Maestría

María Belén Jiménez Amoroso

ADMINISTRACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA NACIONAL DE COMUNICACIÓN ENFOCADO A LA INFRAESTRUCTURA TECNOLÓGICA

Disertación presentada como requisito parcial para la obtención del Título de Magíster en Administración de Empresas de la Universidad Del Pacífico bajo la dirección de la Profesora Magister Nélcar Thais Camacho Salas.

UNIVERSIDAD DEL PACÍFICO

Quito, 2017

JIMÉNEZ, María Belén, Administración del sistema de gestión de seguridad de la información de la Secretaría Nacional de Comunicación enfocado a la infraestructura tecnológica. Quito: UPACÍFICO, 2017, 214p. Mg. Nélcar Thais Camacho Salas (Trabajo de Conclusión de Maestría presentado a la Facultad de Negocios y Economía de la Universidad Del Pacífico).

Resumen: La Secretaría Nacional de Comunicación siendo una entidad cuyo enfoque está dirigido puntualmente a brindar información clara y oportuna sobre los hechos y acontecimientos del entorno gubernamental, debe precautelar los activos de información vinculados a la infraestructura tecnológica, recurso por el cual circula la información digital.

El Servicio Ecuatoriano de Normalización del Ecuador, señala que la seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, incluidas las estructuras organizacionales, políticas, procesos, procedimientos, entre otros.

Estos controles se deben planificar, implementar, revisar y mejorar; es decir gestionar cuando sea necesario, para asegurar que se cumplen los objetivos de seguridad y por ende los objetivos estratégicos de una organización.

Bajo este contexto, el presente trabajo realiza una radiografía a la situación actual en la que se encuentra el sistema de gestión de seguridad de la información y plantea mejoras en la administración del mismo, dentro de la Secretaría Nacional de Comunicación enfocándose en la infraestructura tecnológica, para de esta manera minimizar los riesgos ante daños a la institución.

Palabras claves: Seguridad, Riesgos, Información.

UNIVERSIDAD DEL PACÍFICO ECUADOR	**ENTREGA DE TRABAJO (CONCLUSIÓN DE CARRERA DE GRADO)**	Fecha: 09/07/2015
		Versión: 001
	PA-FR-67	Página: 1 de 1

DECLARACIÓN

Al presentar este Trabajo de Maestría como uno de los requisitos previos para la obtención del grado de Magister en Administración de Empresas de la Universidad Del Pacífico, hago entrega del documento digital, a la Biblioteca de la Universidad.

El estudiante certifica estar de acuerdo en que se realice cualquier consulta de este Trabajo de Maestría dentro de las Regulaciones de la Universidad, acorde con lo que dictamina la L.O.E.S. 2010 en su Art. 144.

Conforme a lo expresado, adjunto a la presente, se servirá encontrar cuatro copias digitales de este Trabajo de Maestría para que sean reportados en el Repositorio Nacional conforme lo dispuesto por el SENESCYT.

Para constancia de esta declaración, suscribe

María Belén Jiménez Amoroso
Estudiante de la Facultad de Negocios
Universidad Del Pacífico

Fecha:	**Quito, julio del 2017**
Título de T.C.C.:	**Administración del sistema de gestión de seguridad de la información de la Secretaría Nacional de Comunicación enfocado a la infraestructura tecnológica**
Autor:	**María Belén Jiménez Amoroso**
Tutor:	**Mgs. Nelcar Thais Camacho Salas**
Miembros del Tribunal:	**Mgs. Alejandro Rodrigo Cueva Rueda**
	Mgs. Antonio José Mendoza García
Fecha de calificación:	**Julio del 2017**

Índice

Índice Gráficos

Índice Tablas

Resumen

La información es uno de los bienes intangibles más sensibles para cualquier organización por lo que es de vital importancia gestionarla de manera adecuada, toda vez que la misma está sujeta a diversos tipos de ataques.

Los ataques pueden presentarse sobre la confidencialidad, integridad o disponibilidad de la información, en forma de vulnerabilidades o amenazas; lo cual causa un impacto que puede llegar, incluso a destruir a una organización.

En este sentido, la Secretaría Nacional de Comunicación siendo una entidad cuyo enfoque está dirigido puntualmente a brindar información clara y oportuna sobre los hechos y acontecimientos del entorno gubernamental, debe precautelar los activos de información vinculados a la infraestructura tecnológica, recurso por el cual circula la información digital.

El Servicio Ecuatoriano de Normalización del Ecuador, señala que la seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, incluidas las estructuras organizacionales, políticas, procesos, procedimientos, entre otros.

Estos controles se deben planificar, implementar, revisar y mejorar; es decir gestionar cuando sea necesario, para asegurar que se cumplen los objetivos de seguridad y por ende los objetivos estratégicos de una organización.

Bajo este contexto, el presente trabajo realiza una radiografía a la situación actual en la que se encuentra el sistema de gestión de seguridad de la información y plantea mejoras en la administración del mismo, dentro de la Secretaría Nacional de Comunicación enfocándose en la infraestructura tecnológica, para de esta manera minimizar los riesgos ante daños a la institución.

Capítulo I

1. El Problema

1.1. Planteamiento del Problema

La información es uno de los bienes intangibles más poderosos, representativos e importantes de cualquier entidad. En este sentido, es fundamental brindarle el debido tratamiento, a fin de que la misma cuente con disponibilidad, confidencialidad e integridad; es decir con seguridad.

Un sistema de gestión de seguridad de la información permite a las entidades regular sus procesos internos a fin de tomar medidas preventivas ante posibles violaciones.

Las violaciones a la información, pueden presentarse a través de la infraestructura tecnológica, toda vez que es el enlace entre una red de datos externa y el entorno institucional por el que circula la información de carácter digital.

En este contexto, se ha revisado que la Secretaría Nacional de Comunicación, pese a estar conformada desde el 30 de mayo de 2013, no cuenta con una correcta administración del sistema de gestión de seguridad de la información en su infraestructura tecnológica, debilitando así, uno de sus objetivos estratégicos, que es el de incrementar la imagen gubernamental, difusión de información y relacionamiento ciudadano de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.

Por lo expuesto, y considerando que la Constitución de la República del Ecuador, establece que todas las personas, en forma individual o colectiva, tienen derecho a buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura

previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior e igualmente acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas; es prioritario y fundamental garantizar que la seguridad de la información sea gestionada correctamente, por lo que se debe hacer uso de un proceso sistemático, documentado y conocido por toda la Secretaría Nacional de Comunicación, desde un enfoque de riesgo institucional.

1.2. Objetivos de la Investigación

1.2.1. Objetivo General

Diseñar y administrar un sistema de gestión de seguridad de información para la infraestructura tecnológica de la Secretaría Nacional de Comunicación.

1.2.2. Objetivo Específico

Evaluar el estado actual en el que se encuentran los activos de la información dentro de la infraestructura tecnológica de la Secretaría Nacional de Comunicación.

Proponer un diseño que permita optimizar los recursos de infraestructura y de esta manera se pueda brindar seguridad a la información.

Realizar un análisis de factibilidad en relación al costo beneficio que involucra el mantener la administración de un sistema de gestión de la información.

1.3. Justificación

La Secretaría Nacional de Comunicación es de vital importancia para todo el aparato gubernamental siendo ésta la imagen estratégica en el entorno político y mediático del Ecuador.

El no contar con una correcta administración y un diseño de un sistema de gestión de seguridad de la información, deja abierto el camino para que aumente el riesgo de la data que circula en la infraestructura de la Secretaría Nacional de Comunicación.

Dicho esto, no se puede descuidar el tratamiento que se brinda a la información en cuanto a confidencialidad, disponibilidad e integridad siendo necesario contar con un diseño y administración que apalanque las mejores prácticas de seguridad sobre todo de la infraestructura tecnológica.

1.4. Alcance y Limitaciones

La visión de la Secretaría Nacional de Comunicación es ser la institución del Gobierno que fomente la democratización de la comunicación en el país, generando nuevos espacios de información, difusión e imagen con atributos de calidad, veracidad y cercanía a todos los ciudadanos y ciudadanas del Ecuador.

En la actualidad la información es uno de los activos más importantes de cualquier organización sea esta pública o privada, en este contexto se debe conocer qué tipo de información se considera sensible, conocer el tipo de personal que maneja la información, y si existe un compromiso real por parte de los gerentes tecnológicos en cuanto al manejo de sus fuentes de almacenamiento; todo esto enfocados en la seguridad de la información, cuya función es la adopción de medidas preventivas y reactivas.

Por lo indicado, la tesis asociará los conceptos gerenciales con los técnicos, pues se aplicará la administración en un sistema de gestión de seguridad de la información, puntualmente de los activos que se vinculan a la infraestructura tecnológica, cuyo impacto sea significativo para la institución. Sobre esto, se obtendrán pautas y emitirán recomendaciones para generar la mejora continua, que es la base de un sistema de gestión para la Secretaría Nacional de Comunicación; comprendiendo el costo beneficio que tiene el proyecto para el Estado ecuatoriano.

La principal limitación que puede presentarse para la puesta en marcha del sistema de gestión de seguridad de la información planteado, es la falta de apoyo por parte de las autoridades de la institución.

Capitulo II

2. Marco Teórico

2.1. Antecedentes de la Investigación

Se ha realizado una búsqueda previa a nivel mundial sobre trabajos de investigación que tengan extractos importantes y vinculados con la presente tesis, encontrando lo siguiente:

En el Repositorio Digital de la Universidad Regional Autónoma de los Andes, UNIANDES – Ecuador, existe la tesis con el tema Plan de Contingencia Informática y la Pérdida de la Información en la Corporación Nacional de Electricidad "CNEL" Regional Santo Domingo, desarrollada en el año 2016, por el Ing. Juan Carlos Simbaña Diaz, de la cual se puede extraer que a la información, nunca está de más tenerla protegida ante a cualquier eventualidad que le pudiese ocurrir como es el "Plagio, Hurto, Infecciones de virus informáticos" o daños físicos a los dispositivos que la contienen como los computadores o los servidores de cada uno de los sistemas de la corporación Nacional de Electricidad "CNEL" regional Santo Domingo; es decir, que invertir en seguridad de la información, a la larga no es un gasto, al contrario es un beneficio que se lo nota a largo plazo. (Simbaña, J. C. (2017). Plan de contingencia informática y la pérdida de la información en la Corporación Nacional de Electricidad CNEL Regional Santo Domingo. (Universidad Regional Autónoma de los Andes)).

En el Repositorio Digital de la Universidad Complutense de Madrid, España, en el año 2012, Ofelia Tejerina Rodríguez presentó la tesis doctoral denominada "Protección de Datos y Seguridad de Estado", la cual se resume en que: el permanente desarrollo tecnológico de la sociedad ha supuesto un replanteamiento del sistema de derechos fundamentales en todos los países

desarrollados, requiriendo nuevos mecanismos legales de amparo ante potenciales amenazas que se supone están surgiendo del ámbito de la "Sociedad de la Información". Concretamente, se analiza la influencia de la tecnología sobre el derecho a la protección de datos de carácter personal, en actuaciones de la Administración Pública que tienen como finalidad preservar la Seguridad del Estado. (Rodríguez, O (2012). Protección de Datos y Seguridad de Estado. (Universidad Complutense de Madrid, España)).

En el Repositorio Documental de la Universidad de Salamanca, apartado de tesis doctorales, año 2014, bajo el tema Calidad de la información en relación con la automedicación en internet, Ana Belén Martín Fombellida, da a conocer la importancia de la protección de datos en la rama de la medicina, mediante la observación efectuada respecto a la influencia de la tecnología en la integridad de la información enfocada a los procesos de automedicación. (Martín, A. B. (2014). Calidad de la información en relación con la automedicación en internet. (Universidad de Salamanca)).

Oscar Rebollo Martínez, mediante su tesis doctoral Marco para el Gobierno de la Seguridad de la Información en servicios Cloud Computing, presentada en la Universidad de Castilla-La Mancha, España 2014, señala que el principal problema de seguridad que está frenando la adopción del Cloud Computing es la pérdida de control de la organización sobre sus activos de información, lo que significa que una estrategia de Gobierno de Seguridad de la Información debe ser desarrollada. Adicionalmente, expone que la seguridad no puede ser entendida únicamente como un aspecto técnico, sino que se trata de una cuestión multidisciplinar que debe involucrar a todos los niveles de la organización. (Rebollo, O. (2014). Marco para el Gobierno de la Seguridad de la Información en servicios Cloud Computing. (Universidad de Castilla)).

Como se puede observar existe una diversidad de áreas y giros de negocio que han considerado importante la seguridad de la información y sobre todo las bondades que se pueden tener una correcta administración de un sistema de gestión.

2.2. Bases Teóricas

Toda tesis debe estar siempre acompañada de los fundamentos conceptuales y teóricos que fortalezcan la comprensión de la misma. Para ello, se han recopilado las descripciones de los términos a utilizar.

2.2.1. Información

Es un recurso que poseen todas las entidades, sean estas públicas o privadas, que le da sentido al giro del negocio, pues permite tomar decisiones o resolver problemas. En ella se enfoca la base de conocimiento y de esta depende el mejoramiento continuo de las organizaciones. (Ponjuán, G. (1998). Gestión de información en las organizaciones: principios, conceptos y aplicaciones).

Para el propósito del presente documento se consideran tres (3) lineamientos esenciales de la información, las cuales son:

Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. ((2012, 01). Obtenido 05, 2017, de http://www.iso27000.es/sgsi.html).

Integridad: Cualidad de la información que se considera exacta, completa, homogénea, sólida y coherente con la intención de los creadores de esos datos. Esta cualidad se obtiene cuando se impide eficazmente la inserción, modificación o destrucción no autorizada, sea accidental o intencional del contenido de una base de datos. ((2017, 01). Obtenido 05, 2017, de http://computer.yourdictionary.com/dataintegrity).

Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. ((2012, 01). Obtenido 05, 2017, de http://www.iso27000.es/sgsi.html).

La información puede ser análoga o digital, por ejemplo, el texto en un libro, una conversación presencial, etc.; se considera información analógica, mientras que la información digital es rápidamente procesable mediante infraestructura tecnológica, permitiendo efectuar búsquedas, modificaciones, es decir dar tratamiento a la información, lo cual de cierta manera la hace más vulnerable.

2.2.2. Activos de la Información

Es todo aquello que tiene algún valor para las entidades y que debe ser protegido. Es decir, todo lo que genera, transmite o destruye información.

Matalobos, J. (2009), señala que es aquello que tiene algún valor para las entidades y que debe ser protegido. Es decir, todo lo que genera, transmite o destruye información.

Por citar varios ejemplos de activos de información se pueden considerar: bases de datos, contratos, acuerdos, manuales de usuarios, aplicaciones desarrolladas o adquiridas, software, equipos informáticos, bienes muebles e inmuebles, e incluso personal; entre otros.

Cada activo que logre identificarse debe mantener un propietario de la información, quien estará a cargo de brindar integridad, confidencialidad y disponibilidad a los activos.

Acciones que se efectúan con los activos de información:

- Identificación de los activos
- Valoración de los activos

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos. (Bertolín, J. A. (2008). Seguridad de la información. Redes, informática y sistemas de información. Editorial Paraninfo).

2.2.3. Vulnerabilidades y Amenazas

La vulnerabilidad corresponde a la predisposición o susceptibilidad que tiene un elemento de ser afectado o de sufrir una pérdida. En consecuencia, la diferencia de vulnerabilidad de los elementos determina el carácter selectivo de la severidad de los efectos de un evento externo sobre los mismos.

La vulnerabilidad, en términos generales, puede clasificarse como de carácter técnico y de carácter social, siendo la primera más factible de cuantificar en términos físicos y funcionales, por ejemplo, en pérdidas potenciales referidas a los daños o la interrupción de los servicios, a diferencia de la segunda, que prácticamente sólo puede valorarse cualitativamente y en forma relativa, debido a que está relacionada con aspectos económicos, educativos, culturales, ideológicos, etc.

En consecuencia, un análisis de vulnerabilidad es un proceso mediante el cual se determina el nivel de exposición y la predisposición a la pérdida de un elemento o grupo de elementos ante una amenaza específica, contribuyendo al conocimiento del riesgo a través de interacciones de dichos elementos con el ambiente peligroso. Los elementos bajo riesgo son los contextos social y material, representados por las personas y por los recursos y servicios que pueden ser afectados por la ocurrencia de un evento, es decir, las actividades humanas, los sistemas realizados por el hombre

tales como edificaciones, líneas vitales o infraestructura, centros de producción, utilidades, servicios y la gente que los utiliza. (Cardona, O. (2009). Evaluación De La Amenaza, la Vulnerabilidad y el Riesgo).

Una amenaza es la existencia de algún mecanismo, que activado, permite explotar una vulnerabilidad. Una amenaza para poder causar daño a un activo debe estar asociada a una vulnerabilidad en el sistema, aplicación o servicio. (Barnes, J. C. (2001). A Guide to Business Continuity Planning).

Un incidente es cuando coinciden una vulnerabilidad y una amenaza afectando el funcionamiento de la organización; es decir, es la concreción de una amenaza. (Hiles, A. (2004). Business Continuity: Best Practices: World-class Business Continuity Management. Rothstein Associates Inc.).

2.2.4. Riesgos

Conocer el riesgo a los que están sometidos los activos es imprescindible para poder gestionarlos, y por ello han surgido una multitud de guías informales, aproximaciones metódicas y herramientas de soporte las cuales buscan objetivar el análisis para saber cuán seguros o inseguros están dichos activos y no llamarse a engaño.

El riesgo es definido como la probabilidad que una amenaza pueda explotar una vulnerabilidad en particular. (Peltier, T. (2001). Information Security Risk Analysis, Auerbach).

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son

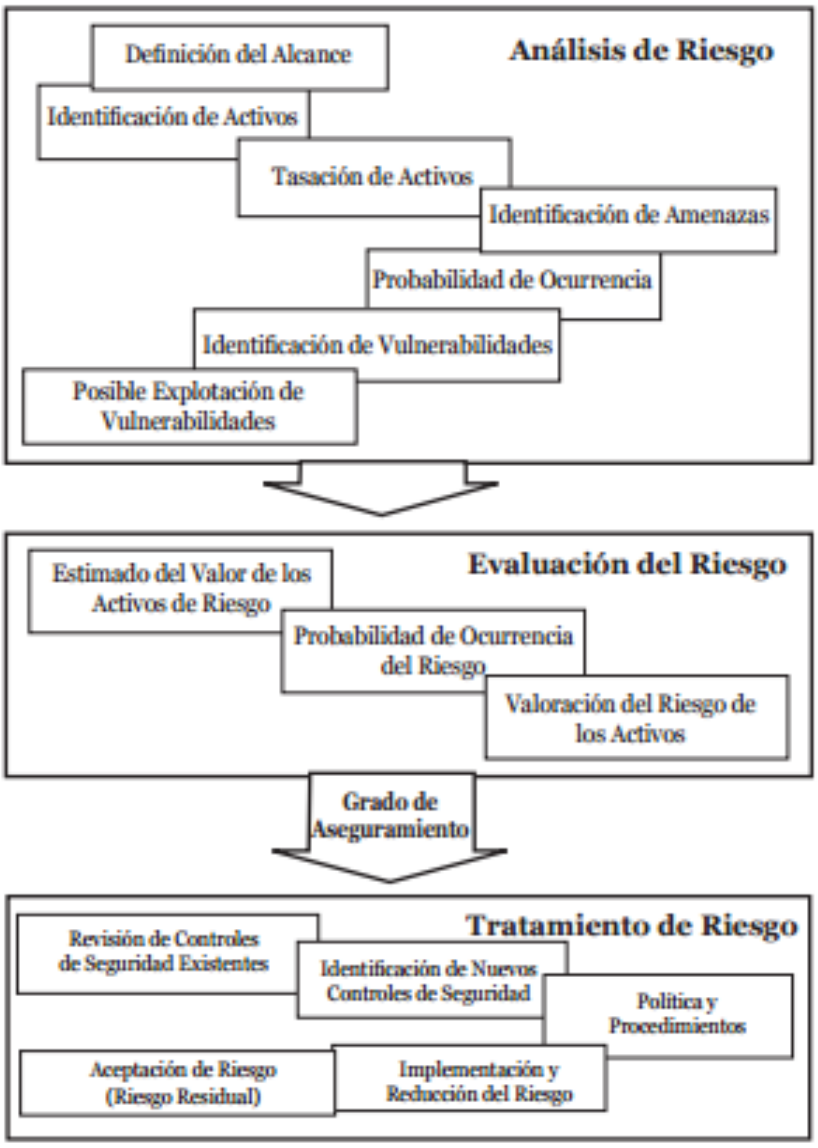
algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un sistema de gestión de seguridad de la información, es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones. El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

En el tratamiento de riesgos, se puede enumerar cuatro opciones:

- Implementar los controles de seguridad que recoge el Anexo A de la norma ISO 27001.
- Transferir el riesgo. Esto podría ser, por ejemplo, cuando contratamos una póliza de seguro y transferimos el riesgo a la compañía de seguros que nos la ha vendido.
- Aceptar el riesgo en cuestión. Esta opción sería para aquellos casos en lo que el coste de eliminar el riesgo es mayor que el daño que causará.

Evitar el riesgo. Esto se puede conseguir paralizando aquella actividad que supone demasiado nivel de riesgo o haciéndola de una manera diferente. ((2012, 01). Obtenido 05, 2017, de http://www.iso27000.es/sgsi.html).



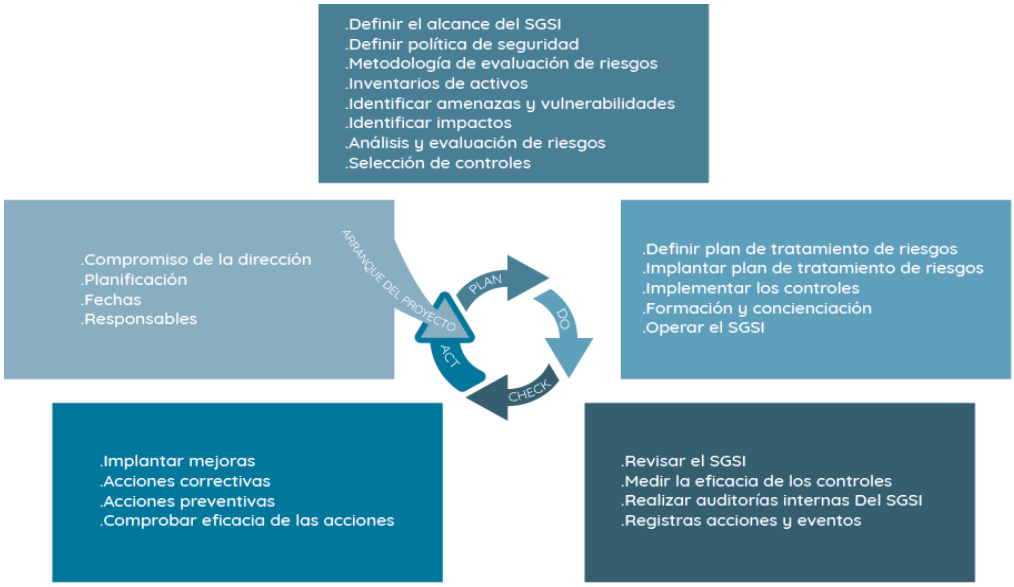
Fuente: Freitas, V. (2009).

Gráfico 1. Gestión de Riesgos

2.2.5. Sistema de Gestión de Seguridad de Información (SGSI)

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente. (Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management).

Para establecer y administrar/gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo de Deming o PDCA (Plan, Do. Check, Act); que es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart.



Fuente: Obtenido de www.ISO27000.es

Gráfico 2. Ciclo de Deming (PDCA) aplicado a Sistemas de Gestión de Seguridad de la Información

Plan (planificar): Establecer el SGSI. Se planifica y diseña el programa, sistematizando las políticas a aplicar en la organización, cuáles son los fines a alcanzar y en qué ayudarán a lograr los objetivos de negocio, qué medios se utilizarán para ello, los procesos de negocio y los activos que los soportan, cómo se enfocará el análisis de riesgos y los criterios que se seguirán para gestionar las contingencias de modo coherente con las políticas y objetivos de seguridad.

Do (hacer): implementar y utilizar el SGSI. Las políticas y los controles escogidos para cumplirlas se implementan mediante recursos técnicos, procedimientos o ambas cosas a la vez, y se asignan responsables a cada tarea para comenzar a ejecutarlas según las instrucciones.

Check (verificar): Monitorizar y revisar el SGSI. Hay que controlar que los procesos se ejecutan como se ha establecido, de manera eficaz y eficiente, alcanzando los objetivos definidos para ellos. Además, hay que verificar el grado de cumplimiento de las políticas y procedimientos, identificando los fallos que pudieran existir y, hasta donde sea posible, su origen, mediante revisiones y auditorías.

Act (actuar): Mantener y mejorar el SGSI. Se deciden y efectúan las acciones preventivas y correctivas necesarias para rectificar los fallos, detectados en las auditorías internas y revisiones del SGSI, o cualquier otra información relevante para permitir la mejora permanente del SGSI.

Esta metodología ha demostrado su aplicabilidad y ha permitido establecer la mejora continua en organizaciones de todas clases. (Andrés, A., Gómez, L. (2009). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. AENOR.).

2.2.6. ISO (Internacional Organization for Standardization) - Organización Internacional de Normalización

Su principal actividad es la elaboración de normas técnicas internacionales.

Las normas ISO contribuyen a que el desarrollo, la producción y el suministro de bienes y servicios sean más eficaces, seguros y transparentes. Gracias a estas normas, los intercambios comerciales entre países son más fáciles y justos. Proporcionan a los gobiernos un fundamento técnico para la legislación en materia de salud, seguridad y medio ambiente. También contribuyen a la transferencia de tecnología a los países en vías de desarrollo y, además, sirven para proteger a los consumidores y usuarios en general, ante cualquier problema surgido de un producto o servicio, haciéndoles la vida más sencilla.

