamiento de los controles y la evidencia que se requiere generar producto de su ejecución. - Definir un período de estabilización para los controles implantados y dar seguimiento con el fin de determinar que estén operando acorde a como fueron diseñados. - Actualizar la documentación para que refleje la realidad de operación de los controles. - Monitorear en conjunto con las áreas responsables la ejecución de dichos controles.			
Dominios Asociados:			
1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 3. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS 4. GESTIÓN DE ACTIVOS 5. CONTROL DE ACCESO 7. SEGURIDAD FISICA Y DEL ENTORNO 8. SEGURIDAD DE LAS OPERACIONES 12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
Brechas:		**Esfuerzo de Resolución:**	
Alta	1	Tiempo	Medio
Media	14	Personas	Medio
Baja	15	Costo	SEI
Duración Estimada:		6 meses (Agosto 2016)	

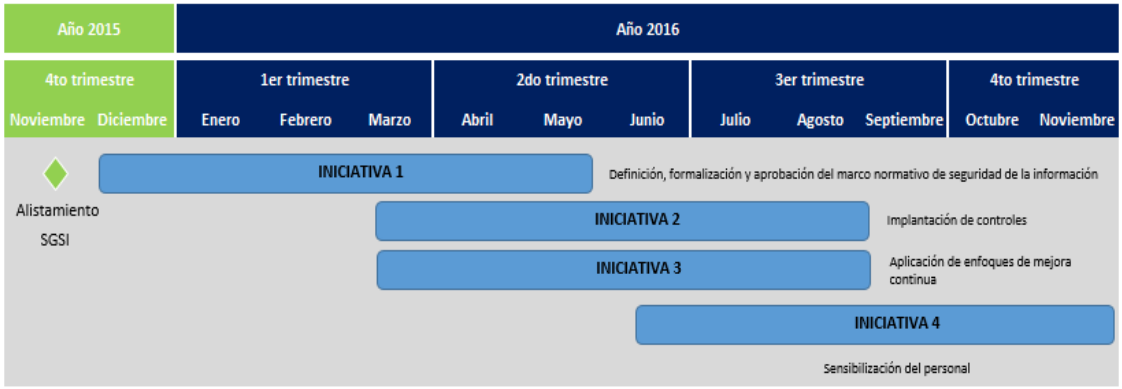
Iniciativa 3

INICIATIVA 3			
Aplicación de enfoques de mejora continua.			
Objetivo:			
Monitear y medir el cumplimiento de los procedimientos y la efectividad de los controles implementados, establecidos en las iniciativas 1 y 2 respectivamente; mediante la implementación de métricas e indicadores, con el fin de establecer acciones de mejora continua.			
Principales actividades:			
- Definir y establecer procedimientos de monitoreo de los documentos establecidos en el marco normativo y los controles implementados. - Realizar revisiones regulares de los procedimientos y la efectividad de controles implementados, considerando los resultados de los monitoreos efectuados. Adicionalmente, para estas revisiones se puede considerar los reportes de incidentes y los resultados de evaluaciones independientes. - Comunicar los resultados de las revisiones a las personas o áreas involucradas. - Establecer acciones de mejoramiento continuo, tanto preventivo como correctivo. - Medir las acciones de mejora, logrando un mejoramiento continuo.			
Dominios Asociados:			
2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 4. GESTIÓN DE ACTIVOS 5. CONTROL DE ACCESO 6. CRIPTOGRAFÍA 7. SEGURIDAD FISICA Y DEL ENTORNO 8. SEGURIDAD DE LAS OPERACIONES 13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO 14. CUMPLIMIENTO			
Brechas:		**Esfuerzo de Resolución:**	
Alta	0	Tiempo	Medio
Media	1	Personas	Medio
Baja	24	Costo	SEI
Duración Estimada:		6 meses (Agosto 2016)	

Iniciativa 4

INICIATIVA 4			
Sensibilización del personal.			
Objetivo:			
Definir la estrategia de concientización y capacitación en temas de Seguridad de la Información. Esta estrategia está enfocada a todos los usuarios de los recursos de información de DIRECTV.			
Principales actividades:			
- Identificar las necesidades de aprendizaje requeridas por los empleados de DIRECTV con temas relacionados a Seguridad de la Información. - Definir las audiencias a quienes se orientará la capacitación. - Determinar el temario a ser impartido en la sesión de sensibilización con base a las necesidades de conocimiento de cada audiencia. - Estimar los tiempos de las sesiones de acuerdo a la audiencia y temario.			
Dominios Asociados:			
1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 3. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS 8. SEGURIDAD DE LAS OPERACIONES 12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
Brechas:		**Esfuerzo de Resolución:**	
Alta	0	Tiempo	Alto
Media	3	Personas	Alto
Baja	2	Costo	SEI
Duración Estimada:	6 meses (Noviembre 2016)		

- Para cada una de las iniciativas propuestas se definió el plazo de implementación, considerando el tiempo establecido en los planes de acción para cada subdominio. A continuación se muestra un cronograma tentativo de ejecución de las iniciativas macro definidas para DIRECTV:



