ESCUELA DE POSGRADOS

MARCO DE REFERENCIA PARA LA IMPLEMENTACIÓN DE UN ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI), BASADO EN LA NORMA TÉCNICA ECUATORIANA INEN ISO/IEC 27001:2010 Y EN CONCORDANCIA CON EL ACUERDO 166

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

Profesora Guía

Ing. Nancy Velásquez, MSc.

Autor

José Adrián Pino Vera

Año

2014

DECLARACIÓN DE LA PROFESORA 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".

_____

Ing. Nancy Velásquez Villagrán, M.Sc.
CI. 1708088008

DECLARACIÓN DE AUTORÍA DEL MAESTRANTE

"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"

José Adrián Pino Vera
CI. 1715287544

AGRADECIMIENTO

Cuando nuestra vida nos enfrenta a ciertas tareas, se necesita el apoyo de una mano amiga, por tal motivo agradezco a mi tutora por su apoyo y compromiso en este proyecto.

DEDICATORIA

A mi esposa, intentando expresarle mi amor y gratitud por su apoyo incondicional, su comprensión generosa y su tolerancia infinita a mis pretensiones intelectuales.

A mis hijos, razón de mi ser y sentido en la vida, ojala pueda servirles de ejemplo de superación con la esperanza de que verán un mundo mejor.

RESUMEN

La investigación documentada en este proyecto de titulación tiene como finalidad brindar un marco de referencia para la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) basado en la Norma Técnica Ecuatoriana ISO/IEC 27001:2010 con el objetivo de cumplir con lo que se dispone en el Acuerdo Ministerial número 166 publicado por la Secretaría Nacional de la Administración Pública en el Registro Oficial número 88 el mes de septiembre del año 2013.

Como parte del marco propuesto se consideran aspectos netamente técnicos como por ejemplo, establecer el proyecto, identificar activos de información, analizar y evaluar riesgos, diferenciar entre seguridad de la información y seguridad informática, sin embargo, también se tratan enfoques basados en buenas prácticas tales como quién debe formar parte de un proyecto de este tipo o cómo seleccionar el alcance adecuado para el EGSI.

El marco de referencia propuesto no solamente se limita al diseño e implementación sino también a las actividades básicas a cubrirse con la finalidad de operar, mantener, evaluar y mejorar el Esquema Gubernamental de Seguridad de la Información para las empresas públicas del Ecuador.

ABSTRACT

The research documented in this titling project aims to provide a framework for the implementation of the Information Security Government Scheme (EGSI for its name in Spanish) based on the Ecuadorian Technical Standard ISO/IEC 2700:2010 in order to comply with the Ministerial Agreement 166 published in September 2013 by the National Secretariat of Public Administration in Official Gazette Number 88.

The proposed framework consider not only purely technical aspects such as establishing the project, identify information assets, analyze and assess risks, differentiate between information security and informatics security, but also, this framework is based on best practices such as who should be part of this kind of project or how to select the right scope for EGSI.

The proposed framework is not limited to the design and implementation but also to the basic cover in order to operate, maintains, evaluate and improve the Information Security Government Scheme for Ecuador's public organizations.

INDICE

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

La seguridad de la información ha llegado a ser uno de los procesos transversales más importantes en las organizaciones debido al valor que aporta al negocio, sin embargo, este valor depende de su gestión y operación.

Un gran porcentaje de su éxito o fracaso irá de la mano con aspectos organizacionales, culturales, de control interno y de compromiso del nivel estratégico.

La Familia de las Normas Técnicas Ecuatorianas INEN ISO/IEC 27000 es la base que la Secretaría de la Administración Pública del Ecuador ha dispuesto para que las organizaciones públicas implementen el Esquema Gubernamental de Seguridad de la Información, mismo que, tiene como objetivo satisfacer la necesidad de aplicar normas y procedimientos para mitigar los riesgos asociados a confidencialidad, integridad y disponibilidad de la información.

El Esquema Gubernamental de Seguridad de la Información (EGSI), cuyo texto se expone en el Anexo 1 del Acuerdo Ministerial No. 166 del 19 de Septiembre del 2013 toma como base los controles de la Norma Técnica Ecuatoriana INEN ISO/IEC 27002, sin embargo, omite el conjunto de requisitos para un diseño e implementación adecuado del EGSI, mismos que se detallan en la Norma Técnica Ecuatoriana INEN ISO/IEC 27001.

Este proyecto de titulación es un marco de referencia ya que ha sido elaborado a partir del conocimiento y experiencias previamente adquiridas por el investigador, mismas que consideran todas las actividades a ser ejecutadas para el diseño e implementación del Esquema Gubernamental de Seguridad de la Información en cualquier entidad pública del Ecuador.

CAPÍTULO 1. MARCO TEÓRICO

Este capítulo se orienta a brindar un panorama general de la seguridad de la información como proceso de negocio, sus ámbitos de acción y sus principales actores, además, de una descripción de las normas que conforman a la familia de la ISO/IEC 27000, enfatizando la ISO/IEC 27001 y su estructura.

1.1. Seguridad de la Información

La seguridad de la información se refiere a un conjunto de actividades que aseguran la confidencialidad, integridad y disponibilidad de los activos de información de las organizaciones por medio del análisis y valoración de sus riesgos asociados, esto quiere decir, que no depende solamente de tecnología, sino también de los procesos de negocio y de las personas que conforman la organización. Aunque en muchas ocasiones se manejan como sinónimos, debe considerarse que la seguridad informática tiene como finalidad proteger solamente los activos tecnológicos de las organizaciones (Sánchez L. S.-O.-M., 2011, pág. 45).

1.2. Seguridad de la Información vs. Seguridad Informática

Entre la seguridad de la información y la seguridad informática, es necesario considerar las siguientes diferencias (Asociación Española de Normalización, 2013, pág. 12):

- El enfoque de la seguridad informática tiene aplicación sobre los activos tecnológicos de las organizaciones, por ejemplo, servidores, antivirus, sistemas operativos, sistemas informáticos, o cualquier herramienta de hardware o software; mientras que la seguridad de la información se concentra en los activos de información, los cuales además de hardware y software, incluyen también documentos electrónicos, documentos físicos y personas.

- La seguridad informática tiene mayor injerencia y aplicación dentro del área funcional de tecnologías de información y comunicaciones (TICS), mientras que, la seguridad de la información debe ser aplicada en toda la organización como un proceso transversal.

- Realizando una analogía basada en la teoría de conjuntos, la seguridad de la información sería el conjunto más grande que contiene a la seguridad informática. La primera tiene un enfoque de personas, procesos y tecnología, mientras que la segunda solamente se enfoca a tecnología.

- La seguridad informática tiene un ámbito técnico y se refiere a la gestión de recursos tecnológicos con perspectiva a cuidar su confidencialidad, integridad y disponibilidad, mientras que, la seguridad de la información tiene su fundamento básico en la gestión de los riesgos asociados a los activos de información de la organización y a las distintas alternativas de tratamiento.

- El Oficial de Seguridad de la Información es el llamado a conocer los riesgos de toda la organización relacionados a los activos de información, y, es el responsable de gestionar la implementación de medidas de tratamiento de dichos riesgos; mismas que pueden derivar en controles directivos, técnicos o físicos.

1.3. Importancia de la Seguridad de la Información para las Organizaciones

La importancia de la seguridad de la información radica en que mediante la identificación de los activos de información y la gestión de sus riesgos asociados a pérdida o degradación de confidencialidad, integridad, disponibilidad o posibles combinaciones entre ellas, se puede lograr mejoría en:

- Enfoque preventivo: Un aspecto muy importante de la seguridad de la información es detectar y tratar oportunamente los riesgos relacionados a los activos de información, las ventajas principales son detectar, reportar y tratar tanto amenazas como vulnerabilidades, que junto con personal capacitado y con el adecuado nivel de sensibilización y compromiso, disminuirán los incidentes de seguridad de la información evitando así pérdidas para la organización (Asociación Española de Normalización, 2013, pág. 24).

- Disminuir costos: Los controles preventivos que una organización debe implementar a partir del análisis de riesgos de seguridad de la información deben complementar a los diferentes procesos de negocio reduciendo las vulnerabilidades detectadas, además, mejoran el uso de recursos tecnológicos, la productividad de los usuarios, y se disminuyen caídas de servicios (Mellado, 2012, pág. 56) .

- Cambiar cultura: La participación de los dueños del negocio y de la alta dirección en las actividades de evaluación de riesgos, su presencia en las jornadas de capacitaciones y su involucramiento en la implementación de controles, junto con su apoyo y ejemplo, producirán que todos los funcionarios adquieran un cambio de cultura organizacional, y, gracias a esto, será cada vez más común el actuar en base a prácticas proactivas de seguridad de la información. (Sánchez L. S.-O.-M., 2011, pág. 76).

- Mejorar imagen y reputación: Mediante el tratamiento adecuado de los riesgos de seguridad de la información a través de controles que además deben incluir jornadas de capacitación, sensibilización y disciplina para el personal, se estarían reduciendo la cantidad de incidentes de seguridad de la información y por lo tanto, la cantidad

de noticias negativas en los medios de comunicación o en la comunidad protegiendo así el prestigio de la organización (Mellado, 2012, pág. 80).

- Cumplimiento legal y regulatorio: La organización siempre debe asesorarse y observar todas las disposiciones que aplican a su entorno legal, regulatorio y comercial (Asociación Española de Normalización, 2013, pág. 45).

1.4. Estructura Organizacional de la Seguridad de la Información

Las actividades de seguridad de la información debieran ser coordinadas por representantes de diferentes partes de la organización con roles y funciones relevantes, es así que el EGSI requiere una estructura organizacional con presencia en todos los niveles y en todos los procesos de negocio (Instituto Ecuatoriano de Normalización, 2010, pág. 31).

Nivel Estratégico: Se refiere al Comité de Seguridad de la Información, conformado por la alta dirección de la institución, este nivel recibe los informes y recomendaciones por parte del nivel táctico, además, tiene la obligación de proponer e implementar cualquier iniciativa estratégica que mejore la seguridad de la información en la entidad (Sánchez L. V., 2005, pág. 71).

Nivel Táctico: Involucra al Oficial de Seguridad de la Información, quien es el encargado de dirigir al negocio hacia una adecuada identificación y tratamiento de todos los riesgos de la seguridad de la información, así mismo, es el llamado a monitorear el cumplimiento de los controles, y, capacitar a todo el personal, con respecto a la relación con el nivel estratégico, el Oficial de Seguridad de la Información debe mantenerlo constantemente informado con respecto al estado de evolución de la seguridad de la información, así como cualquier acción que deba tomarse para mejorarla.

Nivel Operativo: En materia de seguridad de la información, este nivel se conforma por los siguientes actores:

- Grupo de profesionales de apoyo al Oficial de Seguridad de la Información conformado por profesionales especializados en distintas ramas, dependiendo de las necesidades de la organización, por ejemplo, pruebas de penetración, desarrollo seguro de software, capacitadores, auditores, etc. (ISC2, 2013, pág. 134)

- Especialistas en Seguridad Informática, debido a que el grupo de apoyo al Oficial de Seguridad da las directrices que seguridad informática deberá implementar y configurar en los equipos de seguridad.

- Terceros especialistas como auditores independientes, investigadores forenses, proveedores de equipos y herramientas de seguridad o entidades de capacitación y certificación (Asociación Española de Normalización, 2013, pág. 87).

Paralelamente a los niveles indicados, cabe señalar ciertos actores que también forman parte de la organización de la seguridad de la información, estos son los dueños, custodios y usuarios:

Dueño de la información: Es el dueño del proceso de negocio (gerente o director de área) donde la información es necesaria para su operación (Sánchez L. S.-O.-M., 2011, págs. 68-69).

Custodio de la información: Es el personal técnico que se encarga de la administración de los activos de información que soportan al proceso de negocio (Artetio, 2008, págs. 30-31).

Usuario de la información: Son los involucrados en los distintos procesos de negocio que hacen uso de los activos de información (Asociación Española de Normalización, 2013, pág. 45).

1.5. Funciones

Para que la seguridad de la información alcance sus objetivos y proporcione valor a la organización, debe ser vista como un proceso, y como tal, debe contar con roles, responsabilidades, debe ser planificada debe considerar la entrega de servicios, gestión de presupuesto, operación y mejora de controles, indicadores de desempeño, rendición de cuentas, informes periódicos y retroalimentación de las partes interesadas.

El proceso llamado seguridad de la información tiene como función principal mitigar todos los riesgos asociados a los activos de información con el objetivo de asegurar la confidencialidad, integridad y disponibilidad de los mismos, sin embargo, esto debe estar sujeto a la premisa de que la seguridad es un facilitador para el negocio, por lo cual, debe ser una fuente de soluciones, con el debido enfoque de gestión de riesgos que permita dar valor a toda la organización (Sánchez L. S.-O., 2012, pág. 126).

Es importante además distinguir perfectamente las funciones que los niveles de la seguridad de la información tendrán en la organización, esto con la finalidad de establecer claramente los ámbitos de responsabilidad de cada uno, por ejemplo, definir las tareas de gestión de la seguridad de la información que recaen sobre el Oficial de Seguridad de la Información, así como las tareas operativas de las herramientas de seguridad que son responsabilidad de los distintos administradores que forman parte del área de tecnología.

En muchos casos, la cultura organizacional de la entidad tendrá una afectación considerable sobre la función de la seguridad de la información ya que, en base a ciertos supuestos, costumbres, valores, expectativas o incluso

comportamientos, el Comité de Seguridad de la Información, el Oficial de Seguridad, todos los profesionales de apoyo y demás involucrados podrían encontrarse con ciertas trabas para desempeñar sus funciones (ISC2, 2013, pág. 234).

Para establecer adecuadamente la función de seguridad de la información, sabiendo que se trata de un proceso, es recomendable (Sánchez L. S.-O.-M., 2011, págs. 89-90):

- Saber diferenciar seguridad de la información de seguridad informática.
- Separar las funciones normativas y de gestión de las funciones operativas de seguridad.
- Evaluar el nivel de madurez de la seguridad de la información en la organización, al menos en comparación con la competencia.
- Tener la opinión de un tercero confiable, por ejemplo un consultor que aporte con un panorama fresco del estado actual y el estado ideal de la seguridad de la información en la entidad.

A fin de cuentas, el llamado a diseñar la función de seguridad de la información en base a las necesidades de la organización es el Comité de Seguridad de la Información bajo la asesoría del Oficial de Seguridad de la Información (Sánchez L. S.-O.-M., 2011, pág. 176).

En base a lo indicado anteriormente, la función de la seguridad de la información siempre debe estar alineada con los objetivos del negocio y basada en una constante evaluación de riesgos que permita la implementación metodológica de controles que aseguren la confidencialidad, integridad y disponibilidad de los activos de información de la organización, sin embargo, es necesario hacer hincapié en que dicha función tiene un componente de gestión que es ejecutado por el Oficial de Seguridad de la Información y su personal de apoyo, y, otro componente operativo ejecutado por el grupo de seguridad

informática, así como otro componente de aplicación que es responsabilidad de toda la organización (Sánchez L. V., 2005, pág. 145).

Una vez diseñada la función de seguridad de la información, es responsabilidad del Comité de Seguridad de la Información revisarla, aprobarla, formalizarla y difundirla a toda la organización.

1.6. Ubicación jerárquica del Oficial de Seguridad de la Información

Según lo dispuesto en el Acuerdo 166 en su Artículo 3, y, en concordancia con lo expuesto en los puntos anteriores, donde se estableció que la seguridad de la información tiene injerencia en toda la organización, el Oficial de Seguridad de la Información debe formar parte del grupo de apoyo a la alta dirección de la organización (Secretaría Nacional de la Administración Pública, 2013, pág. 6).

Las razones que justifican la ubicación del Oficial de Seguridad, en base a sus funciones son:

- En caso de que el Oficial reporte al Gerente de Tecnología, se dificultaría el cambio de cultura de seguridad de la información con respecto al cambio de paradigma tradicional donde seguridad de la información es confundido con seguridad informática, además, las áreas de la organización no verían al Oficial de Seguridad como un actor que complementa a todos los procesos de negocio, sino, sería visto como uno más de tecnología, incluso, el Oficial no tendría una visión general de los riesgos de la seguridad de la información debido a que en su día a día estaría más asociado a la realidad de la gerencia de tecnología de la organización.
- El Oficial de Seguridad debe tener cierto nivel de autoridad otorgado por la alta dirección o por el Comité de Seguridad de la Información para realizar monitoreo de cumplimiento, convocar al personal a las jornadas de capacitación, atender incidentes de seguridad de la

información, coordinar con las demás áreas funcionales la implementación de controles, etc.

- El Oficial de Seguridad de la Información es el llamado a operar la gestión de la seguridad de la información, sin embargo, su operación y aplicación son responsabilidad de todos en la organización.
- El Oficial de Seguridad de la Información puede fungir como asesor de la alta dirección para la implementación de estrategias e iniciativas de control interno.

1.7. Control interno

El control interno de una organización puede ser descrito como el entorno de la empresa con respecto a los deberes y responsabilidades de sus funcionarios, así como todas las políticas, medidas, métodos y estrategias aplicadas para estimular y evaluar el cumplimiento de todos los controles implementados (Sánchez L. V., 2005, págs. 120-121).

Forman parte del control interno de una organización todas las políticas, normas, disposiciones y directrices que nacen de la alta dirección y que se aplican por todos los funcionarios tanto internos como externos.

La seguridad de la información tiene un papel muy importante y muchas veces decisivo dentro del control interno de una organización debido a que en base a la evaluación de riesgos y a los planes de tratamiento que el Oficial de Seguridad de la Información proporcione al negocio, nacerán iniciativas de control operativo, legal, regulatorio, así como medidas de capacitación, toma de conciencia, monitoreo y reporte a la alta gerencia, incluso, en coordinación con la gerencia de recursos humanos, deberán establecerse esquemas sancionatorios que consideren acciones tanto administrativas como legales para quienes cometan infracciones o peor aún, fraudes.

Dentro del esquema de control interno de una organización, bajo la perspectiva de seguridad de la información, debe existir (ISC2, 2013, págs. 234-238):

- Proceso de implementación de controles: es el proceso mediante el cual se establecen qué controles son necesarios en la organización (tomando como insumo el resultado del análisis de riesgos), este proceso debe ser dinámico e integrado con todos los demás procesos de negocio; su ejecución debe ser patrocinada por la alta dirección de la organización bajo el soporte y guía del Oficial de Seguridad de la Información.

  Se entiende que un control ha sido implementado cuando está documentado en un formato aceptado en la empresa, formalizado por la alta gerencia, difundido y publicado en medios oficiales de la organización y cuando el personal ha recibido cierto nivel de entrenamiento para aplicarlo, dicho entrenamiento debe tener evidencia de evaluación del nivel de asimilación.

- Proceso de monitoreo: el ambiente de control interno de una organización, debe contar con un proceso de monitoreo de cumplimiento de controles cuyo objetivo es indicar a la alta dirección el nivel de incumplimiento así como todas sus causas y acciones de remediación, sabiendo que, el incumplimiento de un control no necesariamente es responsabilidad de los funcionarios por que pudiera ser el caso de que un control haya sido mal diseñado o que simplemente no se ajuste a la realidad de la empresa.

- Proceso de mantenimiento y actualización: otro proceso que forma parte del control interno de una organización es el de mantenimiento y actualización de los controles de seguridad de la información, mismo que basado en un análisis de riesgos y en el monitoreo permitirá determinar si los controles implementados a la fecha aún

son vigentes y se ajustan a las necesidades del negocio, así como, determinar si existe la necesidad de nuevos controles; para el caso de seguridad de la información, el Oficial de Seguridad debe ejecutar por lo menos una vez al año (o cuando la organización sufra cambios impactantes) un análisis de riesgo, esto daría ciertas luces con respecto a la necesidad de nuevos controles. Parte de este proceso es la mejora continua de los controles, para lo cual se debe:

- Brindar apertura a los funcionarios para que proporcionen sus sugerencias con respecto a los controles implementados o posibles controles a implementarse.
- Realizar encuestas de satisfacción con el objetivo de determinar la aplicabilidad de los controles y de sus canales de difusión, así como de las capacitaciones realizadas.
- Es vital que el nivel estratégico de la organización no solo impulse el control interno, sino además, deben ser los primeros en practicarlo.
- Proporcionar canales de comunicación adecuados y oficiales tanto para la difusión así como para la publicación de todos los controles de tipo administrativo o directivo, esto es, políticas, normativas, procedimientos, etc.
- Proporcionar canales de comunicación y un único punto de contacto para que los funcionarios reporten cualquier incumplimiento a controles, así como cualquier debilidad de estos.
- Debe existir un ambiente de confianza mutua entre todos los que conforman la organización, así habrá un respaldo en el flujo de información tanto del que da como del que recibe, de esta forma se respaldan aspectos como el trabajo en equipo y la cooperación, así también, un ambiente de confianza estimula a la gente y la hace más colaborativa, reduciendo la

dependencia de la organización hacia el capital intelectual de sus funcionarios.

- La filosofía y estilo de la alta gerencia también son un factor transversal a todo el control interno debido a que es su obligación transmitir a toda la organización (también a terceros relacionados) de manera contundente y permanente su compromiso y liderazgo con respecto a la implementación, monitoreo, operación y mejora de los controles internos.
- Deben existir acciones enfocadas a que toda la organización comprenda y sobre todo respete los controles existentes, considerando que, siempre deben considerarse esquemas de sanción tanto administrativa como legal para los infractores.

- Proceso de reporte: este es el proceso mediante el cual se reporta el cumplimiento o no de los indicadores del proceso de seguridad de la información. Se comunica cómo se encuentra todo el ambiente de control interno en términos de seguridad de la información.

En definitiva, el control interno es todo lo que la alta dirección impulsa, aplica y transmite a los funcionarios para que se asuman conductas enfocadas al bienestar de toda la organización; esto incluye a la seguridad de la información (SGS, 2013, pág. 98).

1.8. Normas Internacionales ISO/IEC 27000

A continuación se describen las distintas normas que forman parte de la familia ISO/IEC 27000 con la finalidad de conocer su diversidad, campo de aplicación, y, así estar en capacidad de seleccionar los documentos que sean aplicables al negocio según la organización.

1.8.1. Familia ISO/IEC 27000

La familia ISO/IEC 27000 es un conjunto de estándares desarrollados, tanto por International Organization for Standardization (ISO) como por International Electrotechnical Commission (IEC), con el objetivo de proporcionar un marco de gestión de la seguridad de la información aplicable para las distintas organizaciones (ISO27000.ES, 2005) .

La familia ISO/IEC 27000 está conformada por las siguientes normas:

ISO/IEC 27000: Este documento básicamente contiene una visión general de las normas que componen la serie 27000, una breve descripción introductoria a los Sistemas de Gestión de Seguridad de la Información (SGSI), aspectos básicos del ciclo Plan-Do-Check-Act, así como términos y definiciones que se emplean en todos los documentos que conforman la serie 27000 (Asociación Española de Normalización, 2013, pág. 3).

ISO/IEC 27001: Es la principal integrante de la familia, contiene los requisitos que debe cumplir un Sistema de Gestión de Seguridad de la Información, por lo tanto es auditable y la única certificable, además, su Anexo A enumera en forma de resumen los objetivos de control y controles que son detallados en ISO/IEC 27002:2005 (Asociación Española de Normalización, 2013, pág. 4).

ISO/IEC 27002: Es así como se le conoce a la extinta ISO 17799:2005, es una guía de buenas prácticas que describe los objetivos de control y controles de seguridad de la información, en total contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios (SGS, 2013, pág. 13).

ISO/IEC 27003: Es una guía que se centra en los aspectos necesarios para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información en concordancia con lo que define la ISO/IEC 27001:2005 (ISO27000.ES, 2005).

ISO/IEC 27004: Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un sistema de gestión de la seguridad de la información (ISO27000.ES, 2005).

ISO/IEC 27005: Proporciona directrices para la gestión del riesgo en la seguridad de la información, además, apoya los conceptos generales especificados en la norma ISO/IEC 27001. Cabe señalar que esta no es una metodología de evaluación de riesgos (Instituto Ecuatoriano de Normalización, 2010, pág. 5).

ISO/IEC 27006: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información (Sánchez L. S.-O.-M., 2011, pág. 53).

ISO/IEC 27007: Es una guía de auditoría de un SGSI, dicta directrices de auditoría para Sistemas de Gestión (SGS, 2013, pág. 17).

ISO/IEC TR 27008: Es una guía para revisar la implementación y operación de los controles que forman parte del sistema de gestión de la seguridad de la información (ISO27000.ES, 2005).