2.2.7. Norma

Es un documento público, consensuado por todas las partes interesadas y aprobado por un organismo de normalización reconocido.

Las normas contienen especificaciones técnicas basadas en los resultados de la experiencia y del desarrollo tecnológico. Son una herramienta de desarrollo económico y social de un país, ya que sirven como base para mejorar la calidad en la gestión, el diseño y producción de los productos y servicios, y para aumentar la competitividad en los mercados nacionales e internacionales. ((2015, 01). Obtenido 05, 2017, de http://fundibeq.es).

2.2.8. ISO/IEC 27001:2005 Tecnología de la información - Técnicas de seguridad - Sistemas de Gestión de la Seguridad de la Información (SGSI)

Esta norma internacional proporciona un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de gestión de Seguridad de la Información (SGSI). (Mesquida, A. L., Mas, A., Amengual, E., & Cabestrero, I. (2010). Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. REICIS. Revista Española de Innovación, Calidad e Ingeniería del Software).

2.2.9. ISO/IEC 27002:2013 Tecnologías de la información - Técnicas de seguridad - Código de práctica para los controles de seguridad de la información

Esta norma establece directrices para la seguridad de la información en las organizaciones y prácticas de gestión de seguridad de la información incluyendo la selección, la implementación, y la gestión de los controles teniendo en consideración el entorno de riesgos de seguridad de la información de la organización.

Está diseñada para ser utilizada por las organizaciones que pretendan:

a) Seleccionar controles en el proceso de implantación de un Sistema de Gestión de Seguridad de la información basado en ISO/IEC 27001;

b) Implementar controles de seguridad de la información comúnmente aceptados;

c) Desarrollar sus propias directrices de gestión de seguridad de la información. ((2017, 01). Obtenido 05, 2017, de www.iso.org).

2.2.10. ISO/IEC 9001:2015

Norma sobre gestión de la calidad con mayor reconocimiento en todo el mundo. Pertenece a la familia ISO 9000 de normas de sistemas de gestión de la calidad (junto con ISO 9004), y ayuda a las organizaciones a cumplir con las expectativas y necesidades de sus clientes, entre otros beneficios. ((2017, 01). Obtenido 05, 2017, de www.iso.org).

2.2.11. Secretaría Nacional de Comunicación

Es importante entender el entorno en el que se desarrollará la tesis, pues permitirá asociar el estudio con la realidad institucional, y a la vez ir comprendiendo la importancia de la aplicabilidad del presente trabajo de conformidad con los objetivos estratégicos de la institución.

La Secretaría Nacional de Comunicación adscrita a la Presidencia de la República se estableció a través del Decreto Ejecutivo No. 1795 de 22 de junio de 2009, y mediante Decreto Ejecutivo No. 3 de 30 de mayo de 2013, suscrito por el Eco. Rafael Correa Delgado Presidente Constitucional de la República, en ejercicio de sus facultades previstas, expidió varias reformas a la Estructura de la Presidencia de la República, entre ellas la determinación de la actual Secretaria Nacional de Comunicación – SECOM como una entidad de derecho público con autonomía administrativa, financiera y técnica, instruyendo que se inicie su proceso de reforma institucional con estructura, responsabilidades y competencias.

2.2.11.1. Misión

Diseñar, dirigir, coordinar y ejecutar las políticas y estrategias de comunicación, información, difusión e imagen del Gobierno Nacional.

2.2.11.2. Visión

Ser la institución del Gobierno que fomente la democratización de la comunicación en el país, generando nuevos espacios de información, difusión e imagen con atributos de calidad, veracidad y cercanía a todos los ciudadanos y ciudadanas del Ecuador.

2.2.11.3. Valores Institucionales

Honestidad: Actuamos con la debida transparencia entendiendo que los intereses colectivos deben prevalecer al interés particular para alcanzar los propósitos comunes.

Transparencia: Garantizamos la nitidez en la información que difundimos a la ciudadanía.

Veracidad: Informamos a la ciudadanía las acciones con veracidad y responsabilidad.

Liderazgo: Somos personas comprometidas en dar ejemplo, influyendo positivamente en el trabajo de los demás, generando un trabajo de equipo que produce resultados exitosos.

Excelencia: Nos consideramos competentes para satisfacer continuamente las expectativas de la ciudadanía, con actitud, agilidad y anticipándonos a sus necesidades.

Eficiencia: Trabajamos por nuestros objetivos y metas programadas, optimizando el uso de los recursos y el tiempo disponibles.

2.2.11.4. Objetivos Institucionales / Estratégicos

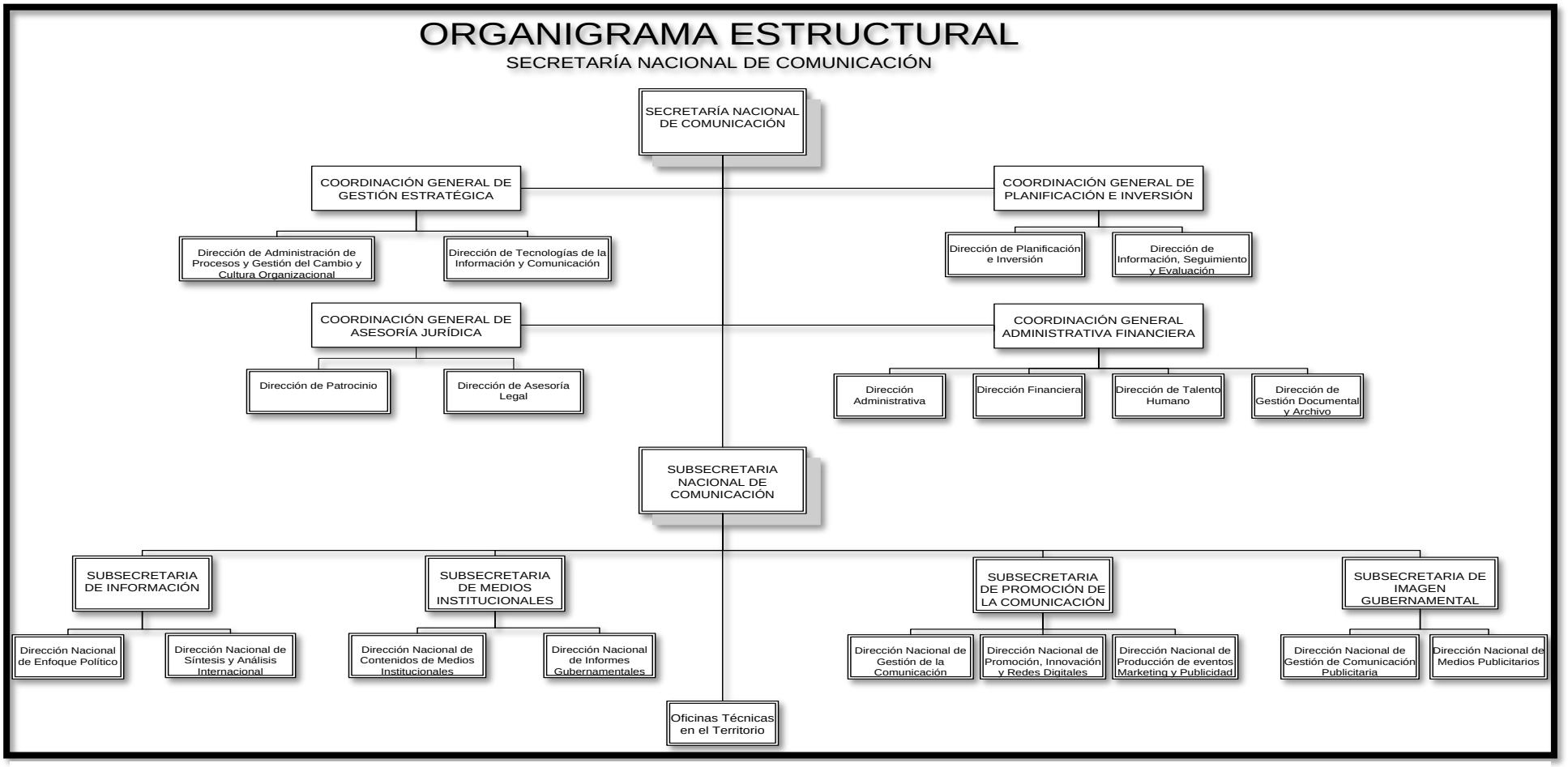
Incrementar la eficiencia, eficacia y calidad de los servicios de la Administración Pública Central, Institucional y que depende de la Función Ejecutiva.

Incrementar la imagen gubernamental, difusión de información y relacionamiento ciudadano de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.

2.2.11.5. Estructura Orgánica

La Secretaría Nacional de Comunicación, para el cumplimiento de sus competencias, atribuciones, misión y visión, desarrolla los siguientes procesos internos:

ORGANIGRAMA SECRETARÍA NACIONAL DE COMUNICACIÓN



Fuente: Repositorio digital de la SECOM, referencia a diciembre de 2016

Gráfico 3. Organigrama Secretaría Nacional de Comunicación

2.2.12. Dirección de Tecnologías de la Información y Comunicación

Debido a el presente trabajo es vinculado a la infraestructura tecnológica es importante conocer la estructura de la Dirección de Tecnologías de la Información y Comunicación.

2.2.12.1. Misión

Proponer, implementar y administrar políticas, normas y procedimientos que optimicen la gestión y administración de las tecnologías de la información y comunicaciones (TICs), garantizando la integridad de la información, optimización de recursos, sistematización y automatización de los procesos institucionales, así como el soporte tecnológico institucional.

Responsable: Director/a de Tecnologías de la Información y Comunicación

2.2.12.2. Atribuciones y Responsabilidades

Analizar periódicamente la estructura, funciones, sistemas, procedimientos y métodos de trabajo del área de recursos tecnológicos a fin de consolidarlos, homologarlos y optimizarlos;

Proponer, implementar y controlar la aplicación de políticas para el uso de las tecnologías de la información y comunicaciones;

Supervisar la implementación y desarrollo de sistemas informáticos de apoyo, que permitan lograr eficiencia, economía y transparencia en las actividades institucionales;

Coordinar con la Dirección Nacional de Talento Humano, la capacitación en el uso de la tecnología informática (TICs);

Supervisar la ejecución de los diferentes proyectos a nivel nacional en el área de redes, desarrollo informático y mantenimiento de toda la infraestructura tecnológica al servicio de la Secretaría Nacional de Comunicación;

Administrar eficiente y eficazmente los recursos informáticos de la Secretaría Nacional de Comunicación;

Regular y controlar el funcionamiento de las unidades de Tecnología de la Información y Comunicaciones en los diferentes niveles de la Secretaría;

Elaborar el plan de desarrollo informático institucional;

Supervisar el mantenimiento de software y hardware informático, además del soporte a los usuarios;

Dar seguimiento a la ejecución de proyectos de tecnologías de la información y comunicación estratégicas;

Brindar asesoría en temas relacionados con TICs;

Ejercer las demás atribuciones y responsabilidades que le delegare el Coordinador/a de Gestión General Estratégica.

2.2.12.3. Gestiones internas

Gestión de Ingeniería de Redes, Seguridades y Comunicaciones

Gestión de Soporte Técnico y Capacitación

Gestión de Desarrollo de Software y Base de Datos

Gestión de Proyectos de Tecnología

Gestión de Ingeniería de Redes, Seguridades y Comunicaciones

Productos:

Plan de operación y mantenimiento de la infraestructura tecnológica informática, dentro del ámbito de la institución;

Manual de políticas de acceso de usuarios a nivel de la red de la institución y a los diferentes servicios y sus servidores;

Reportes de administración y configuración de los enlaces de comunicación;

Reportes de internet, voz, datos y video a nivel local, nacional de la institución, interinstitucional y entidades externas (nacionales e internacionales);

Informe de evaluaciones de equipos en la red de la institución a nivel nacional;

Plan de contingencia de infraestructura tecnológica e información de la planta central;

Reportes de administración y configuración de la seguridad de la información;

Políticas de seguridad en tecnologías de información y comunicación y utilización de buenas prácticas;

Reportes de administración y configuración del correo electrónico institucional.

Plan operativo anual de la unidad.

Gestión de Soporte Técnico y Capacitación

Productos:

Reporte de soporte al usuario e ingreso en bitácora de casos;

Informe de inventario de equipos a nivel local y nacional;

Reporte de entrega de equipamiento tecnológico a nivel nacional;

Informe de mantenimiento preventivo y correctivo de los equipos informáticos a nivel de software y hardware;

Reporte de soporte técnico de software a nivel nacional;

Reportes de recursos tecnológicos implementados y por implementar a nivel nacional respecto del hardware y software institucional;

Políticas, estándares y manuales sobre el uso de software, configuración de equipos e inventario para la institución;

Plan de capacitaciones a usuarios sobre la utilización y manejo de aplicaciones implementadas y por implementarse.

Gestión de Desarrollo de Software y Base de Datos

Productos:

Políticas y estándares para la elaboración de software para la institución;

Informes del diseño y desarrollo de sistemas informáticos, bases de datos para la automatización de los procesos de la institución;

Informes de la homologación de los sistemas informáticos que permitan su fácil consolidación y la toma de decisiones;

Reporte de administración y coordinación de sistemas informáticos, bases de datos implementados y por implementar en la red institucional;

Aplicaciones multimedia para planta central y en territorio;

Planes de migración a tecnologías de software libre o sistemas implementados a nivel nacional

Aplicativos (software) para la ejecución de inteligencia de negocios;

Informe de mantenimiento las diferentes bases de datos existentes en la Secretaría Nacional de Comunicación;

Informes sobre criterios técnicos necesarios para avalar herramientas o aplicaciones a implementarse en la Institución;

Procesos automatizados de la institución, sea como conceptualización de software o desarrollo interno;

Informes de pruebas de software y asegurar la calidad en las aplicaciones desarrolladas.

Gestión de Proyectos de Tecnología

Políticas y estándares para la generación y aprobación de proyectos en tecnología para la institución;

Proyectos y términos de referencia revisados y aprobados para la implementación de tecnología informática a nivel nacional;

Reportes de análisis, evaluación y gestión de proyectos de tecnología informática;

Planes de contingencia en proyectos (TI) para la institución a corto, mediano y largo plazo e informes de implementación;

Reporte de proyectos de tecnologías informáticas implementadas y por implementar en la institución;

Manual de políticas y normativas para la ejecución, administración y control de procesos informáticos en coordinación con la Dirección de Procesos;

Plan estratégico de tecnología informática, su cumplimiento y evaluación de los proyectos ejecutados;

Plan de programación presupuestaria anual;

Informes de control sobre los procesos de tecnología y sus mejoramientos;

Informe de aprobación sobre las aplicaciones de software desarrolladas para ser llevadas a un ambiente de producción. (Estructura Orgánica Estructural de la Secretaría Nacional de Comunicación. (2014)).

2.3.Glosario de Términos[1]

El glosario, permitirá tener un acercamiento y familiarización de términos utilizados a lo largo de la tesis, a fin de garantizar la comprensión total del documento. Para el efecto se han detallado los siguientes términos:

Hacking ético: Forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño.

Ataque informático: Método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera).

Probabilidad: Medida de la certidumbre asociada a un suceso o evento futuro.

Material impreso: Todo documento que se encuentra en formato físico como informes, reportes, hojas membretadas, balances, etc.

Bienes inmuebles: Propiedades que no pueden moverse del lugar en el que están, tales como tierras, locales o viviendas

Material de oficina: Todo aquello que sirve para llevar a cabo actividades dentro de una oficina, estos pueden ser esferos, lápices, carpetas, marcadores, hojas no impresas, etc.

Bienes muebles: Que pueden ser trasladados sin alterar su naturaleza o calidad, como dinero, acciones y participaciones, joyas, obras de arte, vehículos, etc.

[1] Las referencias bibliográficas de cada uno de los términos se encuentran presentes al final del documento.

Recurso Humano: Personas.

Equipo de almacenamiento, servidores NAS, discos externos, repositorio digital: Dispositivo que almacena y facilita el acceso abierto a todo tipo de contenido digital incluyendo texto, imágenes, vídeos, etc.

Control de accesos: Mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos.

Correo Electrónico: Servicio de red que permite a los usuarios enviar y recibir mensajes digitalizados.

Acuerdos de Niveles de Servicio: Acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

Redes de datos: Conjunto de elementos de telecomunicaciones cuyo diseño posibilita la transmisión de información a través del intercambio de datos.

Cableado estructurado: Sistema de cables, conectores, canalizaciones y dispositivos que permiten establecer una infraestructura de telecomunicaciones en un edificio.

Enlaces temporales: Red de datos de área extensa usados en diferentes lugares por tiempos cortos.

Colaboración unificada: Interacción en tiempo real que integra voz, video, datos, mensajería, conferencia, movilidad y más.

Antivirus: Programa que detecta la presencia de un virus informático en un disquete o en una computadora y lo elimina.

Internet: Red de redes que permite la interconexión descentralizada de computadoras.

Páginas web: Documento o información electrónica capaz de contener texto, sonido, vídeo, programas, enlaces, imágenes, etc. accedida desde un navegador.

Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Hardware: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Equipos de protección perimetral: Permiten la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles.

Acuerdos de confidencialidad: Contrato legal entre al menos dos entidades para compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.

Producto crítico: Producto o servicio que es importante para una organización.

Escaneo activo de puertos: Revisión de estado de los puertos de una máquina conectada a una red de comunicaciones. Detecta si un puerto está abierto, cerrado, o protegido.

Escaneo de vulnerabilidades: Examina específicamente el perfil de seguridad de la organización desde la perspectiva de alguien interno o de alguien que tiene acceso a los sistemas y las redes detrás del perímetro de seguridad externo de la empresa.

Inyección de código: Ocurre cuando es posible enviar datos inesperados a un intérprete.

Inyección de comandos: Permite a un atacante inyectar arbitrariamente comandos del sistema en una aplicación.

Suplantación de credenciales: Tomar credenciales de un tercero y hacerlas propias.

Manejo de sesiones: Si el contenido de la sesión se almacena como archivos temporales cualquier usuario que acceda a los registros en el servidor pueden ver el contenido de todas las sesiones.

Escalamiento de privilegios: Cuando un atacante comienza con una cuenta de usuario comprometida y es capaz de ampliar o elevar los privilegios de usuario único que tiene cuando obtiene privilegios administrativos completos o "raíz".

Ataques de autenticación: "Hacerse pasar por otro" y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios. Una forma común es conseguir el nombre y contraseña de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él.

2.4.Bases Legales

Al ser la Secretaría Nacional de Comunicación, un organismo del Estado Ecuatoriano, derivado del Poder Ejecutivo, de derecho público; es importante conocer las dos bases legales con las que se trabajarán para la presente tesis, toda vez que, si bien es un trabajo de desarrollo técnico/investigativo, no se pueden descartar los lineamientos normativos, regulatorios y legales con los que se maneja la institución.

2.4.1. Constitución de la República del Ecuador

La Constitución de la República del Ecuador, a más de ser la base legal sobre la cual se soportan todos los poderes del Estado, es de vital importancia para esta tesis, pues potencializa la necesidad de contar con un Sistema de Gestión de Seguridad de la Información, toda vez que:

En los numerales 1, 2, 4 y 5 del Artículo 16, establece que todas las personas, en forma individual o colectiva, tienen derecho a una comunicación libre, intercultural, incluyente, diversa y

participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos; tener acceso universal a las tecnologías de información y comunicación; el acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad; e integrar los espacios de participación previstos en la Constitución en el campo de la comunicación.

Así mismo los numerales 1 y 2 del Artículo 18 de la Carta Magna, establece que todas las personas, en forma individual o colectiva, tienen derecho a: buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior e igualmente acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información; Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las, competencias y facultades que les sean atribuidas en la Constitución y la Ley, además tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución. (Constitución de la República del Ecuador (2008), Artículos 16 & 18).

2.4.2. Acuerdo Ministerial No. 166 de 25 de septiembre de 2013

La aplicabilidad de los Sistemas de Gestión de Seguridad de la Seguridad de la Información se encuentra respaldada legalmente para las entidades que se derivan del Poder Ejecutivo del Estado Ecuatoriano, mediante acuerdo Ministerial No. 166 Registro Oficial Suplemento 88 de 25 de septiembre de 2013, pues considera:

Que, mediante Acuerdos Ministeriales Nos. 804 y 837 de 29 de julio y 19 de agosto de 2011, respectivamente, la Secretaría Nacional de la Administración Pública creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación conformada por delegados del Ministerio de Telecomunicaciones y de la Sociedad de la Información, la Secretaría Nacional de Inteligencia y la Secretaría Nacional de la Administración Pública y dentro de sus atribuciones tiene la de establecer lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con ésta, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional.

Que, es importante adoptar políticas, estrategias, normas, procesos, procedimientos, tecnologías y medios necesarios para mantener la seguridad en la información que se genera y custodia en diferentes medios y formatos de las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.

Que, la Administración Pública de forma integral y coordinada debe propender a minimizar o anular riesgos en la información, así como proteger la infraestructura gubernamental, más aún si es estratégica, de los denominados ataques informáticos o cibernéticos.

Que, las Tecnologías de la Información y Comunicación son herramientas imprescindibles para el cumplimiento de la gestión institucional e interinstitucional de la Administración Pública en tal virtud, deben cumplir con estándares de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información;

Que, la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación en referencia ha desarrollado el Esquema Gubernamental de Seguridad de la

Información (EGSI), elaborado en base a la norma NTE[2]INEN[3]-ISO/IEC[4] 27002 "Código de Práctica para la Gestión de la Seguridad de la Información".

Que, el artículo 15, letra i) del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva establece como atribución del Secretario Nacional de la Administración Pública, impulsar proyectos de estandarización en procesos, calidad y tecnologías de la información y comunicación; En uso de las facultades y atribuciones que le confiere el artículo 15, letra n) del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva.

Dispone:

Artículo 1.- A las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.

"…La implementación del EGSI se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información…"

Artículo 4.- La Secretaría Nacional de la Administración Pública coordinará y dará seguimiento a la implementación del EGSI en las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.

[2] Norma Técnica Ecuatoriana
[3] Servicio Ecuatoriano de Normalización
[4] Comisión electrotécnica Internacional

El seguimiento y control a la implementación de la EGSI se realizará mediante el Sistema de Gestión por Resultados (GPR) u otras herramientas que para el efecto implemente la Secretaría Nacional de la Administración Pública.

Artículo 5.- La Secretaría Nacional de la Administración Pública realizará de forma ordinaria una revisión anual del EGSI en conformidad a las modificaciones de la norma INEN ISO/IEC 27002 que se generen y de forma extraordinaria o periódica cuando las circunstancias así lo ameriten, además definirá los procedimientos o metodologías para su actualización, implementación, seguimiento y control.

Artículo 6.- Es responsabilidad de la máxima autoridad de cada entidad mantener la documentación de la implementación del EGSI debidamente organizada y registrada de acuerdo al procedimiento específico que para estos efectos establezca la Secretaría Nacional de la Administración Pública.

Artículo 7.- Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos de su institución, en base a la norma INEN ISO/IEC 27005 "Gestión del Riesgo en la Seguridad de la Información". (Esquema Gubernamental de Seguridad de la Información (2013). Acuerdo Ministerial 166. Registro Oficial del Ecuador. Suplemento 88).

2.5. Operacionalización de las variables

Al ser una tesis que trabaja con variables que pueden tener subjetividad expresa, es necesario parametrizarlas, por ello es importante comprender el presente concepto.

Operacionalizar las variables significa explicar cómo se miden. Para lograr la operacionalización se transforma una variable en otras que tengan el mismo significado, descomponiéndolas en otras

más específicas llamadas dimensiones y a su vez, traducir estas dimensiones en indicadores para permitir la observación directa. (Clementina, J. G. (2015). Operacionalización De Variables).

Una variable es operacionalizada con el fin de convertir un concepto abstracto en uno empírico, susceptible de ser medido a través de la aplicación de un instrumento. Dicho proceso tiene su importancia en la posibilidad que un investigador poco experimentado pueda tener la seguridad de no perderse o cometer errores que son frecuentes en un proceso investigativo, cuando no existe relación entre la variable y la forma en que se decidió medirla, perdiendo así la validez (grado en que la medición empírica representa la medición conceptual). La precisión para definir los términos tiene la ventaja de comunicar con exactitud los resultados.

Algunas variables son tan concretas, o de igual significado en el ámbito mundial, que no requieren operacionalización, por ejemplo: el sexo de los individuos, los colores del semáforo como señal de tránsito, la ubicación o estructura de órganos en el cuerpo humano, entre otros.

2.5.1. Variable

Una variable es una característica que se va a medir.

Es una propiedad, un atributo que puede darse o no en ciertos sujetos o fenómenos en estudio, así como también con mayor o menor grado de presencia en los mismos y por tanto con susceptibilidad de medición.

2.5.1.1. Tipos de variable

Hace referencia a conceptos clasificatorios de las variables que puede ser de distinto orden a saber:

- Según el nivel de medición: nominal, ordinal, de intervalo y de razón.
- Según el tipo de estudio: en estudios de investigación donde se supone la determinación de

una o más variables sobre otra, los estudios son de relación causa-efecto, y en ellos las variables son denominadas: independiente, que representa la causa eventual, dependiente o de criterio, que representa el efecto posible, e interviniente aquella que representa una tercera variable que actúa entre la independiente y la dependiente y que puede ayudar a una mejor comprensión de dicha relación.

Ejemplo: en un estudio donde se trata de probar la influencia de los medios de comunicación con un mayor nivel de instrucción de los individuos, se consideraría como variable dependiente (vd) el mayor nivel de instrucción, como variable independiente, la exposición a los medios de comunicación (vi) y sería una variable interviniente (vt) el interés particular de los individuos por ciertos programas de los medios de comunicación.