Iniciativa 1

Brechas		Esfuerzo	
Alta	1	Tiempo	Medio
Media	29	Personas	Bajo
Baja	39	Costo	SEI

Iniciativa 2

Brechas		Esfuerzo	
Alta	1	Tiempo	Medio
Media	14	Personas	Medio
Baja	15	Costo	SEI

Iniciativa 3

Brechas		Esfuerzo	
Alta	0	Tiempo	Medio
Media	1	Persona	Medio
Baja	24	Costo	SEI

Iniciativa 4

Brechas		Esfuerzo	
Alta	0	Tiempo	Alto
Media	3	Personas	Alto
Baja	2	Costo	SEI

Anexo 4. Planes de Acción

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	1.1 Políticas para la seguridad de la información	a) Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	1	3	Largo Plazo	1.1.1 Realizar un estudio del conjunto de políticas de seguridad de la información que ya se encuentran documentadas, para proceder con la aprobación y difusión de las mismas a todo el personal de DIRECTV. 1.1.2 Desarrollar las políticas o procedimientos que no se encuentren consideradas dentro del conjunto de políticas de seguridad de la información que ya fueron definidas por DIRECTV. 1.1.3 Establecer y ejecutar un plan para la comunicación y sensibilización de las políticas de seguridad de la información a todo el personal de DIRECTV.	Noviembre 2016
	1.2 Revisión de las políticas para la seguridad de la información	a) Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	2	4	Mediano plazo	1.2.1 Establecer intervalos de tiempo para la revisión del conjunto de políticas de seguridad de la información en DIRECTV. En caso que existan cambios significativos en la Compañía, esto deberá verse reflejado en la actualización de las políticas y procedimientos de seguridad de la información de DIRECTV.	Mayo 2016
2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	2.1 Roles y responsabilidades en seguridad de la información	a) Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.	5	5	Se Mantiene	2.1.1 No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.	No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.
	2.2 Segregación de tareas	a) Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.	3	5	Mediano Plazo	2.2.1 El Information Security & Networking de DIRECTV deberá definir y establecer un cronograma de revisión para validar que las funciones y áreas de responsabilidad se encuentren segregadas. En cada departamento deberá existir una correcta distribución de tareas, con el objetivo de reducir el riesgo de modificaciones indebidas por personal no autorizado.	Mayo 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	2.3 Contacto con las autoridades	a) Deben mantenerse los contactos apropiados con las autoridades pertinentes.	1	3	Mediano Plazo	2.3.1 Establecer un registro de datos de los contactos de las autoridades pertinentes, ya sean internas o externas. Para el caso de proveedores externos, el registro deberá contener entre otros datos: nombre del contacto, empresa a la pertenece, servicio que presta a DIRECTV, dirección, teléfono y extensión, número de celular, correo electrónico y horarios de atención. 2.3.2 Documentar, aprobar y difundir la política de seguridad de la información en DIRECTV. Esta política contendrá una sección sobre todas las actividades relacionadas con los contactos con las autoridades pertinentes, ya sean internas o externas.	Mayo 2016
	2.4 Contacto con grupo de interés especial	a) Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializadas en seguridad.	1	3	Mediano Plazo	2.4.1 Establecer un registro de datos de los contactos de foros, grupos y asociaciones profesionales especializadas en seguridad de la información. Este registro deberá contener entre otros datos: nombre del contacto, foro o asociación a la pertenece, dirección, teléfono y extensión, número de celular y correo electrónico. 2.4.2 Documentar, aprobar y difundir la política de seguridad de la información en DIRECTV. Esta política contendrá una sección sobre todas las actividades relacionadas con los contactos de grupos especializados en seguridad de la información.	Mayo 2016
	2.5 Seguridad de la información en la gestión de proyectos	a) La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.	3	4	Corto Plazo	2.5.1 En la herramienta de control de cambios de DIRECTV, se deberá incluir las consideraciones de seguridad de la información que se deben definir al inicio de cada uno de los proyectos de la Compañía. Esto ayudará a tener un control y monitoreo sobre la inclusión de medidas de seguridad a la gestión de proyectos de DIRECTV.	Febrero 2016
	2.6 Política de dispositivos móviles	a) Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.	1	3	Largo Plazo	2.6.1 Documentar, aprobar y difundir la política o procedimiento de dispositivos móviles.	Noviembre 2016
	2.7 Teletrabajo	a) Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en operaciones de teletrabajo.	1	3	Largo Plazo	2.7.1 Documentar, aprobar y difundir la política o procedimiento de teletrabajo.	Noviembre 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
3. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	3.1 Investigación de antecedentes	a) La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normas y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.	2	4	Mediano Plazo	3.1.1 Documentar, aprobar y difundir la política o procedimiento de seguridad de recursos humanos.	Mayo 2016
	3.2 Términos y condiciones del empleo	a) Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones de su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.	2	4	Mediano Plazo	3.2.1 Documentar, aprobar y difundir la política o procedimiento de seguridad de recursos humanos.	Mayo 2016
	3.3 Responsabilidades de gestión	a) La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.	1	3	Mediano Plazo	3.3.1 Ver Plan de Acción 1.1.3. 3.3.2 Documentar, aprobar y difundir la política o procedimiento de seguridad de recursos humanos.	Mayo 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	3.4 Concienciación, educación y capacitación en seguridad de la información	a) Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.	1	3	Mediano Plazo	3.4.1 Ver Plan de Acción 1.1.3. 3.4.2 Documentar, aprobar y difundir la política o procedimiento de seguridad de recursos humanos.	Mayo 2016
	3.5 Proceso disciplinario	a) Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.	0	2	Mediano Plazo	3.5.1 Recursos Humanos, con apoyo del Área Jurídica de DIRECTV deberá actualizar el Reglamento Interno, incluyendo temas relacionados con el proceso disciplinario referente a brechas e incidentes de seguridad de la información. 3.5.2 Documentar la política o procedimiento de seguridad de recursos humanos.	Mayo 2016
	3.6 Responsabilidades ante la finalización o cambio	a) Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir.	1	3	Mediano Plazo	3.6.1 Incluir en el Reglamento Interno de DIRECTV las siguientes responsabilidades de terminación de contrato: - Acuerdos de confidencialidad y no divulgación de información posterior a la finalización del contrato del funcionario. - Si existen cambios en las responsabilidades o contrato laboral del funcionario, se deberá establecer un acuerdo de confidencialidad de la información, atado a las nuevas funciones o contrato. - Transferencia de la documentación e información al nuevo funcionario a cargo. En caso de ausencia de este, el responsable de esta acción deberá ser el Oficial de Seguridad de la Información. - Acuerdos de confidencialidad y no divulgación de información posterior a la finalización de contratos de terceras partes (Proveedores, entre otros). 3.6.2 Documentar, aprobar y difundir la política o procedimiento de seguridad de recursos humanos.	Mayo 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
4. GESTIÓN DE ACTIVOS	4.1 Inventario de activos	a) Los activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.	2	3	Mediano Plazo	4.1.1 Aprobar y difundir la política o procedimiento de gestión de activos.	Mayo 2016
	4.2 Propiedad de los activos	a) Todos los activos que figuran en el inventario deben tener un propietario.	3	4	Mediano Plazo	4.2.1 El Gerente de cada departamento deberá ser el encargado de asignar un responsable, para el monitoreo y control de los activos asignados a cada uno de los funcionarios de dicho departamento.	Mayo 2016
	4.3 Uso aceptable de los activos	a) Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.	3	4	Mediano Plazo	4.3.1 El departamento encargado de la administración de los activos de DIRECTV, deberá definir e implementar métricas a utilizar para la gestión de inventarios (uso de activos).	Mayo 2016
	4.4 Devolución de activos	a) Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.	3	4	Mediano Plazo	4.4.1 Recursos Humanos en conjunto con el departamento encargado de la administración de los activos de DIRECTV, deberán ser los responsables de validar la devolución de todos los activos a cargo de los funcionarios que finalicen los contratos laborales con DIRECTV.	Mayo 2016
	4.5 Clasificación de la información	a) La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.	0	3	Corto Plazo	4.5.1 DIRECTV se encuentra en el proceso de clasificar su información de acuerdo a la importancia de la misma, sensibilidad y criticidad de los datos que se manejan en la Compañía. Este es un proyecto que lo están trabajando en conjunto con la regional de DIRECTV, para poder finalizarlo en los primeros meses del próximo año. 4.5.2 Documentar, aprobar y difundir la política o procedimiento de gestión de activos.	Febrero 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	4.6 Etiquetado de la información	a) Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.	0	3	Largo Plazo	4.6.1 DIRECTV se encuentra en el proceso de etiquetado de la información de la Compañía. 4.6.2 Documentar, aprobar y difundir la política o procedimiento de gestión de activos.	Noviembre 2016
	4.7 Manipulado de la información	a) Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.	0	3	Largo Plazo	4.7.1 DIRECTV se encuentra en la definición y establecimiento de lineamientos y procedimientos específicos para la manipulación de la información de la Compañía. 4.7.2 Documentar, aprobar y difundir la política o procedimiento de gestión de activos.	Noviembre 2016
	4.8 Gestión de soportes extraíbles	a) Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.	0	2	Corto Plazo	4.8.1 Documentar la política o procedimiento de gestión de activos con respecto a la administración y uso de soportes extraíbles.	Febrero 2016
	4.9 Eliminación de soportes	a) Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.	0	2	Corto Plazo	4.9.1 Documentar la política o procedimiento de gestión de activos con respecto a la administración de la correcta eliminación de soportes.	Febrero 2016
	4.10 Soportes físicos en tránsito	a) Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.	2	4	Corto Plazo	4.10.1 Se deberá trabajar en conjunto con el departamento de Recursos Humanos para validar que el proceso de alta de usuarios y entrega de activos se esté cumpliendo. Dentro de los procesos mencionados anteriormente, se establece que las máquinas que se entregan a los funcionarios deben estar cifradas. 4.10.2 Monitorear el proceso de cifrado a los equipos portátiles que son asignados a los funcionarios de DIRECTV. 4.10.3 Aprobar y difundir la política o procedimiento de gestión de	Febrero 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
						activos.	
5. CONTROL DE ACCESO	5.1 Política de control de acceso	a) Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	2	4	Corto Plazo	5.1.1 El departamento de Sistemas deberá ser el encargado de proporcionar los accesos correspondientes, en base a lo enviado por el departamento de Recursos Humanos. 5.1.2 El departamento de Recursos Humanos deberá ser el encargado de notificar al departamento de Sistemas, para que ellos procedan con la eliminación de los accesos de los funcionarios que salieron de la Compañía. 5.1.3 Una vez al mes, se deberá correr un barrido de todas las bajas de usuarios, para validar que los accesos de los funcionarios que salieron de la Compañía se encuentren eliminados. 5.1.4 Aprobar y difundir la política o procedimiento de control de acceso.	Febrero 2016
	5.2 Acceso a las redes y a los servicios de red	a) Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.	2	4	Mediano Plazo	5.2.1 Se deberá definir una metodología de análisis de riesgos, con el objetivo de realizar una evaluación de riesgos y poder identificar los segmentos de red donde se encuentran los activos críticos de la Compañía. Luego de esta definición, se deberá proporcionar el acceso a las redes únicamente a personal autorizado. 5.2.2 Aprobar y difundir la política o procedimiento de control de acceso.	Mayo 2016
	5.3 Registro y baja de usuario	a) Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.	4	5	Mediano Plazo	5.3.1 Ver Plan de Acción 5.1.1. 5.3.2 Ver Plan de Acción 5.1.2. 5.3.3 Ver Plan de Acción 5.1.3.	Mayo 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	5.4 Provisión de acceso de usuario	a) Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.	4	4	Se Mantiene	5.4.1 No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.	No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.
	5.5 Gestión de privilegios de acceso	a) La asignación y el uso de privilegios de acceso debe estar restringida y controlada.	2	3	Largo Plazo	5.5.1 Ver Plan de Acción 5.1.1. 5.5.2 Ver Plan de Acción 5.1.2. 5.5.3 Ver Plan de Acción 5.1.3. 5.5.4 Ver Plan de Acción 5.1.4.	Noviembre 2016
	5.6 Gestión de la información secreta de autenticación de los usuarios	a) La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.	3	4	Mediano Plazo	5.6.1 Ver Plan de Acción 5.1.1.	Mayo 2016
	5.7 Revisión de los derechos de acceso de usuario	a) Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.	1	2	Mediano Plazo	5.7.1 Ver Plan de Acción 5.1.1. 5.7.2 Documentar la política o procedimiento de control de acceso.	Mayo 2016
	5.8 Retirada o reasignación de los derechos de acceso	a) Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.	5	5	Se Mantiene	5.8.1 No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.	No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.
	5.9 Uso de la información secreta de autenticación	a) Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.	3	4	Corto Plazo	5.9.1 Ver Plan de Acción 5.1.1.	Febrero 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	5.10 Restricción del acceso a la información	a) Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.	3	4	Corto Plazo	5.10.1 Ver Plan de Acción 5.1.1.	Febrero 2016
	5.11 Procedimientos seguros de inicio de sesión	a) Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.	3	4	Corto Plazo	5.11.1 La política de control de acceso deberá contener los pasos para el inicio seguro de sesión, o a su vez, se deberá desarrollar un procedimiento para el inicio seguro de sesión a los equipos de DIRECTV.	Febrero 2016
	5.12 Sistema de gestión de contraseñas	a) Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.	3	4	Corto Plazo	5.12.1 La política de control de acceso deberá contener los lineamientos de seguridad como lo exige las buenas prácticas para la gestión de las contraseñas, o a su vez, se deberá desarrollar un procedimiento para establecer contraseñas seguras y robustas en DIRECTV.	Febrero 2016
	5.13 Uso de utilidades con privilegios del sistema	a) Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.	2	4	Largo Plazo	5.13.1 Ver Plan de Acción 5.1.1. 5.13.2 Ver Plan de Acción 5.1.4.	Noviembre 2016
	5.14 Control de acceso al código fuente de los programas	a) Se debe restringir el acceso al código fuente de los programas.	2	4	Mediano Plazo	5.14.1 Ver Plan de Acción 5.1.1. 5.14.2 Ver Plan de Acción 5.1.4.	Mayo 2016
6. CRIPTOGRAFÍA	6.1 Política de uso de los controles criptográficos	a) Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.	5	5	Se Mantiene	6.1.1 No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.	No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	6.2 Gestión de claves	a) Se debe desarrollar e implementar una política de sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.	4	5	Corto Plazo	6.2.1 Se deberá establecer un monitoreo continuo a la gestión de claves para el cifrado de los equipos de DIRECTV.	Febrero 2016
7. SEGURIDAD FISICA Y DEL ENTORNO	7.1 Perímetro de seguridad física	a) Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.	2	3	Mediano Plazo	7.1.1 Aprobar y difundir la política o procedimiento de seguridad física y del entorno.	Mayo 2016
	7.2 Controles físicos de entrada	a) Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.	2	3	Mediano Plazo	7.2.1 Ver Plan de Acción 7.1.1.	Mayo 2016
	7.3 Seguridad de oficinas, despachos y recursos	a) Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.	2	3	Mediano Plazo	7.3.1 Ver Plan de Acción 7.1.1.	Mayo 2016
	7.4 Protección contra las amenazas externas y ambientales	a) Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.	2	3	Mediano Plazo	7.4.1 Ver Plan de Acción 7.1.1.	Mayo 2016
	7.5 El trabajo en áreas seguras	a) Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.	2	3	Largo Plazo	7.5.1 Ver Plan de Acción 7.1.1.	Noviembre 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	7.6 Áreas de carga y descarga	a) Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.	4	5	Mediano Plazo	7.6.1 Se deberá establecer un monitoreo continuo a los puntos de acceso a DIRECTV.	Mayo 2016
	7.7 Emplazamiento y protección de equipos	a) Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.	4	5	Mediano Plazo	7.7.1 Se deberá establecer un monitoreo continuo a todos los accesos de DIRECTV, especialmente a los accesos que correspondan a las áreas donde se encuentra la información sensible de la Compañía.	Mayo 2016
	7.8 Instalaciones de suministro	a) Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.	3	4	Mediano Plazo	7.8.1 Deberá existir un cronograma de revisión a todas las entradas de alimentación eléctrica de la Compañía, para validar que las instalaciones de suministro se encuentren funcionando en óptimas condiciones.	Mayo 2016
	7.9 Seguridad del cableado	a) El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.	3	4	Mediano Plazo	7.9.1 Deberá existir un cronograma de revisión al cableado eléctrico y de telecomunicaciones de la Compañía, para validar que estos medios se encuentren protegidos frente a daños o interferencias.	Mayo 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	7.10 Mantenimiento de los equipos	a) Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.	4	5	Mediano Plazo	7.10.1 Adquirir e instalar una herramienta que permita monitorear el funcionamiento de los principales equipos de DIRECTV.	Mayo 2016
	7.11 Retirada de materiales propiedad de la empresa	a) Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.	4	5	Mediano Plazo	7.11.1 Incrementar el control de salida de equipos en la recepción de la Compañía.	Mayo 2016
	7.12 Seguridad de los equipos fuera de las instalaciones	a) Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.	3	4	Mediano Plazo	7.12.1 Ver Plan de Acción 4.10.1. 7.12.2 Ver Plan de Acción 4.10.2.	Mayo 2016
	7.13 Reutilización o eliminación segura de equipos	a) Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.	2	3	Mediano Plazo	7.13.1 Se deberá definir y establecer un procedimiento para la validación de información crítica de la Compañía o software bajo licencia, antes de proceder con la eliminación del contenido de los equipos. 7.13.2 Ver Plan de Acción 7.1.1.	Mayo 2016
	7.14 Equipo de usuario desatendido	a) Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.	3	4	Mediano Plazo	7.14.1 Deberá existir un cronograma de revisión a todos los equipos desatendidos de DIRECTV, para validar que dichos equipos se encuentren protegidos y no contengan información sensible de la Compañía.	Mayo 2016
	7.15 Política de puesto de trabajo despejado y pantalla limpia	a) Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la	3	4	Mediano Plazo	7.15.1 Deberá existir un cronograma de revisión a todos los puestos de trabajo de cada uno de los funcionarios de DIRECTV, con el objetivo de validar que los puestos de trabajo se encuentren despejados de papeles y medios de almacenamiento desmontables.	Mayo 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
		información.					
8. SEGURIDAD DE LAS OPERACIONES	8.1 Documentación de procedimientos de operación	a) Deben documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.	2	3	Largo Plazo	8.1.1 Aprobar y difundir la política o procedimiento de garantizar, mantener y restablecer las operaciones de la Compañía.	Noviembre 2016
	8.2 Gestión de cambios	a) Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de información deben ser controlados.	5	5	Se Mantiene	8.2.1 No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.	No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.
	8.3 Gestión de capacidades	a) Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	0	4	Largo Plazo	8.3.1 Desarrollar, documentar, aprobar y difundir la política o procedimiento de monitoreo de recursos de los servicios y sistemas informáticos. 8.3.2 En la política de monitoreo de recursos de los servicios y sistemas informáticos, definir y establecer las proyecciones de los requisitos futuros de capacidad, con el objetivo de garantizar los rendimientos requeridos de los sistemas informáticos de DIRECTV.	Noviembre 2016
	8.4 Separación de los recursos de desarrollo, prueba y operación	a) Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.	3	4	Mediano Plazo	8.4.1 Deberá existir un cronograma de revisión a los principales servidores de DIRECTV, con el objetivo de validar que los ambientes de desarrollo, pruebas y operación se encuentren debidamente separados, evitando el acceso no autorizado a los ambientes de producción de la Compañía.	Mayo 2016
	8.5 Controles contra el código malicioso	a) Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.	4	5	Mediano Plazo	8.5.1 Se deberá implementar un monitoreo constante para evitar que código malicioso infecte los equipos de DIRECTV. 8.5.2 Ver Plan de Acción 1.1.3.	Mayo 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	8.6 Copias de seguridad de la información	a) Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.	3	4	Mediano Plazo	8.6.2 Definir y establecer una fecha programada (mínimo una vez al año) para realizar pruebas de legibilidad de los respaldos de información de DIRECTV. 8.6.1 Ver Plan de Acción 8.1.1.	Mayo 2016
	8.7 Registro de eventos	a) Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.	0	3	Mediano Plazo	8.7.1 Documentar, aprobar y difundir la política o procedimiento de gestión de incidentes de seguridad.	Mayo 2016
	8.8 Protección de la información de registro	a) Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.	0	3	Mediano Plazo	8.8.1 Desarrollar, aprobar y difundir la política o procedimiento de control de acceso.	Mayo 2016
	8.9 Registros de administración y operación	a) Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.	2	3	Mediano Plazo	8.9.1 Aprobar y difundir la política o procedimiento de protección y revisión de las pistas de auditoría.	Mayo 2016
	8.10 Sincronización del reloj	a) Los relojes de todos los sistemas de tratamiento de información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente precisa y acordada de tiempo.	2	3	Mediano Plazo	8.10.1 Definir y establecer que todos los servidores principales de DIRECTV se encuentren sincronizados a un servidor central.	Mayo 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	8.11 Instalación del software en uso	a) Se deben implementar procedimientos para controlar la instalación del software en uso.	2	3	Mediano Plazo	8.11.1 Aprobar y difundir la política o procedimiento de adquisición, cambio y mantenimiento del software de sistemas.	Mayo 2016
	8.12 Gestión de las vulnerabilidades técnicas	a) Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.	5	5	Se Mantiene	8.12.1 No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.	No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.
	8.13 Restricción en la instalación de software	a) Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.	2	3	Mediano Plazo	8.13.1 Ver Plan de Acción 8.11.1.	Mayo 2016
	8.14 Controles de auditoría de sistemas de información	a) Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.	2	3	Mediano Plazo	8.14.1 Ver Plan de Acción 8.9.1.	Mayo 2016
9. SEGURIDAD DE LAS COMUNICACIONES	9.1 Controles de red	a) Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.	2	3	Mediano Plazo	9.1.1 Aprobar y difundir la política o procedimiento de administración de seguridades de la red.	Mayo 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	9.2 Seguridad de los servicios de red	a) Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.	2	3	Mediano Plazo	9.2.1 Ver Plan de Acción 9.1.1.	Mayo 2016
	9.3 Segregación en redes	a) Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.	2	3	Mediano Plazo	9.3.1 Ver Plan de Acción 9.1.1.	Mayo 2016
	9.4 Políticas y procedimientos de intercambio de información	a) Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.	2	3	Mediano Plazo	9.4.1 Aprobar y difundir la política de seguridad de la información en DIRECTV.	Mayo 2016
	9.5 Acuerdos de intercambio de información	a) Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.	2	3	Mediano Plazo	9.5.1 Ver Plan de Acción 9.4.1.	Mayo 2016
	9.6 Mensajería electrónica	a) La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.	2	3	Mediano Plazo	9.6.1 Ver Plan de Acción 9.4.1.	Mayo 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	9.7 Acuerdos de confidencialidad o no revelación	a) Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación.	2	3	Mediano Plazo	9.7.1 Ver Plan de Acción 9.4.1.	Mayo 2016
10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	10.1 Análisis de requisitos y especificaciones de seguridad de la información	a) Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.	1	3	Mediano Plazo	10.1.1 Documentar, aprobar y difundir la política o procedimiento de gestión de cambios a los sistemas de información.	Mayo 2016
	10.2 Asegurar los servicios de aplicaciones en redes públicas	a) La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizada.	2	3	Mediano Plazo	10.2.1 Ver Plan de Acción 9.1.1.	Mayo 2016
	10.3 Protección de las transacciones de servicios de aplicaciones	a) La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizado.	2	3	Mediano Plazo	10.3.1 Ver Plan de Acción 9.1.1.	Mayo 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	10.4 Política de desarrollo seguro	a) Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.	2	3	Mediano Plazo	10.4.1 Aprobar y difundir la política o procedimiento de desarrollo seguro.	Mayo 2016
	10.5 Procedimiento de control de cambios en sistemas	a) La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios.	4	4	Se Mantiene	10.5.1 No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.	No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.
	10.6 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	a) Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.	1	3	Mediano Plazo	10.3.1 Ver Plan de Acción 8.11.1.	Mayo 2016
	10.7 Restricciones a los cambios en los paquetes de software	a) Se deben restringir las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.	4	4	Se Mantiene	10.7.1 No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.	No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.
	10.8 Principios de ingeniería de sistemas seguros	a) Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.	2	3	Mediano Plazo	10.8.1 Ver Plan de Acción 10.4.1.	Mayo 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	10.9 Entorno de desarrollo seguro	a) Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.	0	3	Mediano Plazo	10.9.1 Documentar, aprobar y difundir la política o procedimiento de desarrollo seguro.	Mayo 2016
	10.10 Externalización del desarrollo de software	a) El desarrollo de software realizado por empresas externas debe ser supervisado y controlado por la organización.	2	3	Mediano Plazo	10.10.1 Ver Plan de Acción 10.4.1.	Mayo 2016
	10.11 Pruebas funcionales de seguridad de sistemas	a) Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.	2	3	Mediano Plazo	10.11.1 Ver Plan de Acción 10.4.1.	Mayo 2016
	10.12 Pruebas de aceptación de sistemas	a) Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.	2	3	Mediano Plazo	10.12.1 Ver Plan de Acción 10.4.1.	Mayo 2016
	10.13 Protección de los datos de prueba	a) Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.	2	3	Mediano Plazo	10.13.1 Ver Plan de Acción 10.4.1.	Mayo 2016
11. RELACIÓN CON PROVEEDORES	11.1 Política de seguridad de la información en las relaciones con los proveedores	a) Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben acordarse con el proveedor y quedar documentados.	2	3	Mediano Plazo	11.1.1 Aprobar y difundir la política de seguridad de la información en DIRECTV. Esta política contendrá una sección que describa todas las actividades a realizarse con respecto a la gestión con los proveedores externos de DIRECTV.	Mayo 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	11.2 Requisitos de seguridad en contratos con terceros	a) Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura IT.	2	3	Mediano Plazo	11.2.1 Ver Plan de Acción 11.1.1.	Mayo 2016
	11.3 Cadena de suministro de tecnología de la información y de las comunicaciones	a) Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.	2	3	Mediano Plazo	11.3.1 Ver Plan de Acción 11.1.1.	Mayo 2016
	11.4 Control y revisión de la provisión de servicios del proveedor	a) Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor.	2	3	Mediano Plazo	11.4.1 Ver Plan de Acción 11.1.1.	Mayo 2016
	11.5 Gestión de cambios en la provisión del servicio del proveedor	a) Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los	2	3	Mediano Plazo	11.5.1 Ver Plan de Acción 11.1.1.	Mayo 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
		riesgos.					
12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	12.1 Responsabilidades y procedimientos	a) Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.	5	5	Se Mantiene	12.1.1 No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.	No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.
	12.2 Notificación de los eventos de seguridad de la información	a) Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.	5	5	Se Mantiene	12.2.1 No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.	No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.
	12.3 Notificación de puntos débiles de la seguridad	a) Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.	3	4	Mediano Plazo	12.3.1 Establecer y ejecutar diferentes charlas respecto a la sensibilización por parte de los usuarios en temas relacionados con la seguridad de la información. En estas charlas se deberá dar énfasis en la participación de empleados, contratistas, proveedores, con respecto a la notificación de puntos débiles en la seguridad de la información de DIRECTV.	Mayo 2016
	12.4 Evaluación y decisión sobre los eventos de seguridad de Información	a) Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.	5	5	Se Mantiene	12.4.1 No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.	No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.
	12.5 Respuesta a incidentes de seguridad de la información	a) Los incidentes de seguridad de la información deben contar con una respuesta de acuerdo con los procedimientos documentados.	5	5	Se Mantiene	12.5.1 No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.	No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	12.6 Aprendizaje de los incidentes de seguridad de la información	a) El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.	1	3	Mediano Plazo	12.6.1 Documentar, aprobar y difundir la política de seguridad de la información en DIRECTV.	Mayo 2016
	12.7 Recopilación de evidencias	a) La organización debe definir y aplicar procedimientos para la identificación, recopilación, adquisición y preservación de información que puede servir de evidencia.	1	3	Mediano Plazo	12.7.1 Ver Plan de Acción 12.6.1.	Mayo 2016
13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	13.1 Planificación de la continuidad de la seguridad de la información	a) La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	3	4	Largo Plazo	13.1.1 Se deberá definir un cronograma de pruebas para validar que la seguridad de la información se encuentra contemplada dentro del plan de continuidad de DIRECTV.	Noviembre 2016
	13.2 Implementar la continuidad de la seguridad de la información	a) La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.	2	3	Largo Plazo	13.2.1 Aprobar y difundir procesos, procedimientos y controles sobre la continuidad de la seguridad de la información en DIRECTV durante situaciones adversas.	Noviembre 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	13.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	a) La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.	0	3	Largo Plazo	13.3.1 Documentar, aprobar y difundir procesos, procedimientos y controles sobre la continuidad de la seguridad de la información en DIRECTV durante situaciones adversas. Se deberá especificar en una sección, los planes definidos para comprobar los controles establecidos de acuerdo a las pruebas de continuidad de la seguridad de la información en DIRECTV.	Noviembre 2016
	13.4 Disponibilidad de los recursos de tratamiento de la información	a) Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.	5	5	Se Mantiene	13.4.1 No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.	No se definirá planes de acción puesto que su nivel de madurez futuro es igual al actual.
14. CUMPLIMIENTO	14.1 Identificación de la legislación aplicable y de los requisitos contractuales	a) Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deben definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.	3	4	Mediano Plazo	14.1.1 Definir y establecer pruebas aleatorias de revisión, con respecto a los requisitos legales y contractuales de los empleados de DIRECTV.	Mayo 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	14.2 Derechos de propiedad intelectual (DPI)	a) Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	3	4	Mediano Plazo	14.2.1 Definir y establecer pruebas aleatorias de revisión para validar la existencia de procedimientos adecuados, con el objetivo de garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, en relación a que pueda existir derechos de propiedad intelectual sobre ellos.	Mayo 2016
	14.3 Protección de los registros de la organización	a) Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.	3	4	Mediano Plazo	14.3.1 Definir y establecer pruebas aleatorias de revisión para validar la correcta protección de los registros de DIRECTV, contra la pérdida, destrucción, falsificación, revelación o accesos no autorizados, de acuerdo con los requisitos legales, regulatorios y contractuales de DIRECTV.	Mayo 2016
	14.4 Protección y privacidad de la información de carácter personal	a) Se debe garantizar la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.	3	4	Mediano Plazo	14.4.1 Definir y establecer pruebas aleatorias de revisión para validar la existencia de procedimientos adecuados, con el objetivo de garantizar la protección y la privacidad de la información, de acuerdo con los requisitos legales, regulatorios y contractuales de DIRECTV.	Mayo 2016
	14.5 Regulación de los controles criptográficos	a) Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.	3	4	Mediano Plazo	14.5.1 Definir y establecer pruebas aleatorias de revisión para validar la existencia de controles criptográficos, de acuerdo con los requisitos legales, regulatorios y contractuales de DIRECTV.	Mayo 2016