ISO/IEC 27010: Consiste en una guía para la gestión de la seguridad de la información cuando ésta comparte entre organizaciones o sectores, o sea, es aplicable a todas las formas de intercambio y difusión de información (ISO27000.ES, 2005).

ISO/IEC 27011: Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002 (ISO27000.ES, 2005).

ISO/IEC 27013: Es una guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI) (ISO27000.ES, 2005).

ISO/IEC 27014: Consiste en una guía de gobierno corporativo de la seguridad de la información (ISO27000.ES, 2005).

ISO/IEC TR 27015: Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002.

ISO/IEC TR 27016: Guía de valoración de los aspectos financieros de la seguridad de la información (ISO27000.ES, 2005).

ISO/IEC TS 27017: Guía de seguridad para Cloud Computing (Artetio, 2008).

ISO/IEC 27018: Se trata de un compendio de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing (Artetio, 2008, pág. 98).

ISO/IEC 27031: Es una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio (Sánchez L. S.-O., 2012, pág. 90).

ISO/IEC 27032: Proporciona orientación para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad, concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas (CIIP) (ISO27000.ES, 2005).

ISO/IEC 27033: Norma enfocada a la seguridad en redes, se conforma de 7 partes: 27033-1, conceptos generales; 27033-2, directrices de diseño e implementación de seguridad en redes; 27033-3, escenarios de referencia de

redes; 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad; 27033-5, aseguramiento de comunicaciones mediante VPNs; 27033-6, convergencia IP; 27033-7, redes inalámbricas (ISO27000.ES, 2005).

ISO/IEC 27034: Norma dedicada a la seguridad en aplicaciones informáticas, consistente en 5 partes: 27034-1, conceptos generales; 27034-2, marco normativo de la organización; 27034-3, proceso de gestión de seguridad en aplicaciones; 27034-4, validación de la seguridad en aplicaciones; 27034-5, estructura de datos de protocolos y controles de seguridad de aplicaciones (Artetio, 2008, pág. 156).

ISO/IEC 27035: Gestión de incidentes de seguridad en la información (ISO27000.ES, 2005).

ISO/IEC 27036: Guía en cuatro partes de seguridad en las relaciones con proveedores: 27036-1, visión general y conceptos; 27036-2, requisitos comunes; 27036-3, seguridad en la cadena de suministro TIC; 27036-4, seguridad en outsourcing (externalización de servicios) (ISO27000.ES, 2005).

ISO/IEC 27037: Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en dispositivos electrónicos (ISC2, 2013, pág. 345).

1.8.2. Norma Técnica Ecuatoriana INEN ISO/IEC 27001:2010

En el Ecuador, el Instituto Ecuatoriano de Normalización (INEN) se encarga, entre otras actividades, adaptar al país las normas publicadas por la ISO. Para el caso de algunas normas, entre ellas la ISO/IEC 27001:2005, esta adaptación básicamente consistió en convocar a representantes de distintas organizaciones, entre ellas sector público y universidades con la finalidad de

conformar Comités Técnicos con la tarea de traducir la Norma Internacional publicada por la ISO y posteriormente hacerla pública mediante Registro Oficial del Ecuador.

En base a lo indicado, a partir del Estándar Internacional ISO/IEC 27001:2005, nació la Norma Técnica Ecuatoriana (NTE) ISO/IEC 27001:2010, misma que, es idéntica a la norma internacional solo que traducida al español adaptado al Ecuador.

1.8.3. Definición del SGSI

Un SGSI es parte del sistema gerencial general, basada en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información (Instituto Ecuatoriano de Normalización, 2010, pág. 23).

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de controles que han sido metodológicamente implementados bajo un enfoque de riesgo comercial cuya finalidad es asegurar la confidencialidad, integridad y disponibilidad de los activos de información (Asociación Española de Normalización, 2013, pág. 64).

1.8.4. Ciclo PHVA

El ciclo de la mejora continua puede ser aplicado a cualquier proceso o actividad, para la gestión de la seguridad de la información, el PHVA implica planear las acciones, implementar lo planeado, revisar lo implementado y corregir lo revisado.

De acuerdo con lo estipulado en la ISO/IEC 27001:2005 (o como se lo analizó, en la Norma Técnica Ecuatoriana INEN ISO/IEC 27001:2010), el PHVA es:

Planear:

Haciendo una concordancia entre el proceso de planeación de un Sistema de Gestión de Seguridad de la Información con los capítulos de la ISO/IEC 27001, esta fase de la mejora continua estaría plasmada en el punto 4.2.1. Establecer el SGSI (Instituto Ecuatoriano de Normalización, 2010, pág. 20) donde debe hacerse lo siguiente:

- Definir el alcance y los límites del Sistema de Gestión de Seguridad de la Información.
- Definir una política del Sistema de Gestión de Seguridad de la Información.
- Definir un enfoque de evaluación de riesgos (se puede apoyar en ISO/IEC 27005)
- Identificar, analizar y evaluar los riesgos
- Identificar planes de tratamiento de los riesgos identificados
- Seleccionar objetivos de control y controles para el tratamiento de los riesgos (Anexo A)

Debido a que la planeación es la base fundamental de todo sistema, cualquier falla, error, omisión o mala interpretación al momento de realizar las actividades indicadas podría derivar en fallas de estructura de todo el SGSI.

Hacer:

El cumplimiento de esta actividad se encuentra enmarcado en el punto 4.2.2, Implementar y Operar el SGSI (Instituto Ecuatoriano de Normalización, 2010, pág. 21):

- Generar un plan de tratamiento de riesgos, en función de las opciones de tratamiento elegidas y de los controles seleccionados.

- Implementar el plan de tratamiento de riesgos, considerando recursos, roles y responsabilidades.
- Implementar controles seleccionados del Anexo A de la ISO/IEC 27001, sabiendo que, un control administrativo debe estar soportado por controles técnicos y físicos, así como por capacitación y difusión.
- Definir métricas enfocadas al monitoreo y mejora de los controles implementados, puede utilizarse ISO/IEC 27004.
- Implementar programas de capacitación y toma de conciencia.
- Operar el Sistema de Gestión de Seguridad de la Información.
- Gestionar los recursos que demanda el Sistema de Gestión de Seguridad de la Información.
- Implementar controles de gestión incidentes de seguridad de la información.

Verificar:

La verificación está plasmada en el punto 4.2.3, Monitorear y Revisar el SGSI (Instituto Ecuatoriano de Normalización, 2010, pág. 22):

- Ejecutar procedimientos de monitoreo y revisión.
- Realizar revisiones regulares de la efectividad del Sistema de Gestión de Seguridad de la Información.
- Medir efectividad de los controles implementados.
- Revisar a intervalos planeados la evaluación de riesgos de la organización, incluyendo riesgo residual y riesgo aceptable.
- Realizar auditorías internas a todo el sistema de gestión de la seguridad de la información.
- Realizar revisiones gerenciales para asegurar que el alcance aún es el adecuado y para asegurarse que se identifican mejoras (también señalado en el punto 7. de la ISO/IEC 27001:2005 Revisión Gerencial del SGSI, pp. 28).

- Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión.
- Registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del sistema de gestión de la seguridad de la información.

Actuar:

Se refiere al punto 4.2.4, Mantener y Mejorar el SGSI (Instituto Ecuatoriano de Normalización, 2010, pág. 23), donde se indica que regularmente debe hacerse lo siguiente:

- Implementar las mejoras identificadas al Sistema de Gestión de Seguridad de la Información.
- Tomar acciones correctivas y preventivas apropiadas (también señalado en el punto 8. Mejoramiento Continuo)
- Comunicar los resultados a las partes interesadas.
- Asegurar que las mejoras implementadas logren sus objetivos señalados.

1.8.5. Estructura

La ISO/IEC 27001:2005 o la NTE INEN ISO/IEC 27001:2010, tienen exactamente la misma estructura conformada por requisitos para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información (capítulos del 4 al 8) y todos los controles que deben formar parte de dicho sistema (Anexo A) en función de su aplicabilidad, así como de los anexos a la norma, todos estos componentes de describen a continuación:

1.8.5.1. Requisitos

Aunque tradicionalmente se conoce que los requisitos de un SGSI parten desde el capítulo 4 y terminan en el capítulo 8 de la ISO/IEC 27001:2005, la norma empieza en el capítulo 0, por lo tanto, no debe descuidarse o pasarse por alto ningún capítulo.

A continuación, un análisis de alto nivel con respecto a los requisitos que según la ISO/IEC 27001:2005 (o la NTE INEN ISO/IEC 27001:2010) un Sistema de Gestión de Seguridad de la Información debe cumplir, sabiendo que todos los requisitos deben ser implementados:

- Ciclo de Vida: Un sistema de gestión, por naturaleza debe evidenciar la existencia de un ciclo de vida basado en el Planear, Hacer, Verificar, Actuar, donde por cada fase se tienen actividades determinadas, mismas que fueron citadas en el punto anterior. (Sánchez L. S.-O.-M., 2011, pág. 156).

- Documentación: El Sistema de Gestión de Seguridad de la Información debe estar basado en documentos, es así que, el alcance, el inventario de activos de información, los entregables del análisis de riesgos, políticas, normativas, procedimientos y demás documentación del proyecto deben haber sido diseñados, revisados, formalizados y difundidos. Cabe recalcar que se considera como documento a uno físico, digital, sea en texto o grabación de audio o video (SGS, 2013, págs. 97-98).

- Compromiso de la Dirección: De acuerdo a lo que indica la ISO/IEC 27001:2005, en el Capítulo 5, es responsabilidad de la gerencia proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo,

revisión, mantenimiento y mejoramiento mediante el establecimiento de controles, proporcionando recursos, decidir el nivel aceptable de riesgos, etc. (SGS, 2013, pág. 56).

- Auditorías Internas: Auditar el SGSI para determinar si los controles son satisfactorios (Asociación Española de Normalización, 2013, pág. 128).

1.8.5.2. Controles

Para tratar los riesgos de seguridad de la información, existe un grupo de controles que en base a los resultados del análisis de riesgos deben ser implementados en función de su aplicabilidad para la organización, dichos controles se encuentran descritos en el Anexo A de la norma, sin embargo, el detalle de cada uno de estos se profundiza en la ISO/IEC 27002.

En lo que tiene que ver a los controles, el Anexo A de la ISO/IEC considera 11 dominios de control que contienen 39 objetivos de control que a su vez se apoyan en 133 controles.

Cabe recalcar que al momento de revisar la Norma ISO/IEC 27001, un lector se percatará que el Anexo A inicia desde A.5 y no desde A.1; este supuesto salto de numeración se debe a que el Anexo A mantiene la numeración de la ISO/IEC 27002, en donde, los controles inician desde el capítulo 5.

A continuación, la descripción de cada uno de los 11 dominios de control (ISO27000.ES, 2005):

- **A5. Política de seguridad de la información (contiene 2 controles)**

El objetivo de este dominio es principalmente tener un instrumento que denote claramente la intención de la alta gerencia de la organización con respecto a la seguridad de la información bajo consideraciones legales, comerciales y de cumplimiento regulatorio, es por esto que, una política de seguridad de la información debe estar claramente definida, aprobada por la gerencia general y difundida en toda la organización, así mismo, todos los funcionarios y terceros relacionados deben conocerla y aceptar su cumplimiento.

- **A6. Organización de la seguridad de la información (contiene 11 controles)**

Este dominio tiene como foco una organización formal de la función de seguridad de la información como un proceso de la organización, es así que, como todo proceso, requiere actores (tanto internos como terceras partes), directrices, asignaciones, compromisos y responsabilidades soportadas por la alta gerencia, además, señala que al ser complementaria a los otros procesos, la seguridad de la información requiere también la participación de los diferentes representantes de los procesos de la organización.

Cabe señalar que este dominio exige la forma de acuerdos de confidencialidad así como la revisión independiente de la seguridad de la información.

- **A7. Gestión de activos de información (contiene 5 controles)**

Este dominio tiene como objetivo la identificación de los activos de información de la organización (de los procesos que forman parte del alcance del Sistema de Gestión de Seguridad de la Información), siendo necesario indicar que un activo de información es todo lo que procesa, genera o almacena información relacionada a los distintos procesos de negocio, es así que, estos activos pudieran ser hardware, software, documentos físicos, documentos electrónicos o personas.

Cada uno de los activos de información debe tener un propietario o un responsable designado por la organización, cuya responsabilidad entre otras, es clasificar el activo en función de su valor, la dependencia del negocio hacia este, requisitos legales, etc., para determinar su criticidad, sensibilidad y etiquetado con la finalidad de aplicar reglas para su uso aceptable (controles).

- **A8. Seguridad de los recursos humanos (contiene 9 controles)**

Este dominio es el nexo entre la seguridad de la información y la administración del activo de información más importante, las personas, es por esto que dentro de este se abarcan controles relacionados a la selección de personal, vinculación, asignación de recursos para el funcionario, esquema de sanciones y desvinculaciones.

Los controles que forman parte de este control se orientan a que las personas conozcan sus roles y responsabilidades en

seguridad de la información, las mismas que deben estar claramente definidas y documentadas.

Se enfocan también a que toda persona que forma parte de la organización debe pasar por un proceso de selección donde se consideren aspectos legales, regulatorios y de ética, todo esto, en función de las exigencias de la organización y del cargo.

Con respecto a las funciones del empleado, este dominio plantea que existan acuerdos contractuales donde se especifiquen los términos y condiciones de la relación laboral, además, que se les dé el entrenamiento necesario y que se les asigne lo que necesitan para ejercer sus funciones.

Un aspecto probablemente conflictivo dentro de las organizaciones, es que este dominio exige un proceso disciplinario para quienes violen la seguridad de la información.

Con respecto a la terminación de la relación laboral, se obliga al funcionario la devolución de todos los activos de información que la organización le entregó para el ejercicio de sus funciones, incluyendo la deshabilitación de accesos a recursos tecnológicos.

- **A9. Seguridad física y ambiental (contiene 13 controles)**

El objetivo de este dominio es prevenir el acceso físico no autorizado, así como, evitar daños e interferencias en las instalaciones y activos de información.

Dentro de este dominio se consideran controles de seguridad física como puertas, archivadores, lectores biométricos, cámaras de seguridad, etc.

Dentro de lo que tiene que ver a seguridad ambiental, este dominio considera reguladores de voltaje, detectores y extintores de incendios, controles contra inundaciones, cableado seguro, transporte de equipos fuera de las instalaciones, etc., además, con respecto a los controles existentes, obliga a que estos sean monitoreados, revisados y que exista soporte.

- **A10. Gestión de operaciones y comunicaciones (contiene 32 controles)**

Este dominio busca asegurar la operación correcta y segura de los activos de información, es por esto que, un aspecto muy importante es que las organizaciones cuenten con procedimientos operativos documentados, recalcando que, documentado quiere decir diseñado, formalizado, difundido y conocido por sus actores.

La gran cantidad de controles que hacen este dominio tienen un enfoque de gestión y operación tecnológica, es así que demanda separar ambientes de pruebas y producción, exige la existencia de segregación de funciones a nivel de las distintas tareas de los procesos (no necesariamente de tecnología), demanda la aceptación del negocio antes de cualquier cambio en ambientes de producción, la seguridad contra código malicioso, respaldos de información, seguridad en la infraestructura de red, gestión de medios de almacenamiento de información, intercambio de información , comercio electrónico y monitoreo.

- **A11. Control de acceso (contiene 25 controles)**

El objetivo general de este dominio es regular y restringir la interacción entre sujetos y objetos a nivel lógico a través de la adecuada gestión de usuarios, contraseñas y perfiles de acceso

tanto a aplicaciones, redes y sistemas operativos, el bloqueo de equipos, caducidad de sesiones y teletrabajo.

- **A12. Adquisición, desarrollo y mantenimiento de sistemas de información (contiene 16 controles)**

Procurar que la seguridad sea una parte integral de los sistemas de información asegurando que en etapas tempranas de los proyectos de desarrollo de software se consideren requisitos de seguridad, validación para el adecuado procesamiento de datos, criptografía, datos de prueba, archivos sensibles y críticos de las aplicaciones, asegurando los códigos fuente, gestionando y probando todo cambio realizado, restricciones de acceso o gestión de vulnerabilidades técnicas.

- **A13. Gestión de incidentes de seguridad de información (contiene 5 controles)**

Este dominio se orienta a asegurar que los eventos y debilidades de seguridad de información sean comunicados de manera tal que, permita una acción oportuna tanto para mitigar el impacto así como para dar una solución definitiva encaminada a que no se vuelva a dar el evento, es por eso que, debe existir un canal conocido y habilitado para reportar incidentes de seguridad de la información, así mismo, deben estar claramente definidos los responsables para dar tratamiento a dichos incidentes.

- **A14. Gestión de continuidad de operaciones (contiene 5 controles)**

Su objetivo principalmente está enfocado a todas las estrategias, incluyendo roles y responsabilidades que la organización debe

ejecutar en caso de desastres que comprometan o interrumpan la continuidad de las operaciones de negocio.

- **A15. Cumplimiento regulatorio (contiene 10 controles)**

Su objetivo es evitar que la organización incumpla cualquier ley, estatuto, obligación, reglamento u obligación contractuales, así como, cualquier aspecto regulatorio que pudiera aplicar, como, propiedad intelectual, ley de contratación pública, ley de comercio electrónico y firma digital, Acuerdo 166, Constitución de la República del Ecuador, etc.

1.8.5.3. Anexos

Habiendo analizado tanto los requisitos como los controles del Anexo A, es necesario indicar que la ISO/IEC 27001:2005 también contiene el Anexo B y el Anexo C.

En el Anexo B está la relación entre los apartados de la ISO/IEC 27001 y los principios de buen gobierno de la OCDE (Organización para la Cooperación y el Desarrollo Económicos, fundada en 1961, agrupa a 34 países miembros y su misión es promover políticas que mejoren el bienestar económico y social de las personas alrededor del mundo) (Instituto Ecuatoriano de Normalización, 2010, pág. 34).

El Anexo C dicta la correspondencia entre las normas ISO/IEC 9001 e ISO/IEC 14001 con la ISO/IEC 27001.

1.8.6. Beneficios del SGSI

Los beneficios de un sistema de Gestión de la Seguridad de la Información adecuadamente implementado, con eficiente operación, en constante mantenimiento y con mejora continua tienen impacto en toda la organización:

- El principal beneficio es el cambio de cultura organizacional porque para implementar y aplicar controles se realizan campañas de difusión y capacitación permanentes, los involucrados obtienen una visión más amplia de las amenazas, las vulnerabilidades, los riesgos y sobre todo, consecuencias de incidentes de seguridad de la información, es así que, el cambio de cultura se da al existir la necesidad de aplicar la seguridad de la información tanto en sus labores diarias como en su vida personal (Asociación Española de Normalización, 2013, pág. 67).

- El análisis de riesgos que la organización ejecuta al implementar su Sistema de Gestión de Seguridad de la Información, en el cual, se analiza a profundidad los procesos de negocio con el fin de identificar los activos de información, amenazas, vulnerabilidades e impactos en la actividad empresarial, genera mayor conocimiento del negocio y su dependencia de los activos de información (ISO/IEC, ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management , 2011, pág. 32).

- La reducción de costos debido a la existencia de un adecuado tratamiento de los incidentes de seguridad y se mitigará al máximo la probabilidad de que algo similar ocurra en el futuro, además, mediante la implementación de controles, los usuarios utilizarán adecuadamente los activos que la

organización les asigne para realizar su trabajo (SGS, 2013, pág. 78).

- El cumplimiento de requisitos legales y regulatorios ya que debe haber una identificación meticulosa de los mismos y su cumplimiento es exigido y monitoreado como parte del Sistema de Gestión de la Seguridad de la Información (Instituto Ecuatoriano de Normalización, 2010, pág. 21).

1.9. Norma Internacional ISO/IEC 27001:2013

El estándar ISO/IEC 27001:2013 es la nueva versión que fue liberada en octubre del 2013, sin embargo, es necesario recalcar que la Secretaría Nacional de la Administración Pública del Ecuador ha basado el Acuerdo 166 en la NTE INEN ISO/IEC 27001:2010, misma que a su vez es igual a la ISO/IEC 27001:2005, sin embargo, en caso de que una organización del sector público opte por implementar la ISO/IEC 27001:2013 cumpliría a su vez con lo expuesto en el Acuerdo 166.

1.9.1. Visión general de la ISO/IEC 27001:2013

El segundo semestre del año 2013 se publica la nueva versión de las normas ISO/IEC 27001 y 27002, incluyendo el año de publicación a continuación del nombre de la norma: ISO/IEC 27001:2013 y ISO/IEC 27002:2013.

La nueva versión de la ISO7IEC 27001, ha sido estructurada con 10 capítulos (en lugar de 8 que tenía la versión del 2005):

- Alcance
- Referencias Normativas
- Términos y definiciones
- Contexto de la Organización y Partes Interesadas

- Liderazgo en Seguridad de la Información y Soporte a la Política
- Planificación del Sistema de Gestión de Seguridad de la Información
- Apoyo al Sistema de Gestión de Seguridad de la Información
- Operación del Sistema de Gestión de Seguridad de la Información
- Evaluación del desempeño del Sistema de Gestión de Seguridad de la Información
- Acción Correctiva

Además, la nueva versión también tiene un Anexo A donde se referencian los controles de la ISO/IEC 27002:2013 (siendo ahora 14 en lugar de 15 objetivos de control):

- A.5 Políticas de seguridad de la información (2 controles)
- A.6 Organización de la seguridad de la información (7 controles)
- A.7 Seguridad de los recursos humanos (6 controles)
- A.8 Gestión de los Activos (10 controles)
- A.9 Control de acceso (14 controles)
- A.10 Criptografía (2 controles)
- A.11 Seguridad física y medioambiental (15 controles)
- A.12 Seguridad de las operaciones (14 controles)
- A.13 Seguridad de las comunicaciones (7 controles)
- A.14.1Adqusición, desarrollo y mantenimiento del sistema (13 controles)
- A.15 Relación con los proveedores (5 controles)
- A.16 Gestión de los incidentes de seguridad de la información (7 controles)
- A.17 Gestión de los aspectos de la seguridad de la información para la continuidad del negocio (4 controles)

- A.18 Cumplimiento (8controles)

1.9.2. Diferencias entre NTE INEN ISO/IEC 27001:2010 y la ISO/IEC 27001:2013

Tabla No. 1: Diferencias entre la NTE INEN ISO/IEC 27001:2010 e ISO/IEC 27001:2013

NTE INEN ISO/IEC 27001:2010	**ISO/IEC 27001:2013**
REQUISITOS	
Desaparecen	**Aparecen**
Acciones preventivas	Cláusula 6.1.2 c) que exige identificar los dueños de los riesgos
	Cláusula 4.2 que exige el conocimiento de las necesidades y expectativas de las partes interesadas.
CONTROLES	
Desaparecen	**Aparecen**
A.6.2.2 Seguridad cuando se trata de clientes	A.6.1.5. Seguridad de la Información en la Gestión de Proyectos
A.10.4.2 Controles contra códigos móviles	A.14.2.1 Política para Desarrollo Seguro
A.10.7.3 Procedimientos para manejo de la información	A.12.2.5 Principios para ingeniería segura de sistemas
A.10.7.4 Seguridad de la documentación del sistema de información	A14.2.6 Ambiente de desarrollo seguro

NTE INEN ISO/IEC 27001:2010	ISO/IEC 27001:2013
A.10.8.5 Sistemas de Información de Negocios	A.14.2.8 Pruebas seguras del sistema
A.10.9.3 Información pública	A.16.1.4 Evaluación de una decisión sobre eventos de seguridad de la información
A.11.4.2 Autenticación de usuario para conexiones externas	A.17.2.1 Disponibilidad de las facilidades donde se procesa información
A.11.4.3 Identificación de los equipos en las redes	
A.11.4.4 Protección de puertos de diagnóstico y configuración remota	
A.11.4.6 Control de conexión a las redes	
A.11.4.7 Control de enrutamiento en la red	
A.12.2.1 Validación de los datos de entrada	
A.12.2.2 Control al procesamiento interno	
A.12.2.3 Autenticación de mensajes	
A.12.2.4 Validación de los datos de salida	
A.11.5.5 Sesión inactiva	
A.11.5.6 Limitación del tiempo de conexión	
A.11.6.2 Aislamiento de sistemas relevantes	

NTE INEN ISO/IEC 27001:2010	ISO/IEC 27001:2013
A.12.5.4 Fuga de información	
A.14.1.2 Continuidad del negocio y evaluación de riesgos	
A.14.1.3 Desarrollo e implementación del plan de continuidad incluyendo seguridad de la información	
A.14.1.4 Planeación de la estructura de la continuidad del negocio	
A.15.1.5 Protección del uso inadecuado de los recursos de procesamiento de la información	
A.15.3.2 Protección de las herramientas de auditoría de sistemas de información	
ANEXOS	
Desaparecen	**Aparecen**
Anexo B	
Anexo C	

1.9.3. Proceso de transición a la NTE INEN ISO/IEC 27001:2010 a la ISO/IEC 27001:2013

Una organización que ya posea la Certificación ISO/IEC 27001:2005 tendrá un periodo de 2 años para migrar a la nueva versión, esto es, hasta septiembre del año 2015 (Asociación Española de Normalización, 2013, pág. 74).