- Según el origen de la variable: activa, cuando el investigador la crea o la diseña y, atributiva o preexistente cuando ya está establecida o existe.
- Según el número de valores que representa: continua, representa valores de manera progresiva y admite fraccionamiento como la edad y, categórica o discreta cuando sólo toma algunos valores discretos o sea que no admite fraccionamiento tales como el género, la raza, el número de hijos o de embarazos; si la variable sólo toma dos valores como el sexo se denomina categórica dicotómica, pero si toma más de dos valores se denominará politómica.
- Según el control de la variable por parte del investigador: la variable que tiene efecto sobre la variable dependiente requiere que sea controlada por e investigador, por ejemplo, el número de cigarrillos que consume por día un fumador y su relación con la aparición prematura de la patología pulmonar, en este caso la variable se denomina controlable o controlada.

2.5.1.2. Categorización o Dimensiones

Cuando el concepto tiene varias dimensiones o clasificaciones o categorías, éstas deben especificarse en el estudio; tal es el caso de la variable "recursos", que puede hacer referencia a "recursos técnicos, financieros, ambientales, humanos entre otros".

2.5.1.3. Indicador

Es la señal que permite identificar las características de las variables.

Se da con respecto a un punto de referencia.

Son señales comparativas con respecto a contextos o a sí mismas.

Su expresión matemática se nutre de la estadística, la epidemiología y la economía.

Se expresa en razones, proporciones, tasas e índices.

Permite hacer "medible" la variable.

Son ejemplos de indicadores: indicadores económicos (el dólar, la libra de café, el gramo de oro). Indicadores de pobreza (las migraciones, los desplazados, el desempleo, los asentamientos suburbanos).

2.5.1.4. Nivel De Medición

La medición de una variable se refiere a su posibilidad de cuantificación o cualificación, y éstas se clasifican según el nivel o capacidad en que permite ser medido el objeto en estudio. Según el tipo de operaciones matemáticas que se puedan realizar con los números asignados al medir la variable, se distinguen cuatro niveles de medición estadística, como son:

Nominal: este nivel sólo permite clasificar, es decir, la única relación existente entre los objetos a los cuales se les ha asignado un número es una relación de equivalencia. Por ejemplo, si en la variable sexo se ha asignado el numeral 1 para designar a los hombres y el 2, para referirse a las mujeres, quiere decir que todos los miembros a los que se les asigne el numeral 1 son hombres, o sea, tienen una condición equivalente.

Ordinal: permite clasificar además ordenar, es decir, establecer una secuencia lógica que mide la intensidad del atributo. Por ejemplo, al medir el grado de satisfacción frente a un servicio de salud, se pueden establecer escalas tales como: satisfacción plena, satisfacción media, poca satisfacción, o insatisfacción; esta escala difiere de la meramente nominal que permite establecer un orden o graduación entre las observaciones.

Intervalar o Numérica: permite clasificar y ordenar, pero además los intervalos son iguales, o sea, que en este nivel de medición no solo es posible ordenar las escalas, sino que es posible conocer las distancias o grados que separan unas de otras. La escala intervalar tiene las mismas propiedades formales de las escalas nominales y ordinales, es decir, las relaciones de equivalencia y de mayor qué; además, se le agrega la propiedad de poder determinar la razón que existe entre dos intervalos, en este caso existe una distancia numéricamente igual entre los objetos 2 y 3 que entre los objetos 3 y 4, porque en ambos la razón equivale a 1.

2.5.1.5. Valor

Es el resultado o número de resultados posibles que se obtiene de una variable. Cuando una variable puede medirse a través de varios indicadores, algunos de ellos pueden tener mayor valor que otros.

(López, S. I. (2015). Operacionalización de variables. hacia la promoción de la salud.).

Lo explicado en cuanto a Operacionalización se resume en el siguiente gráfico:

MATRIZ DE OPERACIONALIZACIÓN DE VARIABLES						
CONCEPTUALIZACIÓN	DIMENSIONES	SUB DIMENSIONES	INDICADORES	ÍTEMS	FUENTES	INSTRUMENTOS
Variable dependiente e independiente.	De la variable conceptualizada.	De la dimensión.	De las dimensiones y sub dimensiones evidencias sensoriales y significativas.	Son preguntas importantes para la recolección de la información en función de los indicadores.	Responde a la pregunta, quienes otorgan información	Responden a la pregunta, con qué instrumentos vamos a recoger la información

Fuente: Cobos, L. (2013). El marco metodológico.

Gráfico 4. Matriz de Operacionalización de Variables

Capítulo III

3. Marco Metodológico

3.1.Naturaleza de la Investigación

La tesis que se presenta está considerada base a una corriente de paradigma positivista. De acuerdo con Dobles, Zúñiga y García (1998), la teoría de la ciencia que sostiene el positivismo se caracteriza por afirmar que el único conocimiento verdadero es aquel que es producido por la ciencia, particularmente con el empleo de su método. En consecuencia, el positivismo asume que sólo las ciencias empíricas son fuente aceptable de conocimiento. (Cascante, L. G. (2015). El paradigma positivista y la concepción dialéctica del conocimiento. Revista Digital: Matemática, Educación e Internet).

Tiene enfoque cuantitativo, pues utiliza la recolección y el análisis de datos para contestar preguntas de investigación y probar hipótesis establecidas previamente, y confía en la medición numérica, el conteo y frecuentemente en el uso de la estadística para establecer con exactitud patrones de comportamiento de una población. (Sampieri, R, Collado, C. & Lucio, P. (2003). Metodología de la Investigación).

De igual manera, se ha visualizado esto desde una metodología de proyecto factible, ya que como su nombre lo indica, tiene un propósito de utilización inmediata, la ejecución de la propuesta.

En este sentido, la UPEL (1998) define el proyecto factible como un estudio "que consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales".

La propuesta que lo define puede referirse a la formulación de políticas, programas,

tecnologías, métodos o procesos, que sólo tienen sentido en el ámbito de sus necesidades. (Moya, R. D. (2002). El proyecto factible: una modalidad de investigación. Sapiens: Revista Universitaria de Investigación).

La investigación está apoyada de campo y carácter de tipo descriptiva, la cual como lo señala Hernández, Fernández y Baptista (2003), los estudios descriptivos buscan especificar las propiedades importantes de las personas, grupo, comunidades o cualquier otro fenómeno que sea sometido a análisis.

En el estudio descriptivo se selecciona una serie de variables y se mide cada una de ella independientemente, para lograr describir lo que se investiga.

3.2.Población y Muestra

Según Tamayo (1997), la población es la totalidad del fenómeno a estudiar en donde las unidades de población posen una característica común, la cual se estudia y da origen a los datos de la investigación

Para Sabino (2000), la muestra es una parte del todo que llamamos universo o población.

En el presente trabajo la población está constituida por todos los funcionarios de la SECOM, es decir por 277 funcionarios (a diciembre 2016), que serán diferenciados en tres grupos:

FUNCIÓN	CANTIDAD	PRINCIPALES ROLES A CUMPLIR EN EL SGSI
Niveles Jerárquicos	30	Toma de decisiones
Funcionarios Dirección de Tecnologías de la Información y Comunicación	11	Ejecutor de acciones en infraestructura tecnológica
Personal de la SECOM (nivel operativo)	236	Receptor de disposiciones para cumplimiento

Fuente: Repositorio digital de la SECOM, referencia a diciembre de 2016

Tabla 1. Diferenciación de la muestra por grupos

Se ha tomado como muestra a todos los funcionarios de niveles jerárquicos (30), de la Dirección de Tecnologías de la Información y Comunicación (11); y a diez (10) funcionarios operativos; es decir a 51 personas de la SECOM, los cuales intervendrán en diferentes procesos de la tesis.

3.3.Instrumento de Recolección de Datos

Se utilizarán el siguiente instrumento de recolección de datos:

Cuestionarios:

El cuestionario consiste en un conjunto de preguntas, normalmente de varios tipos, preparado sistemática y cuidadosamente, sobre los hechos y aspectos que interesan en una investigación o evaluación, y que puede ser aplicado en formas variadas, entre las que destacan su administración a grupos o su envío por correo. (Pérez Juste, R. (1991). Pedagogía Experimental. La Medida en Educación. Curso de Adaptación. Uned. 106).

Los cuestionarios fueron realizados tanto al personal de las áreas críticas de la SECOM, como al personal de la Dirección de Tecnologías de la Información y Comunicación; es decir a los procesos agregadores de valor y al área transversal, pues son ellos quienes poseen la información más sensible de esta Cartera de Estado. (Referirse al adjunto).

Capítulo IV

4. Análisis de los Datos e Información

Se ha aplicado la estrategia de mejora continua basada en el círculo de Deming, por lo que se irá cumpliendo con las fases de conformidad con lo requerido por la Secretaría Nacional de Comunicación.

4.1. Fase I: Planificar

En esta fase es preciso analizar los hallazgos en cuanto al estado actual de los activos de la información, análisis de riesgos, el tratamiento de los mismos y conocer la inversión que el Estado ecuatoriano ha efectuado sobre los productos críticos de la institución a fin de evaluar si es factible mantener un sistema de gestión de la seguridad de la información en el ámbito tecnológico.

4.1.1. Hallazgos SGSI

Es necesario generar un plan de hallazgos referentes al SGSI, de conformidad con normas de auditoría e ISO 27001, toda vez que esto nos permitirá identificar el estado actual de la administración del sistema de gestión de seguridad de la información en la SECOM, puntualmente en la infraestructura tecnológica.

En la documentación adjunta se encuentra el plan de hallazgos, el cual pretende:

- Revisar la documentación del sistema de gestión.
- Evaluar la ubicación y las condiciones específicas del sitio e intercambiar información con el personal.
- Recopilar la información necesaria correspondiente al alcance del sistema de gestión,

a los procesos y a las ubicaciones de la SECOM, así como a los aspectos legales y reglamentarios relacionados y su cumplimiento (por ejemplo, aspectos de calidad, ambientales, legales del funcionamiento de la SECOM, los riesgos asociados, etc.);

De lo revisado se ha extendido el debido informe de hallazgos (Ver adjunto), que se resume en lo siguiente:

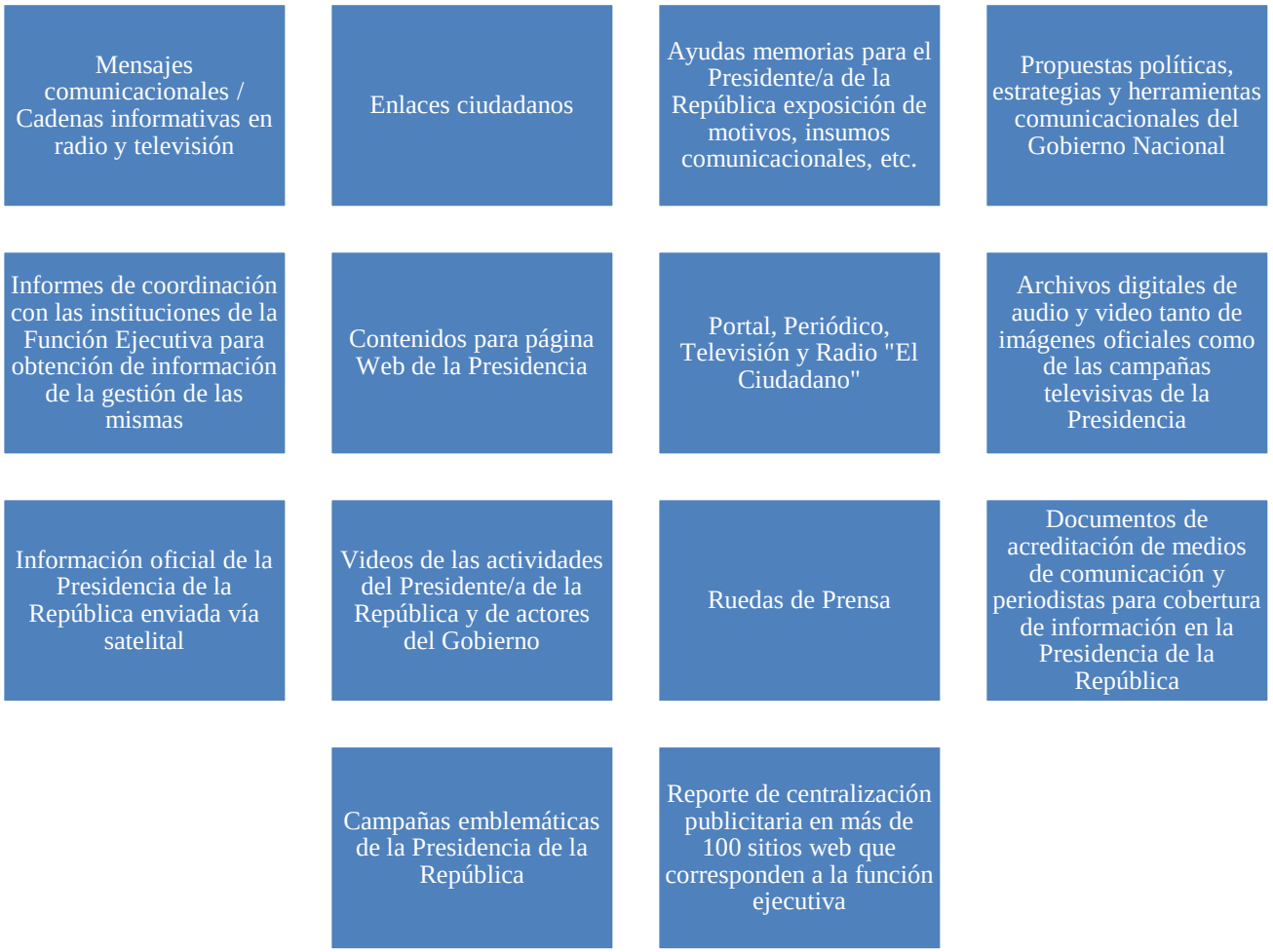
- La documentación encontrada no asegura que la administración de un sistema de seguridad de la información sea manejada de manera correcta dentro de la SECOM o que exista un sistema de gestión como tal.
- Se ha efectuado un análisis Político, Económico, Social, Tecnológico, Legal, Ecológico (PESTLE), en el cual se ha encontrado que existe una relación directa entre el contexto interno y el externo de la SECOM, sin embargo; no se ha manejado un grado de compresión de los requisitos de la norma INEN-ISO/IEC 27001, en particular en lo que concierne a la identificación de aspectos clave o significativos del desempeño procesos, objetivos y funcionamiento del sistema de gestión.
- Para el análisis PESTLE se consideraron las áreas (direcciones) que agregan valor a la SECOM, así como los productos críticos que se desprenden de estas.

En la siguiente figura se expone la cadena de valor de la SECOM.

Fuente: Estatuto Orgánico Estructural SECOM 2014

Gráfico 5. Cadena de Valor de la SECOM

En este sentido, se han determinado los productos críticos de la SECOM:



Fuente: Autora

Gráfico 6. Productos Críticos de la SECOM

Los productos críticos de la SECOM, hacen referencia a aquellos que no pueden descartarse, pues le dan importancia a la institución como tal.

Se ha considerado preciso identificarlos, pues más adelante se evaluará la inversión que el Estado ecuatoriano ha efectuado en cada uno; entendiendo de esta manera la gran necesidad de mantener administrado un sistema de gestión de la seguridad de la información, conceptualizándolos de la siguiente manera:

Mensajes comunicacionales / Cadenas informativas en radio y televisión:

Permiten transparentar las gestiones y actividades realizadas en referencia al material generado por el equipo de cobertura de la SECOM, el cual se encarga de cubrir las actividades del primer mandatario o su Gabinete.

Enlaces ciudadanos:

Se encarga de recopilar información pre y post eventos en los que participa el Presidente/a de la República o demás autoridades con el propósito de exponerlos a la ciudadanía. Muestra la gestión efectuada durante un tiempo determinado.

Ayudas memorias para el Presidente/a de la República exposición de motivos, insumos comunicacionales, etc.:

Recopila los principales hechos y conclusiones de un evento a fin de que el Presidente pueda dar seguimiento a su Gabinete, y de esta manera dar cumplimiento a acuerdos efectuados.

Propuestas políticas, estrategias y herramientas comunicacionales del Gobierno Nacional:

Permiten segmentación de público para evaluar el impacto de las estrategias comunicacionales y las áreas de enfoque donde estas se generan.

Informes de coordinación con las instituciones de la Función Ejecutiva para obtención de información de la gestión de las mismas:

Son medios para interrelacionar las acciones de las diferentes Carteras de Estado, a fin de dar cumplimiento a las estrategias gubernamentales.

Contenidos para la página Web de la Presidencia:

Conjunto recopilado de imágenes, videos, información que evidencia la gestión efectuada por el Gobierno Nacional de manera periódica. El contenido es modificado diariamente.

Portal, Periódico, Televisión y Radio "El Ciudadano":

Son medios de comunicación, mediante los cuales se administra y difunde las entrevistas, reportajes y noticias de actualidad respecto de la labor que realiza el Gobierno Nacional.

Archivos digitales de audio y video tanto de imágenes oficiales como de las campañas televisivas de la Presidencia:

Información histórica de la gestión de la Presidencia, de la cual suelen extraerse datos para alimentar otros productos críticos.

Información oficial de la Presidencia de la República enviada vía satelital:

Informes, estrategias, comunicados que se difunden por medio de transmisión satelital para que sea receptada a nivel global.

Videos de las actividades del Presidente/a de la República y de actores del Gobierno:

Grabación, edición y producción de las actividades del Presidente y actores políticos para su posterior difusión.

Ruedas de Prensa:

Información respecto al contacto entre el Presidente y los medios de comunicación.

Documentos de acreditación de medios de comunicación y periodistas para cobertura de información en la Presidencia de la República:

Habilitan a los medios de comunicación y periodistas que desean acceder a los eventos en los que participa el primer mandatario o su Gabinete, respetando los protocolos mediáticos que la SECOM o la Presidencia establezca.

Campañas emblemáticas de la Presidencia de la República:

Permite concientizar al Estado ecuatoriano sobre determinados temas relacionados exclusivamente con la actividad de la Presidencia de la República.

Reporte de centralización publicitaria en más de 100 sitios web que corresponden a la función ejecutiva:

Permite emitir políticas de imagen gubernamental a ser aplicadas en los diferentes contenidos institucionales de la Función Ejecutiva, a través de la adecuada implementación de metodologías de comunicación publicitaria de manera centralizada.

4.1.2. Gestión de Activos de información de la SECOM

4.1.2.1. Inventario

Los activos de información están presentes en toda la Secretaría Nacional de Comunicación, en el área Administrativa, de Talento Humano, etc. Sin embargo; para la tesis se han considerado los activos que hacen referencia a la infraestructura tecnológica, pues el enfoque se lo realizará tomando en consideración la información digital.

Del hallazgo se ha identificado que la mayor cantidad de activos de información se vinculan directamente con el área de Tecnologías de la Información y Comunicación, de acuerdo al siguiente detalle:

Dueño del activo	Tipo de Activo
Dirección Administrativa	Material impreso
	Material de oficina
	Bienes inmuebles
	Bienes muebles
Dirección de Talento Humano	Recurso Humano
Dirección de Tecnologías de la Información y Comunicación	Equipo de almacenamiento, servidores NAS, discos externos, repositorio digital
	Control de Accesos
	Correo Electrónico
	Acuerdos de Niveles de Servicio
	Redes de datos
	Cableado estructurado
	Enlaces temporales
	Colaboración Unificada
	Antivirus
	Internet
	Páginas web
	Desarrollo de software
	Equipo computacional (Hardware)
	Equipos de protección perimetral
Dirección de Tecnologías de la Información y Comunicación / Dirección de Talento Humano	Acuerdos de confidencialidad

Fuente: Autora

Tabla 2. Activos de la Información SECOM

4.1.2.2. Identificación de amenazas y vulnerabilidades

Para esta sección se ha utilizado el instrumento de recolección de datos “cuestionario” mediante encuestas a cada uno de los directores de las áreas agregadoras de valor y se han considerado las tres variables (aspectos) de la información: Confidencialidad, Integridad y Disponibilidad; para poder calificar las amenazas o vulnerabilidades de los activos inventariados.

En este sentido se han operacionalizado las variables antes mencionadas dándoles valores de 0 y 1 a las escalas de SI y NO de cada una de las dimensiones de dichas variables como se puede observar en los adjuntos.

De estos resultados se han escogido únicamente las amenazas y vulnerabilidades (dimensiones de las variables) que sobrepasen el valor promedio de 0,5; toda vez que, de conformidad con lo manifestado verbalmente por los encuestados, estos son los principales focos de riesgo que deben ser considerados para el sistema de gestión de seguridad de la información.

De lo expuesto se han definido las siguientes vulnerabilidades / amenazas en concordancia con la Confidencialidad, Integridad y Disponibilidad.

CONFIDENCIALIDAD

- Permisos no autorizados a la red
- Mala asignación y Uso indebido de credenciales
- Manipulación inadecuada o divulgación de la información
- Omisión en bloqueo de puertos
- Ataque físico/lógico
- Robo de información
- Ausencia o Falta de Cumplimiento de Acuerdos de confidencialidad
- Ejecución / Utilización de programas no autorizados

INTEGRIDAD

- Falta de inducción, capacitación y sensibilización sobre riesgos
- Utilización de programas no autorizados
- Perdida de datos
- Utilización indebida de hardware de almacenamiento
- Manejo inadecuado de datos críticos (codificar, borrar, etc.)
- Transmisión no cifrada de datos críticos
- Manejo inadecuado de credenciales
- Exposición o extravío de equipo, unidades de almacenamiento, etc
- Acceso electrónico no autorizado a sistemas

DISPONIILIDAD

- Fallas de conectividad
- Red expuesta al acceso no autorizado
- Ausencia de controles en apertura o cierre de puertos
- Incumplimiento de Acuerdos de Niveles de Servicio por parte de Proveedores
- Fallas eléctricas

Fuente: Autora

Gráfico 7. Identificación de Amenazas / Vulnerabilidades

4.1.2.3. Impacto

Este factor ha sido considerado en función de los efectos que puede traer consigo la ocurrencia de un evento de vulnerabilidad/amenaza por cada uno de los activos inventariados. Es claro que al ser la SECOM una entidad que se vincula con todo el Poder Ejecutivo del Estado, el impacto que se discute, es el social, toda vez que mediante la SECOM se da a conocer información oficial a todos los ecuatorianos, ya sea a través de medios de comunicación públicos o privados.

4.1.2.4. Valoración de las amenazas / vulnerabilidades e impacto

Para el presente trabajo, se ha asignado una valoración cuantitativa a cada una de las amenazas/vulnerabilidades antes expuestas, así como del impacto sobre los activos de la información.

Para la valoración de las amenazas/vulnerabilidades e impacto se ha considerado la experiencia tanto del personal directivo encargado de los productos críticos de la SECOM, ya que son quienes toman decisiones sobre la actividad fundamental de la SECOM; como del personal operativo, pues son quienes conocen el real giro del negocio.

Los valores propuestos están sujetos a una medición diaria, de la siguiente manera:

Afectación: Paralización de la actividad comunicacional de la SECOM	
Probabilidad	**Descripción**
Alta (4)	> 45 minutos
Media (3)	>= 31 <= 45 minutos
Baja (2)	>= 11 <= 30 minutos
Insignificante (1)	<= 10 minutos
Efecto: Pérdida de Credibilidad en el Gobierno	
Impacto (Social)	**Descripción**
Alto (4)	>1%
Media (3)	>=0,6% <=1%
Baja (2)	>=0,2% <=0,5%
Insignificante (1)	<=0,1%

Fuente: Autora

Tabla 3. Valoración de Amenazas / Vulnerabilidades e Impacto

4.1.2.5. Análisis/Evaluación de Riesgos

Para el análisis y evaluación de riesgos se ha elaborado una matriz tomando en cuenta las recomendaciones la norma ISO 27001. Dicha matriz ha sido elevada y completada por la muestra establecida para el presente trabajo.

Recordando que el método de cálculo del riesgo resulta de multiplicar la probabilidad por el impacto.

RIESGO= PROBABILIDAD x IMPACTO

Y, que a todos los niveles de riesgo es factible asignarles un tratamiento, los cuales pueden ser:

Mitigación: Implementando algún control que reduzca el riesgo, enfocándose en normas ISO.

Transferencia: Ocurre cuando se delega la acción de mitigación a un tercero, por ejemplo, a proveedores a través de Acuerdos de Niveles de Servicio.

Aceptación: Se presenta cuando el impacto es suficientemente bajo para que la organización decida no tomar ninguna acción de mitigación o cuando el costo de la aplicación de un control supera el valor del activo.

Existe un tratamiento de eliminación, que es considerada como una actividad ideal, ya que difícilmente se puede reducir a cero un riesgo.

Sin embargo, para el presente documento únicamente se trabajarán con los tres primeros tratamientos.

Mendoza (2015), señala que; cuando se ha definido una acción para cada riesgo valorado, es necesario que los resultados sean aceptados y las medidas de seguridad aplicadas. Esto se vuelve necesario ya que al aplicar una un control, todavía se cuenta con un riesgo denominado residual, es decir, un remanente que debe ser aprobado.

En este estudio, se han tomado valores límites por cada uno de los niveles de riesgo en concordancia con lo que demanda el giro del negocio.