Dominio del Control	Subdominio	Directriz	Nivel actual	Nivel Futuro	Categorización Nivel Futuro	Planes de Acción	Fecha máxima de implementación
	14.6 Revisión independiente de la seguridad de la información	a) El enfoque de la organización para la gestión de seguridad de la información y su implantación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.	2	3	Mediano Plazo	14.6.1 Aprobar y difundir la política de seguridad de la información en DIRECTV.	Mayo 2016
	14.7 Cumplimiento de las políticas y normas de seguridad	a) Los directivos deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable.	0	2	Mediano Plazo	14.7.1 Documentar, aprobar y difundir la política de seguridad de la información en DIRECTV.	Mayo 2016
	14.8 Comprobación del cumplimiento técnico	a) Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.	4	5	Mediano Plazo	14.8.1 Definir y establecer pruebas aleatorias de revisión para validar que los sistemas de información están cumpliendo las políticas y normas de seguridad de la información de DIRECTV.	Mayo 2016

Anexo 5. Hoja de Ruta de Implementación

INICIATIVAS

#	Iniciativas
1	Definición, formalización y aprobación del marco normativo de seguridad de la información (políticas, procedimientos, reglamentos, manuales, etc).
2	Implantación de controles.
3	Aplicación de enfoques de mejora continua.
4	Sensibilización del personal.

ESCALAS

Brecha	No. de saltos para alcanzar Nivel Futuro
Alta	De 4 a 5
Media	De 2 a 3
Baja	1

Nivel de esfuerzo

Se trata del nivel de esfuerzo involucrado para llevar adelante los planes de acción. Se medirá con base en 3 elementos claves:

Nivel de esfuerzo				
Criterio	*Bajo*	*Medio*	*Alto*	
Tiempo	De 1 a 3 meses	De 4 a 6 meses	Mayor a 6 meses	
Personas	1-2 personas / áreas	3-6 personas / áreas	Más de 6 personas / áreas	
Costo	Hasta $20K	De $20K a $50K	Más de $50K	Sólo esfuerzo interno

Iniciativa 1 - Planes de Acción

INICIATIVA 1						
Definición, formalización y aprobación del marco normativo de seguridad de la información (políticas, procedimientos, reglamentos, manuales, etc).						
Subdominio	**Planes de Acción:**	**Plazo**	**Brecha**	**Esfuerzo**		
				Tiempo	**Personas**	**Costo**
1.1 Políticas para la seguridad de la información	1.1.1 Realizar un estudio del conjunto de políticas de seguridad de la información que ya se encuentran documentadas, para proceder con la aprobación y difusión de las mismas a todo el personal de DIRECTV. 1.1.2 Desarrollar las políticas o procedimientos que no se encuentren consideradas dentro del conjunto de políticas de seguridad de la información que ya fueron definidas por DIRECTV.	Largo Plazo	Media	Alto	Medio	Medio
2.3 Contacto con las autoridades	2.3.2 Documentar, aprobar y difundir la política de seguridad de la información en DIRECTV. Esta política contendrá una sección sobre todas las actividades relacionadas con los contactos con las autoridades pertinentes, ya sean internas o externas.	Mediano Plazo	Media	Medio	Bajo	SEI
2.4 Contacto con grupo de interés especial	2.4.2 Documentar, aprobar y difundir la política de seguridad de la información en DIRECTV. Esta política contendrá una sección sobre todas las actividades relacionadas con los contactos de grupos especializados en seguridad de la información.	Mediano Plazo	Media	Medio	Bajo	SEI
2.6 Política de dispositivos móviles	2.6.1 Documentar, aprobar y difundir la política o procedimiento de dispositivos móviles.	Largo Plazo	Media	Alto	Bajo	SEI
2.7 Teletrabajo	2.7.1 Documentar, aprobar y difundir la política o procedimiento de teletrabajo.	Largo Plazo	Media	Alto	Bajo	SEI
3.1 Investigación de antecedentes	3.1.1 Documentar, aprobar y difundir la política o procedimiento de seguridad de recursos humanos.	Mediano Plazo	Media	Medio	Bajo	SEI
3.2 Términos y condiciones del empleo	3.2.1 Documentar, aprobar y difundir la política o procedimiento de seguridad de recursos humanos.	Mediano Plazo	Media	Medio	Bajo	SEI
3.3 Responsabilidades de gestión	3.3.2 Documentar, aprobar y difundir la política o procedimiento de seguridad de recursos humanos.	Mediano Plazo	Media	Medio	Bajo	SEI
3.4 Concienciación, educación y capacitación en seguridad de la información	3.4.2 Documentar, aprobar y difundir la política o procedimiento de seguridad de recursos humanos.	Mediano Plazo	Media	Medio	Bajo	SEI

INICIATIVA 1						
Definición, formalización y aprobación del marco normativo de seguridad de la información (políticas, procedimientos, reglamentos, manuales, etc).						
Subdominio	**Planes de Acción:**	**Plazo**	**Brecha**	**Esfuerzo**		
				Tiempo	**Personas**	**Costo**
3.5 Proceso disciplinario	3.5.2 Documentar la política o procedimiento de seguridad de recursos humanos.	Mediano Plazo	Media	Medio	Bajo	SEI
3.6 Responsabilidades ante la finalización o cambio	3.6.2 Documentar, aprobar y difundir la política o procedimiento de seguridad de recursos humanos.	Mediano Plazo	Media	Medio	Bajo	SEI
4.1 Inventario de activos	4.1.1 Aprobar y difundir la política o procedimiento de gestión de activos.	Mediano Plazo	Baja	Medio	Bajo	SEI
4.5 Clasificación de la información	4.5.2 Documentar, aprobar y difundir la política o procedimiento de gestión de activos.	Corto Plazo	Media	Bajo	Bajo	SEI
4.6 Etiquetado de la información	4.6.2 Documentar, aprobar y difundir la política o procedimiento de gestión de activos.	Largo Plazo	Media	Alto	Bajo	SEI
4.7 Manipulado de la información	4.7.2 Documentar, aprobar y difundir la política o procedimiento de gestión de activos.	Largo Plazo	Media	Alto	Bajo	SEI
4.8 Gestión de soportes extraíbles	4.8.1 Documentar la política o procedimiento de gestión de activos con respecto a la administración y uso de soportes extraíbles.	Corto Plazo	Media	Bajo	Bajo	SEI
4.9 Eliminación de soportes	4.9.1 Documentar la política o procedimiento de gestión de activos con respecto a la administración de la correcta eliminación de soportes.	Corto Plazo	Media	Bajo	Bajo	SEI
4.10 Soportes físicos en tránsito	4.10.3 Aprobar y difundir la política o procedimiento de gestión de activos.	Corto Plazo	Media	Bajo	Bajo	SEI
5.1 Política de control de acceso	5.1.4 Aprobar y difundir la política o procedimiento de control de acceso.	Corto Plazo	Media	Bajo	Bajo	SEI
5.2 Acceso a las redes y a los servicios de red	5.2.2 Aprobar y difundir la política o procedimiento de control de acceso.	Mediano Plazo	Media	Medio	Bajo	SEI
5.5 Gestión de privilegios de acceso	5.5.4 Ver Plan de Acción 5.1.4.	Largo Plazo	Baja	Alto	Bajo	SEI
5.7 Revisión de los derechos de acceso de usuario	5.7.2 Documentar la política o procedimiento de control de acceso.	Mediano Plazo	Baja	Medio	Bajo	SEI