Para organizaciones que hayan implementado su Sistema de Gestión de Seguridad de la Información según los requisitos de ISO/IEC 27001:2005 y que requieran actualizar su sistema a la versión 2013, a continuación, un análisis de tareas que se recomienda realizar:

- Identificar todas las partes interesadas en seguridad de la información:

  Es muy importante que la organización identifique y enliste todas las partes interesadas en la seguridad de la información tales como clientes, proveedores, socios comerciales, accionistas, entes de regulación, funcionarios, comunidad, etc.

  Una vez identificadas las partes interesadas, se debe identificar sus requerimientos y necesidades tales como contratos, mandatos, leyes, expectativas.

  Los insumos indicados serán utilizados para definir los objetivos del sistema de gestión de la seguridad de la información cuyo fin será satisfacer a las partes interesadas, principalmente al negocio debió a que es mandatorio alinear los objetivos del SGSI (o del EGSI) con los objetivos estratégicos de la organización.
- Redefinir el alcance del Sistema de Gestión de Seguridad de la Información

  De acuerdo a la versión 2013 de la ISO/IEC 27001, es necesario además definir los vínculos y las interacciones entre las actividades propias ejecutadas por la organización y las actividades ejecutadas por terceras partes.
- Hacer cambios pertinentes a la metodología de evaluación de riesgos de seguridad de la información

  Con respecto a la versión 2005, esta nueva obliga la identificación de los dueños de los riesgos, los cuales podrían ser los mismos que los dueños de los activos siempre y cuando pertenezcan al nivel estratégico o nivel táctico.

Es necesario también considerar los riesgos relacionados a los procesos que la organización contrata a terceros y la forma de controlarlos.

- Declaración de Aplicabilidad
  En el documento donde se enlistan los controles aplicables, debe aumentarse una nueva columna que indique si el control, por ejemplo, está implementado, está planeado ser implementado o si está parcialmente implementado, obviamente, se deberá tener evidencia de cada uno.
- Aprobación de los dueños de los riesgos
  La versión 2013 indica que los dueños identificados de los riesgos deben ser quienes aprueben el Plan de Tratamiento de Riesgos y el Riesgo Residual (ISO/IEC, ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements , 2013, págs. 23-26).
- Decidir qué se hará con los documentos obsoletos
  El cambio de versión resultará también en ciertos documentos en desuso, por ejemplo, la versión 2013 no exige control sobre acciones preventivas o auditorías internas, por lo que la organización puede decidir si lo conserva o no, sin embargo, debe saber que si opta por mantenerlos, estos son sujeto de ser auditados.
- Reorganizar los controles existentes

Un cambio de versión implica que en un punto la organización tendrá controles tanto de la versión 2005 como de la versión 2013, sin embargo, lo importante es establecer un adecuado proceso de migración para evitar redundancia de controles, o, posible ausencia de estos.

1.10. Proceso de Certificación

Una organización puede certificar su Sistema de Gestión de Seguridad de la Información mediante una auditoría de tercera parte de acuerdo con lo siguiente:

1.10.1. La Certificación ISO/IEC 27001

La certificación internacional ISO/IEC 27001 es un reconocimiento emitido por un tercero llamado entidad certificadora, este certificado es una garantía de que el Sistema de Gestión de Seguridad de la Información cumple con los requisitos que demanda la norma, los mismos que se orientan al diseño, implementación, operación, mantenimiento y mejora continua (SGS, 2013, pág. 23).

1.10.2. Camino a seguir para obtener el certificado

Una organización que desee obtener una certificación ISO/IEC 27001 debe realizar las siguientes actividades (Asociación Española de Normalización, 2013, pág. 12):

- Diseñar e implementar un Sistema de Gestión de Seguridad de la Información en base a todos los requisitos de la norma, sin descuidar ninguno de sus capítulos.
- Los controles que surjan de la evaluación de riesgos deben ser implementados considerando que todo control administrativo necesita de una base otorgada por un control técnico o físico.
- Capacitar al personal y generar la cultura de seguridad de la información.
- Realizar auditorías internas o pre auditorías, manteniendo la premisa de que nadie debe auditar su propio trabajo.

- Cuando la organización tenga sus controles maduros, personal capacitado y disciplinado, puede optar por contratar los servicios de la entidad certificadora que tiene auditores certificados para el caso.
- La entidad certificadora realiza la auditoría en una fase inicial con un enfoque documental y una fase final que es una auditoría en sitio.
- La auditoría de certificación genera un informe que será utilizado por la certificadora para que, ante un ente superior llamado acreditadora se recomiende la otorgación del certificado ISO/IEC 27001 al Sistema de Gestión de Seguridad de la Información de la Organización.
- La acreditadora a su vez tiene procesos internos de validación.
- Finalmente, con la autorización de la acreditadora, la entidad de certificación emite el certificado.

Cabe señalar que un Certificado ISO/IEC 27001 tiene una vigencia de 3 años contados a partir de su emisión, y que además, la entidad certificadora realizará auditorías anuales de seguimiento (2 auditorías), es por eso que, al finalizar el tercer año, la organización decide si se recertifica o no, es así que durante este periodo, dependiendo de los hallazgos en las auditorías de seguimiento, una certificación puede ser revocada (ISO27000.ES, 2005).

1.10.3. Valor agregado de la Certificación ISO/IEC 27001

Una entidad que obtiene la certificación ISO/IEC 27001, además de los beneficios propios del SGSI, se ve beneficiada en los siguientes aspectos (SGS, 2013, pág. 45):

- Ventaja Competitiva: La certificación ISO/IEC 27001, dependiendo de la organización y de su industria, así como de las exigencias comerciales de sus clientes puede obtener gran

ventaja competitiva con respecto a la competencia, incluso, tendría un valor adicional para el cumplimiento de licitaciones.

- Excelencia en la Gestión: Básicamente este beneficio se materializa ya que al tener un enfoque de personas, procesos y tecnología se estaría optimizando recursos y tiempos de respuesta por medio de los controles implementados, es así que, se genera mayor confianza en los clientes.

- Mejora Continua: Por las exigencias inherentes a una certificación ISO/IEC 27001, las organizaciones están obligadas a revisar contantemente su sistema de gestión enmarcando sus mediciones en el ciclo de mejora continua.

- Imagen y Reputación: El aumento del valor comercial y mejora de la imagen y reputación de la organización es otro de los beneficios que se asocia a la disminución u óptimo tratamiento de incidentes de seguridad de la información, se genera mejor servicio, los procesos de negocio maduran considerablemente y los activos de información son controlados, a nivel comercial.

1.10.4. Entidades de Certificación

Las entidades que se encuentran acreditadas y autorizadas para realizar auditorías de tercera parte (de certificación) en el Ecuador, deben estar reconocidas por el Organismo Ecuatoriano de Acreditación (OAE).

Cabe señalar que para la Certificación ISO/IEC 27001, ningún organismo ecuatoriano se encuentra acreditado como entidad certificadora, existen entidades internacionales con representación en el Ecuador como por ejemplo, SGS, Bureau Veritas y AENOR.

CAPÍTULO 2. MARCO DE REFERENCIA PARA DISEÑO E IMPLEMENTACIÓN DEL EGSI

2.1. Análisis del Acuerdo Ministerial Número 166 y del EGSI

El mes de septiembre del año 2013 la Secretaria Nacional de la Administración Pública (SNAP), hizo público en el Registro Oficial No. 88 el Acuerdo Ministerial No. 166; en el que se dispone que todas las entidades Públicas y que dependan de la Función Ejecutiva utilicen obligatoriamente las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información (Secretaría Nacional de la Administración Pública, 2013, pág. 1).

Este Acuerdo dispone diseñar e implementar el Esquema Gubernamental de Seguridad de la Información (EGSI), y, su implementación está en función de los siguientes hitos:

- Designar un Comité de Seguridad de la Información, que debe estar liderado por el Oficial de Seguridad de la Información, este hito debió cumplirse hasta el 30 de octubre del año 2013.
- Implementación de controles prioritarios, hasta el 31 de marzo del 2014.
- Hasta el 30 de septiembre del 2015, deberá estar implementado todo el EGSI.

Fuera de los hitos señalados, mismos que deben ser ejecutados por las distintas entidades públicas, la SNAP también adquiere ciertos compromisos, los cuales básicamente están enfocados a coordinación y seguimiento:

- Recibir por parte de las entidades públicas un comunicado acerca de la designación del Oficial de Seguridad de la Información de cada institución.

- Coordinar y dar seguimiento a la implementación del EGSI mediante el Sistema de Gestión por Resultados (GPR) y otras herramientas que pudiera utilizar la SNAP.
- Realizar revisiones anuales al EGSI.
- Definir metodologías o procedimientos para actualización, implementación, seguimiento y control del EGSI.
- Recibir del Oficial de Seguridad de la Información de las distintas instituciones propuestas para incluir controles o directrices adicionales al EGSI.
- Definir metodologías o procedimientos para actualización, implementación, seguimiento y control del EGSI.

Con respecto al último compromiso, existe cierto vacío por parte del SNAP ya que hasta la fecha de documentación de este proyecto de titulación que no ha publicado dichas metodologías o procedimientos conforme lo establece la Disposición Transitoria Tercera del Acuerdo 166.

2.2. Situación Actual del Cumplimiento del Acuerdo 166 en el Ecuador

Con la finalidad de llevar un reporte y control de los distintos proyectos y programas de las instituciones del Estado, la Secretaría de la Administración Pública utiliza el sistema de Gobierno por Resultados (GPR), y, debido a que la implementación del EGSI es obligatoria, su avance debe ser registrado en este sistema, es por esto que se creó un programa institucional llamado "Gestión de la Seguridad de la Información en las Entidades de la Administración Pública Central Institucional y Dependiente de la Función Ejecutiva".

En base a lo indicado, la Secretaría Nacional de la Administración Pública con corte a 25 de marzo del 2014 tomó como referencia los datos ingresados por las distintas entidades en el sistema de Gobierno por Resultados (GPR) y generó un Ranking de Entidades Públicas con respecto al cumplimiento de la implementación del Esquema Gubernamental de la Información (el documento

se encuentra como Anexo 1), los resultados son los siguientes (Secretaría de la Administración Pública, 2014):

- De ciento veinte y seis (126) instituciones, solamente una (1) de ellas, lo que corresponde al 0,7% ha implementado su EGSI en un 96.83%, lo cual para el SNAP es un nivel de cumplimiento alto.
- Alrededor del 5,6% de entidades (7 de las 126 listadas) tienen un nivel de cumplimiento medio, esto es, entre el 75% y 89% del EGSI implementado.
- Otro 5,6% de entidades tiene un nivel de cumplimiento regular con un margen de implementación del EGSI situado entre el 50% y 74%.
- El 88,1% de entidades restantes tiene un cumplimiento considerado bajo, lo cual es no tener el 50% de su EGSI implementado, este porcentaje corresponde a ciento once (111) entidades.

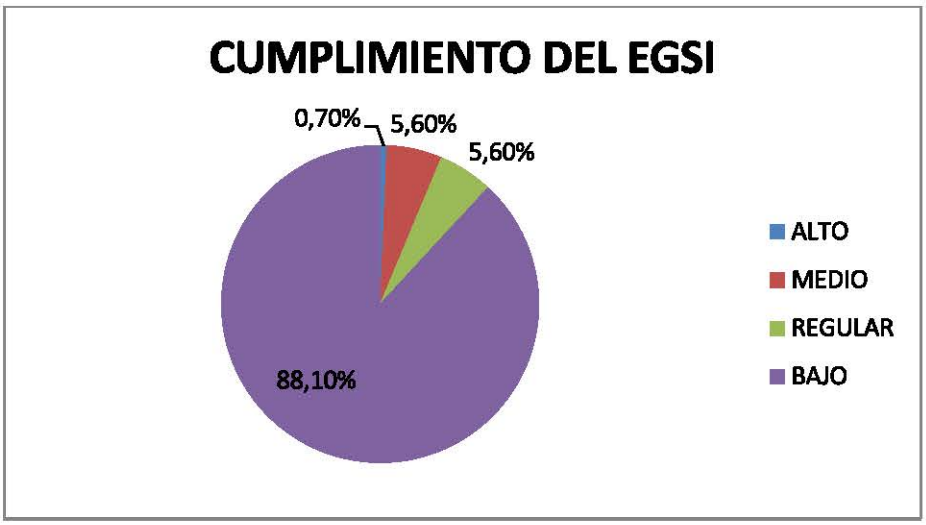


Figura No. 1: Porcentaje de Cumplimiento del EGSI

Considerando los hitos dispuestos por la Secretaría Nacional de la Administración Pública para el cumplimiento del Acuerdo Ministerial 166, y tomando como referencia el ranking publicado, se puede determinar que no ha

existido el cumplimiento esperado y dispuesto, es por esto que este proyecto de titulación apunta a ser una base de apoyo para que las entidades públicas diseñen e implementen su Esquema de Seguridad de la Información solucionando así el problema planteado.

Una vez publicado el Ranking de Cumplimiento del EGSI por el SNAP (Referencia Anexo 1) con corte a 25 de marzo del 2014, se seleccionaron (por afinidad) a siete (7) de las ciento veinte y seis (126) entidades listadas para conocer su opinión y retroalimentación del resultado publicado en el mencionado documento (para acceder a las entrevistas, ninguno de los representantes autorizó la publicación de su nombre o del nombre de la institución).

Debido al tamaño de la muestra, los resultados obtenidos en estas entrevistas no necesariamente reflejan la realidad de toda la población, como si lo hace el Ranking publicado por el SNAP.

Las entrevistas se basaron en las siguientes preguntas:

1. ¿Considera que la implementación del EGSI dará valor a la organización?
2. ¿Cuentan con el conocimiento y la experiencia para llevar a cabo este tipo de proyectos?
3. ¿La institución ya cuenta con un Oficial de Seguridad de la Información?
4. ¿Cuál es su opinión con respecto a la disposición de implementar el EGSI hasta septiembre del 2015?
5. ¿Cuál es la prioridad que la institución le ha dado al proyecto de diseño e implementación del EGSI, considerando las fechas dispuestas en el Acuerdo Ministerial No. 166?

6. ¿Considera que el EGSI es suficiente para gestionar los riesgos asociados a la confidencialidad, integridad o disponibilidad de los activos de información de la entidad?

Los resultados obtenidos se resumen en lo siguiente:

- La implementación del EGSI, en cinco (5) de las siete (7) instituciones entrevistadas, aún no ha sido visto como algo que genere valor a la organización, en lugar de eso, el personal tiene la concepción de que esto les quitará tiempo útil para desempeñar las funciones inherentes a su cargo, especialmente porque no cuentan con un Oficial de Seguridad de la Información.
- De los siete (7) entrevistados, dos (2) indicaron que en sus organizaciones hay el conocimiento y la experiencia para ejecutar el proyecto de diseño e implementación del EGSI; una institución tiene personal propio mientras que otra tiene una persona contratada por un año bajo servicios profesionales cuya función es solamente implementar el EGSI.
- De las siete (7) instituciones, solamente una (1) tiene un Oficial de Seguridad de la Información nombrado y que cumple con el perfil, el resto, o no tiene, o nombró un Oficial solamente por dar cumplimiento al Artículo 3 del Acuerdo Ministerial 166 (comunicar la designación del Oficial de Seguridad de la información al SNAP), esto genera que los Oficiales nombrados no tengan el perfil y no cumplan con las funciones inherentes al cargo.
- Todos los entrevistados indicaron no estar de acuerdo con la disposición de implementar el EGSI bajo lo estipulado en el Acuerdo 166 ya que no existe el personal, no se tiene la experiencia, no se tiene el presupuesto, y, sobre todo, ya existe priorización de proyectos hasta la fecha límite (septiembre 2015), en resumen, se tiene la percepción de que para implementar el

EGSI es necesario dejar de hacer ciertas tareas de mayor importancia para las instituciones.

- Solamente uno (1) de los siete (7) entrevistados indicó que se ha dado prioridad al EGSI, sin embargo, para avanzar con las actividades fue necesario contratar un profesional específicamente para este proyecto bajo el esquema de servicios profesionales, caso contrario, no se lo hubiera logrado.
- Ninguno de los entrevistados considera que el EGSI sea suficiente para mitigar los riesgos de seguridad de la información, básicamente por que, bajo el esquema actual de monitoreo por parte del SNAP, la estrategia que podrían adoptar es generar documentos sin valor, solamente para cumplir con los hitos establecidos en el Sistema de Gobierno por Resultados.

En base a los resultados obtenidos, aunque como se lo indicó anteriormente, no necesariamente reflejen la realidad de toda la población debido al tamaño de la muestra, reflejan que existe cierta probabilidad de que las entidades cumplan por obligación con el EGSI, esto es, documentando controles sin un fundamento técnico amparado en un análisis de riesgos, lo cual derive en carencia de controles técnicos y físicos que verdaderamente provean seguridad a los activos de información, así también, nombrar como Oficiales de Seguridad de la Información que no cumplan con el perfil ni con la experiencia que este cargo involucra.

El proyecto al que deberían apuntar las entidades del sector público es a diseñar e implementar el Esquema Gubernamental de Seguridad de la Información o EGSI, mismo que fue diseñado a partir de la Norma Técnica Ecuatoriana INEN ISO/IEC 27002:2009, y establece un conjunto de directrices que deben ser implementadas con la finalidad de gestionar la seguridad de la información bajo un proceso de mejora continua, en definitiva, indica qué controles de seguridad de la información deben utilizarse en el sector público del Ecuador, algo que, no ha sido concebido por al menos la muestra de siete

(7) representantes entrevistados y que a su vez se demuestra en el Ranking publicado por el SNAP.

2.3. Marco de Referencia

Este trabajo de titulación se desarrolló con la finalidad de ser un marco de referencia generado en base al conocimiento previamente adquirido por el investigador, mismo que forma parte de una estructura teórica ya existente que ha sido, en este caso, adaptada para el diseño e implementación del Esquema Gubernamental de Seguridad de la Información en concordancia a lo que demanda el Acuerdo Ministerial No. 166.

Este Marco de Referencia ha sido diseñado a partir de revisión bibliográfica de documentos de relevancia para el caso, mismos que se encuentran referenciados bajo el título de Bibliografía en este mismo documento, además, se utilizaron prácticas de diseño e implementación de la ISO/IEC 27001 utilizadas en el contexto nacional, específicamente en el sector público, así como, la experiencia del investigador.

La construcción de este marco de referencia se dio por medio de la integración lógica y cronológica de la información recopilada.

2.3.1. Orden Cronológico del Marco de Referencia

El marco de referencia para proyectos de diseño e implementación del Esquema Gubernamental de Seguridad de la Información se basa en el siguiente orden cronológico:

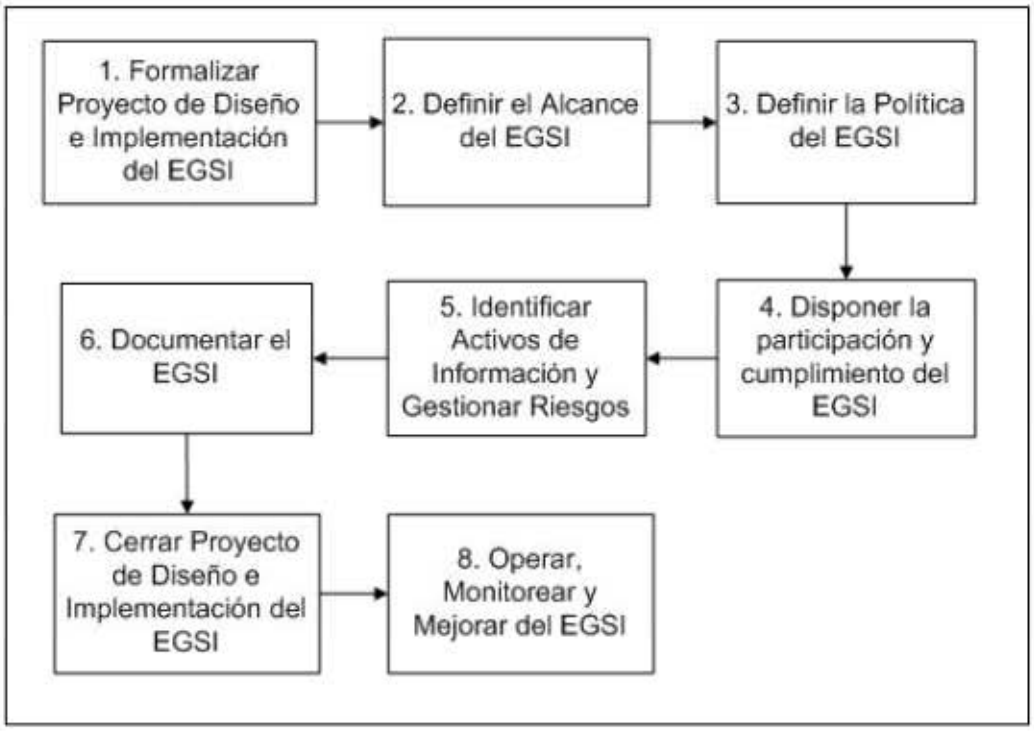


Figura No. 2: Orden Cronológico del Marco de Referencia

A continuación, la descripción de cada fase señalada:

2.3.2. Formalizar Proyecto de Diseño e Implementación del EGSI

A pesar de no ser mandatorio dentro de los requisitos que la Secretaría Nacional de la Administración Pública solicita en el Acuerdo 166, el establecer el Plan de Proyecto de Diseño e Implementación del EGSI es de suma utilidad debido a que esto ayuda a definir formalmente por lo menos los siguientes aspectos:

- **Objetivos del proyecto**

  Los objetivos del proyecto deben apuntar al diseño e implementación de un EGSI según lo que obliga el Acuerdo 166, sin embargo, los objetivos del EGSI deberán estar

alineados a la visión, misión, objetivos estratégicos de la organización y a crear cultura de seguridad de la información. No deben confundirse los objetivos del Proyecto de Diseño e Implementación de un EGSI con los objetivos de Seguridad de la Información de la Institución.

- Cronograma

  Se debe realizar un cronograma estimado del proyecto y definir la línea base ajustada a la realidad de la institución, las fechas de entrega de los distintos hitos del Acuerdo 166 son:

  - Designar un Comité de Seguridad de la Información y un Oficial de Seguridad de la Información deberá ser nombrado y notificado al SNAP hasta octubre del 2013.
  - Los controles prioritarios deberán implementarse hasta marzo del 2014, entre estos se encuentra la Política de Seguridad de la Información.
  - El EGSI completo deberá estar implementado para septiembre del 2015

Aquellas instituciones que no pudieran cumplir con las fechas, deben solicitar prórroga con las debidas justificaciones a la Secretaría Nacional de la Administración Pública (SNAP).

Este cronograma debe marcar el inicio y el fin del proyecto de diseño e implementación del Esquema Gubernamental de Seguridad de la Información.

- Sponsor del proyecto

  Como todo proyecto, es natural que este también cuente con un sponsor; este debe ser un delegado de la alta dirección de

la organización (Gerente General, Ministro, Secretario, etc.), debe ser la persona que se encargue de la asignación de recursos para el proyecto, así como de velar que los objetivos del proyecto sean alcanzados en los tiempos previstos.

- Gerente del proyecto

  Este rol debe ser asumido por el Oficial de Seguridad de la Información, quien es responsable de liderar en base a fundamentos técnicos la implementación del EGSI según los tiempos, recursos y alcance establecidos, además, debe reportar avances por lo menos quincenales al Sponsor del Proyecto. Su designación debe hacerse por el sponsor del proyecto, considerando también que el Acuerdo 166 responsabiliza al Oficial de Seguridad de la Información por el EGSI.