El criterio de ubicación de los umbrales por cada nivel de riesgo ha sido establecido en reunión mantenida por los directivos conforme la realidad de la SECOM, de la siguiente manera:

Nivel de riesgo	Valoración del Riesgo	Tratamiento del Riesgo
Nivel de riesgo alto	>= 9,2	Transferir
Nivel de riesgo medio	>6,25 <= 9,1	Mitigar
Nivel de riesgo bajo	<=6,25	Aceptar

Fuente: Autora

Tabla 4. Umbrales por Nivel de Riesgo

A continuación, se ha efectuado una revisión pormenorizada del riesgo que se tiene sobre cada activo de información inventariado, la valoración monetaria por producto crítico de la SECOM y la concentración de los riesgos en cuanto a Confidencialidad, Integridad y Disponibilidad; a fin de tener un juicio de valor real sobre la importancia de brindar protección a los activos que maneja la institución:

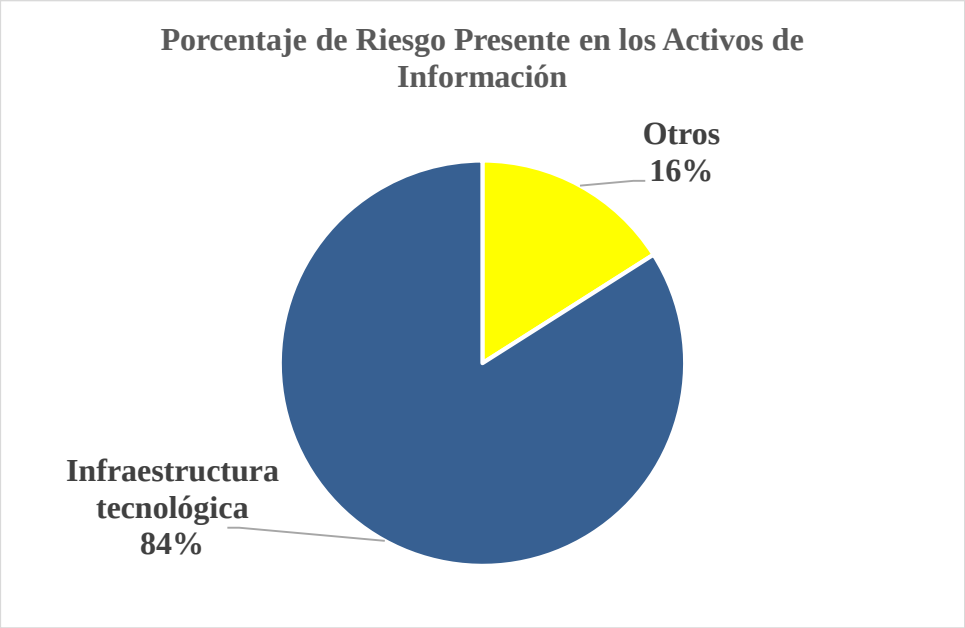
Matriz de Análisis de Riesgo por Activo Inventariado			
Dueño del activo	**Activo Inventariado**	**Valoración de Riesgo Promedio**	**Tratamiento del Riesgo**
Dirección Administrativa	Material impreso	4,5	Aceptar
	Material de oficina	2,3	Aceptar
	Bienes inmuebles	2,3	Aceptar
	Bienes muebles	4,5	Aceptar
Dirección de Talento Humano	Recurso Humano	4,5	Aceptar
Dirección de Tecnologías de la Información y Comunicación	Equipo de almacenamiento, servidores NAS, discos externos, repositorio digital	9,1	Mitigar

Matriz de Análisis de Riesgo por Activo Inventariado			
Dueño del activo	**Activo Inventariado**	**Valoración de Riesgo Promedio**	**Tratamiento del Riesgo**
	Control de Accesos	9,1	Mitigar
	Correo Electrónico	9,1	Mitigar
	Acuerdos de Niveles de Servicio	4,5	Aceptar
	Redes de datos	9,1	Mitigar
	Cableado estructurado	6,8	Mitigar
	Enlaces temporales	9,1	Mitigar
	Colaboración Unificada	6,8	Mitigar
	Antivirus	6,8	Mitigar
	Internet	9,1	Mitigar
	Páginas web	9,1	Mitigar
	Desarrollo de software	9,1	Mitigar
	Equipo computacional (Hardware)	6,8	Mitigar
	Equipos de protección perimetral	9,1	Mitigar
Dirección de Tecnologías de la Información y Comunicación / Dirección de Talento Humano	Acuerdos de confidencialidad	4,5	Aceptar

Fuente: Autora

Tabla 5. Matriz de Análisis de Riesgo por Activo Inventariado

Como se puede observar en el inventario existe un gran porcentaje de activos de información vinculados a la infraestructura tecnológica, que intervienen en la obtención de productos críticos, con un riesgo asociado significativo, tal como se muestra a continuación:



Fuente: Autora

Gráfico 8. Porcentaje de Riesgo presente en Activos de Información

La valoración monetaria real de cada producto crítico de la SECOM se la ha realizado con el afán de conocer cuanta inversión efectuada por el Estado ecuatoriano se encuentra en riesgo. Para ello, se han revisado los montos adjudicados y ejecutados de todos los contratos de bienes y servicios atados a cada uno de los productos críticos de la SECOM.

La información ha sido recopilada del Sistema Oficial de Contratación Pública y del sitio web de la SECOM en el apartado vinculado con Transparencia de los años 2014 al 2016.

Matriz de Análisis de Riesgo por Producto Crítico vinculado a la Inversión		
Productos críticos	**Promedio Riesgo por producto (Nivel Riesgo)**	**Inversión en producto crítico (2014-2016) (Dólares Americanos)**
Mensajes comunicacionales / Cadenas informativas en radio y televisión	6,3	$ 431.110,55
Enlaces ciudadanos	6,5	$ 210.372,27
Ayudas memorias para el Presidente/a de la República exposición de motivos, insumos comunicacionales, etc.	6,5	$ 122.951,90
Propuestas políticas, estrategias y herramientas comunicacionales del Gobierno Nacional	6,4	$ 319.181,90
Informes de coordinación con las instituciones de la Función Ejecutiva para obtención de información de la gestión de las mismas	7,0	$ 69.441,90
Contenidos para la página Web de la Presidencia	7,0	$ 23.881,90
	6,8	$ 1.215.009,03

Matriz de Análisis de Riesgo por Producto Crítico vinculado a la Inversión		
Productos críticos	**Promedio Riesgo por producto (Nivel Riesgo)**	**Inversión en producto crítico (2014-2016) (Dólares Americanos)**
Portal, Periódico, Televisión y Radio "El Ciudadano"		
Archivos digitales de audio y video tanto de imágenes oficiales como de las campañas televisivas de la Presidencia	6,9	$ 212.713,30
Información oficial de la Presidencia de la República enviada vía satelital	6,7	$ 23.881,90
Videos de las actividades del Presidente/a de la República y de actores del Gobierno	7,0	$ 59.595,90
Ruedas de Prensa	6,8	$ 248.713,30

Matriz de Análisis de Riesgo por Producto Crítico vinculado a la Inversión		
Productos críticos	**Promedio Riesgo por producto (Nivel Riesgo)**	**Inversión en producto crítico (2014-2016) (Dólares Americanos)**
Documentos de acreditación de medios de comunicación y periodistas para cobertura de información en la Presidencia de la República	6,8	$ 332.246,40
Campañas emblemáticas de la Presidencia de la República	6,7	$ 159.713,30
Reporte de centralización publicitaria en más de 100 sitios web que corresponden a la función ejecutiva	6,8	$ 923.881,90
TOTAL INVERTIDO EN PRODUCTOS CRÍTICOS		**4´352.695,45**

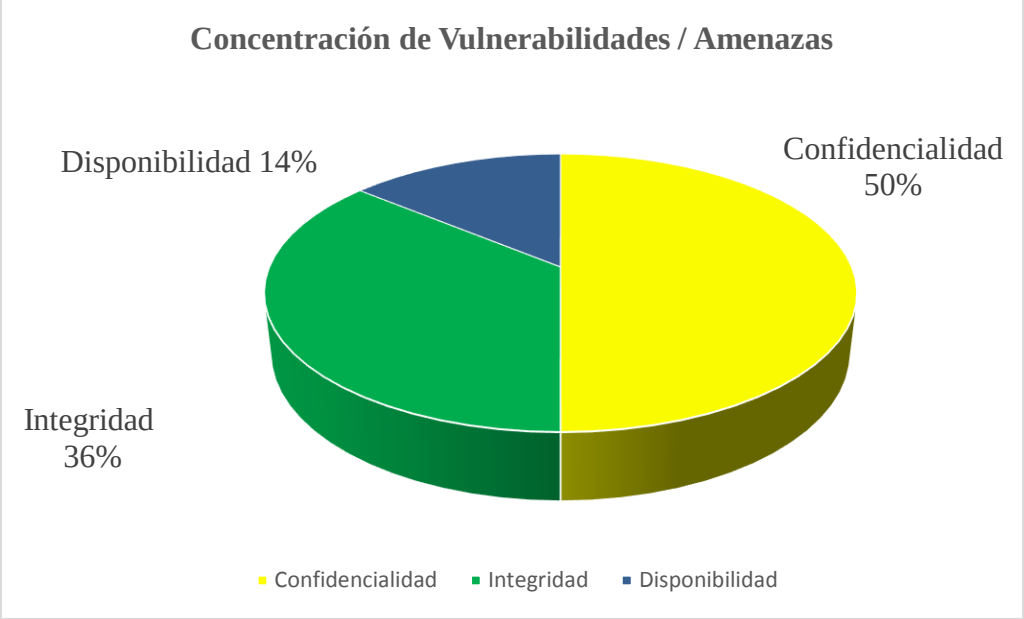
Fuente: Autora

Tabla 6. Matriz de Análisis de Riesgo por Producto Crítico vinculado a la Inversión

Una vez hechas las revisiones, se evidencia que existe una inversión total de USD 4´352.695,45 dólares de los Estados Unidos de América más impuestos, que intervienen en los productos críticos de la SECOM.

Del valor indicado se debe recordar que el 84% corresponde los activos vinculados a la infraestructura tecnológica, los cuales están catalogados en un nivel de riesgo MEDIO, mismo que puede ser mitigado.

Por otra parte, se ha revisado la concentración de riesgos por cada una de las vulnerabilidades y amenazas que atentan contra los principios de la Confidencialidad Integridad y Disponibilidad de los activos de información de la Secretaría Nacional de Comunicación; obteniendo lo siguiente:

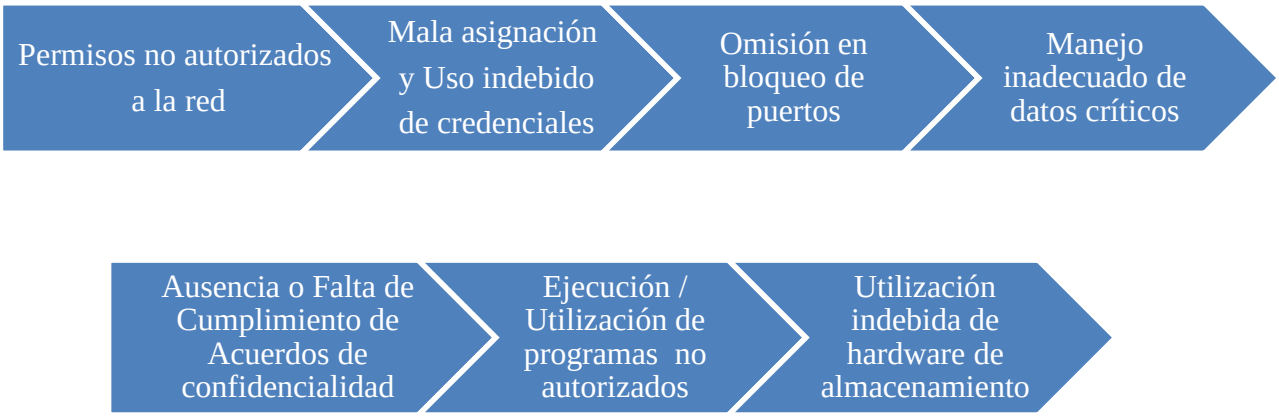


Fuente: Autora

Gráfico 9. Concentración de Vulnerabilidades/Amenazas

Es preciso señalar que en los anexos de este trabajo se encuentra el detalle ampliado de la concentración de las vulnerabilidades/amenazas.

Las vulnerabilidades/amenazas que tienen mayor impacto y concentración en los activos de información, se resume en lo siguiente:



Fuente: Autora

Gráfico 10. Vulnerabilidades / Amenazas Potencialmente Concentradas

Una vez analizado de manera global el riesgo asociado tanto para los activos como para los productos críticos y para la afectación en lo que refiere a Confidencialidad, Integridad y Disponibilidad, se efectuará una selección de los controles que mejor se adapten de conformidad con la norma INEN ISO/IEC 27002.

4.1.2.6. Selección de Controles para Mitigar el Riesgo

Dentro de la norma ISO/IEC 27002 se hace referencia a los controles que se pueden utilizar para gestionar riesgos por secciones. En este sentido, se han revisado las que mejor se adaptan para mitigar los riesgos conforme cada uno de los activos inventariados en la infraestructura tecnológica en concordancia con las amenazas /vulnerabilidades concentradas, obteniendo lo siguiente:

Sección 6.- Gestión de comunicaciones y operaciones

Sección 7.- Control de acceso

Sección 8.- Adquisición, desarrollo, y mantenimiento de sistemas de información

Fuente: Autora

Gráfico 11. Selección de Controles

La Sección 6, ha sido elegida debido a que dentro de ésta existen hitos vinculados con documentación de procedimientos y operación, controles contra códigos maliciosos y controles de las redes.

En lo que refiere a la Sección 7, ésta se enfoca en los controles de acceso, privilegios y contraseñas. Mientras que la Sección 8, es enfática en el tratamiento de especificaciones de los requerimientos de seguridad, control de procesamiento interno y fuga de información.

Las tres secciones están estrechamente relacionadas con las vulnerabilidades/amenazas que se desea sean objeto de refuerzo dentro del SGSI de la SECOM.

Capítulo V

5. La propuesta

Dando continuidad al capítulo anterior, se considerarán las tres etapas restantes del ciclo de Deming.

5.1. Fase II: Hacer - Diseño del Sistema de Gestión de Seguridad de la Información (SGSI)

5.1.1. Alcance del SGSI

A fin de asegurar la confidencialidad, integridad y disponibilidad de la información crítica de la institución se desarrolla el presente Sistema de Gestión de Seguridad de la Información.

Para el logro del objetivo a plantear, es fundamental contar con el compromiso y apoyo de todos los involucrados y el respaldo de las autoridades de la institución, tomando en consideración el impacto que debe afrontar por la materialización de riesgos que no se controlan y que se asocian al tema de seguridad y privacidad de la información.

Mediante el desarrollo del Sistema de Gestión de Seguridad de la Información se establecerá el SoA (Declaración de Aplicabilidad) ante los riesgos hallados en lo que respecta a los activos de información vinculados a la infraestructura tecnológica de la SECOM.

5.1.2. Objetivo del SGSI

Generar un mecanismo de mejora continua que permita proteger los activos de información de la infraestructura tecnológica a través de lineamientos y medidas de seguridad.

5.1.3. Declaración de Aplicabilidad (SoA - Statement of Applicability)

Una vez que se han definido los controles, es necesario llevarlos a la práctica mediante la declaración de aplicabilidad (SoA por las siglas en inglés de Statement of Applicability).

La declaración de aplicabilidad lo que persigue es el tener salvaguardas o medios con los cuales se cumplan los controles sugeridos por la ISO conforme las necesidades, en este caso; de la infraestructura tecnológica.

Controles ISO 27002:2013 Número de Sección	Descripción	Razón de Selección	Salvaguarda a aplicar
6	Gestión de comunicaciones y operaciones	Detección de riesgo (Mitigar)	Política de Seguridad de la Infraestructura Tecnológica
7	Control de acceso		
8	Adquisición, desarrollo, y mantenimiento de sistemas de información		

Fuente: Autora

Tabla 7. Declaración de Aplicabilidad (SoA)

Cabe señalar, que a pesar de haber seleccionado de manera global las secciones 6,7 y 8 de la norma ISO 27002:2013 para implementación en la SECOM, existen controles dentro de cada apartado que han sido excluidos debido a que no se apegan a la realidad del estudio o el giro del negocio institucional.

La salvaguarda aplicada en el SGSI para los activos de infraestructura tecnológica es la Política de Seguridad de la Infraestructura Tecnológica de la SECOM, misma que se encuentra adjunta al presente documento.

En concordancia con la norma ISO 27002:2013 y con el Acuerdo Ministerial No. 166 Oficial Suplemento 88 de 25 de septiembre de 2013, para que la aplicabilidad surja efecto es necesario contar con la participación de las autoridades de la institución; en este sentido se ha conformado un Comité de Seguridad de la Información, el mismo que tiene las siguientes funciones:

- Definir y mantener la política y normas institucionales particulares en materia de seguridad de la información y gestionar la aprobación y puesta en vigencia por parte de la máxima autoridad de la institución, así como el cumplimiento por parte de los funcionarios de la institución.
- Monitorear cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
- Acordar y aprobar metodologías y procesos específicos, relativos a la seguridad de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro de la institución.
- Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de la institución frente a incidentes de seguridad imprevistos.
- Designar a los custodios o responsables de la información de las diferentes áreas de la entidad, que deberá ser formalizada en un documento físico o electrónico.

- Gestionar la provisión permanente de recursos económicos, tecnológicos y humanos para la gestión de la seguridad de la información.
- Velar por la aplicación de la familia de normas técnicas ecuatorianas INEN ISO/IEC 27000 en la institución según el ámbito de cada norma.
- Designar formalmente a un funcionario como Oficial de Seguridad de la Información quien actuará como coordinador del Comité de Seguridad de la Información.
- El Oficial de Seguridad no pertenecerá al área de Tecnologías de la Información y reportará a la máxima autoridad de la institución.
- Designar formalmente al responsable de seguridad del área de Tecnologías de la Información en coordinación con el director o responsable del área de Tecnologías de la Información de la Institución.

El Oficial de Seguridad de la Información tendrá las siguientes responsabilidades:

- Definir procedimientos para el control de cambios a los procesos operativos, los sistemas e instalaciones, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.
- Establecer criterios de seguridad para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas antes de su aprobación definitiva.
- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
- Controlar los mecanismos de distribución y difusión de información dentro y fuera de la institución.
- Definir y documentar controles para la detección y prevención del acceso no autorizado, la

protección contra software malicioso, garantizar la seguridad de los datos y los servicios conectados a las redes de la institución.

- Desarrollar procedimientos adecuados de concienciación de usuarios en materia de seguridad, controles de acceso a los sistemas y administración de cambios.
- Verificar el cumplimiento de las normas, procedimientos y controles de seguridad institucionales establecidos.
- Coordinar la gestión de eventos de seguridad con otras entidades gubernamentales.
- Convocar regularmente o cuando la situación lo amerite al Comité de Seguridad de la Información, así como llevar registros de asistencia y actas de las reuniones.

El responsable de Seguridad del área de Tecnologías de la Información y Comunicación tendrá las siguientes responsabilidades:

- Controlar la existencia de documentación física o electrónica actualizada relacionada con los procedimientos de comunicaciones, operaciones y sistemas.
- Evaluar el posible impacto operativo a nivel de seguridad de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.
- Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad para soportar potenciales amenazas a la seguridad de la información que procesan.
- Controlar la obtención de copias de resguardo de información, así como la prueba periódica de su restauración.

- Asegurar el registro de las actividades realizadas por el personal operativo de seguridad de la información, para su posterior revisión.
- Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.
- Implementar los controles de seguridad definidos (ej., evitar software malicioso, accesos no autorizados.
- Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento (ej., cintas, discos, etc.) e informes impresos, y verificar la eliminación o destrucción segura de los mismos, cuando proceda.
- Gestionar los incidentes de seguridad de la información de acuerdo a los procedimientos establecidos.
- Otras que por naturaleza de las actividades de gestión de la seguridad de la información deban ser realizadas. (Esquema Gubernamental de Seguridad de la Información (2013). Acuerdo Ministerial 166. Registro Oficial del Ecuador. Suplemento 88).

El Comité de Seguridad de la SECOM, está conformado por los siguientes integrantes:

Designación de Comité de Seguridad de la Información
Oficial de Seguridad de la Información (OSI)
Responsable de área Administrativa
Responsable de Tecnologías de la Información y Comunicación
Responsable de Recursos Humanos

Fuente: Autora

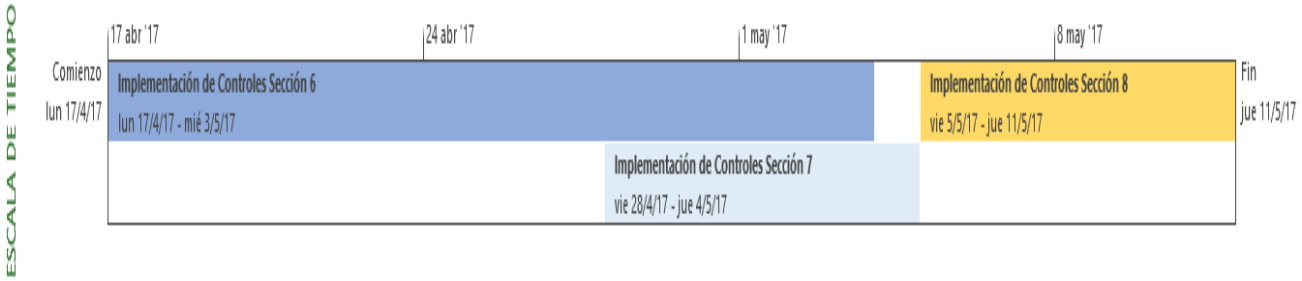
Tabla 8. Designación de Comité de Seguridad de la Información

5.1.4. Implementación y Operación de Plan de Tratamiento de Riesgos

De acuerdo con el análisis de riesgos y la salvaguarda seleccionada se ha considerado la implementación de controles para los activos de la infraestructura tecnológica, mediante una planificación. Dicha planificación ha sido prevista tomando en cuenta las prioridades institucionales, la facilidad y disponibilidad de recursos para la implementación por parte de la Dirección de Tecnologías de la Información y Comunicación, pues dicha dirección es la encargada de proponer, implementar y administrar políticas, normas y procedimientos que optimicen la gestión y administración de las tecnologías de la información y comunicaciones (TICs), garantizando la integridad de la información, optimización de recursos, sistematización y automatización de los procesos institucionales, así como el soporte tecnológico institucional.

Los criterios en cuanto a prioridades y facilidades de aplicación se encuentran sujetos a la decisión de los líderes de las gestiones internas de la Dirección mencionada.

La implementación ha sido desarrollada por fases de la siguiente manera:



Fuente: Autora

Gráfico 12. Fases de Implementación

Para ampliar el detalle de la planificación de actividades para implementación refiérase a los documentos adjuntos.

5.1.5. Formación y Concienciación

El Sistema de Gestión de Seguridad de la Información involucra cambios y mejoras constantes, por ello es importante manejar un criterio de formación y concienciación sobre su aplicación dentro de la entidad.

Es decir, todos los funcionarios de la SECOM deben estar familiarizados con el SGSI y tener conocimiento de la Política de Seguridad de la Infraestructura Tecnológica; sobre todo el personal tecnológico, por ello, la Dirección de Tecnologías de la Información y Comunicación trabajará, periódicamente; en conjunto con la Dirección de Administración de Procesos y Gestión de Cambio y Cultura Organizacional, que es la encargada de la difusión de comunicados internos.

Para el efecto, se ha previsto una campaña de difusión que incluya lo siguiente:

Tipo de Difusión	Conocimiento/Aplicación/Cumplimiento
Tiempo de difusión	Continua
Periodicidad de difusión	Mensual/Trimestral/Anual
Destinatarios:	Funcionarios SECOM
Cuerpo /Asunto de difusión	Sistema de Gestión de Seguridad de la Información

Fuente: Autora

Tabla 9. Modelo para Campaña de Difusión

5.2.Fase III: Monitorear - Supervisión y Revisión del SGSI

En esta fase se revisarán si se han aplicado los controles y si los mismos están teniendo efecto sobre los activos de infraestructura tecnológica a fin de mitigar los riesgos.

5.2.1. Medición de eficacia de controles

El diccionario de la Real Academia de la Lengua Española señala que la "eficacia" significa "virtud, actividad, fuerza y poder para obrar".

María Moliner interpreta esa definición y sugiere que "eficacia" "se aplica a las cosas o personas que pueden producir el efecto o prestar el servicio a que están destinadas". Algo es eficaz si logra o hace lo que debía hacer.

Los diccionarios del idioma inglés indican definiciones semejantes. Por ejemplo, el Webster's International define eficacia ("efficacy") como "el poder de producir los resultados esperados".

Por tanto, una iniciativa resulta eficaz si cumple los objetivos esperados en el tiempo previsto y con la calidad esperada. (Mokate, K. M. (2001). Eficacia, eficiencia, equidad y sostenibilidad: ¿qué queremos decir? Inter-American Development Bank).

El modo de medición para este caso, está basado en pruebas técnicas las cuales se fundamentan en incumplir los controles de confidencialidad, integridad y disponibilidad; y, de las que se debe obtener resultados negativos.

El activo tecnológico que se tomará para efectuar las pruebas es el equipo de almacenamiento, servidores NAS, discos externos, repositorio digital, sobre el que se deseará ingresar para manipular (modificar/eliminar) información de la Dirección de Informes Gubernamentales al producto crítico Mensajes comunicacionales / Cadenas informativas en radio y televisión.

Para el efecto se ha experimentado lo que en tecnología se denomina un hacking ético, simulando dirigir un ataque hacia puntos definidos con el objetivo de ganar acceso al activo y extraer información.

Esta fase será un compendio de una serie de ataques, tales como:

- Escaneo activo de puertos: Revisión de estado de los puertos de una máquina conectada a una red de comunicaciones. Detecta si un puerto está abierto, cerrado, o protegido.
- Escaneo de vulnerabilidades: Examina específicamente el perfil de seguridad de la organización desde la perspectiva de alguien interno o de alguien que tiene acceso a los sistemas y las redes detrás del perímetro de seguridad externo de la empresa.
- Inyección de código: Ocurre cuando es posible enviar datos inesperados a un intérprete.
- Inyección de comandos: Permite a un atacante inyectar arbitrariamente comandos del sistema en una aplicación.
- Suplantación de credenciales: Tomar credenciales de un tercero y hacerlas propias.
- Manejo de sesiones: Si el contenido de la sesión se almacena como archivos temporales cualquier usuario que acceda a los registros en el servidor pueden ver el contenido de todas las sesiones.
- Escalamiento de privilegios: Cuando un atacante comienza con una cuenta de usuario comprometida y es capaz de ampliar o elevar los privilegios de usuario único que tiene cuando obtiene privilegios administrativos completos o "raíz".
- Ataques de autenticación: "hacerse pasar por otro" y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios. Una forma común es conseguir el nombre y contraseña de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él.