INICIATIVA 1						
Definición, formalización y aprobación del marco normativo de seguridad de la información (políticas, procedimientos, reglamentos, manuales, etc).						
Subdominio	**Planes de Acción:**	**Plazo**	**Brecha**	**Esfuerzo**		
				Tiempo	**Personas**	**Costo**
5.11 Procedimientos seguros de inicio de sesión	5.11.1 La política de control de acceso deberá contener los pasos para el inicio seguro de sesión, o a su vez, se deberá desarrollar un procedimiento para el inicio seguro de sesión a los equipos de DIRECTV.	Corto Plazo	Baja	Bajo	Bajo	SEI
5.12 Sistema de gestión de contraseñas	5.12.1 La política de control de acceso deberá contener los lineamientos de seguridad como lo exige las buenas prácticas para la gestión de las contraseñas, o a su vez, se deberá desarrollar un procedimiento para establecer contraseñas seguras y robustas en DIRECTV.	Corto Plazo	Baja	Bajo	Bajo	SEI
5.13 Uso de utilidades con privilegios del sistema	5.13.2 Ver Plan de Acción 5.1.4.	Largo Plazo	Media	Alto	Bajo	SEI
5.14 Control de acceso al código fuente de los programas	5.14.2 Ver Plan de Acción 5.1.4.	Mediano Plazo	Media	Medio	Bajo	SEI
7.1 Perímetro de seguridad física	7.1.1 Aprobar y difundir la política o procedimiento de seguridad física y del entorno.	Mediano Plazo	Baja	Medio	Bajo	SEI
7.2 Controles físicos de entrada	7.2.1 Ver Plan de Acción 7.1.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
7.3 Seguridad de oficinas, despachos y recursos	7.3.1 Ver Plan de Acción 7.1.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
7.4 Protección contra las amenazas externas y ambientales	7.4.1 Ver Plan de Acción 7.1.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
7.5 El trabajo en áreas seguras	7.5.1 Ver Plan de Acción 7.1.1.	Largo Plazo	Baja	Alto	Bajo	SEI
7.13 Reutilización o eliminación segura de equipos	7.13.2 Ver Plan de Acción 7.1.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
8.1 Documentación de procedimientos de operación	8.1.1 Aprobar y difundir la política o procedimiento de garantizar, mantener y restablecer las operaciones de la Compañía.	Largo Plazo	Baja	Alto	Bajo	SEI

INICIATIVA 1						
Definición, formalización y aprobación del marco normativo de seguridad de la información (políticas, procedimientos, reglamentos, manuales, etc).						
Subdominio	**Planes de Acción:**	**Plazo**	**Brecha**	**Esfuerzo**		
				Tiempo	**Personas**	**Costo**
8.3 Gestión de capacidades	8.3.1 Desarrollar, documentar, aprobar y difundir la política o procedimiento de monitoreo de recursos de los servicios y sistemas informáticos.	Largo Plazo	Alta	Alto	Bajo	SEI
8.6 Copias de seguridad de la información	8.6.1 Ver Plan de Acción 8.1.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
8.7 Registro de eventos	8.7.1 Documentar, aprobar y difundir la política o procedimiento de gestión de incidentes de seguridad.	Mediano Plazo	Media	Medio	Bajo	SEI
8.8 Protección de la información de registro	8.8.1 Desarrollar, aprobar y difundir la política o procedimiento de control de acceso.	Mediano Plazo	Media	Medio	Bajo	SEI
8.9 Registros de administración y operación	8.9.1 Aprobar y difundir la política o procedimiento de protección y revisión de las pistas de auditoría.	Mediano Plazo	Baja	Medio	Bajo	SEI
8.11 Instalación del software en uso	8.11.1 Aprobar y difundir la política o procedimiento de adquisición, cambio y mantenimiento del software de sistemas.	Mediano Plazo	Baja	Medio	Bajo	SEI
8.13 Restricción en la instalación de software	8.13.1 Ver Plan de Acción 8.11.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
8.14 Controles de auditoría de sistemas de información	8.14.1 Ver Plan de Acción 8.9.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
9.1 Controles de red	9.1.1 Aprobar y difundir la política o procedimiento de administración de seguridades de la red.	Mediano Plazo	Baja	Medio	Bajo	SEI
9.2 Seguridad de los servicios de red	9.2.1 Ver Plan de Acción 9.1.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
9.3 Segregación en redes	9.3.1 Ver Plan de Acción 9.1.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
9.4 Políticas y procedimientos de intercambio de	9.4.1 Aprobar y difundir la política de seguridad de la información en DIRECTV.	Mediano Plazo	Baja	Medio	Bajo	SEI

INICIATIVA 1						
Definición, formalización y aprobación del marco normativo de seguridad de la información (políticas, procedimientos, reglamentos, manuales, etc).						
Subdominio	**Planes de Acción:**	**Plazo**	**Brecha**	**Esfuerzo**		
				Tiempo	**Personas**	**Costo**
información						
9.5 Acuerdos de intercambio de información	9.5.1 Ver Plan de Acción 9.4.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
9.6 Mensajería electrónica	9.6.1 Ver Plan de Acción 9.4.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
9.7 Acuerdos de confidencialidad o no revelación	9.7.1 Ver Plan de Acción 9.4.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
10.1 Análisis de requisitos y especificaciones de seguridad de la información	10.1.1 Documentar, aprobar y difundir la política o procedimiento de gestión de cambios a los sistemas de información.	Mediano Plazo	Media	Medio	Bajo	SEI
10.2 Asegurar los servicios de aplicaciones en redes públicas	10.2.1 Ver Plan de Acción 9.1.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
10.3 Protección de las transacciones de servicios de aplicaciones	10.3.1 Ver Plan de Acción 9.1.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
10.4 Política de desarrollo seguro	10.4.1 Aprobar y difundir la política o procedimiento de desarrollo seguro.	Mediano Plazo	Baja	Medio	Bajo	SEI
10.8 Principios de ingeniería de sistemas seguros	10.8.1 Ver Plan de Acción 10.4.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
10.9 Entorno de desarrollo seguro	10.9.1 Documentar, aprobar y difundir la política o procedimiento de desarrollo seguro.	Mediano Plazo	Media	Medio	Bajo	SEI
10.10 Externalización del desarrollo de	10.10.1 Ver Plan de Acción 10.4.1.	Mediano Plazo	Baja	Medio	Bajo	SEI

INICIATIVA 1						
Definición, formalización y aprobación del marco normativo de seguridad de la información (políticas, procedimientos, reglamentos, manuales, etc).						
Subdominio	**Planes de Acción:**	**Plazo**	**Brecha**	**Esfuerzo**		
				Tiempo	**Personas**	**Costo**
software						
10.11 Pruebas funcionales de seguridad de sistemas	10.11.1 Ver Plan de Acción 10.4.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
10.12 Pruebas de aceptación de sistemas	10.12.1 Ver Plan de Acción 10.4.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
10.13 Protección de los datos de prueba	10.13.1 Ver Plan de Acción 10.4.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
11.1 Política de seguridad de la información en las relaciones con los proveedores	11.1.1 Aprobar y difundir la política de seguridad de la información en DIRECTV. Esta política contendrá una sección que describa todas las actividades a realizarse con respecto a la gestión con los proveedores externos de DIRECTV.	Mediano Plazo	Baja	Medio	Bajo	SEI
11.2 Requisitos de seguridad en contratos con terceros	11.2.1 Ver Plan de Acción 11.1.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
11.3 Cadena de suministro de tecnología de la información y de las comunicaciones	11.3.1 Ver Plan de Acción 11.1.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
11.4 Control y revisión de la provisión de servicios del proveedor	11.4.1 Ver Plan de Acción 11.1.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
11.5 Gestión de cambios en la provisión del servicio	11.5.1 Ver Plan de Acción 11.1.1.	Mediano Plazo	Baja	Medio	Bajo	SEI

INICIATIVA 1						
Definición, formalización y aprobación del marco normativo de seguridad de la información (políticas, procedimientos, reglamentos, manuales, etc).						
Subdominio	**Planes de Acción:**	**Plazo**	**Brecha**	**Esfuerzo**		
				Tiempo	**Personas**	**Costo**
del proveedor						
12.6 Aprendizaje de los incidentes de seguridad de la información	12.6.1 Documentar, aprobar y difundir la política de seguridad de la información en DIRECTV.	Mediano Plazo	Media	Medio	Bajo	SEI
12.7 Recopilación de evidencias	12.7.1 Ver Plan de Acción 12.6.1.	Mediano Plazo	Media	Medio	Bajo	SEI
13.2 Implementar la continuidad de la seguridad de la información	13.2.1 Aprobar y difundir procesos, procedimientos y controles sobre la continuidad de la seguridad de la información en DIRECTV durante situaciones adversas.	Largo Plazo	Baja	Alto	Bajo	SEI
13.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	13.3.1 Documentar, aprobar y difundir procesos, procedimientos y controles sobre la continuidad de la seguridad de la información en DIRECTV durante situaciones adversas. Se deberá especificar en una sección, los planes definidos para comprobar los controles establecidos de acuerdo a las pruebas de continuidad de la seguridad de la información en DIRECTV.	Largo Plazo	Media	Alto	Bajo	SEI
14.6 Revisión independiente de la seguridad de la información	14.6.1 Aprobar y difundir la política de seguridad de la información en DIRECTV.	Mediano Plazo	Baja	Medio	Bajo	SEI
14.7 Cumplimiento de las políticas y normas de seguridad	14.7.1 Documentar, aprobar y difundir la política de seguridad de la información en DIRECTV.	Mediano Plazo	Media	Medio	Bajo	SEI

Saltos Nivel Futuro					***Esfuerzo***
Alta	1	12	0	0	Alto
Media	29	50	1	1	Medio
Baja	39	7	68	0	Bajo
				68	Sólo esfuerzo

Corto Plazo	7	interno
Mediano Plazo	50	
Largo Plazo	12	

Iniciativa 2 - Planes de Acción

INICIATIVA 2						
Implantación de controles.						
Subdominio	**Planes de Acción:**	**Plazo**	**Brecha**	**Esfuerzo**		
				Tiempo	**Personas**	**Costo**
1.1 Políticas para la seguridad de la información	1.1.3 Establecer y ejecutar un plan para la comunicación y sensibilización de las políticas de seguridad de la información a todo el personal de DIRECTV.	Largo Plazo	Media	Alto	Alto	SEI
1.2 Revisión de las políticas para la seguridad de la información	1.2.1 Establecer intervalos de tiempo para la revisión del conjunto de políticas de seguridad de la información en DIRECTV. En caso que existan cambios significativos en la Compañía, esto deberá verse reflejado en la actualización de las políticas y procedimientos de seguridad de la información de DIRECTV.	Mediano Plazo	Media	Medio	Alto	SEI
2.3 Contacto con las autoridades	2.3.1 Establecer un registro de datos de los contactos de las autoridades pertinentes, ya sean internas o externas. Para el caso de proveedores externos, el registro deberá contener entre otros datos: nombre del contacto, empresa a la pertenece, servicio que presta a DIRECTV, dirección, teléfono y extensión, número de celular, correo electrónico y horarios de atención.	Mediano Plazo	Media	Medio	Bajo	SEI
2.4 Contacto con grupo de interés especial	2.4.1 Establecer un registro de datos de los contactos de foros, grupos y asociaciones profesionales especializadas en seguridad de la información. Este registro deberá contener entre otros datos: nombre del contacto, foro o asociación a la pertenece, dirección, teléfono y extensión, número de celular y correo electrónico.	Mediano Plazo	Media	Medio	Bajo	SEI
2.5 Seguridad de la información en la gestión de proyectos	2.5.1 En la herramienta de control de cambios de DIRECTV, se deberá incluir las consideraciones de seguridad de la información que se deben definir al inicio de cada uno de los proyectos de la Compañía. Esto ayudará a tener un control y monitoreo sobre la inclusión de medidas de seguridad a la gestión de proyectos de DIRECTV.	Corto Plazo	Baja	Bajo	Bajo	SEI
3.5 Proceso disciplinario	3.5.1 Recursos Humanos, con apoyo del Área Jurídica de DIRECTV deberá actualizar el Reglamento Interno, incluyendo temas relacionados con el proceso disciplinario referente a brechas e incidentes de seguridad de la información.	Mediano Plazo	Media	Medio	Medio	SEI

INICIATIVA 2						
Implantación de controles.						
Subdominio	**Planes de Acción:**	**Plazo**	**Brecha**	**Esfuerzo**		
				Tiempo	**Personas**	**Costo**
3.6 Responsabilidades ante la finalización o cambio	3.6.1 Incluir en el Reglamento Interno de DIRECTV las siguientes responsabilidades de terminación de contrato: - Acuerdos de confidencialidad y no divulgación de información posterior a la finalización del contrato del funcionario. - Si existen cambios en las responsabilidades o contrato laboral del funcionario, se deberá establecer un acuerdo de confidencialidad de la información, atado a las nuevas funciones o contrato. - Transferencia de la documentación e información al nuevo funcionario a cargo. En caso de ausencia de este, el responsable de esta acción deberá ser el Oficial de Seguridad de la Información. - Acuerdos de confidencialidad y no divulgación de información posterior a la finalización de contratos de terceras partes (Proveedores, entre otros).	Mediano Plazo	Media	Medio	Bajo	SEI
4.5 Clasificación de la información	4.5.1 DIRECTV se encuentra en el proceso de clasificar su información de acuerdo a la importancia de la misma, sensibilidad y criticidad de los datos que se manejan en la Compañía. Este es un proyecto que lo están trabajando en conjunto con la regional de DIRECTV, para poder finalizarlo en los primeros meses del próximo año.	Corto Plazo	Media	Bajo	Alto	SEI
4.6 Etiquetado de la información	4.6.1 DIRECTV se encuentra en el proceso de etiquetado de la información de la Compañía.	Largo Plazo	Media	Alto	Medio	Bajo
4.7 Manipulado de la información	4.7.1 DIRECTV se encuentra en la definición y establecimiento de lineamientos y procedimientos específicos para la manipulación de la información de la Compañía.	Largo Plazo	Media	Alto	Medio	SEI
4.10 Soportes físicos en tránsito	4.10.1 Se deberá trabajar en conjunto con el departamento de Recursos Humanos para validar que el proceso de alta de usuarios y entrega de activos se esté cumpliendo. Dentro de los procesos mencionados anteriormente, se establece que las máquinas que se entregan a los funcionarios deben estar cifradas.	Corto Plazo	Media	Bajo	Bajo	SEI
5.1 Política de control de acceso	5.1.1 El departamento de Sistemas deberá ser el encargado de proporcionar los accesos correspondientes, en base a lo enviado por el departamento de Recursos Humanos. 5.1.2 El departamento de Recursos Humanos deberá ser el encargado de notificar al departamento de Sistemas, para que ellos procedan con la eliminación de los accesos de los funcionarios que salieron de la Compañía.	Corto Plazo	Media	Bajo	Bajo	SEI