- Equipo del proyecto

  Un equipo de proyecto debe ser seleccionado por el Oficial de Seguridad de la Información para el diseño e implementación del EGSI deberá estar conformado por al menos el Responsable de Seguridad del Área de Tecnologías de la Información (2.3 del Anexo A del Acuerdo 166) y el grupo de apoyo al Oficial de Seguridad de la Información que en conjunto tengan las siguientes especialidades para cumplir con los distintos requisitos de la Norma ISO7IEC 27001:2005:

Tabla No. 2: Roles del Proyecto de Diseño e Implementación del EGSI

ROL	REQUISITO A CUMPLIR
Implementador	Todos
Evaluación de Riesgos	4.2.1 (ISO/IEC 27001:2005, 2005, pp. 20, 21 y 22)
Documentador	4.3.3 (ISO/IEC 27001:2005, 2005, pp. 25, 26)
Capacitador	5.2.2 (ISO/IEC 27001:2005, 2005, pp. 27)

En segunda instancia, el equipo del proyecto sumará integrantes dependiendo del alcance establecido para el EGSI, los cuales pudieran ser personal experto de los procesos de negocio inmersos en el alcance.

- Riesgos del proyecto

  Un proyecto de diseño e implementación de un EGSI también tiene ciertos riesgos inherentes, mismos que deben ser identificados por el Gerente del Proyecto con la finalidad de que se les dé el tratamiento adecuado y oportuno.
  Algunos riesgos típicos en este tipo de proyectos pueden estar asociados a incumplimientos de fechas acordadas en el plan de tratamiento de riesgos, rotación de personal clave, falta de asignación de recursos o alcance del EGSI mal identificado.

Este Plan del Proyecto de Diseño e Implementación del EGSI deberá ser elaborado por el Gerente del Proyecto y deberá ser aprobado por el Sponsor, así mismo, se recomienda que sea publicado para uso de la alta dirección y para el personal inmerso en el proyecto.

2.3.3. Definir el alcance del EGSI

La primera actividad, y, una de las más importantes dentro del proyecto de diseño e implementación del EGSI es definir su alcance (Instituto Ecuatoriano de Normalización, 2010, pág. 90), sin embargo, es necesario considerar que el Acuerdo 166 no establece ningún lineamiento con respecto a este punto.

Un alcance adecuado debe considerar un proceso del negocio y su dimensión tanto geográfica como a nivel de personas involucradas.

Uno de los primeros insumos que la entidad debe proporcionar al Esquema Gubernamental de Seguridad de la Información es el llamado enfoque por procesos, mismo que se refiere a un principio de gestión básico y fundamental para la obtención de resultados, para esto, es importante saber que un proceso es un conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados o salidas (Asociación Española de Normalización, 2013, pág. 87).

Este enfoque ayuda a la organización a establecer las siguientes actividades (www.calidad-gestion.com.ar):

- Definir de manera sistemática las actividades que componen el proceso.
- Identificar la interrelación con otros procesos.
- Definir las responsabilidades respecto al proceso y sus actividades.
- Analizar y medir los resultados del proceso en base a indicadores.
- Centrarse en los recursos y métodos que permiten la mejora del proceso.

En base a lo indicado, el primer paso para determinar el alcance del EGSI es precisamente reflexionar sobre qué procesos son los suficientemente significativos para la organización.

Los principales factores para la identificación y selección del alcance del EGSI son los siguientes (www.calidad-gestion.com.ar):

- Influencia en la satisfacción del cliente o ciudadanía
- Los efectos en la calidad del producto/servicio entregado
- Factores Clave de Éxito
- Relación con la visión, misión y estrategia de la organización
- Cumplimiento de requisitos legales o reglamentarios
- Los riesgos económicos y de insatisfacción
- Impacto en imagen y reputación
- Ventaja competitiva

Esta definición puede ser tomada en base a diferentes herramientas de gestión, por ejemplo, lluvia de ideas o dinámicas de equipos de trabajo, sin embargo, siempre es importante la participación del nivel estratégico de la organización.

Una vez identificado el proceso alcance del EGSI, se debe definir y reflejar las interrelaciones existentes con sus respectivos procesos de soporte, siendo la manera más efectiva a través de un mapa de procesos, que viene a ser la representación gráfica de la estructura de procesos que conforman el Esquema Gubernamental de Seguridad de la Información.

El alcance debe ser elegido en función de los procesos que apuntalan los objetivos estratégicos de la organización; por citar algunos ejemplos de alcances para el EGSI:

- Para ENFARMA (Empresa Pública de Fármacos), el alcance pudiera ser el Proceso de Distribución de Medicamentos para

Centros de Salud Públicos dentro del Distrito Metropolitano de Quito.

- Para el Ministerio de Turismo, un alcance pudiera ser el Proceso de licenciamiento para establecimientos turísticos de la Provincia de Pichincha.

El criterio para la selección del alcance debe estar fundamentado en la cadena de valor de la organización o en los procesos de mayor relevancia para la sociedad, por ejemplo, no es recomendable que el alcance del EGSI de una organización se enmarque a los procesos propios del área de Tecnología debido a que no se estaría involucrando al negocio debido a que no sería de enfoque comercial.

El alcance debe ser formalizado en un documento que haya sido elaborado por el Gerente del Proyecto, revisado por el Sponsor del Proyecto, y, finalmente aprobado por la máxima autoridad de la institución; una vez formalizado debe ser difundido.

A continuación una figura que tiene como finalidad mostrar el formato de un mapa de procesos:

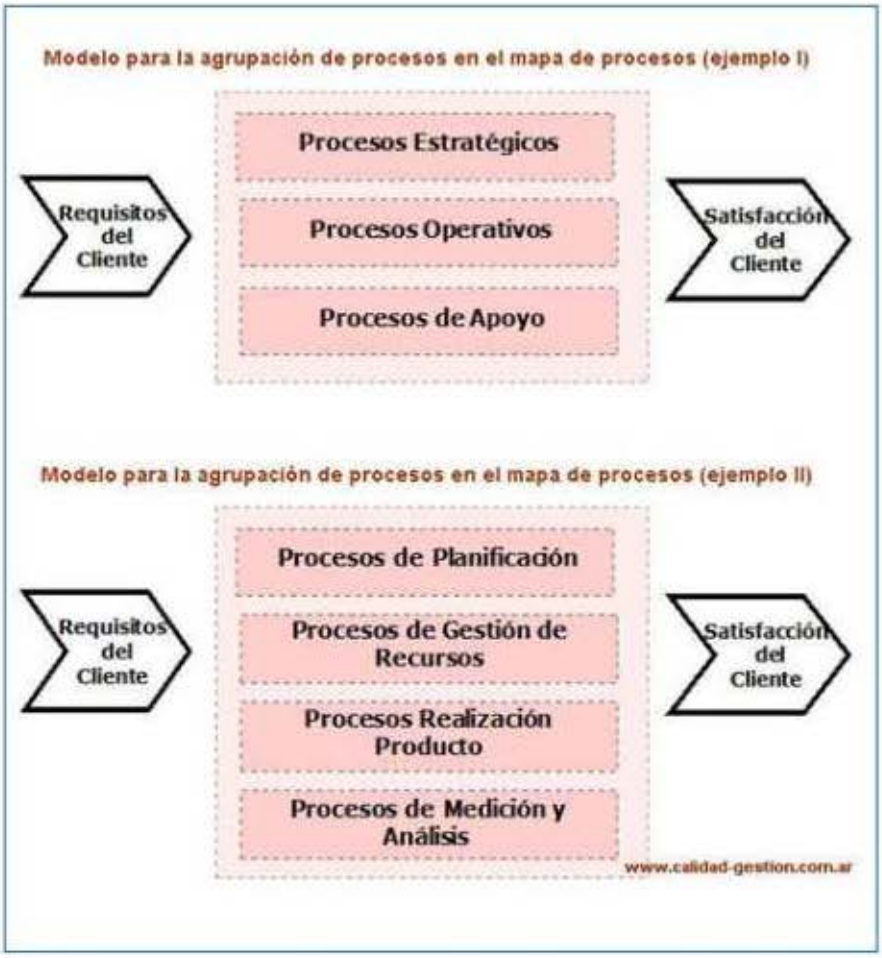


Figura No. 3: Formatos Mapa de Procesos
Tomado de: (www.calidad-gestion.com.ar)

2.3.4. Definir la Política del EGSI

Una vez definido el alcance del proyecto, se debe establecer la intención de la alta dirección, esto es, la Política del EGSI. Es muy importante recalcar que la Política del EGSI no es la Política de Seguridad de la Información, la primera define una intención de la organización hacia la sociedad mientras que la segunda define la Intención Interna u operativa (Instituto Ecuatoriano de Normalización, 2010).

La Política del EGSI debe ser una intención corporativa y estratégica, debe ser la carta de presentación que la entidad utilizará ante el mundo en cuanto a su seguridad de la información, por ejemplo:

> "La institución, preocupada por la seguridad de la información se compromete a velar por la confidencialidad, integridad y disponibilidad de sus activos de información, proporcionando los recursos y directrices necesarias para el cumplimiento del Esquema Gubernamental de Seguridad de la Información e instando a su personal para que forme parte activa en su cumplimiento diario."

Al igual que con el alcance, la Política del EGSI también debe ser formalizada en un documento que haya sido elaborado por el Gerente del Proyecto, revisado por el Sponsor del Proyecto, y, finalmente aprobado por la máxima autoridad de la institución; una vez formalizado debe ser difundido para consumo de toda la institución.

2.3.5. Disponer la participación y cumplimiento del SGSI

Una vez formalizado y difundido el Plan de Proyecto, el Alcance y la Política del EGSI, la máxima autoridad de la institución deberá socializar mediante un comunicado dirigido a toda la organización el Proyecto de Diseño e Implementación del EGSI, disponiendo a su vez el apoyo al Oficial de Seguridad de la Información y recalcando que los controles del EGSI serán de cumplimiento obligatorio a toda la empresa y no solo dentro del alcance, considerando que el alcance nos ayuda a delimitar el ámbito de la identificación de los activos de información y el análisis de riesgos, sin embargo, la política del EGSI, por ejemplo, debe ser obligatoria para toda la organización.

La idea es contar con un documento que ampare al Oficial de Seguridad de la Información para que pueda realizar sus funciones dentro del proyecto y posteriormente dentro de la operación del EGSI.

2.3.6. Identificar Activos de Información y Gestionar Riesgos

2.3.6.1. Inventario de Activos de Información

La identificación e inventario de los activos de información consiste en determinar qué información es utilizada o generada durante la ejecución del proceso definido como alcance del EGSI y todos los procesos de soporte, para ello es fundamental la participación activa de los dueños de los procesos.

La identificación de los activos de información debe realizarse mediante talleres con los dueños de los procesos o los usuarios expertos ya que ellos son los únicos que los conocen a profundidad las entradas, salidas y actividades de dichos procesos y lo que se utiliza.

Para establecer los activos de información de un proceso, el Oficial de Seguridad de la Información (o su delegado) deberán programar un taller con los dueños del proceso alcance del EGSI (y sus procesos de soporte) y sus usuarios expertos con la finalidad de que ellos sean quienes indiquen cuáles son los activos utilizados.

Para que la información obtenida sea más completa, el Oficial de Seguridad podría realizar las siguientes preguntas:

¿Cuáles son las entradas del proceso y en qué formatos llegan?, ¿Qué información utiliza en el desarrollo del proceso?, ¿En qué formatos puede ser encontrada?, durante el proceso, ¿En qué fuentes o sitios se almacenan los activos de información?, ¿Existen personas sin las cuales el proceso se vea

degradado o interrumpido?, entre otras, dependiendo del desenvolvimiento del taller.

Es muy importante tener presente que los delegados del proceso que asistan al taller, en principio no demuestren total apertura, por lo cual, el Oficial de Seguridad de la Información deberá dar una introducción al taller, explicar su importancia, y, sobre todo, contar con el apoyo de la máxima autoridad, incluso si esto lo realiza un consultor.

El principal objetivo es llegar a detectar todos los activos de información que existen dentro de un proceso de negocio, considerando que estos pueden ser documentos electrónicos o físicos, personas, hardware o software.

Un aspecto a considerar es que los procesos de negocio pudieran requerir de la participación de activos que no tengan relación directa con su operatividad, sin embargo, pudieran ser importantes, por ejemplo, pasantes, mensajeros, sitios web de terceros, decretos de entes de regulación, etc., debe considerarse el proceso de forma integral.

Debe también considerarse que los activos de información deben ser establecidos como uno solo, a pesar de estar relacionados, esto debido a que cada uno tiene distintos riesgos asociados y por lo tanto tendrá distintos controles, por ejemplo:

- Sistema contable
- Base de datos del sistema contable
- Sistema operativo del servidor del sistema contable
- Servidor del sistema contable
- Administrador del sistema contable
- Administrador de la base de datos del sistema contable
- Mensajero
- Actas de Reunión

Finalmente, el Oficial de Seguridad de la Información deberá asesorar plenamente a los delegados del proceso de negocio para que ningún activo de información se pase por alto, por ejemplo, mensajeros, pasantes, cuadernos de anotaciones, memorias extraíbles, etc., de preferencia dejando por escrito actas de reunión.

Un formato para el inventario de los activos de información pudiera ser:

Tabla No. 3: Ejemplo Formato Inventario de Activos de Información

Activo	**Descripción**	**Tipo**	**Propietario**	**Clasificación**
1	Sistema Contable	Software	Contador General	Privado
2	Sistema Comercial	Software	Gerente Comercial	Privado

- Activo: Indicar un identificador o el nombre del activo.
- Descripción: Dar una breve descripción de lo que el activo hace dentro del proceso.
- Propietario: Dueño del proceso que a su vez es dueño del activo.
- Tipo: Indicar si el activo es hardware, software, documento electrónico, documento físico o persona
- Nivel de Clasificación: Indicar si es público o confidencial, según la clasificación utilizada en la organización.

2.3.6.2. Definir metodología de análisis gestión de riesgos

La gestión de riesgos es el proceso medular dentro de la seguridad de la información, este debe ser recurrente, y, debe contener actividades como análisis, planificación, ejecución, control y seguimiento de los controles implementados (ISO/IEC, ISO/IEC 27001:2013 Information technology —

Security techniques — Information security management systems — Requirements , 2013, págs. 78-80).

El EGSI demanda una clara evidencia de que la organización está aplicando un enfoque sistemático para la identificación, evaluación y gestión de riesgos de seguridad de la información.

El llamado a liderar la ejecución de este proceso dentro de la organización es el Oficial de Seguridad de la Información (ISACA, 2013, pág. 67).

Para tener conocimiento del proceso a ser sometido a la evaluación de riesgos, el Oficial de Seguridad de la Información deberá conocer las entradas, actividades y salidas del proceso, por demás está indicar que los dueños del proceso y usuarios expertos son los llamados enseñarle al Oficial de Seguridad todo lo necesario.

Una organización, sin importar su giro de negocio o industria a la que pertenece, debe gestionar adecuadamente sus riesgos relacionados a la seguridad de la información, o sea, la probabilidad de que los activos de información de la organización pudieran perder confidencialidad, integridad o disponibilidad causando un impacto tanto cuantitativo como cualitativo a la organización (ISO/IEC, ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management , 2011, págs. 23-25).

Tener y ejecutar al menos anualmente una metodología es importante porque:

- Permite establecer la relación entre la función de seguridad de la información y los procesos del negocio, debido a, cuando se realiza la identificación de los activos de información, se estima su impacto para el negocio, su nivel de vulnerabilidad y se los asocia a escenarios de riesgo, el negocio empieza a

tomar conciencia acerca de la importancia de los controles de seguridad de la información, así mismo, empieza a conocer que la seguridad de la información no solamente es tecnología.

- Permite alinear el proceso llamado seguridad de la información con los demás procesos de negocio, lo cual permite obtener alineación con toda la organización.
- Un análisis de riesgos metodológicamente planeado y ejecutado donde el Oficial de Seguridad de la Información es guía al negocio pero donde se involucra a representantes de los distintos procesos (alcance del EGSI), empezará a generar mayor compromiso e involucramiento entre los interesados.
- En muchas ocasiones, la gestión de riesgos permite que gracias a la función de seguridad de la información, la organización sepa que utiliza activos que ni siquiera sabía que tienen relevancia para los procesos del negocio.

Dentro de las familias ISO/IEC 27000, la norma ISO/IEC 27005 es una directriz que contiene los aspectos básicos que una metodología de evaluación de riesgos de seguridad de la información debe cumplir, y, a pesar de que el Acuerdo 166 dispone su utilización, es muy importante señalar que esta norma no es una metodología per se, sin embargo, lo que propone es un proceso para gestionar riesgos de la seguridad de la información, lo cual implica que, al ser un proceso, la evaluación de riesgos podrá ser sometida a una mejora continua:

- Planificar: en esta fase se establece la metodología a utilizarse, se formaliza el alcance de la evaluación.
- Hacer: se ejecuta la metodología y se implementan controles o acciones de tratamiento de riesgos.

- Verificar: se realiza un monitoreo contante de los controles y acciones implementadas, se determina si el nivel de riesgo residual se mantiene.
- Actuar: Se toman todas las acciones que pudieran mejorar al proceso de gestión de riesgos de seguridad de la información, por ejemplo, adoptar una nueva metodología de ser necesario.

Para ejecutar una metodología de gestión de riesgos, deben conocerse ciertos términos, por ejemplo:

Riesgo inherente y residual: El riesgo inherente es aquel que existe sobre los activos de información en ausencia de acciones de la dirección para modificar su probabilidad o impacto, o sea, el riesgo existente antes de implementar controles. Por otro lado, el riesgo residual es aquél que permanece después de que la organización haya implementado sus respuestas a los riesgos o haya implementado controles.

Riesgo Residual = Riesgo Inherente – Controles Implementados

Impacto: Se refiere a la afectación que el proceso de negocio alcance del EGSI tendría si un riesgo llegara a materializarse, dicha afectación puede ser tanto cuantitativa como cualitativa.

Vulnerabilidad: Indica el nivel de exposición que los activos de información tendrían ante determinado escenario de riesgo, este nivel de exposición está dado por los controles existentes y su operación.

La metodología de evaluación de riesgos debe tener una escala que sea diseñada en función de la realidad y la naturaleza de la institución u organización, estas escalas podrían tener diferentes niveles, ejemplo, alto, medio, bajo, o, escala del uno al cinco (1, 2, 3, 4 y 5), sin embargo, debe existir

una escala tanto para estimar el impacto como el nivel de vulnerabilidad o probabilidad de ocurrencia.

De igual manera, esta escala diseñada en función de la organización, debe considerar los niveles de aceptación de los riesgos asociados a los activos de información, esto se conoce como riesgo aceptable y debe ser establecido por la máxima autoridad en función del apetito de riesgo (esto es, cuánto riesgo está dispuesta a aceptar la organización para lograr sus objetivos estratégicos) de la organización; justamente, la participación de la máxima autoridad es lo que hace que la metodología de evaluación de riesgos sea el punto central de la definición de una estrategia de seguridad adecuadamente alineada con la organización y su entorno de operación.

Para analizar los riesgos de la seguridad de la información se puede utilizar tanto métodos tanto cualitativos, como cuantitativos, para la asignación de valores de impacto, vulnerabilidad y riesgo, es esta metodología la que permitirá al Oficial de Seguridad de la Información asesorar a la alta dirección a la hora de tomar decisiones de tipo financiero, por ejemplo, en el caso de la adquisición de herramientas tecnológicas de seguridad (antivirus, filtro de contenido web, lectores biométricos, etc.).

La importancia de contar con una metodología de evaluación de riesgos radica en que la función de seguridad de la información estará alineada a los objetivos y a la operación del negocio y así se encarga de identificar y tratar riesgos asociados a los activos de información, o sea, todo lo que procesa, genera o almacena información necesaria para la operación y para el cumplimiento de los objetivos estratégicos de la organización.

El Oficial de Seguridad de la Información debe contar con un documento de la Metodología de Evaluación de Riesgos utilizada en la organización, misma que deberá estar formalizada por el nivel estratégico y difundido a toda la organización.

2.3.6.3. Ejecutar metodología y tratar riesgos

Una vez obtenido el inventario de activos de información, la metodología de evaluación de riesgos de seguridad de la información debería considerar:

- Estimación de Impacto

Una vez identificados e inventariados los activos de información, el Oficial de Seguridad de la Información debe gestionar un nuevo taller, ahora sin la presencia de los dueños de los procesos de soporte sino solamente con los dueños del proceso alcance del EGSI, en caso de que se los desee incluir, no tendrán participación activa, sino, su presencia debe ser para solventar dudas de los dueños del proceso principal.

El objetivo de esta actividad consiste en hacer una estimación, sea cualitativa o cuantitativa (depende de la escala establecida) del impacto que una pérdida de confidencialidad, integridad o disponibilidad en los activos de información identificados, pudiera tener para el negocio, en este caso, el negocio es el proceso alcance del EGSI.

Por cada uno de los activos identificados, debe hacerse una estimación del impacto independiente para confidencialidad, integridad y disponibilidad.

Con la finalidad de asentar la idea de la estimación del impacto, y, en base a la metodología que haya adoptado la organización, el impacto pudiera medirse por ejemplo en términos de pérdida de imagen y reputación, incumplimientos legales y regulatorios, o, cuantificar dicho impacto en valor monetario.

Con respecto a las tres características de la información, el impacto en pérdidas de integridad, disponibilidad o confidencialidad pudiera estimarse de la siguiente manera:

Pérdida de integridad: cuando la información no refleja la realidad debido a modificaciones no autorizadas o procesamientos erróneos, las causas pudieran ser tanto accesos físicos como accesos lógicos no autorizados; pérdida de integridad también es un cambio hecho por una persona autorizada que no ha seguido los procedimientos establecidos en la organización.

En el caso de integridad, el impacto pudiera ser retrasos en tiempos de ejecución de procesos, desconfianza de clientes, sanciones regulatorias, toma de decisiones basada en información errada, pérdida financiera, etc.

Pérdida de Disponibilidad: Quiere decir que la información o el activo de información no se encuentra disponible cuando el proceso de negocio lo necesita, el proceso se interrumpe o sus tiempos sufren retardos.

Nuevamente, el impacto para la organización que una eventual pérdida de disponibilidad pudiera ocasionar multas, pérdida de clientes, pérdida de oportunidades de negocio o costos no presupuestados.

Pérdida de Confidencialidad: La información es conocida por personas no autorizadas, por ejemplo, acceso a documentación física, que el personal tenga conversaciones de contenido privado en sitios públicos sin las precauciones del caso, que existan equipos desatendidos y desbloqueados, etc.

Con la finalidad de que el Oficial de Seguridad de la Información pueda llevar el taller de estimación de impacto de una forma más amigable para los asistentes, se recomienda que estos sean talleres distendidos donde prime un ambiente de trabajo relajado, si los asistentes no se sienten a gusto, su participación no será la apropiada.

Una vez obtenido el insumo de la estimación de impacto por parte de los representantes del proceso del negocio (alcance del EGSI), es momento de clasificar a los activos de información, esta clasificación debe estar en función del impacto estimado versus la escala de riesgos que maneja la organización.

Aunque el taller debe generar un acta de asistencia de todos los involucrados, el entregable de esta fase debe ser el Informe de Estimación de Impacto que, entre otra información, tendrá los siguientes campos: nombre del activo, impacto para pérdida de integridad, impacto para pérdida de disponibilidad e impacto para la pérdida de integridad. Es de recalcar que, para facilidad del análisis, en caso de que la escala haya sido establecida cuantitativamente con valores, podría obtenerse un promedio del impacto por cada activo analizado.

Por ejemplo, un registro tipo de esta actividad pudiera ser:

Tabla No. 4: Ejemplo de Estimación de Impacto

ACTIVO	**IMPACTO**		
	Confidencialidad	**Integridad**	**Disponibilidad**
Activo XYZ	Alto	Medio	Medio
Activo ABC	Bajo	Alto	Bajo

El ejemplo muestra el resultado final, sin embargo, la tabla indicada muestra el resumen de la estimación de todos los dueños del proceso alcance del EGSI.

Por resumir, esta actividad tiene como finalidad obtener un estimado por parte del negocio con respecto a ¿Qué tan malo será para el proceso si el activo de información pierde confidencialidad, integridad o disponibilidad?