Se ha efectuado dos tipos de pruebas: externas e internas.

- Pruebas internas: Se lo efectuará desde adentro de las instalaciones de la Institución, simulando ser un atacante con acceso a la infraestructura física.
- Pruebas externas: Se lo efectuará desde afuera de las instalaciones de la SECOM, intentando vulnerar los servicios que están visibles ante Internet.

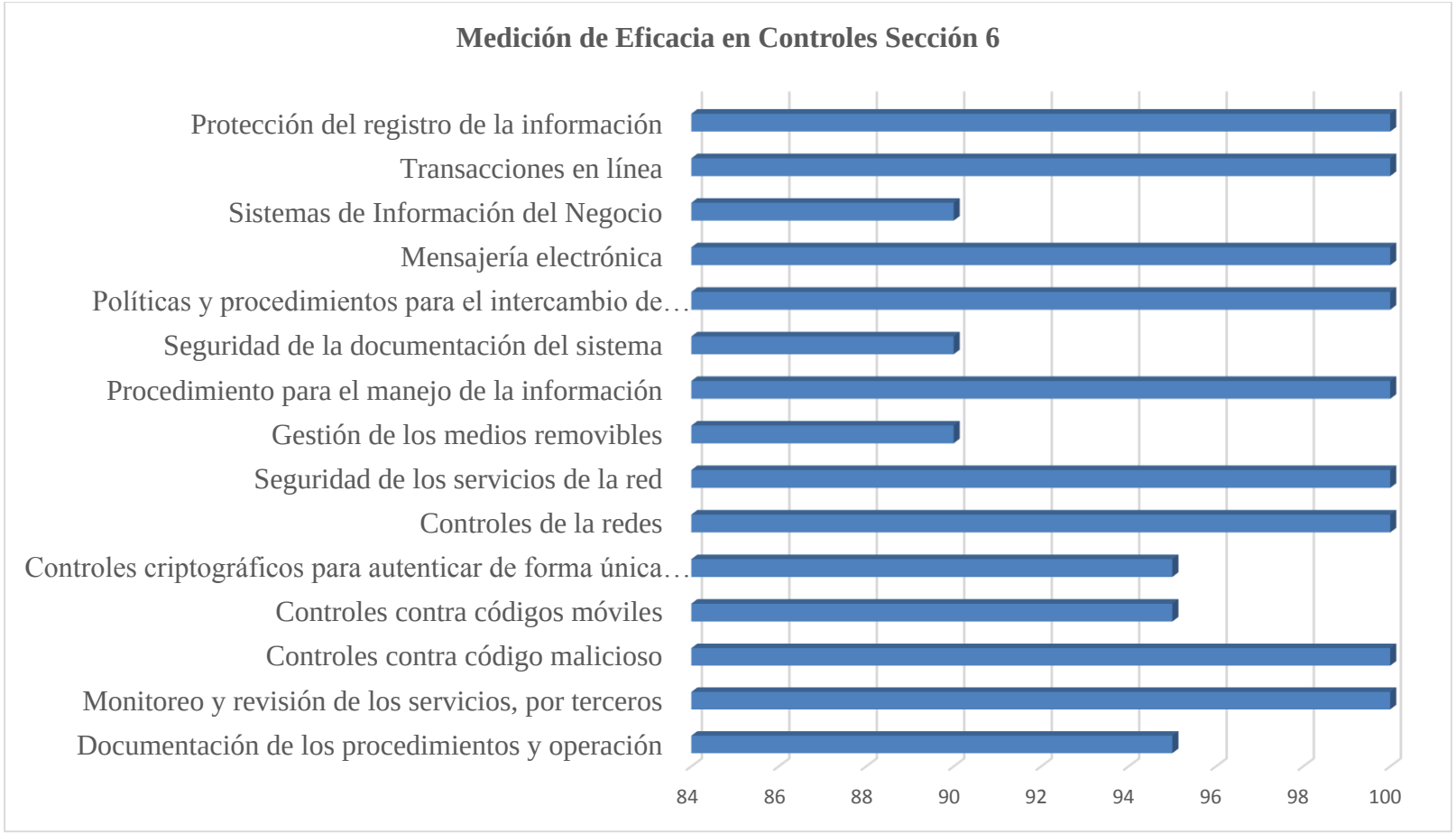
La valoración para medir la eficacia de los controles es el siguiente:

Condición	**Valoración (%)**
Si la prueba es no satisfactoria, es decir el bloqueo se efectúa o la vulnerabilidad no es trascendida completamente.	100%
Si la prueba trasciende hasta cierto nivel y después de esto existe restricción. (Dependiendo del nivel al que haya avanzado el atacante)	90% - 99%
Si la prueba es satisfactoria, y se lograron romper todos los niveles de seguridad.	0%

Fuente: Autora

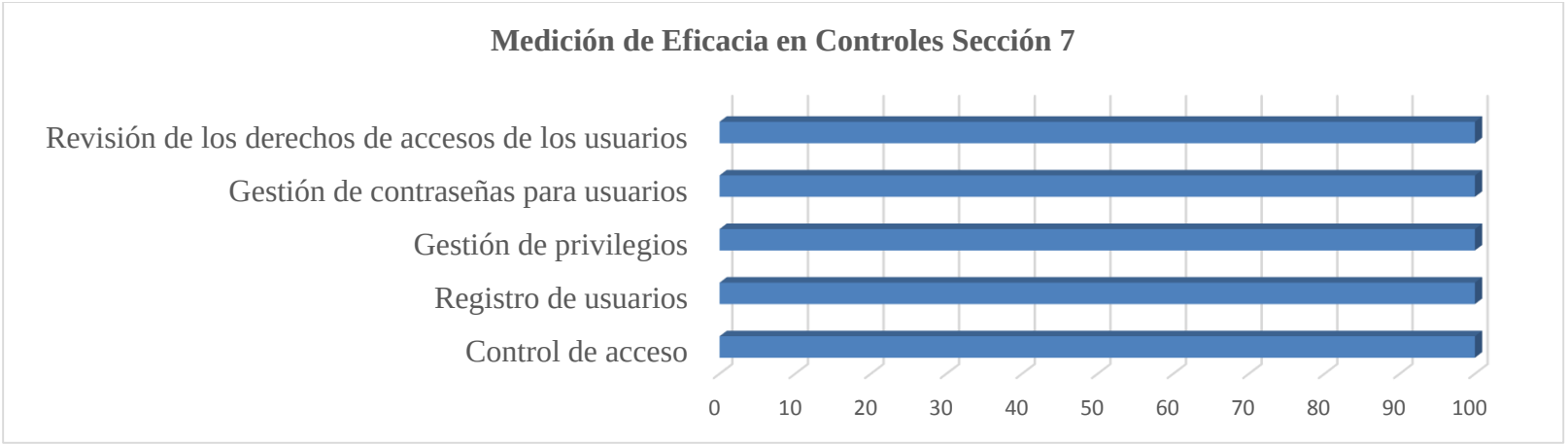
Tabla 10. Valoración para Medición de Eficacia

Las pruebas disparan la siguiente información:



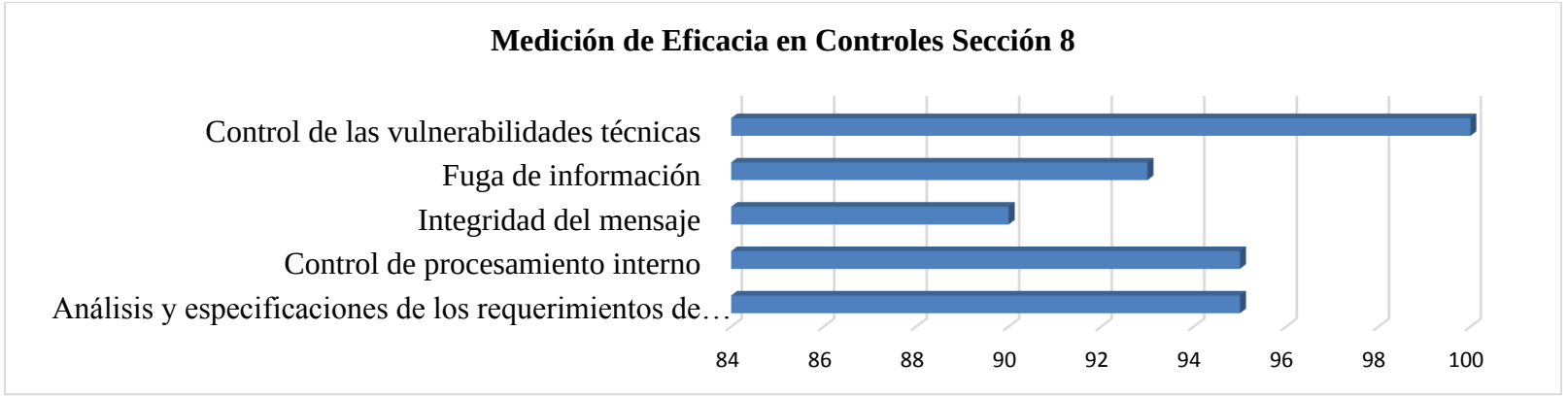
Fuente: Autora

Gráfico 13.Medición de Eficacia en Controles Sección 6



Fuente: Autora

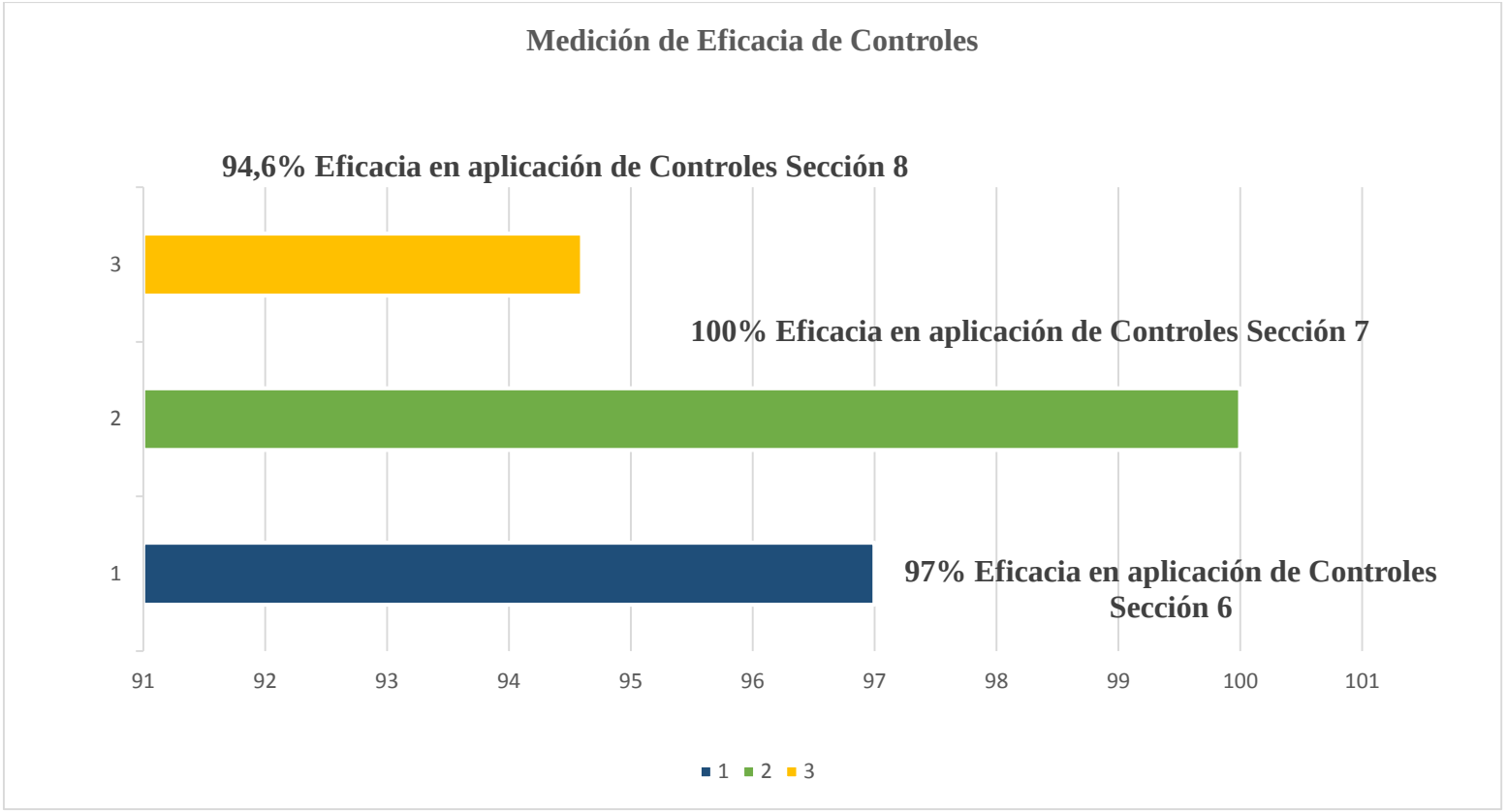
Gráfico 14. Medición de Eficacia en Controles Sección 7



Fuente: Autora

Gráfico 15. Medición de Eficacia en Controles Sección 8

Resumido en lo siguiente:



Fuente: Autora

Gráfico 16. Medición de Eficacia en Controles Aplicados

Con el resultado promedio de la medición de eficacia, se puede determinar que existe un riesgo residual (riesgo que no ha logrado ser controlado) de un 2,8 %, que en términos de nivel de riesgo equivale a 0,448. Por lo que de conformidad con el umbral de análisis y evaluación de riesgos se lo puede aceptar.

5.2.2. Auditoría Interna al SGSI

Para el proceso de auditoría se han efectuado revisiones sobre la política de seguridad y las secciones de los controles evidenciados para aplicación mediante las recomendaciones de auditoría de la ISO 9001:2015, tal como se demuestra en los adjuntos.

Los procesos de auditoría al estar presentes en un sistema de gestión, estos deben ser constantes con los siguientes parámetros mínimos:

Tipo de auditoría	Certificación / Seguimiento / Rectificación /Complementaria
Periodicidad de la auditoría	Trimestral / Semestral / Anual
Dirección auditada	Dirección de Tecnologías de la Información y Comunicación
Responsable de la Auditoría	Nombre de quien la efectúa
Interpretaciones	Conformidad / No Conformidad / Oportunidad de Mejora

Fuente: Autora

Tabla 11.Requisitos procesos de auditoría

Para este caso se efectuarán auditorías semestrales, apuntando a la mejora continua del SGSI implementado.

La auditoría pretende:

- Verificar si el sistema de gestión de seguridad es conforme a todos los requerimientos de

la ISO 27001.

- Evaluar la implementación y la eficacia del SGSI de la organización auditada
- Verificar el mantenimiento y la mejora continua del SGSI de la SECOM.
- Evaluar si el SGSI es capaz de lograr los objetivos y política(s) definidas por la SECOM

Los hallazgos fueron:

- La SECOM ha demostrado la implementación, mantenimiento y mejora continua de su SGSI.
- La SECOM ha realizado la medición, análisis y acciones de mejora para lograr objetivos y metas claves de desempeño y política(s) del SGSI.
- El programa de auditoría interna ha sido completamente implementado y funciona como una herramienta de mantenimiento y mejora de la eficacia del SGSI.
- La revisión por la Dirección asegura la conveniencia, adecuación y la eficacia continua del SGSI.
- El sistema de gestión demostró el cumplimiento mayoritario de los requerimientos de la ISO 27001.

De manera global la SECOM ha implementado, mantenido y mejorado en gran medida su SGSI de acuerdo con los requerimientos de la ISO 27001 y demostrado la capacidad del sistema de satisfacer el alcance propuesto, la política y objetivos institucionales.

No obstante, se ha encontrado no conformidades mayores y menores que deben ser subsanadas, se pueda realizar una auditoría complementaria y de esta manera mejorar el SGSI.

5.3.Fase IV: Actuar- Mejora continua del SGSI

Mejora continua. - La organización debe mejorar de forma continua la eficacia del SGSI a través del uso de la Política de Seguridad de la Información, Objetivos de Seguridad de la Información, resultados de auditorías, análisis de eventos monitorizados, acciones correctivas y preventivas y la revisión por la Dirección. (Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management).

5.3.1. Acciones preventivas y correctivas

Acción correctiva. - La organización debe tomar acciones para eliminar la causa de las no conformidades respecto de los requisitos del SGSI de cara a evitar que éstas vuelvan a ocurrir. El procedimiento documentado para acción correctiva debe definir los requisitos para:

- Identificar no conformidades
- Determinar la causa de las no conformidades
- Evaluar la necesidad de acciones para asegurar que éstas no vuelven a ocurrir
- Determinar e implementar la acción correctiva requerida
- Registrar los resultados de la acción acometida
- Revisar la acción correctiva acometida. (Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management.)

Acción preventiva. - La organización debe determinar acciones para eliminar la causa de no conformidades potenciales respecto de los requisitos del SGSI de cara a prevenir que estas ocurran. Las acciones preventivas tomadas deben de ser apropiadas al impacto de los potenciales problemas. El procedimiento documentado para acciones preventivas debe definir requisitos para:

- Identificar no conformidades potenciales y sus causas

- Evaluar la necesidad de acciones para prevenir la ocurrencia de no conformidades
- Determinar e implementar las acciones preventivas requeridas
- Registrar los resultados de las acciones acometidas
- Revisar la acción preventiva acometida.

La prioridad de las acciones preventivas debe determinarse en base a los resultados de la valoración de riesgos.

Las acciones para prevenir no conformidades son usualmente más eficaces en cuanto a coste que las acciones correctivas. (Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management.)

En este sentido se ha dado a conocer a las diferentes áreas que forman parte de la Dirección de Tecnologías de la Información y Comunicación, los informes de no conformidades detectadas a fin de que puedan realizar las acciones correctivas y de esta manera volver a contar con una evaluación.

Como parte del plan de mejora continua se tienen los informes de no conformidad en los cuales se expone claramente los hallazgos, el análisis de la causa raíz del problema y la solicitud de acción, para este caso correctiva. Para mayor detalle de lo señalado referirse a los informes adjuntos al presente trabajo.

5.3.2. Comprobación de las acciones

Para la comprobación de las acciones el Oficial de Seguridad notificará al responsable de la Dirección de Tecnologías de la Información y Comunicación sobre los cambios, quien a su vez tendrá un plazo de 90 de días para realizar correcciones de mejora continua para el SGSI implementado.

5.4.Fase V: Evaluación de costos y beneficios

Dentro del círculo de Deming, a pesar de no estar referido como una fase formal, es mandatorio considerar el compromiso que se tiene para mantener activo un SGSI, por ello en esta fase se han revisado los costos que se han utilizado para llevar a cabo el presente trabajo en comparación con la inversión que el Estado ecuatoriano ha efectuado por cada producto crítico de la SECOM, a fin de tener un panorama más claro del costo y beneficio respecto a una implementación, administración y mejora continua del SGSI, de la siguiente manera:

Análisis de Costos durante el Tiempo de Implementación del SGSI			
Costo Fijos Considerados (CF)		**Costos Variables Considerados (CV)**	
Sueldos y Salarios	$7.524,00	Horas extra	$1.332,00
Bien inmueble (equipamiento /hardware)	$0,00	Materiales de Oficina	$75,00
		Licencias	$200,00
		Servicios básicos	$0,00
Total CF	$7.524,00	**Total CV**	$1.607,00
Total Costo Invertido: $ 9.131,00			

Fuente: Autora

Tabla 12. Análisis de Costos de Implementación del SGSI

Es preciso señalar que en el análisis de costos invertidos durante la fase de implementación del SGSI, no se hace referencia a valores en hardware, ya que no fue necesaria su adquisición, pues dentro de la SECOM se contaba con los recursos materiales suficientes para poner en acción los controles de mitigación seleccionados.

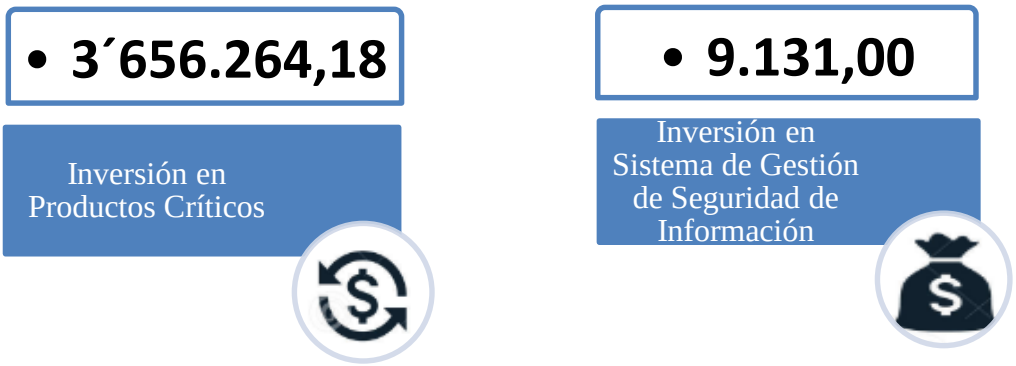
No obstante, para el caso de software fue necesaria su adquisición toda vez que el licenciamiento debe ser original.

Valores Invertidos en Productos Críticos (2014-2016)			
Mensajes comunicacionales/ Cadenas informativas en radio y televisión	$431.110,55	Archivos digitales de audio y video tanto de imágenes oficiales como de las campañas televisivas de la Presidencia	$212.713,30
Enlaces ciudadanos	$210.372,27	Información oficial de la Presidencia de la República enviada vía satelital	$23.881,90
Ayudas memorias para el Presidente/a de la República exposición de motivos, insumos comunicacionales, etc.	$122.951,90	Videos de las actividades del Presidente/a de la República y de actores del Gobierno	$59.595,90
Propuestas políticas, estrategias y herramientas comunicacionales del Gobierno Nacional	$319.181,90	Ruedas de Prensa	$248.713,30
Informes de coordinación con las instituciones de la Función Ejecutiva para obtención de información de la gestión de las mismas	$69.441,90	Documentos de acreditación de medios de comunicación y periodistas para cobertura de información en la Presidencia de la República	$332.246,40
Contenidos para la página Web de la Presidencia	$23.881,90	Campañas emblemáticas de la Presidencia de la República	$159.713,30
Portal, Periódico, Televisión y Radio "El Ciudadano"	$1.215.009,03	Reporte de centralización publicitaria en más de 100 sitios web que corresponden a la función ejecutiva	$923.881,90
Total Valor Invertido: $4´352.695,45			
84% Infraestructura Tecnológica: 3´656.264,18			

Fuente: Autora

Tabla 13. Análisis de Valores Invertidos en Productos Críticos de la SECOM

Las tablas antes expuestas se resumen en lo siguiente:



Fuente: Autora

Gráfico 17. Inversión en Producto Crítico e Inversión en SGSI

Se puede evidenciar que utilizando únicamente el 0,25 % del valor invertido en los productos críticos, se ha dado atención a uno de los ejes más importantes en cuanto a protección de la información sensible de la SECOM; el cual es administrar el Sistema de Gestión de Seguridad de Información, mediante la implementación de controles en los activos de la infraestructura tecnológica.

Es preciso señalar que; adicional a obtener seguridad sobre la información también se están alcanzando beneficios secundarios, como el de minimizar al máximo el impacto social que se puede derivar de una mala gestión sobre la data; generando así conmociones mediáticas, económicas y de reacción indebida por parte de la colectividad.

Capítulo VI

6. Conclusiones y Recomendaciones

6.1. Conclusiones

Se ha logrado diseñar y administrar un sistema de gestión de seguridad de la información a nivel de los activos vinculados a la infraestructura tecnológica en la Secretaría Nacional de Comunicación (SECOM) de manera correcta.

Con la implementación del sistema de gestión, se ha disminuido en gran medida el riesgo asociado a los activos de información vinculados a la infraestructura tecnológica e la SECOM y por ende a los productos críticos que hacen uso de ella, protegiendo de esta manera el dinero que el Estado ecuatoriano ha invertido y seguirá invirtiendo en éstos; pues, se ha podido observar que utilizando únicamente el 0,25% del valor invertido en activos de infraestructura para los productos críticos, se ha dado protección a la información, fortaleciendo así los valores institucionales y dando facilidades a la ciudadanía para que pueda buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, de conformidad con lo señalado en la Constitución de la República del Ecuador.

Con la implementación del Sistema de Gestión de la Seguridad de la Información se han obtenido beneficios transversales para la institución, mejorando la cultura organizacional, tanto a nivel de los usuarios de los servicios y sistemas tecnológicos, como del personal que forma parte del Comité de Seguridad de la Información, pues las responsabilidades y obligaciones se tienen claras por parte de todos los funcionarios de la Secretaría Nacional de Comunicación, por lo que existe un

método más seguro y ordenado sobre el manejo de información, lo cual está evidenciado en los resultados de eficacia en la aplicabilidad del SGSI.

A partir de la implementación del Sistema de Gestión de Seguridad dentro de la Dirección de Tecnologías de la Información y Comunicación, se trabaja con procedimientos estructurados en cuanto a asignaciones de permisos y accesos a la información; así como del manejo de riesgos.

6.2.Recomendaciones

Si bien con la administración y el diseño implementado del SGSI, se ha tratado de cubrir en su totalidad las vulnerabilidades y amenazas que tiene la información digital institucional, siempre se cuenta con un riesgo residual, para este caso de 0,448; mismo que de conformidad con los umbrales de riesgo puede ser aceptado, pues no trae consigo un impacto significativo sobre la gestión de la SECOM. No obstante, haciendo efectivo el ciclo de Deming se lo podría mitigar, por ello se recomienda mantener una cultura de mejora continua para el Sistema de Gestión de Seguridad de la Información instaurado.