INICIATIVA 2						
Implantación de controles.						
Subdominio	**Planes de Acción:**	**Plazo**	**Brecha**	**Esfuerzo**		
				Tiempo	**Personas**	**Costo**
5.2 Acceso a las redes y a los servicios de red	5.2.1 Se deberá definir una metodología de análisis de riesgos, con el objetivo de realizar una evaluación de riesgos y poder identificar los segmentos de red donde se encuentran los activos críticos de la Compañía. Luego de esta definición, se deberá proporcionar el acceso a las redes únicamente a personal autorizado.	Mediano Plazo	Media	Medio	Medio	Bajo
5.3 Registro y baja de usuario	5.3.1 Ver Plan de Acción 5.1.1. 5.3.2 Ver Plan de Acción 5.1.2.	Mediano Plazo	Baja	Medio	Medio	Bajo
5.5 Gestión de privilegios de acceso	5.5.1 Ver Plan de Acción 5.1.1. 5.5.2 Ver Plan de Acción 5.1.2.	Largo Plazo	Baja	Alto	Medio	Bajo
5.6 Gestión de la información secreta de autenticación de los usuarios	5.6.1 Ver Plan de Acción 5.1.1.	Mediano Plazo	Baja	Medio	Medio	Bajo
5.7 Revisión de los derechos de acceso de usuario	5.7.1 Ver Plan de Acción 5.1.1.	Mediano Plazo	Baja	Medio	Medio	Bajo
5.9 Uso de la información secreta de autenticación	5.9.1 Ver Plan de Acción 5.1.1.	Corto Plazo	Baja	Bajo	Medio	Bajo
5.10 Restricción del acceso a la información	5.10.1 Ver Plan de Acción 5.1.1.	Corto Plazo	Baja	Bajo	Medio	Bajo
5.11 Procedimientos seguros de inicio de sesión	5.11.1 La política de control de acceso deberá contener los pasos para el inicio seguro de sesión, o a su vez, se deberá desarrollar un procedimiento para el inicio seguro de sesión a los equipos de DIRECTV.	Corto Plazo	Baja	Bajo	Bajo	SEI
5.12 Sistema de gestión de contraseñas	5.12.1 La política de control de acceso deberá contener los lineamientos de seguridad como lo exige las buenas prácticas para la gestión de las contraseñas, o a su vez, se deberá desarrollar un procedimiento para establecer contraseñas seguras y robustas en DIRECTV.	Corto Plazo	Baja	Bajo	Bajo	SEI
5.13 Uso de utilidades con privilegios del	5.13.1 Ver Plan de Acción 5.1.1.	Largo Plazo	Media	Alto	Medio	Bajo

INICIATIVA 2						
Implantación de controles.						
Subdominio	**Planes de Acción:**	**Plazo**	**Brecha**	**Esfuerzo**		
				Tiempo	**Personas**	**Costo**
sistema						
5.14 Control de acceso al código fuente de los programas	5.14.1 Ver Plan de Acción 5.1.1.	Mediano Plazo	Media	Medio	Medio	Bajo
7.11 Retirada de materiales propiedad de la empresa	7.11.1 Incrementar el control de salida de equipos en la recepción de la Compañía.	Mediano Plazo	Baja	Medio	Bajo	SEI
7.12 Seguridad de los equipos fuera de las instalaciones	7.12.1 Ver Plan de Acción 4.10.1.	Mediano Plazo	Baja	Medio	Bajo	SEI
7.13 Reutilización o eliminación segura de equipos	7.13.1 Se deberá definir y establecer un procedimiento para la validación de información crítica de la Compañía o software bajo licencia, antes de proceder con la eliminación del contenido de los equipos.	Mediano Plazo	Baja	Medio	Bajo	SEI
8.3 Gestión de capacidades	8.3.2 En la política de monitoreo de recursos de los servicios y sistemas informáticos, definir y establecer las proyecciones de los requisitos futuros de capacidad, con el objetivo de garantizar los rendimientos requeridos de los sistemas informáticos de DIRECTV.	Largo Plazo	Alta	Alto	Medio	SEI
8.5 Controles contra el código malicioso	8.5.2 Ver Plan de Acción 1.1.3.	Mediano Plazo	Baja	Medio	Alto	SEI
8.10 Sincronización del reloj	8.10.1 Definir y establecer que todos los servidores principales de DIRECTV se encuentren sincronizados a un servidor central.	Mediano Plazo	Baja	Medio	Bajo	SEI
12.3 Notificación de puntos débiles de la seguridad	12.3.1 Establecer y ejecutar diferentes charlas respecto a la sensibilización por parte de los usuarios en temas relacionados con la seguridad de la información. En estas charlas se deberá dar énfasis en la participación de empleados, contratistas, proveedores, con respecto a la notificación de puntos débiles en la seguridad de la información de DIRECTV.	Mediano Plazo	Baja	Medio	Bajo	SEI

Saltos Nivel Futuro					***Esfuerzo***
Alta	1	6	4	0	Alto

INICIATIVA 2							
Implantación de controles.							
Subdominio	**Planes de Acción:**	**Plazo**	**Brecha**	**Esfuerzo**			
				Tiempo	**Personas**	**Costo**	
	Media		14	16	13	0	Medio
	Baja		15	8	13	10	Bajo
						20	Sólo esfuerzo interno

Corto Plazo	8
Mediano Plazo	16
Largo Plazo	6

Iniciativa 3 - Planes de Acción

INICIATIVA 3						
Aplicación de enfoques de mejora continua.						
Subdominio	**Planes de Acción:**	**Plazo**	**Brecha**	**Esfuerzo**		
				Tiempo	**Personas**	**Costo**
2.2 Segregación de tareas	2.2.1 El Information Security & Networking de DIRECTV deberá definir y establecer un cronograma de revisión para validar que las funciones y áreas de responsabilidad se encuentren segregadas. En cada departamento deberá exitir una correcta distribución de tareas, con el objetivo de reducir el riesgo de modificaciones indebidas por personal no autorizado.	Mediano Plazo	Media	Medio	Bajo	SEI
2.5 Seguridad de la información en la gestión de proyectos	2.5.1 En la herramienta de control de cambios de DIRECTV, se deberá incluir las consideraciones de seguridad de la información que se deben definir al inicio de cada uno de los proyectos de la Compañía. Esto ayudará a tener un control y monitoreo sobre la inclusión de medidas de seguridad a la gestión de proyectos de DIRECTV.	Corto Plazo	Baja	Bajo	Medio	SEI
4.2 Propiedad de los activos	4.2.1 El Gerente de cada departamento deberá ser el encargado de asignar un responsable, para el monitoreo y control de los activos asignados a cada uno de los funcionarios de dicho departamento.	Mediano Plazo	Baja	Medio	Bajo	SEI
4.3 Uso aceptable de los activos	4.3.1 El departamento encargado de la administración de los activos de DIRECTV, deberá definir e implementar métricas a utilizar para la gestión de inventarios (uso de activos).	Mediano Plazo	Baja	Medio	Bajo	SEI
4.4 Devolución de activos	4.4.1 Recursos Humanos en conjunto con el departamento encargado de la administración de los activos de DIRECTV, deberán ser los responsables de validar la devolución de todos los activos a cargo de los funcionarios que finalicen los contratos laborales con DIRECTV.	Mediano Plazo	Baja	Medio	Medio	SEI
5.3 Registro y baja de usuario	5.3.3 Ver Plan de Acción 5.1.3.	Mediano Plazo	Baja	Medio	Bajo	SEI
6.2 Gestión de claves	6.2.1 Se deberá establecer un monitoreo continuo a la gestión de claves para el cifrado de los equipos de DIRECTV.	Corto Plazo	Baja	Bajo	Bajo	SEI
7.6 Áreas de carga y descarga	7.6.1 Se deberá establecer un monitoreo continuo a los puntos de acceso a DIRECTV.	Mediano Plazo	Baja	Medio	Bajo	SEI
7.7 Emplazamiento y protección de equipos	7.7.1 Se deberá establecer un monitoreo continuo a todos los accesos de DIRECTV, especialmente a los accesos que correspondan a las áreas donde se encuentra la información sensible de la Compañía.	Mediano Plazo	Baja	Medio	Bajo	SEI
7.8 Instalaciones de suministro	7.8.1 Deberá existir un cronograma de revisión a todas las entradas de alimentación eléctrica de la Compañía, para validar que las instalaciones de suministro se encuentren funcionando en óptimas condiciones.	Mediano Plazo	Baja	Medio	Bajo	SEI

INICIATIVA 3						
Aplicación de enfoques de mejora continua.						
Subdominio	**Planes de Acción:**	**Plazo**	**Brecha**	**Esfuerzo**		
				Tiempo	**Personas**	**Costo**
7.9 Seguridad del cableado	7.9.1 Deberá existir un cronograma de revisión al cableado eléctrico y de telecomunicaciones de la Compañía, para validar que estos medios se encuentren protegidos frente a daños o interferencias.	Mediano Plazo	Baja	Medio	Bajo	SEI
7.10 Mantenimiento de los equipos	7.10.1 Adquirir e instalar una herramienta que permita monitorear el funcionamiento de los principales equipos de DIRECTV.	Mediano Plazo	Baja	Medio	Medio	Bajo
7.12 Seguridad de los equipos fuera de las instalaciones	7.12.2 Ver Plan de Acción 4.10.2.	Mediano Plazo	Baja	Medio	Bajo	SEI
7.14 Equipo de usuario desatendido	7.14.1 Deberá existir un cronograma de revisión a todos los equipos desatendidos de DIRECTV, para validar que dichos equipos se encuentren protegidos y no contengan información sensible de la Compañía.	Mediano Plazo	Baja	Medio	Medio	SEI
7.15 Política de puesto de trabajo despejado y pantalla limpia	7.15.1 Deberá existir un cronograma de revisión a todos los puestos de trabajo de cada uno de los funcionarios de DIRECTV, con el objetivo de validar que los puestos de trabajo se encuentren despejados de papeles y medios de almacenamiento desmontables.	Mediano Plazo	Baja	Medio	Medio	SEI
8.4 Separación de los recursos de desarrollo, prueba y operación	8.4.1 Deberá existir un cronograma de revisión a los principales servidores de DIRECTV, con el objetivo de validar que los ambientes de desarrollo, pruebas y operación se encuentren debidamente separados, evitando el acceso no autorizado a los ambientes de producción de la Compañía.	Mediano Plazo	Baja	Medio	Medio	SEI
8.5 Controles contra el código malicioso	8.5.1 Se deberá implementar un monitoreo constante para evitar que código malicioso infecte los equipos de DIRECTV. 8.5.2 Ver Plan de Acción 1.1.3.	Mediano Plazo	Baja	Medio	Alto	SEI
8.6 Copias de seguridad de la información	8.6.2 Definir y establecer una fecha programada (mínimo una vez al año) para realizar pruebas de legibilidad de los respaldos de información de DIRECTV.	Mediano Plazo	Baja	Medio	Medio	Bajo
13.1 Planificación de la continuidad de la seguridad de la información	13.1.1 Se deberá definir un cronograma de pruebas para validar que la seguridad de la información se encuentra contemplada dentro del plan de continuidad de DIRECTV.	Largo Plazo	Baja	Alto	Medio	SEI

INICIATIVA 3						
Aplicación de enfoques de mejora continua.						
Subdominio	**Planes de Acción:**	**Plazo**	**Brecha**	**Esfuerzo**		
				Tiempo	**Personas**	**Costo**
14.1 Identificación de la legislación aplicable y de los requisitos contractuales	14.1.1 Definir y establecer pruebas aleatorias de revisión, con respecto a los requisitos legales y contractuales de los empleados de DIRECTV.	Mediano Plazo	Baja	Medio	Medio	SEI
14.2 Derechos de propiedad intelectual (DPI)	14.2.1 Definir y establecer pruebas aleatorias de revisión para validar la existencia de procedimientos adecuados, con el objetivo de garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, en relación a que pueda existir derechos de propiedad intelectual sobre ellos.	Mediano Plazo	Baja	Medio	Medio	SEI
14.3 Protección de los registros de la organización	14.3.1 Definir y establecer pruebas aleatorias de revisión para validar la correcta protección de los registros de DIRECTV, contra la pérdida, destrucción, falsificación, revelación o accesos no autorizados, de acuerdo con los requisitos legales, regulatorios y contractuales de DIRECTV.	Mediano Plazo	Baja	Medio	Medio	SEI
14.4 Protección y privacidad de la información de carácter personal	14.4.1 Definir y establecer pruebas aleatorias de revisión para validar la existencia de procedimientos adecuados, con el objetivo de garantizar la protección y la privacidad de la información, de acuerdo con los requisitos legales, regulatorios y contractuales de DIRECTV.	Mediano Plazo	Baja	Medio	Medio	SEI
14.5 Regulación de los controles criptográficos	14.5.1 Definir y establecer pruebas aleatorias de revisión para validar la existencia de controles criptográficos, de acuerdo con los requisitos legales, regulatorios y contractuales de DIRECTV.	Mediano Plazo	Baja	Medio	Medio	SEI
14.8 Comprobación del cumplimiento técnico	14.8.1 Definir y establecer pruebas aleatorias de revisión para validar que los sistemas de información están cumpliendo las políticas y normas de seguridad de la información de DIRECTV.	Mediano Plazo	Baja	Medio	Medio	SEI

Saltos Nivel Futuro					***Esfuerzo***
Alta	0	1	1	0	Alto
Media	1	22	14	0	Medio
Baja	24	2	10	2	Bajo
				23	Sólo esfuerzo interno

Corto	2
Mediano Plazo	22
Largo Plazo	1

Iniciativa 4 - Planes de Acción

INICIATIVA 4						
Sensibilización del personal.						
Subdominio	**Planes de Acción:**	**Plazo**	**Brecha**	**Esfuerzo**		
				Tiempo	**Personas**	**Costo**
1.1 Políticas para la seguridad de la información	1.1.3 Establecer y ejecutar un plan para la comunicación y sensibilización de las políticas de seguridad de la información a todo el personal de DIRECTV.	Largo Plazo	Media	Alto	Alto	SEI
3.3 Responsabilidades de gestión	3.3.1 Ver Plan de Acción 1.1.3.	Mediano Plazo	Media	Alto	Alto	SEI
3.4 Concienciación, educación y capacitación en seguridad de la información	3.4.1 Ver Plan de Acción 1.1.3.	Mediano Plazo	Media	Alto	Alto	SEI
8.5 Controles contra el código malicioso	8.5.2 Ver Plan de Acción 1.1.3.	Mediano Plazo	Baja	Alto	Alto	SEI
12.3 Notificación de puntos débiles de la seguridad	12.3.1 Establecer y ejecutar diferentes charlas respecto a la sensibilización por parte de los usuarios en temas relacionados con la seguridad de la información. En estas charlas se deberá dar énfasis en la participación de empleados, contratistas, proveedores, con respecto a la notificación de puntos débiles en la seguridad de la información de DIRECTV.	Mediano Plazo	Baja	Medio	Bajo	SEI

Saltos Nivel Futuro					***Esfuerzo***
Alta	0	4	4	0	Alto
Media	3	1	0	0	Medio
Baja	2	0	1	0	Bajo
				5	Sólo esfuerzo interno

Corto Plazo	0
Mediano Plazo	4
Largo Plazo	1

Anexo 6. Manual de la Función de Seguridad de la Información

1. OBJETIVO

Establecer los lineamientos específicos bajo los cuales operará la Seguridad de la Información en DIRECTV, como parte de los mecanismos de gobierno, gestión y control de la Compañía.