- Identificación del Universo de Amenazas y Vulnerabilidades

La evaluación de los riesgos asociados a los activos de información de la organización debe incluir un universo de amenazas y vulnerabilidades, es así que, el objetivo de esta fase consiste en identificar vulnerabilidades típicas que pudieran ser explotadas por una amenaza, según el tipo de activo de

información, sin embargo, también debe indicarse a qué propiedad de la información afectarían, por ejemplo:

Tabla No. 5: Ejemplo de Universo de Amenazas y Vulnerabilidades

Amenaza	**Vulnerabilidad**	**Tipo de Activo de Información**				**Atributo de la Información**		
		SW	**DF**	**DE**	**HW**	**CON**	**INT**	**DIS**
Incendio	No existe contingencia geográfica			X	X			X
Empleado Descontento	No existe adecuada segregación de funciones	X	X	X	X	X	X	X

Dónde:

SW = Software
DF = Documento Físico
DE = Documento Electrónico
HW = Hardware
CON = Confidencialidad
INT = Integridad
DIS = Disponibilidad

En base a lo indicado, se debe considerar que las amenazas y vulnerabilidades asociadas, por ejemplo, a personas no son las mismas asociadas a software o documentos físicos, es por esto que se deben definir escenarios de riesgo para todos los tipos de activos de información.

- Estimación de Vulnerabilidad

Una vez estimado el impacto que una probable pérdida de confidencialidad, integridad o disponibilidad de los activos de información pudiera tener para el proceso alcance del EGSI, y, habiendo definido el universo de amenazas y vulnerabilidades que podrían afectar a los activos de información de la organización, se debe estimar que tan probable es que los riesgos sean materializados, esto es, determinar qué tan vulnerables son los activos de información (ISO/IEC, ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management , 2011, págs. 89-90).

Es recomendable que haciendo uso del Informe de Análisis de Impacto (tomado como insumo de la actividad anterior, Estimación del Impacto), el equipo del proyecto analice en base a la escala de riesgos de la organización aquellos activos cuyo impacto es inaceptable para el negocio (proceso alcance) y solamente sobre estos trabajar las demás etapas de la evaluación de riesgos ya que, en caso de que se materialicen riesgos para los activos cuyo impacto es aceptable (bajo), la organización no se verá afectada, al menos dentro del alcance del EGSI.

La tarea de estimar el nivel de vulnerabilidad depende netamente del criterio del equipo de trabajo, siendo responsabilidad del Oficial de Seguridad de la Información y de su equipo de apoyo que realiza trabajo en campo para determinar los controles existentes, su operación, su monitoreo y mejora.

El ámbito de las revisiones que permiten determinar el nivel de vulnerabilidad debe considerar controles administrativos, técnicos y físicos que aplican sobre los activos de información impactantes para el proceso, los cuales podrían ser, documentos electrónicos, documentos físicos, hardware, software y personas.

El equipo de trabajo debe enfocar su revisión tomando como referencia un universo de amenazas y vulnerabilidades que podrían afectar a cada tipo de

activo de información, de modo que, por cada escenario de riesgos dado por una amenaza y una vulnerabilidad (tomadas del universo), se debe analizar la existencia o no de controles para determinar qué tan probable es que el escenario de riesgo en cuestión llegue a materializarse.

La metodología de evaluación dependerá del apetito de riesgo de la organización, por ejemplo, si es de banca o telecomunicaciones, este puede ser menor en comparación a instituciones educativas; es así que podrían utilizarse entrevistas, listas de verificación, pruebas de penetración a dependencias físicas, a redes o aplicaciones, etc.

Todas las reuniones de revisión deben generar actas donde se indique con quienes se realizó el análisis y los hallazgos detectados; el entregable principal de esta fase es el Informe de Análisis de Vulnerabilidad, mismo que, a cada activo de información se le estima un nivel de vulnerabilidad para cada uno de los escenarios determinado por el universo de amenazas y vulnerabilidades, esta estimación debe indicar el nivel de vulnerabilidad (en base a la escala de riesgos que utilice la organización).

Como herramienta, el equipo de seguridad de la información a cargo de estimar el nivel de vulnerabilidad puede generar listas de verificación de controles cuya finalidad es ayudar a establecer si los controles implementados a la fecha mitigan los riesgos asociados a los activos de información, riesgos que están dados por cada amenaza y vulnerabilidad del universo.

Al aplicar esta lista de chequeo, el equipo del proyecto podrá sistemáticamente determinar el nivel de vulnerabilidad o de exposición del activo, a continuación una lista (parcial) de verificación para un activo de información tipo persona:

Tabla No. 6: Ejemplo de Lista de Verificación de Controles

CRITERIO	CONTROL IMPLEMENTADO Y OPERANDO		
	SI	NO	PARCIAL
Acuerdo de confidencialidad			
Capacitación constante			
Inducciones formales			
Conoce rutas de evacuación			
Proceso de desvinculación			
Procedimientos de selección			
Proceso disciplinario			

La matriz indicada muestra un ejemplo de controles que deberían haber para un activo de información de tipo persona, es así que esta matriz deberá ser llenada para cada activo de este tipo, la columna "Criterio" indica los controles que según el Oficial de Seguridad de la Información deberían existir.

En base a la información recopilada, el Oficial de Seguridad de la Información podrá estimar qué tan vulnerable es el activo, en el caso del ejemplo, qué tan probable es que la persona como activo de información sufra pérdida de confidencialidad, integridad o disponibilidad.

Esta actividad tiene como finalidad obtener un estimado con respecto a ¿Qué tan probable es que el activo de información pierda confidencialidad, integridad o disponibilidad?

- Análisis y Evaluación de Riesgos

La determinación del riesgo es compuesto por la combinación del nivel de impacto y del nivel de vulnerabilidad (ambos ya estimados), de modo que, por

medio de los resultados obtenidos se podrá establecer el nivel de riesgo al que se encuentra expuesto cada activo de información (ISO/IEC, ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management , 2011, pág. 36).

Por cada activo de información en cada escenario de riesgo analizado (que está dado por amenaza y vulnerabilidad del universo), se debe, en base a la escala utilizada en la organización tener un riesgo estimado posible de ubicar en un mapa similar al siguiente:

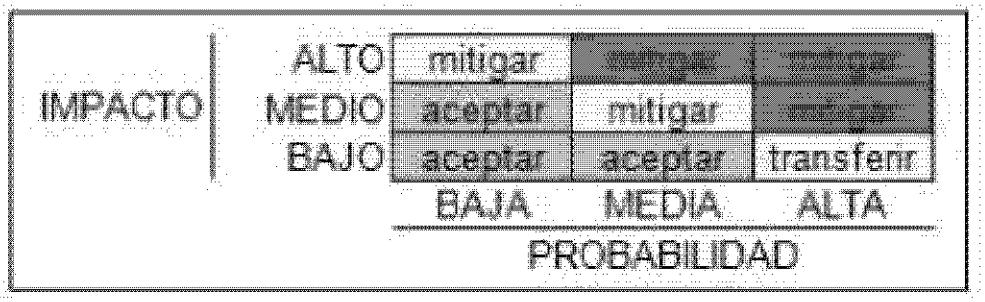


Figura No. 3: Matriz de tratamiento de riesgos

Debe considerarse que la figura es ilustrativa y tiene como finalidad mostrar una escala de ejemplo y acciones de ejemplo, sin embargo, esto puede variar en función de la naturaleza y apetito de riesgo de la organización, mientras más alto sea el impacto y el nivel de vulnerabilidad, el riesgo será mayor, sin embargo, depende del apetito de riesgo de la organización determinar el nivel de aceptabilidad.

Para aquellos riesgos que hayan sido evaluados como NO Aceptables, la dirección de la organización debe tomar alguna de las siguientes opciones de tratamiento:

Aceptar el Riesgo: Esta medida de tratamiento debe darse únicamente para aquellos escenarios de riesgo que podrían afectar a activos de información con

impacto tolerable según la escala de riesgos definida, o sea, para aquellos activos que en caso de perder confidencialidad, integridad o disponibilidad no causen impacto al proceso de negocio.

Por otro lado, la organización pudiera aceptar los escenarios de riesgo identificados para activos de alto impacto para el proceso y seguir operando tal cual se lo ha venido haciendo, esta acción, a pesar de ser posible es la menos recomendada ya que seguiría siendo vulnerable a los escenarios de riesgo identificados, haber aplicado la metodología solamente habrá servido para identificar los riesgos.

Transferir el Riesgo: Se trata de repartir el impacto entre un tercero y la organización, por ejemplo, aseguradoras, pólizas, servicios en la nube, etc., esta acción es recomendada, especialmente si consideramos que las nuevas tendencias de gestión de procesos impulsan a contratar como servicios todo lo que no sea parte de la cadena de valor de la organización.

Evitar el Riesgo: Se refiere a eliminar el activo de información que podría ser afectado por el escenario de riesgo, la organización dejaría de trabajar con dicho activo, esta acción muchas veces no es posible y por lo tanto su aplicabilidad es muy rara.

Mitigar el Riesgo: Consiste en la implementación de controles que reduzcan el nivel de vulnerabilidad identificado, cabe recalcar que, para el caso de EGSI, los controles a ser implementados deben ser tomados del Anexo 1 del Acuerdo 166, mientras que para un SGSI, los controles a ser implementados deberán ser tomados del Anexo de la ISO/IEC 27001, esto no quiere decir que pudieran complementarse con controles tomados de otras normas.

Una vez que la alta dirección de la organización ha establecido el tratamiento a dar a cada uno de los riesgos identificados sobre sus activos de información, el entregable de esta actividad es el Informe de Análisis de Riesgo, y

básicamente su contenido debe indicar si los riesgos son o no aceptables, y, en caso de no serlo, debe indicar la opción de tratamiento seleccionada por la alta gerencia de la organización.

- Plan de Tratamiento de Riesgos

Una vez tomada la decisión acerca de la opción de tratamiento que se dará a los riesgos identificados, todas las actividades e iniciativas a tomarse para su cumplimiento deberán ser plasmadas en un Plan de Tratamiento de Riesgos, por ejemplo, en caso de que la decisión sea mitigar los riesgos, el plan de tratamiento debe indicar qué controles del Anexo 1 del Acuerdo 166 serán implementados, quién es el responsable de hacerlo y las fechas de compromiso para su entrega.

Se puede decir que el Plan de Tratamiento de Riesgos es el entregable o la salida de todo el proceso de gestión de riesgos, de hecho este documento plasma la estrategia de la organización para la reducción de todos los riesgos que en el análisis superan el umbral de aceptación, es por esto que, se tienen que seleccionar los controles más apropiados para reducir todos esos riesgos excesivos identificados. Esta selección de controles es responsabilidad del Oficial de Seguridad de la Información, de modo que, para cada riesgo debe analizar la efectividad y coste de los controles aplicables, y seleccionar solamente los más adecuados tanto financiera como operativamente.

Una vez que el Oficial de Seguridad de la Información ha generado un primer listado de controles aplicables, es decisión de la alta dirección (bajo la respectiva asesoría tanto técnica como financiera) definir los controles que serán implementados, esto principalmente en función de los recursos de la organización, todo control que no sea implementado derivará en un riesgo aceptado, por ejemplo, el Plan de Tratamiento de Riesgos puede derivar en la implementación de un Plan de Continuidad del Negocio, pero por temas de

presupuesto, la dirección puede decidir no implantarlo y aceptar los riesgos asociados.
Habiendo seleccionado los controles a implementarse, el Oficial de Seguridad de la Información es el llamado a definir los proyectos de implementación correspondientes, especificando tareas, responsables, tiempos y recursos. Este plan de proyectos constituirá el Plan de Tratamiento de Riesgos.

Es importante mencionar que el Plan de Tratamiento debe ser un plan a corto plazo que busca la reducción de los riesgos identificados como no aceptables mediante la implementación de controles, y, al igual que todo el proceso de gestión de riesgos, este plan debe ser estructurado, repetible y consistente.

El Plan de Tratamiento de Riesgos es un paso previo al Plan Director de Seguridad de la Información ya que el primero contiene todos los controles administrativos a ser implementados, mientras que el segundo contiene también controles técnicos y físicos (ISO/IEC, 2013, pág. 56).

Es responsabilidad del Oficial de Seguridad de la Información asesorar a la organización para que se apliquen acciones eminentemente prácticas y fijando unos objetivos claros y asumibles.

2.3.6.4. Gestionar y aceptar riesgo residual

Debido a que un riesgo, por más controles y medidas de tratamiento que sean implementadas, nunca podrá ser reducido a una probabilidad de ocurrencia de cero (a menos que la opción de tratamiento haya sido eliminar), la organización debe manejar un nivel de aceptabilidad de los riesgos, esto es, dentro de la escala definida, qué riesgos deben ser tratados y qué riesgos son aceptados.

Por medio de los controles implementados, todos los riesgos inaceptables deben ser reducidos a un nivel aceptable, es por esto que, el Oficial de Seguridad de la Información deberá realizar una estimación del riesgo que

quedaría luego de haber sido implementado el plan de tratamiento de riesgos, esta estimación debe ser plasmada en un acta de aceptación del riesgo residual, y debe ser aprobada por la máxima autoridad o su delegado.

Es de recalcar que esta estimación no debe hacerse luego de haber implementado el Plan de Tratamiento de Riesgos.

2.3.6.5. Aplicabilidad de los Controles del EGSI

Una vez definida y ejecutada la metodología de evaluación de riesgos para los activos de información que forman parte del proceso alcance del EGSI, así como para los activos de información de sus procesos soporte, el plan de tratamiento de riesgos, si la decisión fue mitigar riesgos, tendrá el conjunto de controles a ser implementados en la organización (Instituto Ecuatoriano de Normalización, 2010).

Los controles de tipo directivo (políticas, procedimientos, estándares o normativas) que constarán en el plan de tratamiento de riesgos, para el caso del EGSI, deberán ser tomados el Anexo 1 del Acuerdo 166.

Con respecto a la implementación de los controles, el Oficial de Seguridad de la Información debe tener perfectamente claro que el Acuerdo 166 orienta a la organización hacia controles administrativos, sin embargo, aunque estos hayan sido diseñados, los riesgos no serán mitigados hasta no haber implementado los controles técnicos y físicos que los soporten.

Es de considerar también que la fortaleza más grande que los controles pudieran tener radica en una adecuada difusión y capacitación al personal, así como de constante monitoreo, esto será tratado puntualmente dentro de las actividades propias de la operación, monitoreo y mejora del EGSI.

Idealmente, aunque no todos los controles (medidas que mitigan riesgos mediante el tratamiento de vulnerabilidades) sean implementados, todos los objetivos de control (intención que se desea cumplir por medio del control) deben serlo, sin embargo, en caso de que alguno no sea aplicable para la organización, su no aplicabilidad deberá ser fundamentada en justificaciones razonables.

El EGSI debe contar con un documento que indique tanto los controles que aplican como los que no aplican a la organización; este documento podría llamarse Declaración de Aplicabilidad.

La Declaración de aplicabilidad es el vínculo que existe entre el plan de tratamiento de riesgos y la implementación de los controles del EGSI ya que, como se indicó, el objetivo de este documento es definir cuáles de los controles definidos en el Anexo 1 del Acuerdo 166 son los que la organización implementará.

La necesidad técnica de contar con este documento se fundamenta en los siguientes aspectos:

- La justificación de los controles a implementarse no solamente se da gracias al resultado arrojado por la ejecución de la metodología de evaluación de riesgos, sino también podría ser impuesta por asuntos legales, regulatorios, comerciales o contractuales. En este documento se indica el motivo de la implementación de cada control.

- La Declaración de Aplicabilidad documenta si cada control aplicable ya está implementado, además, debe indicar el documento de referencia, por ejemplo, una política, procedimiento, normativa o manual.

La utilidad de contar con una declaración de aplicabilidad radica en que obliga al Oficial de Seguridad de la Información a implementar los controles de forma sistemática. Este documento es la principal declaración en la que la organización define su seguridad de la información (ISO/IEC, 2013, pág. 32).

La Declaración de Aplicabilidad es el inventario de los controles que existen en la organización, recalcando que en este documento constarán los controles de tipo administrativo solamente, no los técnicos ni tecnológicos (Instituto Ecuatoriano de Normalización, 2010, pág. 45).

Independientemente del análisis de aplicabilidad de los controles, existen controles que siempre deberán existir dentro del EGSI (más aún si se desea optar por una certificación ISO/IEC 27001), estos controles de tipo administrativo (procedimientos) son los siguientes:

- Política de Seguridad de la Información: Es el documento madre del EGSI, debe reflejar la intención de la alta dirección con respecto a la seguridad de la información. Cabe señalar que el Anexo 1 del Acuerdo 166 indica el texto de la política de seguridad de la información a ser implantado en el sector público.

- Procedimiento de Control de Documentos: debe definir quién es el responsable de revisar los documentos, así como el responsable de aprobarlos, también, debe definir el registro e identificación de cambios y versiones, clasificación, distribución y publicación de documentos, formatos, etc.
- Procedimiento de Control de Registros: debe definir los lineamientos de gestión de toda la evidencia de cumplimiento de los controles que forman parte del EGSI, se debe establecer el responsable de custodio, lugar de custodio, periodo de retención, clasificación, etc.

- Procedimientos de Auditorías Internas: este debe definir las responsabilidades sobre la planificación y realización de auditorías al EGSI, su periodicidad (al menos semestral), debe indicar también cómo y a quienes se informan los resultados y qué entregables (registros) serán generados.

- Procedimiento de Acciones Correctivas y Preventivas: con respecto a las acciones correctivas, este documento define cómo la organización identifica los incumplimientos al EGSI y sus causas, además, cómo se definen e implementan las acciones necesarias para remediar los incumplimientos y para eliminar dichas causas, el fundamento básico de este documento es que debe definir cómo las distintas acciones correctivas deben eliminar la causa del incumplimiento para que este no vuelva a ocurrir debido a la misma causa.

  Con respecto a las acciones preventivas, este documento debe forzar a que toda la organización reporte cualquier amenaza, vulnerabilidad o riesgo que pudiera derivar en incumplimientos del EGSI o llegar a atentar contra la seguridad de la información. Es muy importante establecer una línea de reporte que debe ser el Oficial de Seguridad de la Información.

Es de vital importancia que las organizaciones sepan que un EGSI o un SGSI tienen como objetivo identificar activos de información, evaluar sus riesgos asociados y tratarlos mediante controles directivos (políticas, normas, procedimientos, etc.) sin embargo, estos controles van a requerir sustento en otros tipos de controles como son técnicos y físicos.

2.3.6.6. Definir quién debe implementar los controles aplicables

En base a lo indicado anteriormente con respecto a los Planes de Tratamiento de Riesgos, este constituye un conjunto de proyectos a corto plazo, y, como tal deben tener conformados equipos (ISO/IEC, 2013, pág. 60).

Independientemente de que el Oficial de Seguridad de la Información deba asegurar el cierre de todos los proyectos, cada uno debe tener un responsable quien a su vez gestionará las acciones con equipos de trabajo (si aplica el caso).

Así como durante la fase de evaluación de riesgos se involucró en ciertas actividades de forma activa a representantes del negocio, este punto es similar ya que así como hay controles transversales a todos los procesos, pudieran requerirse controles puntuales a la operación, por ejemplo, en el proceso de selección de personal o en el proceso de desarrollo de software.

El llamado a ser responsable de la implementación de los controles transversales debe ser el mismo Oficial de Seguridad de la Información, mientras que para los controles propios de cada proceso, debe ser el dueño del proceso, ya sea jefe, gerente o director.

Mientras el plan de tratamiento de riesgos se encuentra en fase de implementación los riesgos seguirán latentes, de modo que es necesario el control y monitoreo constante por parte del Comité de Seguridad de la Información por medio de notificaciones del Oficial de Seguridad de la Información con respecto al avance y cualquier novedad.

Es necesario recalcar que, pudiera darse el caso en que mientras se implementa el plan de tratamiento de riesgos, nuevos controles o mejoras pudieran surgir; es responsabilidad de todos los involucrados reportarlas al

Oficial de Seguridad de la Información para que este determine si pueden ser implementadas a la par del resto o si deben ser dejadas para después.

En el caso de los controles administrativos, se entenderá que un control existe siempre y cuando cumpla con los siguientes requisitos:

- Haya sido documentado: El acuerdo 166 no exigen ningún formato en cuanto al documento, es así que podría ser texto, audio o video, aunque, tradicionalmente las organizaciones documentan sus políticas y normativas en formatos de texto.
- Haya sido formalizado: Un control administrativo debe ser formalizado, esto quiere decir, debe constar con las firmas de responsabilidad en cuanto a creación, revisión y aprobación, la aprobación deberá ser por parte de la máxima autoridad o su delegado.
- Haya sido difundido: Un control administrativo debe ser puesto en manos de todos quienes deban aplicarlo, mejor aún, si los conoce toda la organización.
- Sea soportado: Un control administrativo muy difícilmente podrá mitigar los riesgos relacionados a los activos de información de la organización, motivo por el cual se entiende que una política, procedimiento o normativa ha sido implementado cuando existen los controles técnicos y físicos que lo respaldan.
- Se haya capacitado al personal: Debido a que el recurso es el eslabón más débil en la cadena llamada seguridad de la información, el Oficial de Seguridad de la Información debe encargarse de capacitar al personal con respecto a los controles implementados, por ejemplo, muchas organizaciones a pesar de contar con un acuerdo de

confidencialidad, parte de su personal no conoce su utilidad, más aún, ni siquiera recuerda haberlo firmado.

2.3.6.7. Definir esquema de medición de efectividad de controles implementados

Una vez que por medio de la identificación de los activos de información y de la evaluación de riesgos, la organización ha determinado qué debe proteger, de qué lo debe proteger, cómo lo va a proteger y quién implementará los controles, es una muy buena práctica que el Oficial de Seguridad de la Información diseñe un esquema de monitoreo de la efectividad de los controles implementados (Sánchez L. S.-O., 2012, págs. 67-68).

A diferencia de una auditoría interna cuya periodicidad es a intervalos medianos (4 o 6 meses), el monitoreo de eficacia de controles es algo que debe hacérselo diariamente asignando responsables para que constantemente se encarguen del monitoreo de cumplimiento del control, esto dependerá de la cantidad de recursos.

Dentro de la gestión de la seguridad de la información, la importancia de las actividades de monitoreo de los distintos controles implementados radica en que es una forma de determinar el éxito o fracaso del Plan de Tratamiento de Riesgos, y, por lo tanto de las inversiones realizadas en su implementación.

La familia de las ISO/IEC 27000, en su estándar 27004 publica las directrices para medir la seguridad de la información considerando que una medición de eficacia oportuna y consciente maximizará el valor de los controles implementados y minimizará la probabilidad de entrar en nuevos gastos, pero, principalmente, ayuda a conocer qué nivel de madurez han alcanzado los controles en la organización, y, por lo tanto, la evolución de la seguridad de la información.

Para que se facilite la medición de eficacia de los controles que forman parte del EGSI, es recomendable que cada control existente cuente con indicadores, mismo que por lo menos deben tener:

- Nombre del indicador
- Descripción del indicador
- Rango tolerable
- Tendencia
- Método de cálculo

Con la finalidad de llevar una medición de eficacia de controles adecuada, es recomendable que el Oficial de Seguridad de la Información distribuya entre su equipo de trabajo responsables de velar por el cumplimiento de ciertos controles, teniendo la premisa de que ningún responsable debe monitorear controles que dependan de sí mismo.

Así mismo, el equipo de trabajo debe generar registros del monitoreo que sean generados en base a formularios o formatos pre establecidos, por ejemplo:

- Formato de revisión que debe tener la siguiente información:
  - Responsable de Revisión
  - Fecha de Revisión
  - Nombre del Control Revisado
  - Objetivo de Control (tomado del Anexo 1 del Acuerdo 166)
  - Objeto(s) de Medición y Atributos
  - Área donde se Realiza Medición
  - Registros
  - Método de Medición
  - Resultado de la Medición
  - Conclusión Parcial
  - Causa Raíz
  - Conclusión Final (Eficaz / No Eficaz)

- Acciones Recomendadas (Indicar si es acción preventiva o correctiva)

- Formato de plan de acción para controles no efectivos:
  - Actividad a desarrollar
  - Fecha de entrega
  - Responsable

Las responsabilidades de ejecución de las acciones correctivas o preventivas que podrían derivar del monitoreo de eficacia de controles debe ser establecida en función de los hallazgos, teniendo la premisa de que, al igual que con la gestión de riesgos, estos planes deben ser de corto plazo, y, se debe reportar al comité de seguridad de la información incumplimientos o retrasos en los cronogramas acordados en los planes de acción.

2.3.7. Documentar el EGSI

A continuación se indican lineamientos para una adecuada documentación del EGSI, sabiendo que este no solo se conforma por controles administrativos sino también por documentos de generados en la fase de diseño (ISO/IEC, 2013, pág. 40).