A fin de manejar una holgura más ampliada en cuanto a tiempos para hacer efectivo el proceso de implementación de Sistemas de Gestión de cualquier índole, es necesario contar con la participación directa de las autoridades, entendiendo los compromisos que puedan tener planificados y sin dejar de lado las responsabilidades encomendadas.

Se recomienda manejar grupos más amplios de personal que actúe en cada fase del Sistema de Gestión, a fin de evitar el sobrecargo de responsabilidades en un solo equipo.

Al momento las acciones efectuadas son únicamente para los activos de información enfocados a la infraestructura tecnológica. Sin embargo, sería factible extender todo el proceso para otras áreas tales como la de Talento Humano, Administrativa, etc. Es decir, se recomienda completar el

entorno del Sistema de Gestión implementado, para ello se debe contar con el compromiso de toda la institución, pues es un proceso de cambio y cultura organizacional.

En caso de efectuar una ampliación del Sistema de Gestión, se recomienda manejar un equipo externo de auditoría, ya que, al tener el grupo inmerso en el personal de la SECOM, se puede cometer el error de levantar información sin objetividad.

REFERENCIAS BIBLIOGRÁFICAS

Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27002 (2016).

Simbaña, J. C. (2017). Plan de contingencia informática y la pérdida de la información en la Corporación Nacional de Electricidad CNEL Regional Santo Domingo. Universidad Regional Autónoma de los Andes.

Rodríguez, O (2012). Protección de Datos y Seguridad de Estado. Universidad Complutense de Madrid, España.

Martín, A. B. (2014). Calidad de la información en relación con la automedicación en internet. Universidad de Salamanca.

Rebollo, O. (2014). Marco para el Gobierno de la Seguridad de la Información en servicios Cloud Computing. Universidad de Castilla.

Ponjuán, G. (1998). Gestión de información en las organizaciones: principios, conceptos y aplicaciones.

((2012, 01). Obtenido 05, 2017, de http://www.iso27000.es/sgsi.html).

((2017, 01). Obtenido 05, 2017, de http://computer.yourdictionary.com/dataintegrity

Matalobos, J. (2009). Análisis de Riesgos de Seguridad de la Información. Universidad Politécnica de Madrid.

Bertolín, J. A. (2008). Seguridad de la información. Redes, informática y sistemas de información. Editorial Paraninfo.

Cardona, O. (2009). Evaluación De La Amenaza, la Vulnerabilidad y el Riesgo.

Barnes, J. C. (2001). A Guide to Business Continuity Planning.

Hiles, A. (2004). Business Continuity: Best Practices: World-class Business Continuity Management. Rothstein Associates Inc.

Peltier, T. (2001). Information Security Risk Analysis, Auerbach.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management.

Andrés, A., Gómez, L. (2009). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. AENOR.

((2015, 01). Obtenido 05, 2017, de http://fundibeq.es.

Mesquida, A. L., Mas, A., Amengual, E., & Cabestrero, I. (2010). Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. REICIS. Revista Española de Innovación, Calidad e Ingeniería del Software.

(2017, 01). Obtenido 05, 2017, de www.iso.org

Estructura Orgánica Estructural de la Secretaría Nacional de Comunicación. (2014).

(2017,01). Obtenido 05, 2017, de http://www.internetglosario.com/1131/Hackingetico.html

(2017, 05). Obtenido 05, 2017, de https://es.wikipedia.org/wiki/Ataque_inform%C3%A1tico.

(2017, 01). Obtenido 05, 2017, de https://www.coursehero.com/file/21070587/PROBABILIDAD-Ndocx/

(2017, 01). Obtenido 05, 2017, de http://es.erp-docs.com/878/conceptos-clave-glosario-de-terminos-de-sap-pm/

(2017, 01). Obtenido 05, 2017, de https://www.significados.com/bienes/

(2017, 01). Obtenido 05, 2017, de http://www.buenastareas.com/materias/carta-de-cesion-de-bienes-muebles/0

(2014, 07). Obtenido 05, 2017, de http://bibdigital.epn.edu.ec/handle/15000/7731

(2017, 01). Obtenido 05, 2017, de https://www.tecnoseguro.com/faqs/control-de-acceso/Page-2.html

(2017, 01). Obtenido 05, 2017, de https://correoelectronico.wordpress.com/2009/10/07/concepto-de-correo-electronico/

(2016, 07). Obtenido 05, 2017, de https://es.wikipedia.org/wiki/Acuerdo_de_nivel_de_servicio

(2017, 01). Obtenido 05, 2017, de https://redesparapc.wordpress.com/2014/11/29/red-de-computadores/

(2017, 01). Obtenido 05, 2017, de http://definicion.de/cableado-estructurado/

(2013, 01). Obtenido 05, 2017, de http://www.istnetgroup.com/index.php/tecnologias-tendencias/tecnologias/colaboracion

(2017, 01). Obtenido 05, 2017, de https://sites.google.com/site/buan10informatica/bloque-ii/antivirus

(2017, 01). Obtenido 05, 2017, de http://definicion.de/internet/

(2017, 01). Obtenido 05, 2017, de https://sites.google.com/site/tecnologiaeducativayami/paginas-web

(2017, 01). Obtenido 05, 2017, de https://www.clubensayos.com/Tecnolog%C3%ADa/Software-Conjunto-de-programas-y-rutinas-que-permiten/3528723.html

(2017, 01). Obtenido 05, 2017, de https://sites.google.com/site/angelsites675/hardware

(2017, 04). Obtenido 05, 2017, de https://es.wikipedia.org/wiki/Seguridad_perimetral

(2017, 04). Obtenido 05, 2017, de https://es.wikipedia.org/wiki/Acuerdo_de_confidencialidad

(2017, 05). Obtenido 05, 2017, de https://es.wikipedia.org/wiki/Esc%C3%A1ner_de_puertos

(2017, 01). Obtenido 05, 2017, de http://www.controlcase.com/es/managed_compliance_int_vulnerability_scan.html

(2016, 12). Obtenido 05, 2017, de https://es.wikipedia.org/wiki/Inyecci%C3%B3n_de_c%C3%B3digo

(2016, 02). Obtenido 05, 2017, de https://www.owasp.org/index.php/Inyecci%C3%B3n_De_Comandos_En_Java

(2017, 01). Obtenido 05, 2017, de https://gitsinformatica.wordpress.com/2013/06/11/ingenieria-socia-robo-y-suplantacion-de-identidad-y-phishing/

(2017, 01). Obtenido 05, 2017, de https://www.icann.org/news/blog/que-es-el-escalonamiento-de-privilegios

(2017, 01). Obtenido 05, 2017, de http://bienvenidos-comunicaciones.blogspot.com/2012/04/ataques-informaticos.html

Constitución de la República del Ecuador (2008), Artículos 16 & 18.

Esquema Gubernamental de Seguridad de la Información (2013). Acuerdo Ministerial 166. Registro Oficial del Ecuador. Suplemento 88.

Clementina, J. G. (2015). Operacionalización De Variables.

López, S. I. (2015). Operacionalización de variables. hacia la promoción de la salud.

Cobos, L. (2013). El marco metodológico.

Dobles, M., Zúñiga, M., y García, J. (1998). Investigación en educación: Procesos, interacciones, construcciones. San José, Costa Rica: EUNED.

Cascante, L. G. (2015). El paradigma positivista y la concepción dialéctica del conocimiento. Revista Digital: Matemática, Educación e Internet.

Sampieri, R, Collado, C. & Lucio, P. (2003). Metodología de la Investigación.

Universidad Pedagógica Experimental Libertador (1998). Proyecto factible.

Moya, R. D. (2002). El proyecto factible: una modalidad de investigación. Sapiens: Revista Universitaria de Investigación.

Hernández, R., Fernández, C. y Baptista, P. (2003). Metodología de la investigación (3ª ed.). México: Editorial Mc Graw-Hill

Tamayo y Tamayo, M. (1997). El Proceso de la Investigación científica. México. Editorial Limusa S.A

Sabino, C. (2000). El proceso de investigación.

Pérez Juste, R. (1991). Pedagogía Experimental. La Medida en Educación. Curso de Adaptación. Uned. 106.

Mendoza, M. (2015). De la identificación y análisis a la gestión de riesgos de seguridad.

Acosta F, C. B. (2014). Diccionario de la real Academia de la Lengua Española. España-Madrid: Edición, 23.

Moliner, María. 1998. "Diccionario del uso del español, 2da. Edición". Herederos de María Moliner. Editorial Gredos, S.A.

Mokate, K. M. (2001). Eficacia, eficiencia, equidad y sostenibilidad: ¿qué queremos decir? Inter-American Development Bank.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management.

ANEXOS

Institución	**SECRETARÍA NACIONAL DE COMUNICACIÓN (SECOM)**	
Representante de la Dirección	**Director de TIC's**	
Tipo de Revisión		
☐ Pre-Revisión	Revisión para Certificación ☒Etapa 1 o ☐ Etapa 2	Re certificación ☐ Etapa 1 o ☐ Etapa 2
☐ Seguimiento ( )	Otros : Revisión inicial de estado del SGSI dentro de la SECOM	
Responsable revisión	María Belén Jiménez (MBJA)	
Objetivos de la revisión	Para Revisión etapa 1 (marcar todo) ☒ revisar la documentación del sistema de gestión. ☒ evaluar la ubicación y las condiciones específicas del sitio e intercambiar información con el personal ☒ revisar el estado de la SECOM y su grado de compresión de los requisitos de la norma, en particular en lo que concierne a la identificación de aspectos clave o significativos del desempeño procesos, objetivos y funcionamiento del sistema de gestión; ☒ recopilar la información necesaria correspondiente al alcance del sistema de gestión, a los procesos y a las ubicaciones de la SECOM, así como a los aspectos legales y reglamentarios relacionados y su cumplimiento (por ejemplo, aspectos de calidad, ambientales, legales del funcionamiento de la SECOM, los riesgos asociados, etc.); Para Revisión etapa 2 (marcar todo) ☐ evaluar el grado de implementación, incluyendo su eficacia del Sistema de gestión. Para Revisión de seguimiento (marcar todo) ☐ evaluar el mantenimiento del sistema de gestión y mejoramiento continuo de su eficacia.	
Alcance de la revisión	Evaluar y comprobar el cumplimiento del Sistema de Gestión de Seguridad de la Información en la SECOM.	

Criterio de revisión & Documentos de referencia	NTE INEN-ISO/IEC 27001 Acuerdo Ministerial No. 166 Documentación de la SECOM para su SGSI
Idioma	Español

Declaración de Confidencialidad Todas las informaciones evidenciadas durante la realización de esta revisión serán tratadas en estricta confidencialidad, y no serán reveladas a un tercero sin el consentimiento escrito de la SECOM, excepto a las autoridades de acreditación para su evaluación del Sistema de Gestión de la Seguridad.

_____ _____

Representante de la Dirección Fecha

Plan Inicial de Hallazgos SGSI Versión 1.0 / Dic2016

	Requerimientos de Sistema de Gestión de Seguridad de la Información **ISO 27001** **Equipo para Revisión:** **María Belén Jiménez (MBJA)**	Requisitos Generales	Establecimiento del SGSI	Implementación y Operación del SGSI	Seguimiento y revisión del SGSI	Mantenimiento y mejora del SGSI	Generalidades de Requisitos de documentación	Control de Documentos	Control de registros	Compromiso de la dirección	Provisión de recursos	Formación, concienciación	Auditoría Interna del SGSI	Revisión por la dirección	Mejora continua	Acción correctiva	Acción preventiva
Hora:	**Procesos de la SECOM**																
08:30	Reunión de Apertura																
09:00	Gestión de la Dirección ***(Política de Seguridad / Aspectos organizativos de la seguridad de la Información, Cumplimiento)*** (MBJA)	X	X	X	X	X				X				X			
09:30-16:15	Gestión de la Seguridad de la Información ***(Política de Seguridad / Aspectos organizativos de la seguridad de la Información / Gestión de Activos, Control de Acceso, Gestión de Incidentes de la Seguridad de la Información)*** (MBJA)	X	X	X	X	X	X		X		X		X		X	X	X
16:30	Revisión de hallazgos																

Día #2																		
09:00	Gestión de Comunicaciones y Operaciones ***(Gestión de Comunicaciones y Operaciones)*** (MBJA)	X	X	X	X	X												
09:00-16:15	Desarrollo y Mantenimiento de Aplicaciones ***(Adquisición, desarrollo y mantenimiento de los sistemas de información)*** (MBJA)	X	X	X	X	X												
09:00	Infraestructura Tecnológica (MBJA)	X	X	X	X	X												
16:30	Revisión de Hallazgos																	
Día #3																		
09:00	Revisión de hallazgos y preparación de las conclusiones e Informe de revisión																	
15:30	Reunión de Cierre de la Revisión																	

Institución	**SECRETARÍA NACIONAL DE COMUNICACIÓN (SECOM)**
Representante de la Dirección	**Director de TIC's**
Análisis de los Hallazgos	
Responsable del informe	María Belén Jiménez (MBJA)

Dentro del análisis inicial de hallazgos, se ha logrado recopilar la siguiente documentación:

Cuadro No.1.- INFORMACION RECOPILADA

	Documento	Contenido	Fecha	Cantidad de Hojas
CARPETA 1	Acuerdo No.166		19/9/2013	6
	Instructivo para Creación del Proyecto para Implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en el sistema de Gobierno por Resultados (GPR) Noviembre 2013		1/11/2013	12
	Instructivo para Creación del Proyecto para Implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en el sistema de Gobierno por Resultados (GPR) Julio 2014		1/7/2014	18
	Oficio No. SNAP-SGE-2014-000338-O	Convocatoria al taller de implementación del EGSI en la herramienta GPR[1]	29/7/2014	2
	Folleto de Implementación de EGSI		1/8/2014	1
	Informe de Cumplimiento de Hitos	Detalle de cumplimiento de 1 hito	22/8/2014	1

[1] Gobierno Por Resultados.

	Informe de Cumplimiento de Hitos	Detalle de cumplimiento de 1 hito	22/8/2014	1
	Informe de Cumplimiento de Hitos	Detalle de cumplimiento de 1 hito	22/8/2014	1
	Informe de Cumplimiento de Hitos	Detalle de cumplimiento de 1 hito	22/8/2014	1
	Acta de Conformación del Comité de Gestión de Seguridad de la Información (CSI[2])		22/8/2014	3
	Acta de Conformación del Comité de Gestión de Seguridad de la Información (CSI)		22/8/2014	3
	Correo electrónico de Nunez Lara David Fernando para Diego Varga	Socialización de link para EGSI Fase II	23/9/2014	1
	Memorando No. SNC-DAP-2014-0013-M	Convocatoria a reunión de comité para implementación de EGSI	24/9/2014	2
	Correo electrónico de Victor Montaluisa para Salgado Chiliquinga Vanessa Nataly	Envío interno SECOM en el cual se da a conocer a la Dirección Administrativa los hitos a cumplir.	1/10/2014	4
	Oficio No. SNAP-SGE-2014-000478-O	Documentación con fechas de cumplimiento.	17/10/2014	9
	Oficio No. SNAP-SGE-2014-000478-O	Documentación con fechas de cumplimiento.	17/10/2014	3

	Oficio No. SNAP-SGE-2014-000531-O	Planificación de talleres para entidades que se encentran debajo del 50% de cumplimiento de	18/11/2014	2
	Oficio No. SNAP-SGE-2014-000580-O	Solicitud de cumplimiento de EGSI fase II	20/12/2014	1
	Oficio No. SNAP-SGE-2014-000580-O	Solicitud de cumplimiento de EGSI fase II	20/12/2014	4
	Informe de Cumplimiento de Hitos	Detalle de cumplimiento de 175 hitos	24/12/2014	3
	Oficio No. SNAP-SGE-2015-000021-O	Documentación con fechas de cumplimiento. Ranking de implementación de EGSI Fase I y II corte al 10 de enero de 2015	16/1/2015	14
	Oficio No. SNAP-SGE-2015-000021-O	Documentación con fechas de cumplimiento. Ranking de implementación de EGSI Fase I y II corte al 10 de enero de 2015	16/1/2015	7
	Oficio No. SNAP-SGE-2015-000047-O	Solicitud de información sobre Oficial de Seguridad y Responsable de TI para tomar capacitación EGSI	5/2/2015	1

	Correo electrónico de Fátima Astudillo Orellana para Victor Montaluisa	Envio de información de SNAP a SECOM, sobre funcionarios considerados para tomar capacitación de GSI	10/3/2015	2
	Informe de Cumplimiento de Hitos	Detalle de cumplimiento de 76 hitos	10/3/2015	7
	Ranking de Entidades Públicas del Cumplimiento de la Implementación del Esquema Gubernamental de Seguridad de la Información (EGSI)	Ranking de implementación de EGSI Fase I y II corte al 13 de marzo de 2015	13/3/2015	9
	Oficio No. SNAP-SGE-2015-000088-O	Documentación con fechas de cumplimiento. Ranking de implementación de EGSI Fase I y II corte al 13 de marzo de 2015	17/3/2015	14
	Oficio No. SNAP-SGE-2015-000099-O	Cumplimiento EGSI-franja naranja-inferior al 75%	19/3/2015	3
	Oficio No. SNAP-SGE-2015-000105-O	Documentación informativa sobre mejoras en servicio Quipux	20/3/2015	2
	Informe de Cumplimiento de Hitos	Detalle de cumplimiento de 85 hitos	25/3/2015	14
	Oficio No. SNAP-SGE-2015-000119-O	Documentación con fechas de cumplimiento.	30/3/2015	2
	Informe de Cumplimiento de Hitos	Detalle de cumplimiento de 5 hitos	13/4/2015	2

	Informe de Cumplimiento de Hitos	Detalle de cumplimiento de 5 hitos	17/4/2015	2
	Oficio No. SNAP-DNASR-2015-000032-O	Documentación con fechas de cumplimiento. Ranking de implementación de EGSI Fase I y II corte al 25 de marzo de 2015	30/4/2015	21
	Manual De Aplicación Del Logotipo		N/A	14
	Reporte EGSI 29 de Junio de 2015	Matriz SNAP en la cual se denota los hitos cumplidos y el documento de respaldo	N/A	11
	Informe de Cumplimiento de Hitos	Documento de ejemplo	N/A	5

Nota: Por temas de confidencialidad no es posible adjuntar fotocopias de los documentos encontrados en la fase inicial.

Del mismo modo se ha logrado generar una revisión del contexto organizacional mediante el análisis PESTLE (Político, Económico, Social, Tecnológico, Legal y Ecológico).

Cuadro 2. CONTEXTO EXTERNO

Factor Económico	**Factor Político**
Incremento en los costos por mantener información digital en medios de almacenamiento propios o arrendados.	Incremento en el uso de la información pública en el entornos político del país.
Factor Social	**Factor Tecnológico**
Incremento en consumo de información a través de plataformas virtuales y redes sociales.	"Nativos digitales" demanda mayor movilidad, flexibilidad en el uso de dispositivos y libertad de acceso a las redes sociales e información digital.
Factor Legal	**Factor Ecológico**
Constitución de la República	Certificación Punto Verde-Acuerdo Ministerial 131
Código Orgánico Integral Penal	
Disposiciones de la Secretaría Nacional de Administración Pública	

Cuadro 3. CONTEXTO INTERNO

Productos / Servicios Críticos de la SECOM	**Capacidad Tecnológica**
Mensajes comunicacionales / Cadenas informativas en radio y televisión	Equipos de almacenamiento como servidores, discos externos, equipos NAS (Network Attached Storage), Cloud Computing, Repositorio Digital de la SECOM Control de accesos / Acuerdos de confidencialidad /Antivirus /Correo Electrónico /Acuerdos de niveles de servicio / Control de accesos / Redes de datos, enlaces de comunicaciones, cableado estructurado, enlaces temporales, colaboración unificada telefonía IP, videoconferencia / Acuerdos de confidencialidad /Antivirus /Correo Electrónico /Acuerdos de confidencialidad / Control de acceso / Internet / Páginas Web /Desarrollo de Software /Equipo computacional (Hardware) /Equipos de protección perimetral
Enlaces ciudadanos	
Ayudas memorias para el Presidente/a de la República exposición de motivos, insumos comunicacionales, etc.	
Propuestas políticas, estrategias y herramientas comunicacionales del Gobierno Nacional	
Informes de coordinación con las instituciones de la Función Ejecutiva para obtención de información de la gestión de las mismas	
Contenidos para página Web de la Presidencia	
Portal, Periódico, Televisión y Radio "El Ciudadano"	
Archivos digitales de audio y video tanto de imágenes oficiales como de las campañas televisivas de la Presidencia	
Información oficial de la Presidencia de la República enviada vía satelital	
Videos de las actividades del Presidente/a de la República y de actores del Gobierno	
Ruedas de Prensa	
Documentos de acreditación de medios de comunicación y periodistas para cobertura de información en la Presidencia de la República	
Campañas emblemáticas de la Presidencia de la República	
Reporte de centralización publicitaria en más de 100 sitios web que corresponden a la función ejecutiva	

Como se puede observar a pesar de que tanto el contexto externo como el interno tienen relevancia en el proceso de administración del sistema de gestión de seguridad de la información, desde el año 2015, el SGSI no ha tenido una continuidad documental y por ende no se ha estado dando cumplimiento a lo indicado en el Acuerdo Ministerial No.166, emitido por la Secretaría Nacional de Administración Pública, respecto al Esquema Gubernamental de Seguridad de la Información.

Ante esto se debe recordar:

- El compromiso de la máxima autoridad de la institución con la seguridad de la información, pues es responsabilidad de la máxima autoridad de cada entidad mantener la documentación de la implementación del EGSI debidamente organizada y registrada de acuerdo al procedimiento específico que para estos efectos establezca la Secretaría Nacional de la Administración Pública
- Realizar el seguimiento de la puesta en marcha de las normas de EGSI.
- Disponer la difusión, capacitación y sensibilización del contenido de EGSI.
- Conformar oficialmente el Comité de Gestión de la Seguridad de la Información de la institución (CSI) y designar a los integrantes.

Hallazgo

La documentación encontrada no asegura que la administración de un sistema de gestión de seguridad de la información sea manejado de manera correcta dentro de la SECOM o que exista un sistema de gestión como tal.

El análisis PESTLE, apunta que existe una relación directa entre el contexto interno y el externo de la SECOM, sin embargo; no se ha manejado un grado de compresión de los requisitos de la norma NTE INEN-ISO/IEC 27001, en particular en lo que concierne a la identificación de aspectos clave o significativos del desempeño procesos, objetivos y funcionamiento del sistema de gestión.

Los productos críticos de la SECOM mantienen una relación directa con la infraestructura tecnológica. De hecho, requiere una gran capacidad de activos de información se de desprenden de dicha área por lo es esencial mantener un sistema de gestión de seguridad de la información.

Criterio de revisión & Documentos de referencia	NTE INEN-ISO/IEC 27001 Acuerdo Ministerial No. 166 Documentación de la SECOM para su SGSI
Idioma	Español

Declaración de Confidencialidad Todas las informaciones evidenciadas durante la realización de esta revisión serán tratadas en estricta confidencialidad, y no serán reveladas a un tercero sin el consentimiento escrito de la SECOM, excepto a las autoridades de acreditación para su evaluación del Sistema de Gestión de la Seguridad.

_____ _____

Representante de la Dirección Fecha

Cuestionario

Presentación
El objetivo del presente cuestionario es obtener información para la correcta administración del Sistema de Gestión de Seguridad de la Información de la SECOM.

Estructura	
Tipo de Pregunta:	Dicotómica
Escala:	SI / NO

Instrucciones de llenado
Este es un cuestionario dirigido a los directores de las áreas agregadoras de valor a fin de conocer el nivel de seguridad que consideran tiene la información de cada una de sus direcciones. Para ello, el encuestado deberá contestar únicamente con SI o NO a cada una de las preguntas. No está permitido obviar preguntas o seleccionar dos respuestas. Para que el estudio surja efecto es necesario contar con total franqueza en las respuestas.

Sobre la Confidencialidad

PREGUNTA	**SI/NO**
¿Considera que los productos que efectúa su dirección se han visto vulnerados en confidencialidad debido a ingresos no permitidos en la red de la SECOM?	SI ( ) NO ( )
¿Considera que existen funcionarios que tienen en su poder credenciales que no les pertenecen para acceder a equipos, carpetas compartidas, la red de datos, etc. de la SECOM, poniendo en duda la confidencialidad de los productos que efectúa su dirección?	SI ( ) NO ( )
¿Considera que en algún momento se ha filtrado información por la intervención de agentes de espionaje en la SECOM?	SI ( ) NO ( )
¿Considera que en algún momento se ha filtrado información, es decir que debido a la mala manipulación de la información se ha entregado información sin fuente fidedigna?	SI ( ) NO ( )
¿Considera que existe la suficiente seguridad y control en la red de datos de la SECOM, una vez que los usuarios han salido de la entidad ?	SI ( ) NO ( )

Cuestionario

¿Considera que la red de datos de la SECOM en algún momento ha tenido ataques, sean estos leves o críticos?	SI ( ) NO ( )
¿Considera que los sistemas de almacenamiento de la información cumplen con los requisitos mínimos de confidencialidad?	SI ( ) NO ( )
¿Considera que se ha elegido correctamente a su personal previo al ingreso a la institución?	SI ( ) NO ( )
¿A firmado alguna vez un documento denominado Acuerdo de Confidencialidad?	SI ( ) NO ( )
¿Utiliza usted software exclusivo para efectuar trabajos sobre la información que maneja su dirección, como para editarla descomprimirla, transformarla?	SI ( ) NO ( )

Sobre la Integridad

PREGUNTA	SI/NO
¿Considera usted que la institución le ha brindado suficiente capacitación para el correcto tratamiento de la integridad de la información?	SI ( ) NO ( )
¿Utiliza usted software exclusivo para efectuar trabajos sobre la información que maneja su dirección, como para editarla descomprimirla, transformarla?	SI ( ) NO ( )
¿Considera que los sistemas de almacenamiento de la información cumplen con los requisitos mínimos de integridad?	SI ( ) NO ( )
¿Utiliza usted hardware propio para manejo y transportación de información de la institución?	SI ( ) NO ( )
¿Considera que en algún momento se ha filtrado información, es decir que debido a la mala manipulación de la información se ha entregado información sin fuente fidedigna?	SI ( ) NO ( )
¿Usted cifra (ubica contraseña de seguridad) la información antes de enviarla o transportarla?	SI ( ) NO ( )

Cuestionario

¿Considera que existen funcionarios que tienen en su poder credenciales que no les pertenecen para acceder a equipos, carpetas compartidas, la red de datos,etc. de la SECOM, poniendo en duda la integridad de los productos que efectúa su dirección?	SI ( ) NO ( )
¿Considera que en la institución existe control de los equipos que ingresan o salen?	SI ( ) NO ( )
¿Considera que los productos que efectúa su dirección se han visto vulnerados en integridad debido a ingresos no permitidos en los sistemas de la SECOM?	SI ( ) NO ( )

Sobre la Disponibilidad

PREGUNTA	SI/NO
¿Ha experimentado fallas en la conectividad, es decir ha tenido corte en el servicio de internet, la red de datos o acceso a sistemas?	SI ( ) NO ( )
¿Considera que los productos que efectúa su dirección se han visto vulnerados en disponibilidad debido a ingresos no permitidos en la red de la SECOM?	SI ( ) NO ( )
¿Considera que existe la suficiente seguridad y control en la red de datos de la SECOM, una vez que los usuarios han salido de la entidad ?	SI ( ) NO ( )
¿Ha recibido notificaciones en las cuales se indica que el proveedor de servicios (internet, red, etc) se está demorando en levantar el servicio?	SI ( ) NO ( )
¿Ha experimentado fallas en la red eléctrica?	SI ( ) NO ( )

Declaración de Confidencialidad Todo lo evidenciados durante la realización de este cuestionario será tratado en estricta confidencialidad, y no será revelado a un tercero sin el consentimiento escrito de la SECOM, excepto a las autoridades de acreditación para su evaluación del Sistema de Gestión de la Seguridad.