2. RESPONSABILIDADES

Todos los empleados, proveedores y terceros de DIRECTV involucrados en la gestión de la Seguridad de la Información, ejecutarán sus actividades diarias teniendo en cuenta los lineamientos definidos en el presente manual.

El Oficial de Seguridad de la Información será el encargado de gestionar el cumplimiento de las responsabilidades relacionadas con seguridad de la información en la Compañía.

El Administrador de Seguridad de la Información será el responsable de la ejecución de actividades referentes a la administración y revisión de los controles implementados utilizando tecnología. Esta persona podrá pertenecer al departamento de Tecnología de la Compañía y deberá reportar al Oficial de Seguridad de la Información.

A continuación se puede visualizar una representación gráfica de la organización de la función de seguridad de la información en DIRECTV:

3. CONSIDERACIONES

La gestión de la Seguridad de la Información debe ser considerada como un factor fundamental dentro de DIRECTV, y su objetivo principal debe enfocarse en la generación de valor a la Compañía.

Complementar el proceso de alineación entre los objetivos estratégicos que persigue el negocio y los objetivos de la Seguridad de la Información de la Compañía.

Para llegar a cumplir con el proceso de alineación, se debe definir los lineamientos específicos de seguridad, tales como, objetivos estratégicos, visión y ubicación de la función de seguridad de la información dentro de la Compañía.

3.1 DEFINICIONES

- **Control**
  Un control se define como una medida que modifica el riesgo.

- **Información**
  La información es un activo que, al igual que otros activos comerciales importantes, tiene un valor para el negocio de una organización y, por consiguiente debe ser adecuadamente protegida.

- **Seguridad de la Información**
  La seguridad de la información se conoce como la preservación de la confidencialidad, integridad y disponibilidad del activo más importante en una organización.

4. ALCANCE

El presente manual debe ser utilizado para la función de Seguridad de la Información dentro de la Compañía.

5. PUBLICACIÓN

A través de los medios que permitan a la función de Seguridad de la Información de DIRECTV, conocer este manual.

6. MANUAL

6.1 OBJETIVOS ESTRATÉGICOS DE SEGURIDAD DE LA INFORMACIÓN

Para definir los objetivos estratégicos de seguridad de la información en DIRECTV, se efectuó un análisis de las funciones y responsabilidades de los principales actores relacionados con la Seguridad de la Información en la Compañía, y poder establecer los objetivos estratégicos a cumplir.

A continuación se presentan los objetivos estratégicos de seguridad de la información:

- Definir, establecer y mantener el marco normativo regulatorio de la Compañía en materia de Seguridad de la Información.

- Administrar la implementación de controles de Seguridad de la Información en DIRECTV, con base a los requisitos de la Compañía y el Sistema de Gestión de Seguridad de la Información (SGSI).

- Identificar el avance respectivo con respecto al cumplimiento de controles de seguridad establecidos.

Los responsables de dar cumplimiento a los objetivos estratégicos definidos en el presente manual, serán el Oficial de Seguridad de la Información Regional y el Administrador de Seguridad de la Información de DIRECTV Ecuador.

6.1.1 Revisión de los Objetivos Estratégicos de Seguridad de la Información

Los objetivos estratégicos de Seguridad de la Información deberán ser revisados una vez por año, con la finalidad de establecer una gestión adecuada para validar el cumplimiento de cada uno de los objetivos definidos por el departamento de Seguridad de la Información.

6.2 VISIÓN DE SEGURIDAD DE LA INFORMACIÓN

La visión de la seguridad de la información en DIRECTV es:

La Compañía será la encargada de proteger la confidencialidad, integridad y disponibilidad de la información. Esta gestión deberá ir de la mano a través de la implementación de un marco normativo, entrenamiento y capacitación al personal, y la utilización de tecnología.

6.3 ESTRUCTURA DEL ÁREA DE SEGURIDAD DE LA INFORMACIÓN

El departamento de Seguridad de la Información debe estar liderado por un Oficial de Seguridad de la Información. El perfil profesional sugerido de dicho oficial es:

Formación Académica

- Ingeniería en Sistemas, Computación, Telemática o carreras afines.
- Opcional: Maestría en Seguridad de la Información, Auditoría de Sistemas o afines.

Experiencia Profesional

- Experiencia de al menos 3 años en cargos relacionados con Seguridad de la Información.

Conocimientos Básicos

- Conocimiento en ISO 27001 (deseable con certificaciones relacionadas).
- Conocimiento en Evaluación de Riesgos (deseable con enfoque a Seguridad de la Información).
- Conocimiento en Auditoría de Sistemas / TI.
- Conocimiento en Gestión de Continuidad del Negocio.
- Conocimiento en Ethical Hacking (opcional).
- Conocimiento en Informática Forense (opcional).

6.3.1 Posición de la función de Seguridad de la Información dentro de DIRECTV

La posición de la función de seguridad de la información dentro de DIRECTV, es clave para la consecución de los objetivos estratégicos de seguridad de la información definidos para dicha Compañía. Existen dos (2) elementos a considerar cuando se habla de la posición de dicha área:

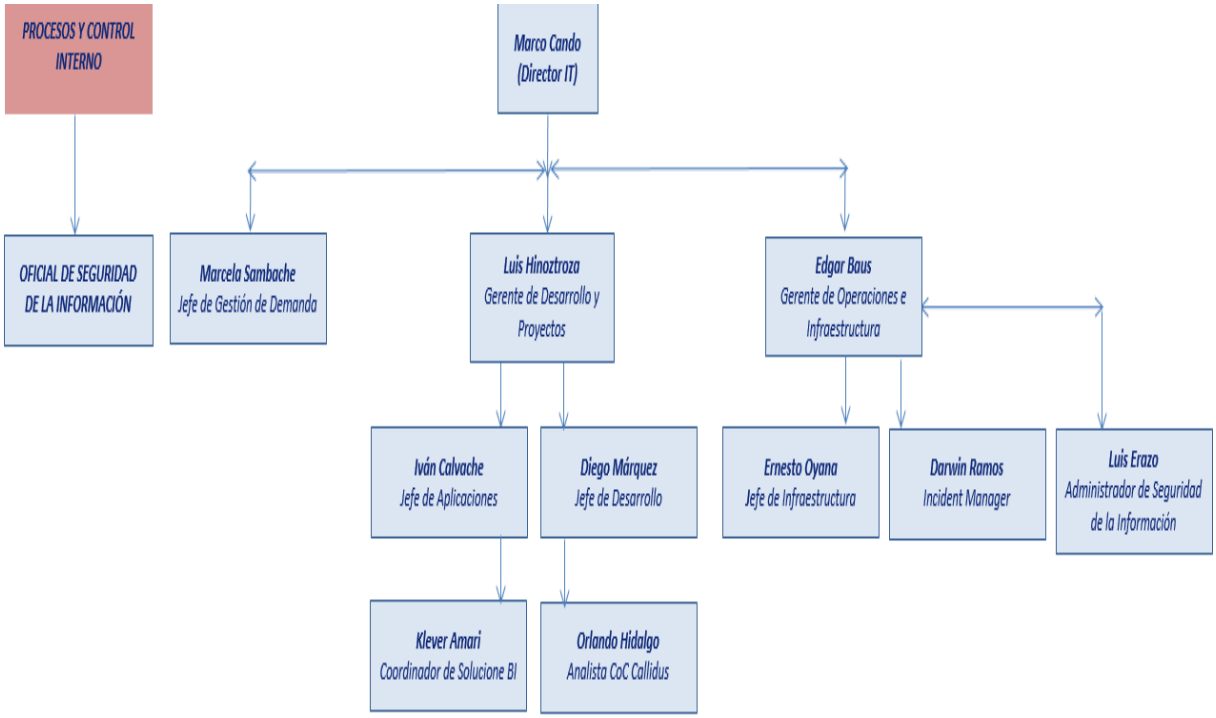
- Departamento o área a la cual pertenece.
- Nivel de profundidad en la Compañía.

El departamento o área a la cual pertenece la función de Seguridad de la Información es muy importante, puesto que su ámbito de acción es amplio, abarcando temas relacionados con Recursos Humanos hasta Cumplimiento Regulatorio. No existe una buena práctica con respecto a la ubicación óptima de dicha función dentro de una Compañía, pero con base al principio de segregación de funciones, el área de Seguridad de la Información en DIRECTV no debería pertenecer a los departamentos de Tecnología de la Información, ni Auditoría Interna.

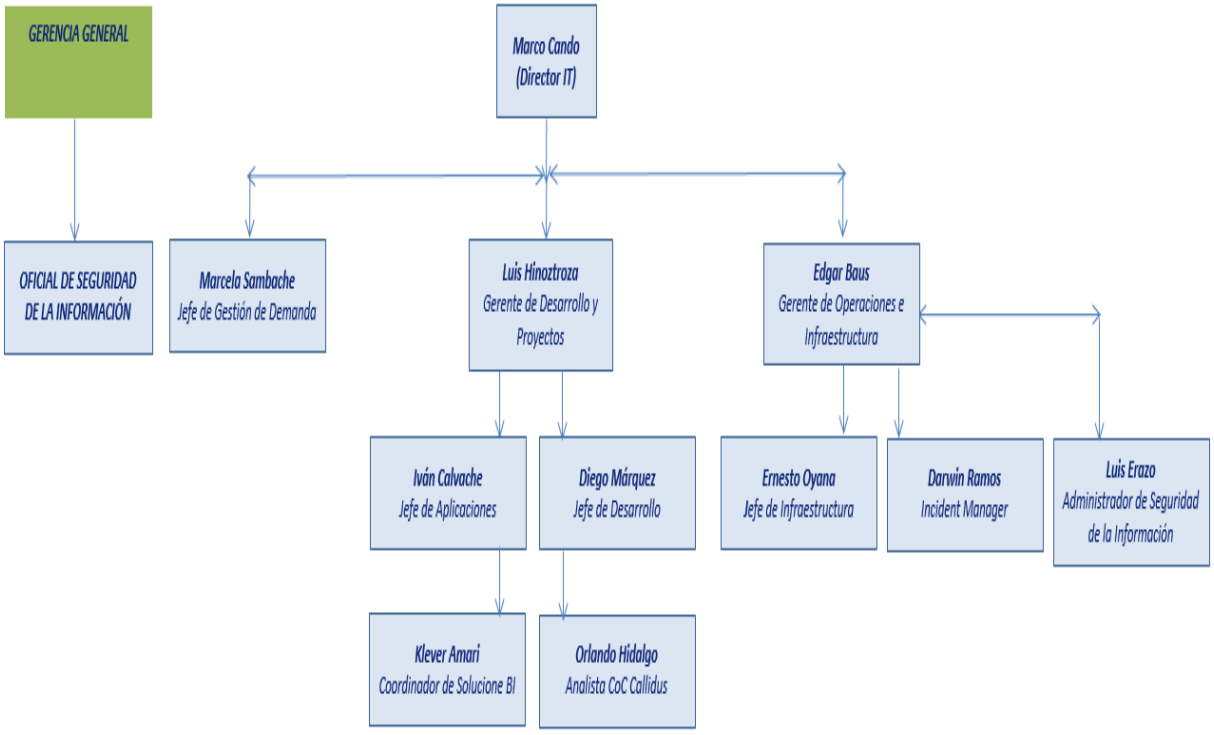
Con respecto al nivel de profundidad dentro de la Compañía, dado que la función de Seguridad de la Información deberá abarcar el tratamiento de temas relacionados con todas las áreas de la Compañía, no es recomendable relegarla en la estructura organizacional, más bien considerar ubicarla en un punto visible con el nivel de empoderamiento adecuado para su gestión.

DIRECTV puede considerar los siguientes modelos para definir la posición de la función de seguridad de la información dentro del Organigrama de la Compañía:

Corto Plazo



Largo Plazo



7. INCUMPLIMIENTOS

Los empleados que incumplan el manual serán sancionados de acuerdo a la normativa interna vigente.

8. REFERENCIAS A OTROS DOCUMENTOS

- Política de Seguridad de la Información.
- Manual de Roles y Responsabilidades de Seguridad de la Información.

Anexo 7. Plan de Concienciación a los Usuarios

DEFINICIÓN Y EJECUCIÓN DEL PROCESO DE ALISTAMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN DIRECTV.

Plan de Concienciación a Usuarios y Entrenamiento a Empleados del departamento de Seguridad de la Información

Versión Final

Fecha: 26/10/2015

1. Objetivo

Definir planes y cronogramas de concientización y capacitación en temas de seguridad de la información, que deberá realizar DIRECTV a los usuarios de los recursos de información de la Compañía y al personal que forma parte del departamento de Seguridad de la Información.

2. Trabajo realizado

Se definió los siguientes aspectos relacionados con el plan de capacitación en DIRECTV:

- Audiencias
- Contenido
- Tiempos

3. Audiencias

Con el objetivo de dar inicio al proceso de sensibilización que permita la implementación de un sistema de gestión de Seguridad de la Información a futuro, se requiere definir y establecer iniciativas de concientización y sensibilización para todos los empleados de DIRECTV.

Las audiencias definidas para DIRECTV son las siguientes:

- **Gerente General, Directores y Gerentes de cada uno de los departamentos de la Compañía:** Personal de la Compañía que gestiona y administra los recursos de DIRECTV. Adicionalmente, los encargados de dirigir cada uno de los departamentos de la Compañía.
- **Usuarios Finales**: Empleados de la Compañía, personal responsable de los activos de información de DIRECTV.

La siguiente tabla presenta los elementos de conocimiento que se requerirán por cada uno de estos grupos:

Audiencia	Elementos de conocimiento
Gerente General, Directores y Gerentes de cada uno de los departamentos de la Compañía.	1. Conocer y estar al tanto de la importancia de la información. 2. Comprender los conceptos de activo de la información, amenaza, vulnerabilidad y control. 3. Entender las características de Seguridad de la Información (integridad, disponibilidad y confidencialidad). 4. Tener claro que la Seguridad de la Información forma parte de la gestión del riesgo de la Compañía.
Usuarios Finales.	1. Conocer y estar al tanto de la importancia de la información. 2. Comprender los conceptos de activo de la información, amenaza, vulnerabilidad y control. 3. Entender las características de Seguridad de la Información (integridad, disponibilidad y confidencialidad). 4. Comprender el impacto de la no protección de la información dentro y fuera de la Compañía. 5. Gestionar el proceso de identificación de riesgos de Seguridad de la Información a los activos de información existentes.