Para dar cumplimiento a los requisitos de cumplimiento que demanda el Acuerdo 166, un EGSI debe por lo menos tener la siguiente documentación:

- Documento del Proyecto (Formato Ejemplo Referencia Anexo 2)
- Documento de formalización, comunicación y disposición de implementar el EGSI (Formato Ejemplo Referencia Anexo 3)
- Documento de formalización del alcance del EGSI
- Documento de la Metodología de Evaluación de Riesgos
- Inventario de Activos de Información

- Informe de Análisis de Impacto
- Informe de Análisis de Vulnerabilidad
- Informe de Análisis de Riesgos
- Plan de Tratamiento de Riesgos (Referencia Anexo 4)

Así también, el Anexo 1 del Acuerdo 166 tiene un listado de controles prioritarios, a continuación, ejemplos de nombres de dichos controles con su respectiva referencia a los ítems del Anexo 1 (Secretaría Nacional de la Administración Pública, 2013):

Tabla No. 7: Controles Prioritarios del EGSI

Documento	**Ítem del Anexo 1 del Acuerdo 166**
Política de Seguridad de la Información	1.1 b)
Actas de reunión de seguimiento por parte del Comité de Seguridad de la Información o de la máxima dirección de los hitos alcanzados y de presentación del plan de proyecto.	2.1 a)
Comunicado a todo el personal de la organización, donde se sociabilice y sensibilice al personal con respecto al Acuerdo 166.	2.1 b)
Documento de Roles y Responsabilidades de Seguridad de la Información	2
Documento de Uso de Acuerdos de Confidencialidad (todos los funcionarios deben tener firmado un acuerdo de confidencialidad)	2.5
Inventarios de hardware, software y equipos de red.	3.1 desde j) hasta y)
Documento de Uso de Correo Electrónico	3.3 d)

Documento	Ítem del Anexo 1 del Acuerdo 166
Documento de uso de Internet	3.3 e)
Documento de uso de Sistemas de Video-Conferencia	3.3 f)
Documento de Clasificación de Información. Clasificar la información como pública o confidencial.	3.4
Documento o procedimiento de selección de personal	4.1 a) y b) 4.4 a)
Documento de Acceso a Edificios	5.1 b) 5.2 a) y c) 5.3 b) 5.5 d) 5.6 a)
Documento de ubicación de equipos de copiado e impresión.	5.3 d)
Documento de Seguridad Física y Ambiental de Equipos	5.4 d) y e) 5.7 c) 5.8 c) 5.9 e)
Documento de Gestión de Incidentes de Seguridad de la Información	6.1 e) 9
Documento de Monitoreo de Niveles de Desempeño de Servicios	6.6 b), c) y d)
Documento de Gestión de la Capacidad	6.8 a)
Documento de Uso de Software	6.10 a) 6.10 d) 7.19
Documento de Protección Contra Código Malicioso	6.10 c)
Documento de Respaldos de Información	6.12

Documento	Ítem del Anexo 1 del Acuerdo 166
Documento de seguridad para la red	6.14 7.11 7.12 7.13 7.15 7.16 7.26
Documento de Registro y Monitoreo de Eventos	6.26 6.27 6.29 6.30
Documento de Gestión de Usuarios y Contraseñas	7.4 a) 7.5 7.9 7.10 7.17 7.18 7.20 7.21
Documento de Seguridad de la Información	7.6 7.7 7.8 7.25
Documento de Especificaciones de Seguridad para Nuevas Aplicaciones	8.1

En los ejemplos dados se utiliza la palabra "documento", sin embargo, los controles citados deberán ser nombrados en función de la estructura documental de controles que maneja la organización, por ejemplo: Políticas, Normativas, Procedimientos, Estándares, etc.
Una política define el gobierno de seguridad de la información, esta debe incluir la definición de seguridad de la información, sus objetivos para con la organización, los objetivos de control y responsabilidades asignadas, por otro lado, las normativas definen reglas inquebrantables que soportan a las políticas.

Un procedimiento define el flujo de trabajo para el desarrollo de las políticas y normativas. Un estándar define los parámetros de unificación a utilizarse, por ejemplo, para nombrar cuentas de usuario o para nombrar objetos de bases de datos, por otro lado, un instructivo define detalles técnicos para realizar tareas específicas que soportan a los controles, por ejemplo, manuales de usuario (ISC2, 2013).

La evidencia de cumplimiento de los distintos controles que hacen parte del EGSI se llaman registros y deben ser gestionados debido a que son de suma importancia en auditorías y monitoreo de eficacia de controles (SGS, 2013, pág. 76).

Es importante mencionar que a pesar de no estar obligado en el Acuerdo 166, el control para documentos y registros es muy importante ya que formaliza la uniformidad y estandarización de formatos y uso de los distintos documentos.

Finalmente, los documentos anteriormente indicados tienen como objetivo dar una base de referencia de los controles prioritarios que demanda el Acuerdo 166 para el EGSI, sin embargo, estos no son todos los que podrían llegar a necesitar; la única forma de determinar qué controles se necesitan es ejecutando la evaluación de riesgos de seguridad de la información.

Con respecto al formato básico que deberían tener los documentos que forman parte del EGSI, al menos se debería considerar:

- Carátula
  - Logo de la Institución
  - Nombre del Documento
  - Versión
  - Fecha de Elaboración
  - Nombre y firma de la persona que elabora el documento
  - Fecha de revisión
  - Nombre y firma de la persona que revisa el documento
  - Fecha de aprobación
  - Nombre y firma de la persona que aprueba el documento
  - Nivel de clasificación
- Objetivos del Documento
- Alcance del Documento
- Glosario de Términos
- Metodología o pasos para la elaboración del documento
- Contenido
- Control de cambios

2.3.8. Cerrar el Proyecto de Diseño e Implementación del EGSI

Una vez terminadas todas las actividades indicadas hasta ahora, el Gerente del Proyecto deberá notificar al Sponsor y este a su vez a la alta dirección de la organización que el EGSI ha sido implementado y que puede entrar a operar.

Para que la operación del EGSI inicie de manera adecuada es necesario considerar las siguientes premisas:

- Los controles documentados como parte del proyecto deben ser difundidos y publicados en un medio de consulta para toda la organización, sabiendo que, dependiendo de su nivel operativo algunos pudieran mantenerse dentro de ciertas áreas.
- Para que los controles del EGSI rindan sus frutos es necesario realizar las respectivas implementaciones de controles tanto físicos como tecnológicos.
- Se requiere capacitar y concientizar al personal con respecto al EGSI, antecedentes, evaluación de riesgos, activos de información y controles existentes.

Es importante también que una vez finalizado el proyecto, la alta dirección de la organización disponga a todo el personal el cumplimiento obligatorio de los controles del EGSI con la finalidad que desde ese momento se empiecen a generar los registros de cumplimiento.

2.3.9. Operación, Monitoreo y Mejora un EGSI

A continuación, el detalle de lo que el Oficial de Seguridad de la Información debe asegurar que se ejecute dentro del ámbito del EGSI, en resumen, esta parte se relaciona con operar, monitorear, mantener y mejorar todos los controles resultantes del análisis de riesgos.

2.3.9.1. Capacitación y toma de conciencia

Dentro de la seguridad de la información, la capacitación y la toma de conciencia del personal, son medidas preventivas enfocadas a minimizar la probabilidad de incidentes de seguridad de la información causados por las personas, si la organización desea que sus funcionarios apliquen todas las nuevas políticas, procedimientos y demás controles, primero es necesario

capacitar para que ellos se comporten según lo esperado (SGS, 2013, pág. 23).

La falta de capacitación y toma de conciencia es uno de los principales motivos para el fracaso de la seguridad de la información, y, por lo tanto para el fracaso del EGSI (o SGSI).

A diferencia de otros tipos de activos de información, las personas no solamente deben ser sometidas a controles sino también deben lograr cultura y hábitos de seguridad de la información (ISACA, 2013, pág. 45).

Como activo de información, una persona es el recurso con mayor vulnerabilidad dentro de la seguridad de la información, esto debido a ciertos factores propios de su naturaleza humana, por ejemplo olvidos, enfermedades, ausentismo, errores, omisiones, acciones dolosas, equivocaciones, presiones externas, estímulos, estado de ánimo, cansancio, etc., por estos y más motivos, una de las medidas preventivas enfocadas a asegurar la confidencialidad, integridad o disponibilidad de este activo de información es la capacitación y la toma de conciencia (ISC2, 2013, pág. 245).

La capacitación debe estar enfocada a aspectos de matiz técnico que los funcionarios deben conocer, por ejemplo, qué es la seguridad de la información, qué es amenaza, vulnerabilidad, riesgo, incidente, reporte de incidentes de seguridad de la información, controles existentes, proceso disciplinario, etc., mientras que, la toma de conciencia debe estar enfocada a que el personal cumpla y aplique lo aprendido durante las capacitaciones, sin esto, todo el EGSI perderá su valor para el negocio; en conjunto, las capacitaciones y la toma de conciencia están encaminados a crear una cultura disciplinada de seguridad de la información.

Desde el enfoque de la operación y mejora del EGSI, un adecuado proceso de capacitación y toma de conciencia proporciona a la organización las siguientes ventajas:

- Personal calificado en términos de seguridad de la información con proyección a adquirir por si solo habilidades y actitudes para un mejor cumplimiento de controles y buenas prácticas.
- Desarrollar el sentido de pertenencia y responsabilidad hacia la organización a través de una mayor competitividad y conocimientos apropiados, sabiendo que, una estrategia apropiada considera contenidos que el personal pudiera aplicar también en su vida personal.
- Mantener al personal permanentemente actualizado frente a los cambios tecnológicos relevantes que pudieran tener injerencia sobre la seguridad de la información de la organización.
- Lograr cambios en el comportamiento del personal con respecto a la aplicación de controles y mejores prácticas de seguridad de la información.

Dentro de la función de la seguridad de la información, la capacitación y toma de conciencia también debe ser visto como un proceso y por lo tanto, también es sujeto a mejora continua.

El proceso de capacitación y toma de conciencia debe considerar al menos:

- Identificar audiencias: En materia de seguridad de la información, a pesar de que ciertos contenidos pueden ser generales, es necesario identificar las audiencias con las que se cuenta debido a que la toma de conciencia tendrá diferente significado, por ejemplo para la alta dirección en contraste con

nivel operativo o proveedores, así mismo, la profundidad con la que se lleguen a los distintos contenidos pudiera no ser el mismo, principalmente por temas de tiempo.

- Analizar las necesidades de cada audiencia: El Oficial de Seguridad de la información deberá una vez identificadas las audiencias, identificar las necesidades de conocimiento de cada una de ellas, para esto, es necesario considerar perfil técnico de los participantes, nivel jerárquico, participación dentro de la función de seguridad de la información, etc.
- Diseñar la forma de enseñanza: En este punto se establece la metodología de enseñanza para cada una de las audiencias, se elabora el plan de capacitación (horarios y contenidos), presentaciones, manuales, actividades u otros recursos que serán utilizados.
- Validación: En este punto, el Comité de Seguridad de la Información se encarga de recibir la presentación de la estrategia y materiales diseñados por parte del Oficial de Seguridad de la Información, el Comité debe aprobar todo lo hecho hasta este momento antes de dar paso a las capacitaciones.
- Ejecución: En este punto se hacen las convocatorias a las jornadas de capacitación y se aplica el plan según lo establecido.
- Evaluación: Parte de la estrategia de capacitación y toma de conciencia debe considerarse una fase de validación de conocimientos adquiridos y practicados, esta estrategia de validación deberá constar en el plan de capacitación; para esto puede recurrirse a evaluaciones al finalizar las charlas, sin embargo, una muy buena práctica es que dentro del monitoreo de efectividad de los controles que hacen parte del EGSI se consideren entrevistas o visitas al personal para

medir el nivel de aplicación de buenas prácticas de seguridad de la información.

Con respecto a las audiencias, lo recomendable es que se establezcan estrategias para capacitar a toda la organización, de modo que se debe capacitar iniciando por el nivel estratégico, luego por el nivel táctico y finalmente por el nivel operativo.

En base a lo indicado, las capacitaciones al nivel estratégico son las más importantes ya que el resto de la organización las tomará como referencia principalmente para asistir y luego para aplicar lo aprendido, es resumen, un factor de éxito en la seguridad de la información es predicar con el ejemplo (esquema top-down).

Por demás está señalar que la asistencia a las capacitaciones debe ser indelegable.

A continuación, un plan de contenidos que una capacitación de seguridad de la información con enfoque EGSI para una entidad donde apenas se empieza con aspectos de seguridad de la información:

Conceptos básicos

- Información
- Activo de Información
- Tipos de Activo de Información
- Amenaza
- Vulnerabilidad
- Riesgo
- Confidencialidad
- Integridad
- Disponibilidad

- Tratamiento de Riesgos
- Incidente de Seguridad de la Información
- Documentos y Registros

Gestión de Incidentes de Seguridad de la Información

- Estrategia de pro actividad (reporte de amenazas, vulnerabilidades y riesgos)
- Medio de reporte de incidentes de seguridad de la información
- Ejemplos de incidentes (casos reales)

Esquema Gubernamental de Seguridad de la Información – EGSI

- Qué es el Acuerdo 166 y el EGSI
- Ciclo de Vida – Mejora continua
- Documentos
- Importancia

Norma Técnica Ecuatoriana INEN ISO/IEC 27001

- Origen y concepto
- Estructura
- Requisitos
- Controles

Cierre de la Capacitación

- Medios de Publicación y Difusión
- Mejores Prácticas y Mensajes finales
- Toma de conciencia
- Evaluación final

Según el ejemplo de plan de contenidos citado, los temas a tratarse deben variar en función del tiempo y del nivel de preparación del personal, este nivel de preparación debe ser estimado en base a la aplicación de los contenidos tratados en su día a día.

Para nuevos funcionarios se recomienda tener charlas de inducción a seguridad de la información (aparte de las capacitaciones), así como para proveedores, por ejemplo, el primer viernes laborable deben asistir a un lugar acordado todos los nuevos funcionarios y los proveedores o terceros.

Con respecto al encargado de ser el capacitador es necesario considerar que deberá ser una persona que forme parte del grupo de seguridad de la información y que además tenga habilidades de comunicación para llevar capacitaciones activas e incluso amenas ya que lo importante es no perder la expectativa e interés del personal. Las capacitaciones no deben estar limitadas al personal que forma parte del alcance del EGSI (Mellado, 2012).

Finalmente, es muy importante considerar dentro de las capacitaciones ciertas técnicas de retroalimentación, por ejemplo, foros al finalizar las charlas o encuestas donde se evalúe del desempeño del capacitador.

2.3.9.2. Registros

Una vez implementados los controles, el EGSI debe pasar a formar parte de la rutina diaria de la organización, es por esto que, el producto de esta rutina son los registros, estos son la prueba de que una actividad se haya realizado realmente o de que un control ha operado según lo esperado (Instituto Ecuatoriano de Normalización, 2010).

La importancia de contar con registros radica en que la organización puede supervisar en qué estado se encuentra su EGSI, así mismo, se podrá

determinar si realmente el personal está aplicando la seguridad de la información según los controles establecidos.

Habitualmente un registro puede ser llevado de dos formas, en formato digital, generados en forma automática o semiautomática, y en papel, donde cada registro se hace manualmente.

Todo el personal debe conocer lo que es un registro y los registros que por sus funciones genera o custodia, algunos ejemplos de registros:

- Actas de reuniones
- Bitácoras de ingreso a edificios
- Informes de revisión, monitoreo o mantenimiento
- Listas de asistencia a capacitaciones
- Reportes de monitoreo
- Informes de auditoría
- Informes de monitoreo de eficacia
- Planes de capacitación

Dentro de la estructura del EGSI los registros deben existir en función de los controles que tiene la organización, es por eso que al momento de diseñar los controles, deben considerarse registros o entregables que estos deben generar.

La organización debe contar también con un documento de control de registros, este debe especificar por lo menos los formatos aceptables por cada registro, su lugar de custodio y su periodo de retención.

Haciendo referencia a la ISO/IEC 27001, sin importar con los controles que la organización haya decidido implementar, como mínimo deben existir los siguientes registros (Asociación Española de Normalización, 2013, pág. 98):

- Registros de capacitación, habilidades, experiencia y calificaciones: Independientemente del departamento que haya estado a cargo de formular e impartir las capacitaciones e inducciones de seguridad de la información, el Oficial de Seguridad de la Información deberá reportar al Comité acerca del nivel de asistencias y ausentismos, es por eso que debe llevar registros de asistencia y evaluaciones, básicamente se debe llevar una carpeta donde se encuentren todos los documentos relacionados.

- Resultados de supervisión y medición: Podrían ser actas de reunión o informes de evidencia de medición de los controles existentes.

- Programa de auditoría interna: El programa de auditoría interna es el documento que se genera anualmente con la finalidad de formalizar la planeación de las auditorías internas; en este programa se debe definir el encargado de hacer las auditorías, el equipo auditor, las fechas a realizarse la auditoría, etc.

- Resultados de las auditorías internas: El equipo de auditores internos debe generar un informe de auditoría, que incluye los resultados obtenidos, de tal manera que un registro muy importante es aquel que evidencia que estos resultados fueron puestos en conocimiento del nivel estratégico de la organización.

- Resultados de la revisión por parte de la dirección: Estos pueden ser actas de reunión y que incluyen todos los asuntos tratados durante la reunión de la dirección.

- Resultados de acciones correctivas: Son los registros que se dejan de las distintas acciones tomadas para corregir incidentes o eventos, por ejemplo, tickets de la mesa de ayuda o correos de notificación y cierre de incidentes.

Fuera de los registros propios que forman parte del EGSI, el Oficial de Seguridad de la Información deberá también velar por que se asegure la confidencialidad, integridad y disponibilidad de otros registros que no necesariamente derivan de controles de seguridad de la información pero que son para cumplimiento legal y regulatorio, por ejemplo:

- Registros contables
- Roles de pago
- Balances contables
- Registros de pago de impuestos
- Expedientes de personal
- Órdenes de pago

2.3.9.3. Monitorear y revisar todo el EGSI

Estas actividades ayudan a la organización a determinar qué está sucediendo con su EGSI, a estimar el nivel de evolución de la seguridad de la información, a saber si se han reportado todos los incidentes de seguridad de la información, qué tipos de incidentes se han dado y finalmente, si todos los controles implementados se encuentran operando correctamente (Sánchez L. S.-O., 2012, págs. 89-90).

La importancia del monitoreo y la revisión del EGSI permitirá a la organización:

- Detectar oportunamente errores, incidentes y violaciones de seguridades.

- Proveer al Oficial de Seguridad de la Información el criterio suficiente para informar adecuadamente al Comité de Riesgos o a la Alta Dirección con respecto a que si la seguridad de la información se encuentra según lo esperado.
- Detectar oportunamente eventos o incidentes de seguridad, tener pro actividad.
- Determinar si las acciones tomadas anteriormente para resolver incidentes de seguridad de la información resultaron ser efectivas.

El monitoreo consiste en realizar revisiones regulares de la efectividad de todo el EGSI tomando en cuenta los resultados de auditorías de seguridad de la información, registro de incidentes, medición de eficacia de los controles, evaluaciones de las capacitaciones, resultados de encuestas, sugerencias y retroalimentación de todas las partes interesadas, etc.

Un factor muy importante para un adecuado monitoreo y revisión del EGSI es que el Oficial de Seguridad de la Información debe ejecutar por lo menos anualmente todo el procesos de análisis y evaluación de riesgos, y debe además revisar el nivel de riesgo residual y riesgo aceptable identificado, tomando en cuenta los cambios en la organización, la tecnología que utiliza, objetivos y procesos de negocio, efectividad de los controles implementados, cambios en el ambiente legal o regulador, cambios en obligaciones contractuales y cambios en el clima social, etc.

Parte del monitoreo consiste en realizar auditorías internas al EGSI en intervalos planeados, sin embargo, esta actividad será profundizada más adelante.

Debido a que el EGSI forma parte integral de un proceso de negocio llamado seguridad de la información, es necesario que este cuente con indicadores de desempeño (así como cada control que lo conforma tiene sus indicadores

propios); es así que parte del monitoreo y mejora consiste en que el Oficial de Seguridad de la Información por lo menos anualmente debe determinar si el EGSI cumplió o no con sus indicadores, y esto deberá ser reportado al Comité de Seguridad de la Información.

A continuación se enlistan a manera de ejemplos, ciertos criterios de revisión que el Oficial de Seguridad de la Información deberá considerar cuando realice la revisión del EGSI:

- Verificar si el plan de tratamiento de riesgos del año anterior se cerró oportunamente
- Verificar si los activos de información han variado con respecto al año anterior
- Ejecutar nuevamente la evaluación de riesgos para los activos de información identificados
- Verificar si cada uno de los controles implementados ha cumplido con sus indicadores de desempeño
- Estimar si se han reportado y registrado todos los incidentes de seguridad de la información.
- Verificar si para los incidentes registrados se ha dado tratamiento y cierre oportuno.
- Verificar si los incidentes registrados y tratados son recurrentes.
- Estimar el nivel de cumplimiento de buenas prácticas de seguridad de la información por parte de todo el personal de la organización.
- Determinar si el EGSI cumplió con sus indicadores de desempeño generales.
- Determinar el nivel de ausentismo a las jornadas de capacitación.

- Estimar si pudieran haber cambios tecnológicos, regulatorios, legales o de la organización que pudieran afectar a la seguridad de la información.

Es importante enfatizar que el monitoreo son las actividades de supervisión que el Oficial de Seguridad de la Información realiza constantemente, sin embargo, esto no es su responsabilidad exclusiva ya que cada jefe de área es responsable de que el personal bajo su cargo cumpla con los controles de seguridad de la información y aplique las mejores prácticas (ISACA, 2013, págs. 23-25).

Lo importante de esta actividad, así como identificar incumplimientos y oportunidades de mejora para el EGSI consiste en implementar estas mejoras identificadas mediante planes de acción a corto plazo que permitan tomar las acciones correctivas y preventivas que serán la base de la mejora continua del EGSI, estos planes de acción nunca deben quedar en papel.

Tal cual se considera a un plan de tratamiento de riesgos, un plan de remediación del EGSI también debe ser considerado como un programa que contiene varios proyectos a corto plazo; en caso de que una mejora deba ser implementada en el mediano o largo plazo, se deben tomar acciones mitigantes a ser utilizadas durante el periodo de implementación.

El objetivo de monitorear y revisar todo el EGSI es garantizar que todo lo que está mal sea corregido desde sus causas, es así que se requiere que las medidas correctivas y preventivas se apliquen sistemáticamente; es decir, que se identifique la raíz de una falla o incumplimiento, esta raíz o causa debe ser solucionada controlada.

2.3.9.4. Medir efectividad de los controles existentes

En base a lo que se revisó en los capítulos anteriores, cada uno de los controles que forman parte del EGSI deben ser diseñados considerando indicadores de gestión que determinen si su operación es la adecuada.

La medición de efectividad de los controles existentes no debe ser una tarea periódica sino un proceso que sea ejecutado diariamente sobre los controles que forman el EGSI, en tal virtud, dependiendo de la cantidad de controles, el Oficial de Seguridad de la Información deberá gestionar la adecuada provisión de recursos para el EGSI como una de las tantas tareas relacionadas a la operación (SGS, 2013, págs. 78-79).

Una guía muy robusta para el apoyo a este proceso es la Norma ISO/IEC 27004 publicada el 7 de diciembre del 2009; esta indica las métricas de seguridad y las técnicas de medida aplicables para determinar la eficacia y eficiencia de los controles relacionados al EGSI, este documento marca criterios de cara a una correcta medición de la eficacia de un SGSI que bien pudiera aplicarse a un EGSI, sin embargo, es necesario recalcar que la ISO/IEC 27004 no aporta una colección de métricas o indicadores a aplicar sino que establece una metodología para determinar la efectividad, motivo por el cual, el diseño de los indicadores o métricas a utilizarse dependen de la organización bajo la asesoría del Oficial de Seguridad.

Los objetivos de medir la efectividad de los controles que forman parte del EGSI son:

- Mejorar de la efectividad de la seguridad de la información en la organización a través de la evaluación constante de los controles del EGSI y su mejora continua.
- Generar información objetiva para soportar a la organización en la revisión del Comité de Seguridad de la Información, así

como en la toma de decisiones y la justificación de mejoras en los controles.

- Evaluar la efectividad de los controles de seguridad.