_____ _____

Representante de la Dirección Fecha

Operacionalización de Variables CID

							TABULACIÓN DE RESULTADOS							
VARIABLE	DIMENSIONES	INDICADORES	ÍTEMS	ESCALA	VALOR	INSTRUMENTO	Dirección Nacional de Síntesis y Análisis Internacional	Dirección Nacional de Enfoque Político	Dirección Nacional de Contenidos de Medios Institucionales	Dirección Nacional de Informes Gubernamentales	Dirección Nacional de Gestión de la Comunicación	Dirección Nacional de Promoción, Innovación y Redes Digitales	Dirección Nacional de Producción de Eventos, Marketing y Publicidad	RESULTADOS PROMEDIO
CONFIDENCIALIDAD	Permisos no autorizados a la red	Número de ingresos no permitidos en redes alámbricas o inalámbricas	¿Considera que los productos que efectúa su dirección se han visto vulnerados en confidencialiad debido a ingresos no permitidos en la red de la SECOM?	SI NO	SI: 1 NO: 0	Cuestionario	1	1	1	1	1	1	1	1
	Mala asignación y Uso indebido de credenciales	Número de funcionarios que tiene en su poder credenciales de terceros	¿Considera que existen funcionarios que tienen en su poder credenciales que no les pertenecen para acceder a equipos, carpetas compartidas, la red de datos,etc. de la SECOM, poniendo en duda la confidencialidad de los productos que efectúa su dirección?	SI NO	SI: 1 NO: 0	Cuestionario	1	1	1	1	1	1	1	1
	Espionaje mediante agentes en cubieto	Cantidad de información filtrada sin consentimiento	¿Considera que en algún momento se ha filtrado información por la intervención de agentes de espionaje en la SECOM?	SI NO	SI: 1 NO: 0	Cuestionario	0	1	1	0	1	0	0	0,428571429
	Manipulación inadecuada o divulgación de la información	Número de noticias sin fuente fidedigna	¿Considera que en algún momento se ha filtrado información, es decir que debido a la mala manipulación de la información se ha entregado información sin fuente fidedigna?	SI NO	SI: 1 NO: 0	Cuestionario	1	1	1	1	1	1	1	1
	Omisión en bloqueo de puertos	Cantidad de ingresos no adecuados pero permitidos en redes alámbricas o inalámbricas	¿Considera que existe la suficiente seguridad y control en la red de datos de la SECOM, una vez que los usuarios han salido de la entidad ?	SI NO	SI: 0 NO: 1	Cuestionario	1	1	1	1	1	1	1	1
	Ataque físico/lógico	Número de ataques efectuaados	¿Considera que la red de datos de la SECOM en algún momento ha tenido ataques, sean estos leves o críticos?	SI NO	SI: 1 NO: 0	Cuestionario	1	1	1	1	1	1	1	1
	Robo de información	Cantidad de documentos extraviados o mal transferida	¿Considera que los sistemas de almacenamiento de la información cumplen con los requisitos mínimos de confidencialidad?	SI NO	SI: 0 NO: 1	Cuestionario	1	1	1	1	1	1	1	1
	Falta de selección de personal adecuado para manejo de información	Número de funcionarios que no cumplen con el perfil del cargo	¿Considera que se ha elegido correctamente a su personal previo al ingreso a la institución?	SI NO	SI: 0 NO: 1	Cuestionario	0	0	0	0	0	0	0	0
	Ausencia o Falta de Cumplimiento de Acuerdos de confidencialidad	Número de acuerdos de confidencialidad firmados	¿A firmado alguna vez un docuemnto denominado Acuerdo de Confidencialidad?	SI NO	SI: 0 NO: 1	Cuestionario	1	1	1	1	1	1	1	1
	Ejecución / Utilización de programas no autorizados	Número de programas no autorizados instalados	¿Utiliza usted software exclusivo para efectuar trabajos sobre la información que maneja su dirección, como para editarla descomprimirla, transformarla?	SI NO	SI: 1 NO: 0	Cuestionario	1	1	0	0	1	1	1	0,714285714

Operacionalización de Variables CID

							TABULACIÓN DE RESULTADOS							
VARIABLE	DIMENSIONES	INDICADORES	ÍTEMS	ESCALA	VALOR	INSTRUMENTO	Dirección Nacional de Síntesis y Análisis Internacional	Dirección Nacional de Enfoque Político	Dirección Nacional de Contenidos de Medios Institucionales	Dirección Nacional de Informes Gubernamentales	Dirección Nacional de Gestión de la Comunicación	Dirección Nacional de Promoción, Innovación y Redes Digitales	Dirección Nacional de Producción de Eventos, Marketing y Publicidad	RESULTADOS PROMEDIO
INTEGRIDAD	Falta de inducción, capacitación y sensibilización sobre riesgos	Número de funcionarios capacitados	¿Considera usted que la institución le ha brindado suficiente capacitación para el correcto tratamiento de la integridad de la informción?	SI NO	SI: 0 NO: 1	Cuestionario	1	1	1	1	1	1	1	1
	Utilización de programas no autorizados	Número de programas no autorizados instalados	¿Utiliza usted software exclusivo para efectuar trabajos sobre la información que maneja su dirección, como para editarla descomprimirla, transformarla?	SI NO	SI: 1 NO: 0	Cuestionario	1	1	1	1	1	1	1	1
	Pérdida de datos	Cantidad de documentos físicos o electrónicos extraviados	¿Considera que los sistemas de almacenamiento de la información cumplen con los requisitos mínimos de integridad?	SI NO	SI: 0 NO: 1	Cuestionario	1	1	1	0	1	1	0	0,714285714
	Utilización indebida de hardware de almacenamiento	Cantidad de equios no autorizados utlizados para almacenar	¿Utiliza usted hardware propio para manejo y transportación de información de la institución?	SI NO	SI: 1 NO: 0	Cuestionario	1	1	1	1	1	1	1	1
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Número de noticias sin fuente fidedigna	¿Considera que en algún momento se ha filtrado información, es decir que debido a la mala manipulación de la información se ha entregado información sin fuente fidedigna?	SI NO	SI: 1 NO: 0	Cuestionario	1	1	1	1	1	1	1	1
	Transmisión no cifrada de datos críticos	Cantidad de datos no cifrados	¿Usted cifra (ubica contraseña de seguridad) la información antes de enviarla o transportarla?	SI NO	SI: 0 NO: 1	Cuestionario	1	0	1	1	1	1	1	0,857142857
	Manejo inadecuado de credenciales	Número de funcionarios que tiene en su poder credenciales de terceros	¿Considera que existen funcionarios que tienen en su poder credenciales que no les pertenecen para acceder a equipos, carpetas compartidas, la red de datos,etc. de la SECOM, poniendo en duda la integridad de los productos que efectúa su dirección?	SI NO	SI: 1 NO: 0	Cuestionario	1	1	1	1	1	1	1	1
	Exposición o extravío de equipo, unidades de almacenamiento, etc	Número de equipos perdidos	¿Considera que en la institución existe control de los equipos que ingresan o salen?	SI NO	SI: 0 NO: 1	Cuestionario	1	0	1	0	1	1	1	0,714285714
	Acceso electrónico no autorizado a sistemas	Número de ingresos no permitidos en sistemas	¿Considera que los productos que efectúa su dirección se han visto vulnerados en integridad debido a ingresos no permitidos en los sistemas de la SECOM?	SI NO	SI: 0 NO: 1	Cuestionario	1	0	1	1	1	1	1	0,857142857

Operacionalización de Variables CID

							TABULACIÓN DE RESULTADOS							
VARIABLE	DIMENSIONES	INDICADORES	ÍTEMS	ESCALA	VALOR	INSTRUMENTO	Dirección Nacional de Síntesis y Análisis Internacional	Dirección Nacional de Enfoque Político	Dirección Nacional de Contenidos de Medios Institucionales	Dirección Nacional de Informes Gubernamentales	Dirección Nacional de Gestión de la Comunicación	Dirección Nacional de Promoción, Innovación y Redes Digitales	Dirección Nacional de Producción de Eventos, Marketing y Publicidad	RESULTADOS PROMEDIO
Disponibilidad	Fallas de conectividad	Cantidad de pérdidas de servicios	¿Ha experimentado fallas en la conectividad, es decir ha tenido corte en el servicio de internet, la red de datos o acceso a sistemas?	SI NO	SI: 1 NO: 0	Cuestionario	1	1	1	1	1	1	1	1
	Red expuesta al acceso no autorizado	Número de ingresos no autorizados detectados	¿Considera que los productos que efectúa su dirección se han visto vulnerados en disponibilidad debido a ingresos no permitidos en la red de la SECOM?	SI NO	SI: 1 NO: 0	Cuestionario	1	1	1	1	1	1	1	1
	Ausencia de controles en apertura o cierre de puertos	Número de ingresos no autorizados detectados	¿Considera que existe la suficiente seguridad y control en la red de datos de la SECOM, una vez que los usuarios han salido de la entidad?	SI NO	SI: 0 NO: 1	Cuestionario	1	1	1	0	1	1	0	0,714285714
	Incumplimiento de Acuerdos de Niveles de Servicio por parte de Proveedores	Cantidad de multas impuestas debido a incumplimiento de servicios	¿Ha recibido notificaciones en las cuales se indica que el proveedor de serivicios (internet, red,etc) se está demorando en levantar el sericio?	SI NO	SI: 1 NO: 0	Cuestionario	1	1	1	1	1	1	1	1
	Fallas eléctricas	Número de cortes eléctricos	¿Ha experimentado fallas en la red eléctrica?	SI NO	SI: 1 NO: 0	Cuestionario	1	1	1	1	1	1	1	1

Concentración de Amenazas / Vulnerabilidades CID

	Amenaza/ Vulnerabilidad	Valoración nivel de riesgo	Valoración Concentración Porcentual
Confidencialidad	**Permisos no autorizados a la red**	5,92	4%
	Mala asignación y Uso indebido de credenciales	8,88	6%
	Manipulación inadecuada o divulgación de la información	8,88	6%
	Omisión en bloqueo de puertos	8,88	6%
	Ataque físico/lógico	11,84	8%
	Robo de información	11,84	8%
	Ausencia o Falta de Cumplimiento de Acuerdos de confidencialidad	8,88	6%
	Ejecución / Utilización de programas no autorizados	8,88	6%
	TOTAL	**73,97**	**50%**

Concentración de Amenazas / Vulnerabilidades CID

	Amenaza/ Vulnerabilidad	Valoración nivel de riesgo	Valoración Concentración Porcentual
Integridad	**Falta de inducción, capacitación y sensibilización sobre riesgos**	5,92	4%
	Utilización de programas no autorizados	2,96	2%
	Pérdida de datos	5,92	4%
	Utilización indebida de hardware de almacenamiento	5,92	4%
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	5,92	4%
	Transmisión no cifrada de datos críticos	2,96	2%
	Manejo inadecuado de credenciales	8,88	6%
	Exposición o extravío de equipo, unidades de almacenamiento, etc	8,88	6%
	Acceso electrónico no autorizado a sistemas	5,92	4%
	TOTAL	**53,26**	**36%**

Concentración de Amenazas / Vulnerabilidades CID

	Amenaza/ Vulnerabilidad	Valoración nivel de riesgo	Valoración Concentración Porcentual
Disponibilidad	**Fallas de conectividad**	$2,96	2%
	Red expuesta al acceso no autorizado	$2,96	2%
	Ausencia de controles en apertura o cierre de puertos	$5,92	4%
	Incumplimiento de Acuerdos de Niveles de Servicio por parte de Proveedores	$5,92	4%
	Fallas eléctricas	$2,96	2%
	TOTAL	**20,71**	**14%**

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

FASE II CÍCLO DE DEMING

FIRMAS DE REVISIÓN Y APROBACIÓN

	Nombre / Cargo	**Firma**	**Fecha**
Elaborado por:			
Revisado por:			
Aprobado por:			

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

CONTENIDO

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA

Versión: 1.0

1. INTRODUCCIÓN

La Secretaría Nacional de Comunicación proporciona a sus funcionarios los servicios tecnológicos para su utilización en actividades laborales, de investigación, desarrollo e innovación, incluyendo las tareas administrativas asociadas.

Dado que estos recursos y servicios son ampliamente utilizados se evidencia la necesidad de implementar una normativa que, partiendo de la ineludible adecuación a la legislación vigente, clarifique la forma correcta de uso de los mismos, delimite las responsabilidades y proporcione un marco para la regulación del uso de cada uno de ellos.

2. PROPÓSITO

Ofrecer a los usuarios una guía sobre los requisitos mínimos que deben ser cumplidos respecto al uso de los servicios informáticos, como también las implicancias del mal uso, con la finalidad de proteger a los funcionarios de la institución de acciones ilegales, exposición de la institución a riesgos innecesarios como los virus informáticos, interrupción de las redes y sus servicios, problemas jurídicos tanto nacionales como internacionales.

3. OBJETIVO

Dotar de la información necesaria a los usuarios de los servicios tecnológicos brindados por la SECOM, en relación a las normas y mecanismos que deben cumplir con el fin de utilizar correctamente los recursos tecnológicos de la institución, así como precautelar la información que

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

es procesada y almacenada en los mismos mediante la planeación, organización y ejecución de políticas.

4. ALCANCE

Las políticas mencionadas en el presente documento cubren el uso apropiado de los recursos informáticos y aplica a todos los miembros de la Institución, a nivel individual y colectivo, incluyendo direcciones, subsecretarías, coordinaciones, servicios, entre otros, así como terceras personas tales como consultores y contratistas con o sin relación de dependencia a la Institución

Se incluye, además, todas las dependencias que son parte de la institución. Estas políticas fueron desarrolladas basadas en el tráfico en la red, ancho de banda y el buen desempeño de los recursos disponibles para todos los usuarios, cuyos niveles de consumo determinan los distintos grados de restricción en el acceso.

La Dirección de Tecnologías de la Información y Comunicación, será la encargada de administrar la presente Política, actualizarla y velar por su cumplimiento y aplicabilidad, así como modificarla en el caso de ser necesario.

5. COMO USAR ESTE DOCUMENTO

Este documento es una Guía sobre las políticas implementadas, que garantizarán una operación y ejecución adecuadas dentro de la Dirección de Tecnologías de la Información y Comunicación y sus Coordinaciones, todo empleado es responsable del cumplimiento de los

estándares, directrices y procedimientos de control de acceso, así como también notificar a su nivel jerárquico superior, cuando por algún motivo no pueda cumplir con las políticas indicando el motivo por el cual no le es posible apegarse a la normativa. Cabe destacar que este nivel de responsabilidad va a ser conocido por las diferentes áreas quienes serán las garantes de que esta información sea conocida por cada integrante de área.

6. VIGENCIA

La documentación presentada como Política de Seguridad de la Infraestructura Tecnológica entrará en vigencia desde el momento que sean aprobadas por la máxima autoridad. Esta normativa deberá ser revisada y actualizada conforme a las exigencias de las autoridades o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica.

7. MARCO LEGAL

A través del Decreto Ejecutivo No. 3 de 30 de mayo de 2013, se creó la Secretaría Nacional de Comunicación como entidad de derecho público, con personalidad jurídica y patrimonio propio, dotada de autonomía presupuestaria, financiera y administrativa.

Dentro de los objetivos y metas institucionales de esta Cartera de Estado, está la de establecer y dirigir la política nacional de comunicación social e información pública del Gobierno Nacional, encaminada a estimular la participación de todos los sectores de la población en el proceso de desarrollo nacional.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

La Dirección de Tecnologías de la Información y Comunicación tiene como misión dentro de la Secretaría Nacional de Comunicación proponer, implementar, administrar políticas, normas y procedimientos que optimicen la gestión y administración de las tecnologías de la información y comunicaciones (TICs), garantizando la integridad de la información, optimización de recursos, sistematización y automatización de los procesos institucionales, así como el soporte tecnológico institucional.

8. CONSIDERACIONES GENERALES

- Las políticas relacionadas a los servicios tecnológicos están enfocadas a:
- Documentación de los procedimientos y operación
- Monitoreo y revisión de los servicios, por terceros
- Controles contra código malicioso
- Controles contra códigos móviles
- Controles de la red
- Seguridad de los servicios de la red
- Gestión de los medios removibles
- Procedimiento para el manejo de la información
- Seguridad de la documentación del sistema
- Políticas y procedimientos para el intercambio de información
- Mensajería electrónica

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

- Sistemas de Información del Negocio
- Transacciones en línea
- Protección del registro de la información
- Control de acceso
- Registro de usuarios
- Gestión de privilegios
- Gestión de contraseñas para usuarios
- Revisión de los derechos de accesos de los usuarios
- Uso de contraseñas
- Análisis y especificaciones de los requerimientos de seguridad
- Control de procesamiento interno
- Integridad del mensaje
- Fuga de información
- Control de las vulnerabilidades técnicas

a. **Políticas Generales, Documentación de los procedimientos y operación**

Las Políticas relacionadas a las Tecnologías de la Información, están enfocadas a los equipos de computación que son asignados a cada funcionario, así como al centro de datos, y a la propiedad de la información que es creada y usada por los usuarios de la Secretaría Nacional de Comunicación, con el fin de evitar la inadecuada utilización de los recursos informáticos que se pone a disposición de los funcionarios para que desarrollen sus actividades institucionales.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

La Dirección de Tecnologías de la Información y Comunicación es la encargada de velar por los recursos y servicios informáticos.

La Dirección Administrativa es la responsable de la entrega de equipos y activos fijos a los funcionarios, así como de la custodia de los equipos informáticos de la Institución.

Los Subsecretarios, Coordinadores Generales, Directores de cada área o Gerentes de Proyectos, son los responsables del pedido de los recursos informáticos y del uso de los servicios de los miembros de su departamento o grupo, destinados a las actividades propias de cada estructura.

Bajo ninguna circunstancia los funcionarios de la Institución, utilizarán los recursos informáticos para realizar actividades prohibidas por las normas establecidas o por normas jurídicas nacionales o internacionales.

Para los equipos informáticos propiedad de la Secretaría Nacional de Comunicación, la Coordinación de Soporte a usuario y mesa de ayuda perteneciente a la Dirección de Tecnologías de la Información y Comunicación, será la única coordinación autorizada a realizar actividades de soporte técnico y cambios de configuración en los equipos informáticos de los funcionarios de la Institución.

En el caso de contratación para labores de mantenimiento, la Dirección de Tecnologías de la Información y Comunicación, aprobará previamente los mantenimientos solicitados.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

En caso de arriendo de computadoras la empresa contratada es la única autorizada para realizar labores de soporte y mantenimiento.

Todo aquello que desee ser implementado en ámbito tecnológico deberá ser documentado.

b. **Políticas para Controles de la red, Seguridad de los servicios de la red, Control de acceso, registro de usuarios, gestión de privilegios, gestión de contraseñas**

Registro de Usuarios, Contraseñas, Privilegios

La Dirección de Talento Humano será la encargada de subir el listado de funcionarios que han ingresado, en la carpeta compartida creada para este fin. Posterior a esto dicha dirección emitirá un correo electrónico a soporte@secom.gob.ec; indicando que existen nuevos funcionarios y solicitando la creación de los usuarios.

Los parámetros mínimos que deben ser considerados para la creación del usuario son: cédula de ciudadanía, nombres completos, unidad organizacional a la que pertenecerá, denominación al cargo que desempeñará, título académico, ciudad en la que laborará.

Una vez que el requerimiento llegue a la Dirección de TIC’s se generará el usuario dentro de la Unidad Organizacional a la cual pertenecerá con perfil de NORMAL_ACCOUNT.

Si, por temas propios de las actividades de los usuarios es necesario elevar permisos en el perfil del usuario, un técnico de TIC’s de nivel 1, una vez revisada y validada la necesidad, se procederá a solicitar al nivel 2 se asignen los privilegios necesarios.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Son usuarios creados para propósitos especiales en manejos de servicios.

Serán solicitados exclusivamente por los líderes de las áreas que conforman la Dirección de Tecnologías de la Información y Comunicación, mediante correo electrónico a soporte@secom.gob.ec

Todas las contraseñas son consideradas como información confidencial de la SECOM, con los siguientes requisitos adicionales.

Los usuarios deben proteger adecuadamente las contraseñas de todas las cuentas y sistemas.

Las contraseñas, no deben ser compartidas con otros individuos o usuarios.

Excepción: Las contraseñas se pueden compartir con el personal autorizado de la Dirección de Tecnologías de la Información. El usuario es el responsable de cambiar la contraseña luego de una actividad de mantenimiento autorizada.

Los usuarios creados poseen clave por defecto de manera inicial. Se solicitará el cambio de contraseña en el siguiente inicio de sesión; excepto de los usuarios de servicios, los cuales mantendrán una contraseña sin fecha de expiración.

La Dirección de Tecnologías de la Información y Comunicación promueve el uso de contraseñas fuertes, con las siguientes características:

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

- No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos.
- Tener una longitud mínima de siete caracteres
- Incluir caracteres de las siguientes categorías:
- Mayúsculas
- Minúsculas
- Dígitos de base 10 (0 al 9)
- Caracteres especiales

Las contraseñas en alfabetos (latino, cirílico o griego) deben contener caracteres de, por lo menos tres (3) de las siguientes cuatro clases (las contraseñas que utilizan caracteres chinos o japoneses no tienen requisitos de complejidad):

Descripción de clase	Ejemplos
1. Letras mayúsculas	A B C…Z
2. Letras minúsculas	a b c…z
3. Numerales arábigos	0 1 2 … 9
4. No alfanumérico ("caracteres especiales", puntuación, símbolos)	{ } [ ] , . < > ; : ‘ “ ? / | \ ` ~ ! @ # $ % ^ & * ( ) _ - + =

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Las contraseñas no deben derivar de palabras o frases utilizadas comúnmente.

Se debe capacitar a los usuarios para que no seleccionen contraseñas con palabras fáciles, como palabras que se encuentran en diccionarios (de inglés o de otro idioma), identificación de usuario, nombres propios y otros nombres o palabras rápidamente asociadas con el usuario individual, como fechas, sobrenombres o apellidos.

El administrador de la red deberá capacitar a los usuarios para que no seleccionen contraseñas que contengan palabras fáciles precedidas o seguidas de uno o más números o un carácter especial. (Por ejemplo, no son aceptables Daniel!, $Roberto, $$Stew, 1Walt2, Ivy123, etc.).

Las nuevas contraseñas no deben ser parecidas a las últimas cinco (5) anteriores.

Todos los usuarios deberán modificar su contraseña cada 45 días

La vigencia mínima de la contraseña será de 1 día.

En caso de requerir cambios de contraseña, el usuario deberá solicitar a la Dirección de Tecnologías de la Información y Comunicación.

Ante la sospecha de que una contraseña haya sido revelada a terceros, se cambiará la misma de forma inmediata, y se procederá a notificar del incidente de seguridad, a la Dirección de Tecnologías de la Información y Comunicación.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Las cuentas de usuario que tengan privilegios de sistema, a través de su pertenencia a grupos o por cualquier otro medio, tendrán contraseñas distintas a otras cuentas mantenidas por dicho usuario en los servicios y recursos.

Las contraseñas de los funcionarios que se desvinculan de la Secretaría Nacional de Comunicación, se desactivarán una vez que la Dirección de Tecnologías de la Información y Comunicación, reciba el listado respectivo por parte de la Dirección de Talento Humano y posterior a la firma de la hoja de ruta respectiva.

Se prohíbe terminantemente la utilización de una identificación de usuario grupal y sus contraseñas asociadas. Sólo deberá permitirse cuando sea necesario para respaldar procesos institucionales.

Se prohíbe terminantemente la anotación de contraseñas. Sólo deberá permitirse cuando sea necesario para respaldar los procesos institucionales. Las contraseñas que se deban anotar, deben estar protegidas adecuadamente para prevenir su divulgación a cualquier otra persona que no fuera su propietario.

Las contraseñas no deben visualizarse en pantalla en ningún momento.

Las contraseñas se deben cambiar cada vez que el sistema lo indique o la contraseña se encuentre comprometida.