Audiencia	Elementos de conocimiento
	6. Aplicar las buenas prácticas de Seguridad de la Información. 7. Entender y comunicar los incidentes de Seguridad de la Información al Oficial de Seguridad de la Información de DIRECTV.

4. Contenido

Los temas a ser desarrollados en las sesiones de concientización y capacitación son los siguientes:

Audiencia	Contenido
Gerente General, Directores y Gerentes de cada uno de los departamentos de la Compañía.	1. ¿Por qué hablar de Seguridad de la Información? a. Estadísticas. b. Casos significativos. 2. ¿Qué abarca la Seguridad de la Información? 3. ¿Qué es un activo de la información? 4. ¿Qué es una amenaza? 5. ¿Qué es una vulnerabilidad? 6. ¿Qué es un control? 7. ¿Qué es la confidencialidad, integridad y disponibilidad de la información? 8. ¿Por qué es importante el apoyo de la máxima autoridad con respecto a la Seguridad de la Información? 9. Política de Seguridad de la Información 10. La administración de riesgos de Seguridad de la Información. 11. Preguntas
Usuarios Finales.	1. ¿Por qué hablar de Seguridad de la Información? • Estadísticas. • Casos significativos. 2. ¿Qué abarca la Seguridad de la Información? 3. ¿Qué es un activo de la información? 4. ¿Qué es una amenaza? 5. ¿Qué es una vulnerabilidad? 6. ¿Qué es un control? 7. ¿Qué es la confidencialidad, integridad y disponibilidad de la información? 8. ¿De qué debemos proteger la información? • Tipos de atacantes. • Algunos tipos de ataque. 9. Uso seguro a los recursos de información. • Email. • Internet. • Laptops. • USBs. • Smartphones. 10. ¿Cuál es el modelo organizacional para la Gestión de la Seguridad de la Información en DIRECTV? • SGSI. • Relaciones de elementos de seguridad. • Política de Seguridad de la Información. 11. Preguntas.

5. Tiempos estimados

La siguiente tabla presenta los tiempos estimados para cada una de las sesiones a realizar:

Audiencia	Asistentes	Tiempo
Gerente General, Directores y Gerentes de cada uno de los departamentos de la Compañía.	Gerente General Directores Gerentes Coordinadores.	Noventa minutos.
Usuarios Finales.	Usuarios finales de los activos de información.	Ciento veinte minutos.

6. Plan de Entrenamiento para Empleados del Departamento de Seguridad de la Información

Los empleados del departamento de Seguridad de la Información de DIRECTV, deberán contar con un plan de entrenamiento orientado a dar cumplimiento a las funciones y responsabilidades aprobadas para cada uno de sus cargos, así como los temas relacionados con la ejecución de sus actividades diarias.

El plan de entrenamiento para los empleados del departamento de Seguridad de la Información de DIRECTV, deberá cubrir de forma general los siguientes tópicos:

- Gestión por procesos.
- Gestión de riesgos de Seguridad de la Información.
- Diseño e implementación de Sistemas de Gestión de Seguridad de la Información (SGSI).
- Administración de la continuidad del negocio.
- Legislación de Seguridad de la información local.

Los objetivos que se conseguirán al cubrir estos tópicos son:

Tópico	Objetivos
Gestión por procesos.	• Entender los principales procesos de la Compañía. • Identificar los procesos que son considerados estratégicos, y los que agregan valor a la Compañía. • Dimensionar el alcance para la implementación de un Sistema de Gestión de Seguridad de la Información.
Gestión de riesgos de Seguridad de la Información.	• Comprender los lineamientos y principios para el análisis de riesgos de Seguridad de la Información. • Identificar principales amenazas y vulnerabilidades a los cuales estaría expuesto DIRECTV. • Analizar y evaluar los riesgos, con la finalidad de

	determinar su nivel de aceptabilidad para DIRECTV. • Establecer un plan de tratamiento para los riesgos inaceptables. • Seguimiento continuo a la implementación del plan de tratamiento de riesgos.
Diseño e Implementación de Sistemas de Gestión de Seguridad de la Información (SGSI).	• Conocer cuáles son los elementos que intervienen en la implementación de un Sistema de Gestión de Seguridad de la Información. • Implementar un Sistema de Gestión de Seguridad de la Información acorde a los objetivos de DIRECTV. • Realizar la auditoría del SGSI. Se debe considerar el análisis y gestión de los elementos claves, los mismos que podrían derivar en No Conformidades.
Administración de la continuidad del negocio.	• Identificar los procesos y servicios considerados como críticos, que requieren de una estrategia de continuidad para no impactar las principales operaciones de la Compañía. • Para definir una estrategia de continuidad, se debe conocer los elementos que requieren de un plan alterno de operación. • Conocer los elementos que conforman un plan de continuidad del negocio. • Conocer los elementos que conforman un plan de recuperación de desastres. • Conocer que se requiere para definir un esquema de pruebas y mantenimiento de un plan de continuidad del negocio.
Legislación de Seguridad de la Información local.	• Conocer las leyes, normas y regulaciones en materia de Seguridad de la Información que puedan tener impacto en DIRECTV.

6.1 Contenido sugerido para el plan de entrenamiento

Para alcanzar los objetivos establecidos en la sección 6, se sugiere que cada tópico cubra los siguientes temas:

Tópico	Temas

Gestión por procesos.	• Indicadores de Gestión
	  ○ Descripción, evaluación, implementación y seguimiento de indicadores.
	• Procesos
	  ○ Tipos de procesos.
	  ○ Componentes de los procesos.
	  ○ Los procesos y los sistemas de gestión de calidad.

Gestión de riesgos de Seguridad de la	• Principios y lineamientos de administración de riesgos. • Gestión del riesgo en la Seguridad de la Información

Información.	○ Identificación de activos de información. ○ Identificación de amenazas y vulnerabilidades. ○ Análisis y evaluación de riesgos. ○ Definición e implementación del plan de tratamiento de riesgos.
Diseño e Implementación de Sistemas de Gestión de Seguridad de la Información (SGSI).	• Requisitos de un SGSI. • Auditoría del SGSI.
Administración de la continuidad del negocio.	• Análisis de Impacto de Riesgos (RIA). • Análisis de Impacto del Negocio (BIA). • Definición de estrategias de continuidad. • Definición de procedimientos alternos de operación. • Definición de gobierno de continuidad del negocio. • Definición del Plan de Recuperación de Desastres. • Definición de esquema de pruebas del Plan de Continuidad del Negocio. • Definición de esquema de revisión del Plan de Continuidad del Negocio.
Legislación de Seguridad de la Información local.	• Leyes, normas y regulaciones en materia de Seguridad de la Información, que puedan tener impacto en DIRECTV.

Anexo 8. Check-list Requisitos Alistamiento SGSI

DEFINICIÓN Y EJECUCIÓN DEL PROCESO DE ALISTAMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN DIRECTV.

Check-list Requisitos Alistamiento SGSI

Versión Final

Fecha: 26/10/2015

1. Objetivo

Definir un check-list de verificación para corroborar el cumplimiento de los requisitos de la norma ISO/IEC 27001:2013 en DIRECTV.

2. Trabajo realizado

La elaboración del check-list de verificación durante la evaluación de los requisitos de la norma ISO/IEC 27001:2013, contempló la siguiente actividad:

- Check-list de cumplimiento para cada requisito de la norma ISO/IEC 27001:2013.

3. Metodología

Como parte de la metodología aplicada para elaborar el check-list de verificación, se realizó la siguiente actividad:

- Se tomó en cuenta cada uno de los requisitos, el estado (cumple/no cumple) y observaciones al respecto.

4. Checklist de Evaluación de los Requisitos de la Norma ISO/IEC 27001:2013

El checklist de cumplimiento de los requisitos previo al alistamiento del SGSI en DIRECTV, se encuentra definido de acuerdo a cada requisito de la norma ISO/IEC 27001:2013.

Requisitos de la Norma ISO/IEC 27001:2013

SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN	Cumple S/N	Observaciones
4 SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN		
4. Contexto de la organización		
4.1 Comprensión de la organización y de su contexto		
Se encuentran definidas las cuestiones externas e internas que son pertinentes para el propósito y que afectan a la capacidad para lograr los resultados previstos del sistema de gestión de seguridad de la información en la Compañía.	S	
4.2 Comprensión de las necesidades y expectativas de las partes interesadas		
En la Compañía se encuentran definidos los siguientes aspectos: - Las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información. - Los requisitos de estas partes interesadas que son relevantes para la seguridad de la información.	S	

SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN	Cumple S/N	Observaciones
4.3 Determinación del alcance del sistema de gestión de seguridad de la información		
La Compañía ha establecido los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance.	S	
4.4 Sistema de gestión de seguridad de la información		
La Compañía ha definido los lineamientos de seguridad para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de seguridad de la información, de acuerdo con los requisitos de esta norma internacional.	S	
5. Liderazgo		
5.1 Liderazgo y compromiso		
La alta dirección ha demostrado liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información.	N	
5.2 Política		
La Compañía cuenta con una política de seguridad de la información.	S	
5.3 Roles, responsabilidades y autoridades en la organización		
Las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se encuentran asignadas y comunicadas a personal autorizado dentro de la Compañía.	S	
6. Planificación		
6.1 Acciones para tratar los riesgos y oportunidades		
6.1.1 Consideraciones generales		
La Compañía ha definido lineamientos de seguridad para asegurar que el sistema de gestión de seguridad de la información pueda conseguir sus resultados previstos, prevenir o reducir efectos indeseados; y lograr la mejora continua.	S	
6.1.2 Apreciación de riesgos de seguridad de la información		
La Compañía ha definido lineamientos de seguridad para identificar los riesgos de seguridad de la información, llevando a cabo el proceso de apreciación de riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el alcance del sistema de gestión de seguridad de la información. Adicionalmente, se ha establecido un proceso para la identificación de los dueños de los riesgos.	S	

SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN	Cumple S/N	Observaciones
6.1.3 Tratamiento de los riesgos de seguridad de la información		
La Compañía ha definido un proceso de tratamiento de riesgos de seguridad de la información.	S	
6.2 Objetivos de seguridad de la información y planificación para su consecución		
La Compañía ha definido los objetivos de seguridad de la información en cada una de las funciones y niveles pertinentes. Los objetivos de seguridad de la información establecidos en la Compañía son coherentes con la política de seguridad de la información, medibles, se encuentran actualizados según el giro del negocio y están comunicados a todo el personal.	S	
7. Soporte		
7.1 Recursos		
La Compañía ha determinado y establecido los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.	N	
7.2 Competencia		
La Compañía ha determinado la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta al desempeño en seguridad de la información.	N	
7.3 Concienciación		
La Compañía ha establecido un plan para que las personas que trabajan bajo el control de la misma, sean conscientes de la política de la seguridad de la información, la contribución a la eficacia del sistema de gestión de seguridad de la información, las implicaciones de no cumplir con los requisitos del sistema de gestión de seguridad de la información.	N	
7.4 Comunicación		
La Compañía ha determinado la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de seguridad de la información.	S	
7.5 Información documentada		
7.5.1 Consideraciones generales		
La Compañía ha definido que en el sistema de gestión de seguridad de la información, se contemple la información documentada requerida por la norma internacional ISO/IEC 27001:2013, y la información documentada que la Compañía ha determinado que es necesaria para la eficacia del sistema de	N	

SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN	Cumple S/N	Observaciones
gestión de seguridad de la información.		
7.5.2 Creación y Actualización		
La Compañía ha definido lineamientos de seguridad para asegurar la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia) de la información documentada. Adicionalmente, el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico); y la revisión y aprobación con respecto a la idoneidad y adecuación.	N	
7.5.3 Control de la información documentada		
La Compañía ha definido lineamientos de seguridad para asegurar que la información documentada se encuentra disponible y preparada para su uso. Adicionalmente, protegida adecuadamente, y almacenamiento, preservación, distribución, acceso, recuperación, retención y disposición de dicha información.	N	
8. Operación		
8.1 Planificación y control operacional		
La Compañía ha definido lineamientos de seguridad para controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, llevando a cabo acciones para mitigar los efectos adversos, cuando sea necesario.	S	
8.2 Apreciación de los riesgos de seguridad de información		
La Compañía ha definido lineamientos de seguridad para efectuar apreciaciones de riesgos de seguridad de la información a intervalos planificados, y cuando se propongan o se produzcan modificaciones importantes	S	
8.3 Tratamiento de los riesgos de seguridad de información		
La Compañía cuenta con un plan de tratamiento de riesgos de seguridad de la información.	S	
9. Evaluación del desempeño		
9.1 Seguimiento, medición, análisis y evaluación		
La Compañía ha definido estrategias de seguridad para la evaluación del desempeño de la seguridad de la información y la eficacia del sistema de gestión de seguridad de la información.	S	
9.2 Auditoría interna		
La Compañía ha definido estrategias de seguridad para llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de seguridad de la información cumple con los requisitos propios de	S	

SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN	Cumple S/N	Observaciones
la Compañía para el sistema de gestión de seguridad de la información.		
9.3 Revisión por la dirección		
La Compañía ha definido lineamientos de seguridad para revisar el sistema de gestión de seguridad de la información a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas.	S	
10. Mejora		
10.1 No conformidad y acciones correctivas		
La Compañía se encuentra capacitada para reaccionar frente a la ocurrencia de una No Conformidad.	S	
10.2 Mejora Continua		
La Compañía se encuentra capacitada para mejorar de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información.	S	

Anexo 9. Manual de Roles y Responsabilidades de Seguridad de la Información

1. OBJETIVO

Establecer responsabilidades respecto a la gestión de la seguridad de la información en DIRECTV, como parte de los mecanismos de gobierno, gestión y control de la Compañía.

2. RESPONSBILIDADES

Todos los empleados, proveedores y terceros de DIRECTV, realizarán sus tareas asignadas normalmente, teniendo en cuenta cada una de sus responsabilidades en lo que se refiere a la administración de la seguridad de la información de la Compañía.

Las Direcciones y Gerencias que componen la Compañía serán las encargadas de gestionar el cumplimiento de las responsabilidades relacionadas con la seguridad de la información.

El Oficial de Seguridad de la Información será el encargado de realizar el seguimiento correspondiente para el cumplimiento de este Manual.

3. CONSIDERACIONES

La gestión de la Seguridad de la Información debe ser considerada como un factor fundamental dentro de DIRECTV, y su objetivo principal debe enfocarse en la generación de valor a la Compañía.