El Oficial de Seguridad de la Información debe asesorar a la organización para que las métricas con que se mida la efectividad de los controles del EGSI estén alineadas con lograr lo siguiente:

- Medir la evolución de la seguridad de la información en el tiempo.
- Las métricas deben considerar, en lo posible, estimación de impactos financieros, y ser coherentes con los objetivos de seguridad implantados.
- Las métricas deben ser objetivas e imparciales, nadie debe monitorear controles cuya ejecución dependa de sí mismo.
- Las métricas de monitoreo de los controles deben ser predictivas, consistentes y relevantes para la organización.
- Los resultados de las métricas deben servir para la toma de decisiones.
- Las métricas deben ser defendibles y justificables.
- Los resultados que las métricas arrojen deben derivar acciones a corto plazo, además, estos resultados deben ser fáciles de recolectar, definir, interpretar, y ser reproducibles.
- Las métricas de monitoreo de los controles del EGSI deben estar alineadas a los objetivos de negocio.

El primer responsable de monitorear el cumplimiento y medir la efectividad de los controles que forman parte del EGSI debe ser el jefe o gerente de cada una de las áreas (dueños de procesos) ya que, a diferencia del Oficial de Seguridad de la Información son quienes están en el día a día de los distintos procesos de negocio donde se deben aplicar los controles.

Mediante el uso de métricas para la evaluación de eficacia de los controles que forman parte del EGSI, el Oficial de Seguridad tendrá:

- Mejor panorama de los riesgos y debilidades de la organización relacionadas a seguridad de la información.
- Adecuada percepción con respecto al desempeño de los controles más acertada.
- Bases más centradas y mejor criterio para apoyar en la toma de decisiones.
- Mayor conocimiento y control de la situación real de la seguridad de la información en la organización.
- Apoyo a la racionalización de costes en los controles e iniciativas de seguridad de la información.
- Mayor eficacia de los procesos y actividades de seguridad de la información.
- Datos e información para la identificación oportuna de problemas e incidentes.
- Oportunidad de verificar del cumplimiento de políticas, normativas y procedimientos.
- Información creíble para mostrar la evolución de la cultura de seguridad de la información en la organización.

La razón más importante de realizar monitoreo de los controles que forman parte del EGSI radica en que lo que no se mide, no se puede mejorar.

2.3.9.5. Auditorías Internas

En medio de todo lo que involucra la operación diaria que demanda un EGSI, y, a pesar de revisarlo y monitorear sus controles, las organizaciones pudieran no ser conscientes de que su EGSI está operando inadecuadamente ya sea por fallas en los controles o por cuestiones relacionadas al personal; esto pudiera

llegar a comprometer a los activos de información, los riesgos pudieran convertirse en incidentes (Sánchez L. S.-O., 2012, págs. 129-130).

El objetivo de las auditorías internas es detectar cualquier deficiencia o incumplimiento tanto en la estructura del EGSI como en los controles que lo conforman, no con el objetivo de tomar acciones disciplinarias, sino aplicar acciones correctivas y/o preventivas (ISO/IEC, 2011, págs. 95-96)

La periodicidad de las auditorías internas es una decisión que deberá tomar el Comité de Seguridad de la Información, de todas formas, para organizaciones pequeñas, pudieran hacerse unas dos auditorías al año, mientras que para las organizaciones más grandes puede ser una serie de, por ejemplo, diez auditorías internas, todo dependerá del tamaño del proceso alcance y su distribución geográfica (ISO/IEC, 2011, pág. 94).

Las auditorías internas al EGSI deben proporcionar conclusiones certeras y confiables con respecto a si el EGSI de la organización:

- Cumple con los requisitos impuestos en el Acuerdo 166, mismos que se detallan en los distintos artículos.
- Cumple con la legislación y regulaciones relevantes
- Cumplen con los requisitos de seguridad de la información identificados
- Se implementa y mantienen de manera efectiva
- Los controles implementados operan adecuadamente
- Los controles existentes son los suficientes

La organización debe planear y formalizar un programa de auditoría tomando en consideración el proceso alcance, sus procesos de soporte y las áreas a ser auditadas, también deberá considerar (en caso de que existan) resultados de auditorías previas. El plan de auditorías internas debe definir el criterio, alcance, frecuencia y métodos de auditoría.

Otro componente del plan es la selección de los auditores internos, mismos que para proveer el valor que el EGSI y la organización requieren, deben por lo menos haber aprobado el curso de auditor interno ISO/IEC 27001, además, deben asegurar la objetividad e imparcialidad del proceso de auditoría, por lo que, los auditores no deben auditar su propio trabajo.

La calendarización de las auditorías también debe estar considerada en el plan, por lo que, como buena práctica se recomienda coordinar con los dueños de los procesos a ser auditados los días y horas de la auditoría con la finalidad de no entorpecer procesos de negocio y obtener la participación esperada de los auditados.

Así mismo, los dueños de los procesos o jefes de cada área a ser auditada deben asegurar que se den sin demora las acciones para eliminar las no-conformidades detectadas y sus causas. Las actividades de seguimiento deben ser realizadas por parte del Oficial de Seguridad de la Información quien deberá incluir la verificación de las acciones tomadas y el reporte de los resultados de verificación.

El plan de auditoría debe ser aprobado por el Comité de Seguridad de la Información, y, para la correcta puesta en marcha del mismo, es necesario que se comunique a todos los departamentos que se van a ver involucrados en la realización de la auditoría.

Es recomendable que en las capacitaciones se realice una inducción al personal involucrado a lo que son las auditorías internas, su periodicidad, su importancia y sus beneficios, con la finalidad de lograr mayor apertura.

El equipo auditor debe contar con una carta emitida ya sea por el Comité de Seguridad de la Información o por el máximo nivel jerárquico de la organización, esta carta es el formalismo que los auditores requieren para que las áreas involucradas participen en la auditoría y le den la prioridad del caso;

esta carta debe ser difundida a toda la organización junto con el plan de auditoría, así todos sabrán acerca de su participación.

El principal resultado de la auditoría interna del EGSI es el informe generado por el equipo auditor interno del que se podrán derivar una serie de acciones que ayuden a remediar los hallazgos detectados y que redunden en un mejor EGSI, por ello, la principal función de las auditorías internas es la de contribuir a la mejora continua y la gestión responsable de la información.

El proceso de auditoría interna no debe ser concebido como un acto dedicado a la inspección de las distintas áreas con tareas a veces incluso con tinte policíaco cuya finalidad es buscar culpables y sancionarlos, todo lo contrario, debe ser una vista como una oportunidad de mejora continua incluyente donde participen todos los involucrados en el EGSI.

Es importante recalcar que el EGSI de una organización tendrá un alcance específico y sus controles serán implementados en base a este alcance, sin embargo, así como existirán controles operativos propios de los procesos alcance, también habrán controles que deberán ser aplicados en toda la organización, es por esto que una auditoría interna, en caso de que el Oficial de Seguridad de la Información lo sugiera y el Comité lo apruebe, pudiera no necesariamente enmarcarse dentro del alcance del EGSI.

En base a lo anterior, también es de considerar que las jornadas de capacitación y toma de conciencia no deben estar enfocadas solamente al personal involucrado en el alcance del EGSI sino a toda la organización.

A continuación se describe un proceso de ejemplo básico para realizar auditorías internas al EGSI (ISO/IEC, 2011, págs. 45-47):

a. Elaborar el programa anual de auditorías internas considerando áreas a auditar, controles a auditar, equipo auditor, calendario, etc.
b. El programa debe ser aprobado por el Comité de Seguridad de la Información.
c. El Oficial de Seguridad de la Información debe socializar a toda la organización el plan de auditoría ya aprobado por el Comité de Riesgos.
d. Debido a que en el programa de auditorías debe considerarse la planificación de todas las auditorías a realizarse en el año, a parte de este plan, el equipo auditor (que estará liderado por un auditor jefe) debe elaborar el documento de planificación específico para cada auditoría.
e. Cada auditor que forma parte del equipo debe elaborar en base a su ámbito, listas de verificación a utilizarse en la próxima auditoría.
f. El Oficial de Seguridad de la Información debe comunicar a toda la organización las fechas de inicio y fin de la próxima auditoría (15 días hábiles antes de iniciar la auditoría)
g. Cada uno de los auditores toma contacto con el jefe de área y acuerda las horas de las entrevistas y visitas de auditoría (al menos 7 días hábiles antes de iniciar la auditoría)
h. El auditor jefe organiza a su equipo de auditores mantienen la reunión de apertura de la auditoría interna
i. El equipo auditor realiza las entrevistas y visitas de auditoría.
j. El equipo auditor analiza sus datos obtenidos y documenta los hallazgos con respecto a incumplimientos tanto en requisitos del Acuerdo 166 como en controles del EGSI.
k. El auditor jefe convoca a la reunión de cierre de la auditoría, en esta reunión cada integrante del equipo auditor expone y defiende sus hallazgos ante el resto del equipo que debe tener como finalidad interpretar y analizar lo expuesto.

l. En caso de que uno de los auditores requiera aclaración o pruebas que solventen su hallazgo, después de la reunión de cierre, el equipo debe tener por lo menos 5 días hábiles para documentar sus informes parciales de auditoría.
m. Con los informes parciales de auditoría, el auditor jefe procede a documentar el informe final de auditoría.
n. El informe final debe ser revisado y aprobado por el Oficial de Seguridad de la Información.
o. Una vez aprobado el informe, el Oficial de Seguridad de la Información realiza la convocatoria al Comité de Seguridad de la Información y a todos los dueños de las áreas involucradas a la presentación final del informe de auditoría interna.
p. El auditor jefe presenta ante el Oficial, el Comité de Seguridad de la Información y todos los jefes de las áreas auditadas los hallazgos de la auditoría interna al EGSI.
q. Luego de presentado el informe, cada auditor debe regresar al área que auditó y junto con un delegado del jefe, elaborar el plan de remediación (acciones preventivas o correctivas)
r. A pesar de que es responsabilidad del Oficial de Seguridad de la Información velar que los planes de acción acordados sean cerrados oportunamente, la siguiente auditoría deberá verificar si esto sucedió o no.
s. Las acciones planteadas en los planes de acción deberán ser analizadas por el Oficial de Seguridad de la Información ya que él debe registrarlas como acciones preventivas o correctivas, según sea el caso.

Con respecto a los registros que el proceso propuesto debe generar, se pueden nombrar los siguientes:

- Plan de auditorías formalizado
- Mail o acta de notificación del plan de auditorías a toda la organización
- Documentos de planificación específicos de cada auditoría
- Documentación soporte de cada auditor
- Mail o acta de comunicación de las fechas de inicio y fin de cada auditoría
- Acta de reunión de apertura de auditoría interna
- Informes parciales de auditoría
- Acta de reunión de cierre de auditoría interna
- Informe final de auditoría
- Acta de reunión de presentación de informe de auditoría interna
- Planes de acción

Con respecto al equipo de auditores, de acuerdo a lo que se indicó, es muy recomendable que hayan aprobado el curso de auditor interno ISO/IEC 27001, además de, conocer claramente la estructura y los requisitos de control que obliga el Acuerdo 166 para el EGSI de las organizaciones. Con el perfil indicado, el auditor interno podrá:

- Planificar y preparar una auditoría interna, así como reunir pruebas de auditoría mediante la observación, la entrevista y la toma de muestras de documentos y registros.
- Redactar informes de auditoría detallados que ayuden a mejorar la efectividad EGSI.

2.3.9.6. Revisión de la Dirección

En base a lo que se ha tratado a lo largo de todo este trabajo, un proyecto de diseño e implementación de un EGSI y su posterior operación, mantenimiento, supervisión y mejora continua depende de actores que funjan bajo escenarios

estratégicos, tácticos y operativos, es así que, la dirección o la alta gerencia de la organización debe saber qué está sucediendo con el EGSI y en general, con la seguridad de la información en su organización (Instituto Ecuatoriano de Normalización, 2010, pág. 47).

A pesar de que la máxima autoridad de la organización pudiera, para tareas tácticas y algunas estratégicas, estar representada por el Comité de Seguridad de la Información, debe de manera indelegable revisar el EGSI por lo menos una vez al año en una reunión donde el Oficial de Seguridad de la Información debe reportar aspectos relevantes relacionados a la operación del EGSI y al cumplimiento de controles, además de, sugerencias para la mejora continua.

Como se mencionó anteriormente, es muy importante que la máxima autoridad se involucre en el proyecto y posterior operación del EGSI, es por eso que la revisión por parte de la dirección está diseñada justamente para eso ya que en la presentación realizada por el Oficial de Seguridad de la Información se decidirá si se han cumplido con los objetivos del EGSI. Antes de finalizar la reunión de presentación, la máxima autoridad con el soporte del Comité y del Oficial de Seguridad de la Información debe decidir qué mejoras se deben implementar, considerando que las mejoras a nivel operativo y táctico serán determinadas en el monitoreo constante de controles y auditorías internas; las mejoras identificadas en esta reunión deben ser estratégicas.

La participación activa de la máxima autoridad dentro del EGSI es un componente primordial para la evolución de la seguridad de la información dentro de la organización, la importancia de esta participación radica en que el EGSI se relaciona con los procesos de la organización y afecta fundamentalmente a la gestión del negocio y requiere, por tanto, de decisiones y acciones que sólo puede tomar la gerencia de la organización.

No se debe caer en el error de considerar un EGSI una mera cuestión técnica o tecnológica relegada a niveles los inferiores operativos y en ciertos, es de vital

importancia tener siempre presente que la seguridad de la información está gestionando riesgos e impactos de negocio que son responsabilidad y decisión de la alta dirección.

El término Dirección no debe confundirse desde el punto de vista del alcance del EGSI, a pesar de que el proceso alcance tendrá una cabeza o propietario, es la máxima autoridad de la organización quien debe recibir el informe por parte del Oficial de Seguridad de la Información debido a que, a pesar de que el EGSI tenga un alcance establecido, los controles y las prácticas de seguridad deben aplicarse en toda la organización.

La máxima autoridad, al menos una vez al año debe revisar el EGSI para asegurar que continúe siendo adecuado y eficaz, para lo cual, debe recibir por parte del Oficial de Seguridad de la Información datos que soporten en la toma de decisiones, estos datos pueden ser:

- Índice de cumplimiento de los indicadores generales del EGSI.
- Resultados de auditorías y revisiones del EGSI.
- Observaciones y recomendaciones de las partes interesadas. Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del EGSI.
- Información sobre el estado de acciones preventivas y correctivas.
- Vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.
- Resultados de las mediciones de eficacia de los controles.
- Estado de las acciones iniciadas a raíz de revisiones anteriores de la dirección (si aplica).
- Cualquier cambio que pueda afectar al EGSI desde la perspectiva interna, comercial, legal o regulatoria.

- Cualquier recomendación de mejora que el Oficial de Seguridad de la Información pudiera sugerir.

Basándose en toda esta información, la dirección debe tomar decisiones y acciones relativas a:

- Mejora de la eficacia y operación del EGSI.
- Revisar el alcance del EGSI.
- Actualización de la metodología de evaluación de riesgos.
- Modificación de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.
- Necesidades de recursos para la gestión y operación de la seguridad de la información.
- Mejora de la forma de medir la efectividad de los controles, considerando indicadores o métricas de cada uno.
- Revisar los indicadores generales de todo el EGSI.

La revisión por la dirección debe comprender también un análisis ejecutivo presentado por el Oficial de Seguridad de la Información en el cual se indique si a través del EGSI la organización ha ganado o no valor en sus distintos procesos ya que es muy importante que la alta dirección conozca su el EGSI convive armónicamente con la entidad y su gente.

Finalmente, por recalcar que ninguno de los procesos de revisión, monitoreo y auditoría buscan establecer responsables y peor aún sanciones, simplemente lo que buscan es la mejora continua de la gestión de la seguridad de la información; el proceso disciplinario debe formar parte del proceso de administración del recurso humano.

CAPÍTULO 3. CONCLUSIONES Y RECOMENDACIONES

3.1. Conclusiones

- La implementación del Esquema Gubernamental de Seguridad de la Información puede ser considerada como un paso previo que permita adquirir experiencia y aprender de lecciones para una futura implementación de un Sistema de Gestión de la Seguridad de la Información con todos los requisitos de la Norma ISO/IEC 27001, mismo que, reforzado con los recursos adecuados, jornadas de capacitación, culturización del personal y madurez de los controles implementados pudiera incluso derivar en una Certificación ISO/IEC 27001.

- Con respecto a la función de seguridad de la información, en el Acuerdo Ministerial No. 166, la parte correspondiente a la evaluación de riesgos debió haberse reforzado debido a que el punto medular de la seguridad de la información es tener y aplicar una metodología de evaluación de riesgos de seguridad de la información, ya que sin esto, esta es incompleta, disfuncional y muy probablemente no tenga los resultados deseados por la dirección. el Acuerdo 166, para la evaluación de riesgos hace referencia a la ISO/IEC 27005, sin embargo, esta norma proporciona lineamientos para la gestión de riesgo de seguridad de la información en una organización de cualquier tipo, pero no provee ninguna metodología específica para el análisis y la gestión del riesgo de la seguridad de la información.

- El Esquema Gubernamental de Seguridad de la Información propone una serie de controles de tipo administrativo que deben ser instrumentados en papel (procedimientos, políticas, estándares, etc.), así también, la medición de su cumplimiento ha sido hecha a partir de los hitos cargados en el Sistema de Gestión de Proyectos

de la SNAP, sin embargo, no se han establecido parámetros de medición con respecto a la implementación de los controles y la capacitación al personal.

- En relación a los distintos controles que hacen parte del Esquema Gubernamental de Seguridad de la Información, por adecuado que sea el diseño y documentación, estos no podrán generar valor al negocio si no existe el apoyo, compromiso y predisposición por parte del personal que forma parte de la organización debido a que varios de estos controles están enfocados al cambio de cultura organizacional y al control interno bajo un esquema de monitoreo y mejora continua.

- El Acuerdo 166 propone un marco de gestión de la seguridad de la información, y, como tal requiere ser operado, mantenido y mejorado en el tiempo bajo la asesoría del Oficial de Seguridad de la Información, sin embargo, existe cierto riesgo que las organizaciones deberán considerar en caso de que opten por contratar los servicios de consultoría para el diseño e implementación de su EGSI ya que pudiera no adquirir los conocimientos para ejecutar todas las actividades inherentes a este.

3.2. Recomendaciones

- Se recomienda que las instituciones públicas aprovechen la disposición de diseñar e implementar el Esquema Gubernamental de Seguridad de la Información para crear y/o formalizar el área de Seguridad de la Información, misma que debe estar conformada por personal especializado en varias disciplinas, por ejemplo, riesgos, auditoría y seguridad informática con la finalidad de que las distintas instituciones gestiones adecuadamente los riesgos asociados a la

confidencialidad, integridad y disponibilidad de la información bajo un esquema de mejora continua de controles y procesos.

- Se recomienda que para el sector público del Ecuador, así como se obliga a la implementación del EGSI, la Secretaría Nacional de la Administración Pública genere una metodología de evaluación de riesgos de seguridad de la información, lo que permitirá que el sector público ser estándar en caso de tratarse de riesgos de seguridad de la información, además, habría mejor control por parte de la SNAP.

- Se recomienda a la Secretaría de la Administración Pública (SNAP) emprender campañas de sensibilización dirigidas a los Oficiales de Seguridad de la Información y a los líderes estratégicos de las organizaciones con la finalidad de dejar claro que el EGSI no es suficiente para detener ataques o mitigar riesgos sin el respectivo soporte físico, soporte tecnológico, la capacitación al personal y la suficiente provisión de recursos, además, se recomienda que las revisiones de seguimiento del SNAP tengan enfoque no solo al cumplimiento del Acuerdo 166 sino también un enfoque de cumplimiento al control interno, básicamente, verificar que se esté cumpliendo lo que está escrito en papel, algo que hasta la fecha no se lo ha realizado.

- Se recomienda a las instituciones públicas manejar estrategias de expectativa, difusión, capacitación, toma de conciencia y resistencia al cambio considerando a todos los niveles de la organización empezando desde el nivel estratégico ya que este es el llamado a predicar con el ejemplo para así disponer y forzar el cumplimiento por parte de los niveles inferiores. La estrategia debe considerar que no a todos los niveles se los debe tratar bajo el mismo foco de interés, e incluso, los tiempos que se tenga para trabajar no serán los mismos, de modo que, el Oficial de Seguridad de la Información

es el llamado a convencer al personal que la seguridad de la información es importante para la organización.

- Se recomienda que en caso de haberlos, como parte de los servicios profesionales contratados para el diseño e implementación del Esquema Gubernamental de Seguridad de la Información, se consideren también jornadas de transferencia de conocimientos y capacitación dirigidas específicamente para el Oficial de Seguridad de la Información y su personal de apoyo con la finalidad de que conozcan cómo operar, cómo evaluar, cómo actualizar y cómo mejorar el EGSI de la organización, incluso se podría considerar la existencia de un equipo del proyecto mixto entre consultor y personal interno.

REFERENCIAS

Artetio, J. (2008). Seguridad de la Información. Redes, informática y sistemas de información. En J. Artetio, Seguridad de la Información. Redes, informática y sistemas de información (págs. 20-22). Paraninfo.

Asociación Española de Normalización. (2013). Material Curso Auditor Interno ISO/IEC 27001.

Instituto Ecuatoriano de Normalización. (2010). Norma Técnica Ecuatoriana *INEN ISO/IEC 27001:2010 "Tecnologías de la Información. Técnicas de* Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI)".

ISACA. (2013). Material de Preparación para el Curso CISM.

ISC2. (2013). Official (ISC)²® Guide to the CISSP® CBK®. Auerbach Publications.

ISO/IEC. (2011). ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management .

ISO/IEC. (2011). ISO/IEC 27007:2011 Information technology — Security techniques — Guidelines for information security management systems auditing .

ISO/IEC. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements .

ISO/IEC. (2013). ISO/IEC 27003:2010 Information technology — Security techniques — Information security management system implementation guidance .

ISO27000.ES. (2005). ISO 27000.ES. Recuperado el 22 de septiembre de 2013, de http://www.iso27000.es/iso27000.html

Kosutic, D. (s.f.). Information Security & Business. Obtenido de www.iso27001standard.com

Mellado, D. S.-M. (2012). IT Security Governance Innovations: Theory and Research. IGI Global USA.

Sánchez, L. S.-O. (2012). Métricas de seguridad en los SGSIs, para conocer el nivel de seguridad de los SSOO y de los SGBD. Latindex.

Sánchez, L. S.-O.-M. (2011). ISMS Building for SMEs through the reuse of knowledge, Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions. IGI Global.

Sánchez, L. V. (2005). Towards a Model of Information Security Management for Small and Medium-Size Enterprises with ISO/IEC 17799. International Journal of Computer Science and Network Security (IJCSNS05).

Secretaría de la Administración Pública. (2014). Ranking de Cumplimiento del EGSI.

Secretaría Nacional de la Administración Pública. (2013). Acuerdo Ministerial No. 166.