Con la finalidad de obtener resultados exitosos en la implementación del Sistema de Gestión de Seguridad de la Información en DIRECTV, todos los empleados, proveedores y terceros, deben tener asignados los roles y responsabilidades relacionados con la administración de la Seguridad de la Información de la Compañía.

3.1 DEFINICIONES

- **Manual**
  Conjunto de reglas o leyes que deben ser cumplidas, dentro de cualquier grupo u organización.

- **Información**
  La información es un activo que, al igual que otros activos comerciales importantes, tiene un valor para el negocio de una organización y, por consiguiente debe ser adecuadamente protegida.

- **Incidente de Seguridad de la Información**
  Se conoce como incidente de seguridad de la información a una serie de eventos no deseados o inesperados, los mismos que pueden comprometer las operaciones de negocio y amenazar la seguridad de la información de una organización.

4. ALCANCE

El presente manual se encuentra dirigido a todos los departamentos de DIRECTV, empleados, proveedores y terceros que acceden a la información de la Compañía.

5. PUBLICACIÓN

A través de los medios que permitan a todos los empleados, proveedores y terceros de DIRECTV, conocer este manual.

6. MANUAL

6.1 DEFINICIONES

Se definirán los siguientes roles relacionados con la administración de seguridad de la información en DIRECTV:

- Departamento de Seguridad
- Oficial de Seguridad de la Información
- Administrador de Seguridad de la Información
- Dueño de la información
- Custodio de la información
- Usuario final

A continuación se describen cada uno de los roles y responsabilidades de Seguridad de la Información en la Compañía:

6.1.1 Departamento de Seguridad

Encargado de definir y establecer lineamientos de seguridad en relación a los objetivos y metas de la Compañía.

Adicionalmente, el Departamento de Seguridad deberá cumplir las funciones de administración, gestión y seguimiento a las tareas de seguridad de la información asignadas a cada uno de los responsables de los activos de información de la Compañía.

Deberá estar conformado por el Oficial de Seguridad y su equipo de trabajo, máximo cuatro en total. Las responsabilidades de los integrantes del Departamento de Seguridad se encuentran enfocadas en la toma de decisiones con respecto a la gestión de Seguridad de la Información.

Sus responsabilidades son:

- Definir, administrar y mantener las políticas, procedimientos y normas, en relación a temas de Seguridad de la Información. Adicionalmente, administrar y gestionar la aprobación y puesta en vigencia de cada uno de los documentos descritos anteriormente.

- Implementar controles específicos de Seguridad de la Información para los nuevos aplicativos o servicios adquiridos por la Compañía.
- Administrar, monitorear y gestionar los incidentes de Seguridad de la Información que se presenten en el trabajo diario dentro de la Compañía.
- Designar formalmente al Oficial de Seguridad de la Información y al responsable de Seguridad del departamento de Tecnología.
- Monitorear la estrategia de Seguridad definida por el Departamento de Seguridad.
- Monitorear iniciativas y proyectos relacionados con la Seguridad de la Información.

6.1.2 Oficial de Seguridad de la Información

El Departamento de Seguridad será el encargado de contratar un Oficial de Seguridad de la Información. Esta persona será la encargada de gestionar el programa de seguridad de la Información para DIRECTV.

Sus responsabilidades son:

- Establecer procedimientos para el manejo de incidentes de seguridad.
- Asesorar a los demás departamentos de la Compañía en los temas que tienen que ver con la Seguridad de la Información.
- Garantizar que las normas, procedimientos y controles de seguridad establecidos se estén cumpliendo dentro de la Compañía.
- Asegurar la implementación de diferentes actividades referente al tratamiento de los riesgos identificados para los activos de información de la Compañía.
- Gestionar una evaluación de riesgos.
- Apoyar e implementar proyectos de Seguridad de la Información.
- Desarrollar procedimientos adecuados de concienciación de usuarios en materia de seguridad, controles de acceso a los sistemas, y administración de cambios en el software, base de datos y aplicativos de la Compañía.

6.1.3 Encargado de Seguridad en el departamento de Tecnología

Deberá ser es un profesional que pertenezca a dicha área y su principal función será apoyar en la implementación de la estrategia de Seguridad de la Información, siendo responsable de la seguridad en el departamento de Tecnología.

Sus responsabilidades son:

- Registrar las actividades realizadas por el personal operativo de Seguridad de la Información, para su posterior revisión.
- Gestionar los incidentes de Seguridad de la Información de acuerdo a los procedimientos establecidos por la Compañía.
- Gestionar el control de la documentación física o electrónica actualizada, relacionada con los procedimientos e infraestructura tecnológica de la Compañía.

- Revisar los procedimientos para la obtención de respaldos de información, así como las pruebas de legibilidad de acuerdo a lo establecido por DIRECTV.
- Monitorear la capacidad de los diferentes sistemas en operación de la Compañía, y proyectar demandas de capacidad a meses futuros, con el objetivo de soportar potenciales amenazas a la información que se procesa.
- Implementar los controles de seguridad definidos.

6.1.4 Dueño de la información

Serán los responsables de definir y asegurar el cumplimiento de los requisitos de seguridad de los activos de información que les sean asignados. Adicionalmente, serán los responsables de la clasificación, control y monitoreo del uso y gestión de los mismos.

Sus responsabilidades son:

- Definir los controles necesarios para los activos de información a su cargo. Esto con respecto a los niveles de clasificación establecidos y el nivel de seguridad requerido.
- Llevar un control del inventario de los activos de información de los procesos a su cargo.
- Validar la operación de los controles definidos.
- Identificar los posibles riesgos que pueden encontrarse expuestos los activos de información a su cargo.
- Monitorear los niveles de acceso de funcionarios y terceras partes a sus activos de información para garantizar la confidencialidad e integridad de la información almacenada, resguardada o procesada en los mismos.
- Llevar un control sobre los accesos de empleados y terceras partes a los activos de información a su cargo. El objetivo de este control, será garantizar la confidencialidad e integridad de la información almacenada en los mismos.

6.1.5 Custodios de la información

Corresponden a los directores, gerentes y coordinadores de cada uno de los departamentos de la Compañía.

Sus responsabilidades son:

- Apoyo incondicional a los dueños de la información, con respecto a la selección de soluciones técnicas para dar cumplimiento de los requisitos de control de Seguridad de la Información que se encuentran establecidos.
- Definir formalmente los procedimientos, normas y estándares de Administración de Seguridad de la Información para los activos de información a su cargo.

- Gestionar el cumplimiento de los niveles de servicio definidos para los activos de información a su cargo.

6.1.6 Usuarios finales

Se refieren a todos los empleados, proveedores, terceros, y/o personal autorizado para utilizar la información de DIRECTV en el cumplimiento de sus funciones y/o la ejecución de sus tareas diarias.

Sus responsabilidades son:

- Utilizar la información y los recursos tecnológicos de la Compañía de forma ética y responsable.
- Mantener la confidencialidad de la información sensible provista por DIRECTV para llevar a cabo sus labores cotidianas.
- En el caso de identificar incidentes de seguridad, reportar inmediatamente al Oficial o Encargado de Seguridad en el departamento de Tecnología.
- Aceptar, comprender y aplicar las políticas, normativas, procedimientos y estándares de Seguridad de la Información de la Compañía en cada una de sus funciones diarias asignadas.

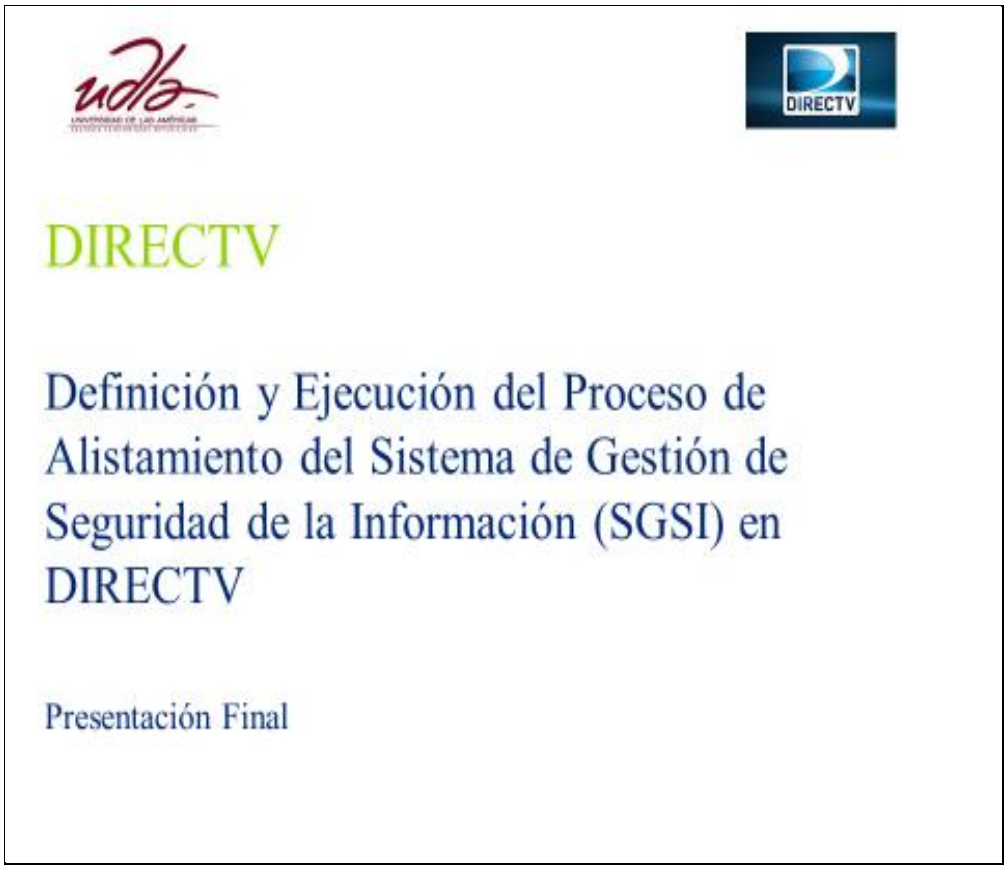
7. INCUMPLIMIENTOS

Los empleados que incumplan el manual serán sancionados de acuerdo a la normativa interna vigente.

8. REFERENCIAS A OTROS DOCUMENTOS

- Política de Seguridad de la Información.
- Manual de la Función de la Seguridad de la Información.

Anexo 10. Presentación Ejecutiva



Agenda

- Objetivo
- Departamentos Involucrados
- Fortalezas y Oportunidades de Mejora
- Resultados Obtenidos

Objetivo

- Socializar los resultados finales del alistamiento del SGSI a la Alta Administración de DIRECTV. Los resultados fueron comunicados por medio de una presentación ejecutiva.

Departamentos Involucrados

Departamento	Cargo
Procesos y Control Interno	Jefe de Control Interno Coordinador de Procesos Analista de Control Interno
Seguridad de la Información	Oficial de Seguridad de la Información Coordinador de Seguridad de la Información Arquitecto de Seguridad Administrador de Seguridad de la Información
Compensaciones y Beneficios	Gerente de Gestión Humana
Finanzas	Contador General
Infraestructura	Jefe de Infraestructura
Desarrollo	Gerente de Desarrollo y Proyectos Jefe de Desarrollo y Proyectos
Departamento Jurídico	Abogado

Fortalezas y Oportunidades de Mejora

FORTALEZAS

- Apoyo fundamental por parte de la Dirección de TI en la consecución del alistamiento del SGSI en DIRECTV.
- Alta colaboración del personal de DIRECTV que gestionó el proyecto.
- Buena disposición por parte del personal entrevistado de los distintos departamentos.
- Entrega de información a tiempo durante las reuniones.
- Alta involucración de personal de DIRECTV, durante la revisión de las políticas y procedimientos relacionados con la seguridad de la información.

Fortalezas y Oportunidades de Mejora (cont.)

OPORTUNIDADES DE MEJORA

- Mejora en los tiempos acordados para las actividades definidas dentro del alistamiento del SGSI en DIRECTV.

Resultados Obtenidos

Resultado 1.- Política de Seguridad de la Información.

Política de Seguridad de la Información

Se refiere a la definición de los lineamientos específicos, relacionados con la gestión y administración de la Seguridad de la Información en DIRECTV.

Se encuentran cada uno de los pasos que se debe seguir, para asegurar el cumplimiento de los tres elementos fundamentales de la Seguridad de la Información (confidencialidad, integridad y disponibilidad).

Adicionalmente, los lineamientos y controles para prevenir o responder a amenazas respecto a temas de seguridad de la información, se encuentran claramente detallados en la política de Seguridad de la Información establecida para DIRECTV.

Resultados Obtenidos (cont.)

Resultado 2.- Plan Estratégico de Seguridad de la Información

Contiene:

- Nivel de madurez deseados del Área a corto, mediano y largo plazo
- Planes de acción y "roadmap" de implementación
- Objetivos estratégicos del Área de Seguridad de la Información
- Plan de concienciación a los usuarios

Resultados Obtenidos (cont.)

Resultado 3.- Marco de Gobierno de Seguridad de la Información

Contiene:

- Organigrama Funcional del Departamento de Seguridad de la Información y TI
- Definición Detallada de Roles y Funciones del Departamento
- Plan de Entrenamiento para Empleados del Departamento de Seguridad de la Información

Resultados Obtenidos (cont.)

Resultado 4.- Marco Normativo de Seguridad de la Información.

Contiene las políticas y procedimientos desarrollados como parte del trabajo de titulación, debido a que ciertos documentos requeridos por el área de Seguridad de la Información no se encontraban documentados, aprobados ni difundidos a todo el personal de la Compañía.

Anexo 11. Carta de Conformidad - DIRECTV

DIRECTV

Quito, Enero 27 del 2016
A quien le interese
Presente.-

De nuestra consideración:

Por la presente, Ing. Edgar Baus, en mi calidad de Gerente de Operaciones e Infraestructura de la empresa Directv, doy fe que el señor Victor Fernando Quezada Neira con cédula de ciudadanía N° 1710106582 en calidad de estudiante de la Universidad de las Américas de la Carrera de Ingeniería en Sistemas de Computación e Informática, realizó la identificación de las capacidades actuales de la Compañía referente a la Gestión de Seguridad de la Información en conjunto con personal responsable de cada departamento. Producto del trabajo realizado se generaron entregables en cada una de las fases del proyecto, los cuales fueron entregados a Luis Erazo - Information Security & Networking, de acuerdo a lo establecido al inicio del Trabajo de Titulación "Definición y Ejecución del Proceso de Alistamiento del Sistema de Gestión de Seguridad de la Información (SGSI) en DIRECTV", desarrollado e implementado en nuestra empresa.

Atentamente
Ing. Edgar Baus
Gerente de Operaciones e Infraestructura
Directv