SGS. (2013). Material del Curso de Auditor Líder ISO/IEC 27001:2005.

www.calidad-gestion.com.ar. (s.f.). Calidad y Gestión. Recuperado el 12 de 10 de 2014, de http://calidadgestion.wordpress.com/2013/03/11/enfoque-basado-en-procesos-como-principio-de-gestion/

ANEXOS

Anexo 1.- Ranking de Cumplimiento del EGSI

Secretaría Nacional de la Administración Pública

RANKING DE ENTIDADES PUBLICAS DEL CUMPLIMIENTO DE LA IMPLEMENTACION DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)

Implementación de los 126 hitos prioritarios
Periodo: 25 de septiembre de 2013 al 25 de marzo de 2014

Fecha de corte: 25 de marzo del 2014

RANKING	ENTIDAD	SIGLAS	EGSI: # DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % CALIDAD DE VERIFICABLES DE LOS HITOS EN EL GPR
1	Dirección Nacional de Registro de Datos Públicos	DINARDAP	122	96,83%	76,20%
2	Instituto Nacional de Economía Popular y Solidaria	IEPS	112	88,89%	99,60%
3	Ministerio de Turismo	MINTUR	107	84,92%	100,00%
4	Banco Central del Ecuador	BCE	107	84,92%	95,60%
5	Secretaría Nacional de Inteligencia	SENAIN	101	80,16%	50,19%
6	Consejo Nacional de Control de Sustancias Estupefacientes y Psicotrópicas	CONSEP	100	79,37%	95,80%
7	Ministerio de Educación	MINEDUC	100	79,37%	100,00%
8	Servicio de Rentas Internas	SRI	98	77,78%	56,12%
9	Secretaría Técnica de Discapacidades	SETEDIS	94	74,60%	93,00%
10	Secretaría Nacional de Planificación y Desarrollo	SENPLADES	82	65,08%	90,44%
11	Corporación del Seguro de Depósitos	COSEDE	80	63,49%	91,25%
12	Secretaría de Gestión de Riesgos	SGR	79	62,70%	100,00%
13	Ministerio de Defensa Nacional	MIDENA	78	61,90%	47,10%
14	Instituto Nacional de Pesca	INP	71	56,35%	77,57%
15	Instituto Nacional de Eficiencia Energética y Energías Renovables	INER	69	54,76%	52,13%
16	(*) Correos del Ecuador EP	CDE	61	48,41%	100,00%

RANKING	ENTIDAD	SIGLAS	EGSI: # DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % CALIDAD DE VERIFICABLES DE LOS HITOS EN EL GPR
17	Secretaría Nacional del Agua	SENAGUA	52	41,27%	78,78%
18	(*) Consejo Nacional de Cinematografía	CNCINE	50	39,68%	100,00%
19	Petromazonas EP	-	40	31,75%	0,00%
20	(*) Consejo Nacional de la Niñez y Adolescencia	CNNA	37	29,37%	100,00%
21	Instituto Nacional de Estadística y Censos	INEC	32	25,40%	60,89%
22	Autoridad Portuaria de Puerto Bolívar	APPB	27	21,43%	98,20%
23	Corporación Financiera Nacional	CFN	27	21,43%	95,60%
24	(*) Museo Ecuatoriano de Ciencias Naturales	MECN	27	21,43%	100,00%
25	Secretaría Técnica del Mar	STM	24	19,05%	94,79%
26	Instituto Geográfico Militar	IGM	21	16,67%	96,73%
27	Autoridad Portuaria de Manta	PPM	21	16,67%	10,80%
28	Servicio Nacional de Contratación Pública	SERCOP	21	16,67%	11,97%
29	Dirección General de Aviación Civil	DGAC	21	16,67%	75,00%
30	Instituto Nacional Autónomo de Investigaciones Agropecuarias	INIAP	17	13,49%	64,47%
31	Corporación de Desarrollo Afro	CODAE	17	13,49%	68,10%
32	Agencia Nacional de Tránsito	ANT	15	11,90%	75,00%
33	Secretaría de Hidrocarburos	SHE	13	10,32%	94,23%
34	Ministerio de Coordinación de la Política Económica	MCPE	10	7,94%	16,70%
35	Ministerio de Coordinación de la Producción, Empleo y Competitividad	MCPEC	10	7,94%	16,70%
36	Instituto Ecuatoriano de Propiedad Intelectual	IEPI	8	6,35%	80,00%
37	Autoridad Portuaria de Guayaquil	APG	8	6,35%	52,30%
38	Ministerio de Salud Pública	MSP	5	3,97%	80,00%
39	Instituto Ecuatoriano de Meteorología e Hidrología	INAMHI	5	3,97%	90,00%
40	Consejo Nacional de Salud	CONASA	5	3,97%	12,10%
41	(*) Instituto Nacional de la Meritocracia	INM	5	3,97%	50,00%

RANKING	ENTIDAD	SIGLAS	EGSI: # DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % CALIDAD DE VERIFICABLES DE LOS HITOS EN EL GPR
42	Ministerio de Coordinación de los Sectores Estratégicos	MICSE	4	3,17%	50,00%
43	Policía Nacional del Ecuador	PN	4	3,17%	100,00%
44	(*) Servicio Ecuatoriano de Capacitación Profesional	SECAP	4	3,17%	100,00%
45	Secretaría Nacional de Telecomunicaciones	SENATEL	4	3,17%	100,00%
46	Ministerio del Deporte	MD	3	2,38%	100,00%
47	Ministerio de Transporte y Obras Públicas	MTOP	3	2,38%	91,66%
48	Secretaría Nacional De Educación Superior, Ciencia, Tecnología e Innovación	SENESCYT	3	2,38%	100,00%
49	Transporte Aéreos Militares del Ecuador	TAME EP	3	2,38%	100,00%
50	Ministerio de Justicia Derechos Humanos y Cultos	MJDHC	3	2,38%	100,00%
51	Agencia de Regulación y Control Minero	ARCOM	2	1,59%	87,50%
52	(*) Agencia Nacional Postal	ANP	2	1,59%	100,00%
53	(*) Consejo Nacional de Discapacidades	CONADIS	2	1,59%	100,00%
54	(*) Instituto Espacial Ecuatoriano	IEE	2	1,59%	100,00%
55	(*) Ministerio del Ambiente	MAE	2	1,59%	100,00%
56	Corporación Nacional de Finanzas Populares y Solidarias	CONAFIPS	2	1,59%	100,00%
57	Dirección General de Registro Civil Identificación y Cedulación	DGRCIC	2	1,59%	100,00%
58	(*) Ecuador Estratégico EP	EE	2	1,59%	100,00%
59	(*) Instituto Nacional de Preinversión	INP	2	1,59%	100,00%
60	(*) Ministerio de Electricidad y Energía Renovable	MEER	2	1,59%	0,00%
61	(*) Transportes Navieros Ecuatorianos	Transnave	2	1,59%	0,00%
62	Fondo de Seguro Obligatorio de Accidentes de Tránsito	FONSAT	2	1,59%	100,00%
63	(*) Ministerio de Finanzas	MINFIN	2	1,59%	100,00%
64	(*) Servicio Nacional de Aduana del Ecuador	SENAE	2	1,59%	100,00%

RANKING	ENTIDAD	SIGLAS	EGSI: # DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % CALIDAD DE VERIFICABLES DE LOS HITOS EN EL GPR
65	Ministerio de Inclusión Económica y Social	MIES	1	0,79%	37,50%
66	Corporación Eléctrica del Ecuador EP	CELEC	1	0,79%	100,00%
67	(*) Astilleros Navales Ecuatorianos EP	ASTINAVE	1	0,79%	100,00%
68	(*) Instituto Nacional de Evaluación Educativa	INEVAL	1	0,79%	100,00%
69	(*) Ministerio de Coordinación de Seguridad	MICS	1	0,79%	100,00%
70	(*) Agencia de Regulación y Control Hidrocarburífero	ARCH	1	0,79%	0,00%
71	(*) Consejo de Gobierno del Régimen Especial de Galápagos	CGG	1	0,79%	0,00%
72	(*) Comisión de Tránsito del Ecuador	CTE	1	0,79%	0,00%
73	(*) Ministerio de Cultura y Patrimonio	MCYP	1	0,83%	50,00%
74	(*) Ministerio de Relaciones Laborales	MRL	1	0,79%	0,00%
75	Ministerio de Agricultura, Ganadería, Acuacultura y Pesca	MAGAP	0	0,00%	0,00%
76	Ministerio de Coordinación de Desarrollo Social	MCDS	0	0,00%	0,00%
77	Ministerio del Interior	MDI	0	0,00%	0,00%
78	Ministerio de Desarrollo Urbano y Vivienda	MIDUVI	0	0,00%	0,00%
79	Ministerio de Industrias y Productividad	MIPRO	0	0,00%	0,00%
80	Ministerio de Coordinación de Conocimiento y Talento Humano	MCCTH	0	0,00%	0,00%
81	Secretaría Nacional de Gestión Política	SNGP	0	0,00%	0,00%
82	Ministerio de Telecomunicaciones y de la Sociedad de la Información	MINTEL	0	0,00%	0,00%
83	Ministerio de Relaciones Exteriores y Movilidad Humana	MREMH	0	0,00%	0,00%

RANKING	ENTIDAD	SIGLAS	EGSI: # DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % CALIDAD DE VERIFICABLES DE LOS HITOS EN EL GPR
84	Ministerio de Recursos Naturales no Renovables	MRNNR	0	0,00%	0,00%
85	Ministerio de Comercio Exterior	MCE	0	0,00%	0,00%
86	Secretaría Nacional de Comunicación	SENACOM	0	0,00%	0,00%
87	Secretaría Técnica de Capacitación y Formación Profesional	SETEC	0	0,00%	0,00%
88	Secretaría Técnica de Cooperación Internacional	SETECI	0	0,00%	0,00%
89	Consejo Nacional de Aviación Civil	CNAC	0	0,00%	0,00%
90	Agencia Ecuatoriana de Aseguramiento de la Calidad del Agro	AGROCALIDAD	0	0,00%	0,00%
91	Consejo Nacional de Electricidad	CONELEC	0	0,00%	0,00%
92	Instituto para el Ecodesarrollo de la Región Amazónica	ECORAE	0	0,00%	0,00%
93	Instituto Ecuatoriano de Crédito Educativo y Becas	IECE	0	0,00%	0,00%
94	Servicio de Gestión Inmobiliaria del Sector Público	INMOBILIAR	0	0,00%	0,00%
95	Instituto (Servicio) de Contratación de Obras	SECOB	0	0,00%	0,00%
96	Agencia de Regulación y Control de la Bioseguridad y Cuarentena para Galápagos	ABG	0	0,00%	0,00%
97	Autoridad Portuaria de Esmeraldas	APE	0	0,00%	0,00%
98	Banco del Estado	BEDE	0	0,00%	0,00%
99	Banco Nacional de Fomento	BNF	0	0,00%	0,00%
100	Casa de la Cultura, Danza y Orquesta Sinfónica	CCDO	0	0,00%	0,00%
101	Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior	CEAACES	0	0,00%	0,00%
102	Corporación Nacional de Electricidad EP	CNEL	0	0,00%	0,00%

RANKING	ENTIDAD	SIGLAS	EGSI: # DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % CALIDAD DE VERIFICABLES DE LOS HITOS EN EL GPR
103	Hidroeléctrica Coca EP	COCASINCLAIR	0	0,00%	0,00%
104	Consejo de Desarrollo de las Nacionalidades y Pueblos Indígenas del Ecuador	CODENPE	0	0,00%	0,00%
105	Consejo de Desarrollo del Pueblo Montubio de la Costa Ecuatoriana y Zonas Subtropicales del Litoral	CODEPMOC	0	0,00%	0,00%
106	Empresa Eléctrica Pública de Guayaquil EP	EEPG	0	0,00%	0,00%
107	Empresa Eléctrica Quito EP	EEQ	0	0,00%	0,00%
108	Empresa de Municiones Santa Bárbara EP	EMSB	0	0,00%	0,00%
109	Empresa Nacional Minera del Ecuador EP	ENAMI	0	0,00%	0,00%
110	Empresa Pública de Fármacos EP	ENFARMA	0	0,00%	0,00%
111	Empresa Pública de Parques Urbanos y Espacios Públicos EP	EPPUEP	0	0,00%	0,00%
112	Empresa de Ferrocarriles del Ecuador EP	FEEP	0	0,00%	0,00%
113	Flota Petrolera Ecuatoriana EP	FLOPEC	0	0,00%	0,00%
114	Fondo de Desarrollo de las Nacionalidades y Pueblos Indígenas del Ecuador	FODEPI	0	0,00%	0,00%
115	Instituto Antártico Ecuatoriano	INAE	0	0,00%	0,00%
116	Instituto Nacional de Donación y Transplante de Órganos, Tejidos y Células	INDOT	0	0,00%	0,00%
117	Instituto Ecuatoriano de Normalización	INEN	0	0,00%	0,00%
118	Agencia Nacional de Regulación, Control y Vigilancia Sanitaria	ARCSA	0	0,00%	0,00%
119	Instituto Nacional de Investigación Geológico, Minero, Metalúrgico	INIGEMM	0	0,00%	0,00%
120	Instituto Oceanográfico de la Armada	INOCAR	0	0,00%	0,00%

RANKING	ENTIDAD	SIGLAS	EGSI: # DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % CALIDAD DE VERIFICABLES DE LOS HITOS EN EL GPR
121	Instituto Nacional de Patrimonio Cultural	INPC	0	0,00%	0,00%
122	Infraestructuras Pesqueras del Ecuador EP	IPEEP	0	0,00%	0,00%
123	Organismo de Acreditación Ecuatoriano	OAE	0	0,00%	0,00%
124	Instituto de Promoción de Exportaciones e Inversiones	PROECUADOR	0	0,00%	0,00%
125	Refinería del Pacífico Eloy Alfaro EP	RDP	0	0,00%	0,00%
126	Yachay EP	YACHAY	0	0,00%	0,00%

LEYENDA	
% HITOS CUMPLIDOS	NIVEL
90% a 100%	Alto
75% a 89 %	Medio
60% a 74 %	Regular
Menor a 60%	Bajo

Fuente del Ranking: Secretaría Nacional de la Administración Pública, Sistema de Gobierno por Resultados (GPR)

(*) Entidad que ha reportado los avances por email o por el QUIPUX debido a la falta de despliegue del GPR en las mismas

Secretaría Nacional
de la **Administración Pública**

ANEXO

RANKING DE ENTIDADES PUBLICAS DEL CUMPLIMIENTO DE IMPLEMENTACION DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)

1.- INTRODUCCION

La Secretaría Nacional de Administración Pública (SNAP), con fecha 19 de septiembre de 2013, emitió el Acuerdo Ministerial No. 166, publicado en el Registro Oficial No. 88 del 25 de septiembre de 2013, el cual dispone la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en todas las entidades de la Administración Pública Central, Institucional y Dependiente de la Función Ejecutiva (APCID). El EGSI está basado en la norma técnica ecuatoriana INEN ISO/IEC 27002 "Código de Práctica para la Gestión de la Seguridad de la Información". El EGSI especifica o señala 126 directrices cuya implementación debe ser prioritaria para las entidades públicas.

El Acuerdo Ministerial No. 166 otorga el plazo de 6 meses para que las entidades de la APCID implementen las 126 directrices marcadas como prioritarias en el EGSI; y el plazo de 12 meses adicionales para la implementación del resto de directrices. El mismo acuerdo determina también que el seguimiento y coordinación de la implementación del EGSI está a cargo de la SNAP, mediante el Sistema de Gobierno por Resultados (GPR).

Para cumplir con el seguimiento, la SNAP procedió a crear en el sistema GPR un programa institucional denominado "Gestión de la Seguridad de la Información en las entidades de la Administración Pública Central Institucional y Dependiente de la Función Ejecutiva". A la fecha, en este programa constan 126 entidades, a cada una de las cuales se solicitó crear un proyecto en el GPR que se alinee al programa y cuyos hitos sean las 126 directrices prioritarias del EGSI. Cada entidad pública debió fijar las fechas de cumplimiento de los hitos y cargar los documentos o verificables respectivos, según instrucciones impartidas por la SNAP.

En este contexto y virtud de lo dispuesto en el Acuerdo Ministerial No. 166, respecto al seguimiento y coordinación de la implementación del EGSI, la SNAP ha elaborado un ranking de entidades públicas que cumplen con la implementación del EGSI a partir de la información registrada en el sistema GPR. El plazo de tiempo de implementación de las directrices prioritarias corrió entre el 25 de septiembre de 2013 hasta el 25 de marzo de 2014 (6 meses).

Secretaría Nacional de la Administración Pública

2.- ELABORACION DEL RANKING

Para la elaboración del ranking, se tomó los datos ingresados por cada entidad en los proyectos de implementación del EGSI en el sistema GPR.

La posición de una entidad en el ranking se calcula en base al número de hitos marcados como cumplidos por la entidad frente al total de hitos a cumplir (126 en total).

Adicionalmente, se evalúa la calidad de los documentos cargados como verificables del cumplimiento de cada hito, en base a 4 criterios como se indica en la tabla 1:

No.	Criterio	Puntaje
1	El documento cargado al GPR cumple con el formato establecido para reportar cumplimiento de hitos	25
2	El documento cargado al GPR contiene las firmas de responsabilidad solicitadas	25
3	El documento cargado al GPR registra las acciones cumplidas relacionadas al hito	25
4	El documento cargado al GPR especifica a su vez el documento(s) interno de la entidad producto de la implementación de un hito	25
Puntaje calidad del verificable(s) de cada Hito		**100**

Tabla 1: Criterios para calificar documentos cargados como verificables de un hito del EGSI en el GPR

La puntuación de la calidad de los documentos cargados como verificables del cumplimiento de los hitos es el promedio de la suma del puntaje de todos los hitos cumplidos y expresada en porcentaje.

El ranking del EGSI se expresa en una tabla cuyas columnas se indican en la siguiente figura:

Ranking	ENTIDAD	SIGLAS	EGSI: # DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % DE CALIDAD VERIFICABLES EN EL GPR
↑ 1	↑ 2	↑ 3	↑ 4	↑ 5	↑ 6

Tabla del Ranking de Implementación del EGSI

- **Columna 1:** Número de orden en el Ranking

- **Columna 2**: Nombre de la entidad
- **Columna 3**: Siglas de la entidad
- **Columna 4**: Registra el número de hitos cumplidos por la entidad. Se toma el dato del sistema GPR y se verifica por cada entidad y la documentación de respaldo cargada al sistema GPR conforme a las directrices establecidas por la SNAP.
- **Columna 5**: Registra el porcentaje de cumplimiento de hitos de cada entidad, en base al número de hitos cumplidos frente al total de hitos que son 126.
- **Columna 6**: Registra el porcentaje de calidad de la documentación cargada al GPR como verificable del cumplimiento de los hitos. Se calcula en base a los criterios establecidos en la tabla 1.

Nota: Las entidades que por alguna razón reportaron los avances de cumplimiento de hitos por medio de correo electrónico o por medio del sistema QUIPUX están señaladas con (*) en el ranking del EGSI.

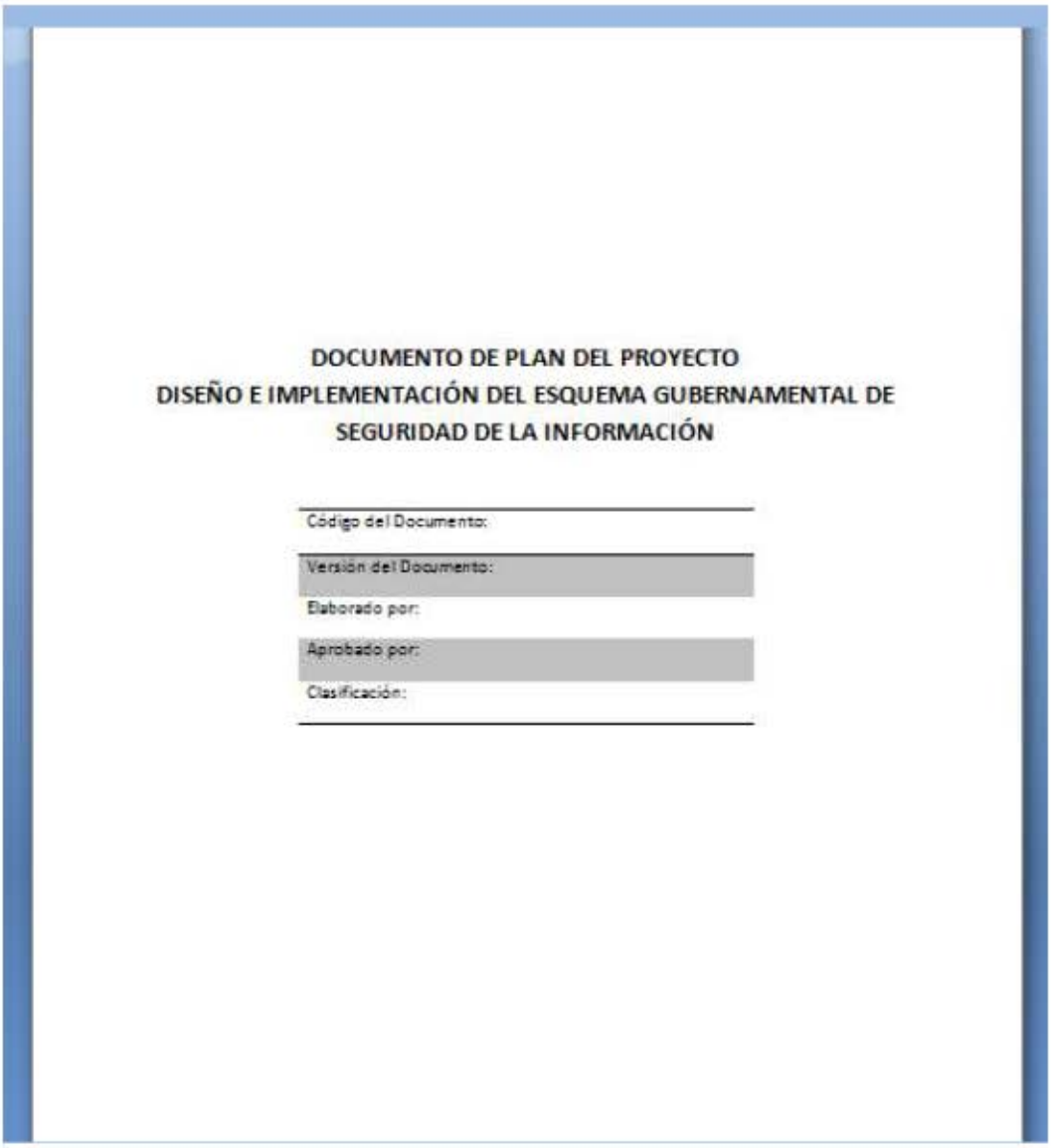
La tabla del ranking del EGSI establece también un nivel de cumplimiento de las entidades públicas en base a la cantidad de hitos, como se indica en la tabla 2.

% DE HITOS CUMPLIDOS EGSI	SEMÁFORO	NIVEL DE CUMPLIMIENTO EGSI
90% a 100%	Verde	Alto
75% a 89 %	Amarillo	Medio
50% a 74 %	Naranja	Regular
Menor a 50%	Rojo	Bajo

Tabla 2. Clasificación de cumplimiento del EGSI

Anexo 2.- Plan de Proyecto para Diseñar e Implementar el EGSI

(Kosutic)



DOCUMENTO DE PLAN DEL PROYECTO
DISEÑO E IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

Código del Documento:
Versión del Documento:
Elaborado por:
Aprobado por:
Clasificación:

Tabla de contenido

Anexo 3.- Texto para Formalizar y Comunicar acerca del EGSI

Fecha

Oficio No. XXX

Sres. Viceministros/Asesores/Gerentes/Directores/Coordinadores

Institución

Por disposición manifestada en el Acuerdo Ministerial No. 166 del mes de septiembre del año 2013, como institución pública, estamos obligados a la implementación del Esquema Gubernamental de Seguridad de la Información, motivo por el cual nombro como gerente del proyecto al Oficial de Seguridad de la Información, Ing. XXX XXX.

Particular que comparto para los fines pertinentes, solicitando a su vez total apoyo y compromiso para cumplir oportunamente los plazos establecidos.

Atentamente,

Máxima Autoridad de la Institución

Anexo 4.- Ejemplo Plan de Tratamiento de Riesgos

Documento (entregable)	Controles del Anexo a del Acuerdo 166	Entrega
Implementar Normativa de Revisión de la Política de Seguridad de la información y de todo el EGSI	1.2	Abril 2014
Actualizar Normativa de Roles y Responsabilidades de Seguridad de la Información en lo que corresponde al Comité de Seguridad de la Información	2.2 / 2.3	Abril 2014
Procedimiento de Control de Cambios	2.3 a) / 6.2 / 6.4 / 6.9 / 8.11 / 8.12 / 8.13	Abril 2014
Proceso de Autorización para nuevos servicios de procesamiento de información	2.4	Abril 2014
Procedimiento de Contacto con Autoridades y con grupos de interés especiales	2.6 / 2.7	Abril 2014
Normativa de Revisiones Independientes de Seguridad de la Información	2.8	Mayo 2014
Normativa de Seguridad de la Información con Terceros	2.9 / 2.10 / 2.11 / 6.7	Mayo 2014
Normativa de Gestión y Uso Aceptable de Activos de Información	3.1 / 3.2 / 3.3 / 6.15 / 6.16 / 6.21 / 7.8 i /	Mayo 2014
Normativa de manejo y etiquetado de activos de información	3.5 / 6.17	Mayo 2014
Normativa de Capacitaciones e Inducciones de Seguridad de la Información	4.5	Mayo 2014
Normativa de Trabajo en Áreas Seguras para Activos de Información	5.2 / 5.3 / 5.4 / 5.5 / 5.6 / 5.7 / 5.8 / 5.9 / 5.10 / 5.11 / 5.12 / 5.13	Mayo 2014
Procedimiento para operación	6.1	Mayo 2014
Normativa de Segregación de Funciones	6.3	Junio 2014
Actualizar Normativa de Respaldos de Información	6.12 d al i	Junio 2014
Normativa de Controles de Redes	6.13 / 6.14 c) / 7.9 / 7.11 / 7.12 / 7.13 / 7.14 / 7.15 / 7.16	Junio 2014