Cualquier sistema de gestión de contraseña debe evitar el ocultar la contraseña, o debe proveer protecciones y controles apropiados si dicho ocultamiento es esencial.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Las contraseñas siempre se deben cifrar cuando se almacenan o cuando se transmiten a través de cualquier red. Se considera cifrado a la utilización de un algoritmo hash aprobado por la DTI para casos de protección de contraseña.

Las contraseñas sin cifrar nunca se deben incluir en utilidades de registro. Por ejemplo, un usuario no autorizado nunca debe estar habilitado para autenticarse solamente mediante el uso de una tecla de función o la ejecución de un programa disponible.

Las contraseñas sin cifrar no deben estar codificadas en el código fuente, los archivos de comando, los archivos de inicialización, secuencias de comandos o paquetes de instalación. Excepción: Las contraseñas se pueden ubicar en archivos de comando, archivos de inicialización o secuencias de comandos si el acceso a estos archivos está restringido sólo a aquellas personas encargadas de la gestión del sistema o la aplicación en la cual residen dichos archivos.

Se deben desactivar en forma automática todas las cuentas que otorgan acceso a la información institucional fundamental luego de (3) intentos secuenciales de inicio de sesión inválidos dentro de un período de quince (15) minutos. Luego de desactivada, la cuenta permanecerá bloqueada por un mínimo de quince (15) minutos.

Se debe otorgar una prueba de identificación adecuada antes de cambiar la contraseña.

Los usuarios que cambian una contraseña por medio de un comando o una pantalla del sistema deben probar conocimiento de la contraseña actual o ser autenticadas en forma criptográfica antes de estar autorizados al cambio.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

El tiempo mínimo entre los cambios de contraseña iniciados por el usuario debe ser de, al menos, un (1) día. Si el usuario cambió recientemente la contraseña y teme que la nueva contraseña pueda verse comprometida, pero está incapacitado de modificarla nuevamente en forma inmediata de acuerdo con esta cláusula, deberá contactar al administrador del sistema en donde se utiliza la contraseña para restablecerla.

Los usuarios que soliciten una nueva contraseña, o soliciten un cambio o restauración de la contraseña por medio de la mesa de ayuda o del administrador, deben probar su identidad antes de iniciar el cambio.

Si un miembro del personal que renuncia o fuere notificado y fuere responsable de la gestión de un sistema, el jefe inmediato de dicha persona asegurará, de acuerdo con el riesgo, se cambien o desactiven los usuarios y contraseñas de forma inmediata.

La Dirección de Tecnologías de la Información gestionará la actualización de las contraseñas en los casos en que se utilicen cuentas de usuario y contraseñas en aplicaciones de terceros (proveedores) mediante Internet.

La entrega de contraseñas al usuario, tanto cuando se crea una cuenta o cuando el administrador restablece la contraseña, requiere atención para asegurar que la entrega se realice en forma eficaz y dentro de las normas de seguridad. No se deben transmitir las contraseñas por medio de ninguna red de voz, video o datos de la SECOM sin la identificación y autenticación adecuada.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

No se debe entregar la identificación del usuario y la contraseña asociada por el mismo medio en forma simultánea (es decir, si se le entregara la identificación del usuario por un medio, la contraseña se debe entregar por un medio distinto o en un momento diferente).

Se debe entregar la contraseña de manera que requiera que el destinatario pruebe su identidad antes de recibirla con las siguientes opciones:

- Persona a persona
- Presentación de la tarjeta de identificación de la Institución

Accesos y Control de Servicios de Red

El acceso a la infraestructura tecnológica es restringido.

Los servidores deberán encontrase en una red protegida y diferenciada de la red de usuarios.

Las contraseñas de administración de los equipos únicamente serán manejadas por los funcionarios de Infraestructura.

Las contraseñas de accesos a los servidores serán ubicadas en un archivo cifrado de una carpeta compartida a la cual únicamente tendrán acceso los usuarios de Infraestructura.

Existirán jerarquías de administración dentro de la infraestructura.

En caso de desvinculación de un miembro del área de Infraestructura, se deberá efectuar un cambio de contraseñas de administración de los servicios.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Todas las modificaciones en los accesos deben ser debidamente documentadas.

Ningún proveedor de servicios podrá conocer los accesos de los servidores, y en caso de ser necesario se deberá suscribir un acuerdo de confidencialidad de la información.

Sobre las redes

Las redes tienen como propósito principal servir en la transformación e intercambio de información dentro de la SECOM entre usuarios, direcciones, oficinas y hacia afuera a través de conexiones con internet.

La Dirección de Tecnología no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que lo genere o solicite.

Para prevenir el uso indebido de contraseñas, el usuario deberá solicitarlas únicamente a la Dirección de Tecnologías de la Información y Comunicación. Está prohibido compartir o revelar las contraseñas de las redes inalámbricas a otros usuarios.

La Dirección de Tecnologías se reserva el derecho de restringir y negar servicios de red (sin previo aviso) a equipos en los que se detecte algún abuso que pueda afectar el buen funcionamiento de la red, por ejemplo: que utilicen programas que puedan generar tráfico o puedan provocar interrupciones en el servicio.

Se restringirá el acceso a la red a aquellos usuarios que intenten violar la seguridad de cualquier equipo computacional o de red.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.

Los derechos especiales de acceso como la capacidad de escribir sobre archivos de otros usuarios se asignarán a quienes ejerzan como administradores de los sistemas.

No se permite el uso de los servicios de la red cuando no cumplan con las labores propias de la empresa.

La Dirección de Tecnología se reserva el derecho de limitar los anchos de banda de cada conexión según sea necesario, para asegurar la confiabilidad y desempeño de la red y de esta manera garantizar que la red sea compartida de una manera equitativa por todos los usuarios de la SECOM.

Es responsabilidad del usuario hacer uso adecuado de los puntos de red de las instalaciones de la SECOM, así como también de los dispositivos de red a los que tengan acceso físicamente como: Access Point, Switch no administrable, entre otros.

Está prohibido extender el alcance de la red por medio de cualquier dispositivo físico o lógico sin autorización de la Dirección de Tecnologías de la Información y Comunicación.

Los usuarios que accedan el Internet lo harán bajo su propio riesgo y responsabilidad, y la Institución no es, de ningún modo, responsable por los actos de los usuarios respecto al Internet. Para disminuir esos riesgos, el uso del Internet está gobernado por las siguientes:

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Los usuarios autorizan expresamente a la SECOM a través de los diferentes departamentos, áreas y autoridades el derecho de controlar, restringir, observar y eliminar, sin limitaciones, todo correo que entra y sale por el Internet, su contenido, sus destinatarios y sus remitentes. De igual modo puede hacer lo mismo con los sitios WEB visitados, grupos de noticias, archivos extraídos y todo tipo de comunicación enviada y/o recibida.

Los usuarios no deben emplear la conexión con Internet para extraer programas de ningún tipo. Cualquier programa que sea requerido y justificado, deberá solicitarse a la Dirección de Tecnologías de la Información, quien evaluará la conveniencia de efectuar la extracción (descarga o compra) e instalación del mismo.

La Institución se reserva el derecho de emplear software que anote en bitácoras toda la actividad realizada por los usuarios, permitiendo también bloquear el acceso a sitios que la SECOM considere impropios o inconvenientes para sus intereses.

Se recomienda especialmente no descargar de Internet programas ejecutables y material protegido por patentes, derechos de autor, marcas registradas y derechos de propiedad intelectual que no sean propiedad de la SECOM .

Se solicita a los usuarios que respeten la privacidad de todos los individuos y las organizaciones que utilizan Internet.

Los privilegios de uso de internet estarán limitados por la necesidad de acceso que requiera el desarrollo de la función de cada usuario.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Los cambios de privilegios de acceso se presentarán por medio de la firma de la solicitud en la cual se detallen los permisos requeridos, con la respectiva aprobación del jefe del área a la que pertenezca el usuario.

Se podrán otorgar derechos de acceso a personas ajenas a la SECOM, siempre y cuando la solicitud haya sido aprobada por el director en la que trabajarán y notificada a la Dirección de Tecnologías de la Información y Comunicación

Es obligación de cada jefe reportar de inmediato a la Dirección de Tecnologías de la Información y Comunicación los cambios de personal que puedan afectar el uso del sistema, como traslados, retiros, suspensiones, vacaciones o permisos.

Entre las medidas de seguridad implementadas se encuentran restringidas algunas palabras y sitios de internet; por lo que pueden existir palabras o sitios que a pesar de ser inofensivos tendrán negado el acceso, en este caso los usuarios podrán notificar esta eventualidad al correo soporte@secom.gob.ec para que sea resuelta a la brevedad posible.

Debe entenderse que Internet es una herramienta estrictamente de trabajo y no debe usarse con otros fines ajenos a las funciones del usuario. La navegación por Internet institucional será regulada por la Dirección de Tecnologías de la Información y Comunicación que con el fin de controlar el buen uso de los recursos ha establecido perfiles de navegación:

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Perfil de Navegación	Contenido bloqueado
Autoridades	Pornografía Sitios Peligrosos
Redes Sociales, Youtube	Redes sociales Youtube Pornografía Sitios Peligrosos
Bloqueo celulares Invitados	Redes sociales Youtube Descargas Stream video / Stream audio Pornografía Whastapp Sitios Peligrosos
Bloqueo Stream	Stream Audio / Stream Video Sitios Peligrosos Pornografía

c. **Políticas de Uso de Correo Electrónico**

El correo electrónico institucional es un medio de comunicación proporcionado a los funcionarios de la Secretaria Nacional de Comunicación, en apoyo a sus funciones.

La cuenta de correo electrónico institucional (ej. nombre.apellido@secom.gob.ec) permite el envío y la recepción de mensajes y está asociada a esta dirección única, para acceder a una cuenta de correo se requiere esa dirección única y una contraseña, las cuales estarán disponibles a través de la herramienta Microsoft Outlook o el navegador web por medio de OWA.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

La cuenta del correo electrónico individual será intransferible, con acceso exclusivo y personal del servidor público, además podrán generarse cuentas para uso especial, atendiendo a las necesidades de cada una de las unidades administrativas.

Para el uso de correo electrónico inicialmente, las listas de distribución públicas serán creadas únicamente por la dirección de TICS, conforme al estatuto orgánico y a los requerimientos de cada una de las unidades que conforman la secretaria, en caso de necesitar la creación o modificación de una lista de distribución enviar un mail a soporte@secom.gob.ec o mediante la mesa de ayuda (helpdesk) con dichos requerimientos, cabe recalcar que para dicho proceso es necesario que el solicitante sea el director/coordinador/subsecretario del área en el que se desea crear la lista de distribución o usuario especial.

Cuando se instale la cuenta en la computadora personal del usuario se requerirá que cambie la clave de acceso, con lo que se brinda la seguridad para que solo el titular de la cuenta de correo la conozca.

Queda prohibido el intercambio de archivos, tanto de datos, imágenes o videos con contenido pornográfico, sádico, propagandístico, o cualquier otro archivo de este tipo, con contenidos ajenos a las funciones que desempeñan los funcionarios de la Secretaria Nacional de Comunicación.

Se prohíbe el uso del correo electrónico con fines de propaganda, manifestaciones u opiniones políticas, partidistas o electorales.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Los envíos de mensajes masivos por correo electrónico solo podrán contener información de interés general para los funcionarios de la Secretaria Nacional de Comunicación y este tipo de correos solo podrá ser enviado por Directores, Coordinadores, Subsecretarios o Secretaria Nacional.

Se prohíbe la distribución masiva de grandes cantidades de mensajes sean o no de contenido Institucional a direcciones externas a la misma, también se prohíbe la distribución general de mensajes a todos los funcionarios de la SECOM con archivos adjuntos donde su peso exceda los 25 MB incluida la cabecera del mensaje.

Las cuentas de correo electrónico, de manera excepcional, serán susceptibles de revisión por parte del titular de la unidad administrativa, siempre que exista causa justificada.

Los Subsecretarios, Coordinadores y Directores son responsables del uso que su personal le da al correo electrónico.

d. **Políticas de uso de colaboración unificada**

La Dirección de Tecnologías Información y Comunicación se encargará de entregar una clave personal a cada uno de los funcionarios autorizados de la Secretaria Nacional de Comunicación para poder hacer uso del servicio de telefonía a celulares.

Los usuarios previos al número telefónico o extensión de destino deberán digitar su clave para poder mantener un registro del uso correcto de esta herramienta de comunicación.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Está prohibido realizar llamadas telefónicas a destinos altamente costosos tal es el caso de líneas con contenido adulto.

La Dirección de Tecnologías Información y Comunicación igualmente restringirá el acceso a llamadas internacionales y telefonía celular a todos los funcionarios, y solo se habilitarán a las solicitudes expresas de las Coordinaciones, Subsecretarias y Secretaria Nacional con sus respectivas justificaciones.

El acuerdo No.28 del 31 de marzo del 2016, establece las directrices mediante el reglamento interno para el uso, administración y control del servicio de telefonía móvil celular, bases celulares fijas y telefonía IP

e. **Políticas de respaldos y restauraciones**

La Dirección de Tecnologías de la Información y Comunicación, es responsable de la programación, ejecución y control de la obtención de los archivos de respaldo y su correspondiente restauración de ser necesario.

Todos los soportes físicos de las copias de respaldo serán almacenados en armarios ignífugos de acceso restringido o guardados en un lugar externo, como parte de la plataforma tecnológica segura.

El DTIC es el responsable de los accesos a la infraestructura donde se ubicarán las unidades de respaldo.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Los usuarios, son responsables de replicar la información más relevante en la unidad de red identificada con el nombre que la DTIC disponga. El mismo que será utilizado como único medio de respaldo.

Los usuarios, son responsables de mantener en la unidad de red asignada, únicamente información relacionada con el giro de negocio.

Todos los aplicativos o programas desarrollados por la DTIC como: Base de Datos, Correo electrónico, repositorio de usuarios, deberán contar con copias de respaldo.

Las copias de respaldo deben almacenarse en lugares seguros y estar disponible para casos de contingencia.

La retención de las copias de respaldo debe satisfacer las necesidades de recuperación.

La DTIC en coordinación con los usuarios, deberá revisar al menos una vez al año las necesidades de recuperación.

Periodicidad y copia de seguridad

Se deberá obtener el respaldo de la información de acuerdo con la frecuencia indicada por la Dirección de Archivo y Gestión Documental y deberá ser archivada por el período que determine la Contraloría General del Estado.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Se deberá efectuar un respaldo de datos de los equipos centrales de procesamiento en forma diaria.

Semanalmente, se deberá efectuar un respaldo de sistemas de todos los equipos centrales de procesamiento.

Para el transporte de los soportes físicos a un sitio externo deben utilizarse mecanismos de inviolabilidad y en caso de que sea un proveedor quien lo efectúe, deberá firmarse el respectivo compromiso de confidencialidad.

Soportes físicos

Se deberá analizar y definir los soportes magnéticos más adecuados sobre los que se efectuarán las copias de respaldo, como ser unidades ópticas, discos ópticos, cintas y/o similares.

El administrador de la infraestructura es responsable de mantener disponibles los dispositivos adecuados para realizar la recuperación de la información almacenada en los diferentes medios magnéticos (ver copias históricas), o en su defecto hacer una conversión de las copias históricas a los dispositivos disponibles.

Las copias de respaldo deben conservarse de acuerdo a las pautas básicas establecidas por el fabricante.

Depuración de datos

Los Dueños de la información son responsables de autorizar cualquier depuración y/o restauración de información a los equipos de procesamiento.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Para situaciones de emergencia en las que disminuya el desempeño del equipo y/o se llegue al límite del espacio en discos, la DTIC, podrá efectuar copias de respaldo y eliminar la información en línea, notificando luego a los Dueños de Datos / Delegados de lo ocurrido.

Pruebas periódicas

Se deben realizar pruebas de recuperación desde los soportes físicos para verificar la correcta recuperación de la información, con frecuencia semestral. Los resultados de estas pruebas deben quedar correctamente documentados y disponibles.

Tolerancia a fallas menores

Se deben implementar, dentro de las posibilidades, mecanismos automáticos del tipo de tolerancia a fallas, tales como otros equipos alternativos, espejado de discos, unidades redundantes y/o similares.

Inventario de los soportes físicos

Se debe llevar en forma permanente un inventario de los soportes existentes, su contenido y el lugar donde están almacenados.

Situaciones de emergencia

La DTIC es responsable de definir las acciones a desarrollar cuando ocurrieran distintos episodios que provoquen la interrupción del normal procesamiento de los sistemas.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Dichas acciones a contemplar deben ser desde interrupciones habituales en el uso de la tecnología hasta desastres de mayor magnitud que impliquen la inoperatividad del data center.

Estos procedimientos de contingencias deben estar alineados con los respectivos planes de recuperación del negocio de la SECOM.

Para la administración de las copias de respaldo se aplicarán las fases:

- Planeación: Garantizar la realización de respaldo
- Hacer: Desarrollar cada una de las actividades contempladas en el procedimiento de Backup. Realizar recuperación de información cuando sea necesario.
- Verificar: Registrar en la bitácora de control de respaldos
- Actuar: Hacer seguimiento al proceso de respaldos.

Procedimiento de respaldos y restauraciones

Nro.	**Actividad**	**Descripción de la actividad**	**Responsable**	**Documento o Registro**
0	Inicio	Inicio del procedimiento		
1	Determinar proceso de respaldos	Se determinan e identifican los archivos a respaldar en los equipos en diferentes áreas.	Funcionarios de la DTIC	
2	Identificar aplicativos y/o Bases de datos	Se Identifica el número de aplicativos y/o bases de datos para respaldo		Inventario de Aplicativos.
3	Determinar mecanismos	Se determinan los mecanismos de copias de respaldo según la base de datos a respaldar en forma manual o automática		Bitácora de respaldos

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Nro.	Actividad	Descripción de la actividad	Responsable	Documento o Registro
4	Verificar Archivos	Se verifican los archivos log del Aplicativo utilizado para la copia de seguridad		
5	Verificar copias de restauración	Se verifican las copas para la restauración cuando se necesiten por cualquier usuario en la entidad.		
6	Realizar copias por segunda vez	Si el archivo log del servidor indica un error, se realiza copia por segunda vez		
7	Grabar Copias	Se graba de manera diaria, semanal, mensual y anualmente de acuerdo con el procedimiento de respaldo, en un repositorio o dispositivo de almacenamiento (servidor o disco externo) todas las copias a guardar en la DTIC.		
8	Almacenar copia	Se almacena la copia y para el caso de ser un medio magnético se marca con la respectiva fecha, usuario, nombre del equipo y/o aplicativo.		Formato de Backup.
9	FIN	Fin del procedimiento		

Procedimiento de restauración

Nro.	Actividad	Descripción de la actividad	Responsable	Documento o Registro
0	Inicio	Inicio del procedimiento		
1	Determinar Aplicativo y/o Base de Datos.	Se determina o identifica el número de Aplicativos y/o	Funcionarios de la DTIC	

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Nro.	Actividad	Descripción de la actividad	Responsable	Documento o Registro
		bases de datos para la restauración		
2	Realizar restauración	Se realiza la restauración de los archivos correspondiente en el equipo del usuario. Se es una base de datos, se determina la hora para la respectiva restauración y se informa a los usuarios para suspender el aplicativo mientras se realiza la respectiva restauración.		
3	Registrar Restauración	Se registra la restauración realizada, si es una bases de datos se guarda en registro o bitácora del mismo	Funcionarios de la Dirección de Tecnologías de la Información	Bitácora de respaldo
4	Fin	Fin del procedimiento		

Se adjunta a este procedimiento el formato de la bitácora de respaldo

f. **Políticas de Monitoreo y revisión de los servicios por terceros**

La DTIC suscribirá Acuerdos de Niveles de Servicio (SLA's) por cada contrato de servicios a suscribir

Los administradores de los contratos serán los responsables de hacer cumplir los SLA's que se adhieran como parte integrante del contrato.

Los SLA's en su cuerpo deberán contener como mínimo lo siguiente:

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

- Definiciones y objetivos
- Relación entre la empresa y la SECOM.
- Condiciones del servicio
- Niveles de servicio
- Personal de escalamiento
- Compromiso de seguridad
- Nota de confidencialidad
- Firmas de los administradores del contrato

Para el efecto se adjunta un modelo de Acuerdo de Niveles de Servicio.

g. **Políticas de gestión de capacidad**

La DTIC será la responsable de realizar proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos, para ello deberá monitorear y utilizar la información del monitoreo para la adquisición y asignación de recursos.

h. **Políticas contra código malicioso**

Antivirus

La DTIC administrará desde una consola de antivirus las protecciones contra código malicioso.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Todos los activos tecnológicos que procesan información de la SECOM o tienen acceso a los recursos de red; deberán tener instalado un software de antivirus comercial configurado apropiadamente y en funcionamiento en todo momento (es decir, nunca inhabilitarlo durante la operación normal)

Los recursos informáticos y de red de la SECOM estarán protegidos de códigos de software malintencionados y virus. Se aplica a todos los sistemas de equipos que accedan a información de la SECOM o la procesen. Todos los sistemas propiedad de la SECOM utilizarán el software aprobado.

La DTIC controlará a través de una política de antivirus o del directorio activo la eliminación automática de todo software que no se encuentre inventariado en la SECOM.

Para el caso de servidores, estos deberán contar con todos los parches actualizados y con el antivirus cuya política sea exclusiva para este tipo de equipamiento.

El control, el análisis y la protección, y la cuarentena o confiscación de cualquier dispositivo informático debe respetar los derechos de privacidad de los usuarios y cumplir con todas las leyes aplicables.

La SECOM se reserva el derecho de analizar los recursos informáticos y de red en caso de actividad de virus en cualquier momento, y controlar o proteger ejemplos de contenido que

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

incluyen la actividad y el tráfico que se originan en forma remota. Los motivos para dicho control o protección incluyen el mantenimiento del sistema, la detección y eliminación de contaminación, la detección y prevención de declaraciones no autorizadas de información comercial fundamental de la SECOM , la detección de acceso no autorizado a recursos informáticos y de red, y la determinación del cumplimiento de las s de la SECOM , pero no se limitan sólo a esos casos.

El usuario autoriza a la SECOM el derecho de cuarentena o confiscación de cualquier recurso informático o de red que pudieran presentar una amenaza, como información, mensajes y tráfico de redes, etc. En caso de que el control, la protección o la cuarentena revelaran una posible evidencia de actividad criminal, se tomarán las acciones adecuadas, las cuales pueden incluir suministrar pruebas del control, el análisis o la protección a las autoridades.

El usuario autoriza a lasco el derecho de desconectar en forma inmediata de la red, sin previa notificación, cualquier dispositivo inadecuado protegido por software de antivirus aprobado o aceptado.

Cuando se deba utilizar un sistema operativo para el cual no existe software de antivirus, la DTIC deber implementar otras medidas en la ausencia de dicho software de antivirus para reducir la posibilidad de infección de virus, de otra manera, el dispositivo deberá ser aislado de la red.

El software de antivirus debe estar configurado para limpiar de manera automática el archivo infectado (es decir, quitar el virus), poner en cuarentena o denegar el acceso al archivo infectado si no es posible limpiarlo de manera automática.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Se contemplará en el software base de la Institución, el antivirus

Todos los equipos pertenecientes a la SECOM, deben tener instalado y debidamente actualizado el antivirus institucional.

Cualquier proceso interno de asignación debe incluir la asignación de un antivirus

La desinstalación o suspensión del antivirus se encuentra restringida para el manejo exclusivo del equipo de TIC's de la SECOM.

Utilizando la consola de administración del antivirus se implementan las siguientes políticas:

Antivirus Seleccionado	Sistema operativo WINDOWS	Sistema operativo MAC	Servidores
Administración centralizada	X	X	X
Antimalware	X		X
Firewall	X	X	X
Seguridad de servidor de archivos			X
Controles para endpoints	X	X	X
Cifrado	X		X
Administración de sistemas	X	X	X
Generación de reportes	X	X	X

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Seguridad Perimetral

La Secretaria Nacional de Comunicación cuenta con un dispositivo de seguridad perimetral, el cual sirve de protección a la red, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

El equipo está cubierto con un sistema de alta disponibilidad que permite la continuidad de los servicios en caso de fallo.

La Dirección de Tecnologías a través de este dispositivo será la encargada de:

Controlar puertos y conexiones, ya sean de clientes o servidores.

Establecer las reglas necesarias en el firewall para bloquear, permitir o ignorar el flujo de datos entrante y saliente de la red.

Automatizar tareas como la actualización de reglas, la obtención y análisis de logs, la configuración de cortafuegos.

Monitorear y analizar las actividades de los usuarios en busca de elementos anómalos.

Habilitar a los usuarios remotos de la institución el acceso a la red interna de SECOM mediante el uso de redes privadas VPN[5] SSL[6].

[5] Virtual Private Network
[6] Secure Socket Layer

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Configurar el software necesario y asignar las claves a los usuarios que soliciten la activación de la VPN.

i. **Política sobre los reportes de incidentes de seguridad**

Los usuarios deben notificar a la Dirección de Tecnologías de la Información cuando se sospecha o detecta un virus en el equipo.

En equipos donde el software admita la alerta de virus, todas las detecciones de virus deben ser informadas de manera automática e inmediata al administrador de la red de la SECOM y al usuario en forma directa del dispositivo infectado.

Luego de toda alerta de virus, el personal calificado de la Dirección de Tecnologías de la Información debe realizar un análisis completo e inmediato de los dispositivos afectados. Las "alertas de virus" incluyen llamadas de usuarios debido a problemas de un posible virus o la clasificación indica que se garantiza una "alerta de virus", control de redes, informes de pruebas de comportamiento de virus (Por ejemplo: barrido de redes, uso sospechoso/irregular de puertos, etc.) y advertencias automáticas del software de antivirus para alertar al personal de detección de virus, pero no se limitan sólo a estos casos.

El administrador de la red debe realizar un informe mensual en donde se documente el número y las clases de incidentes de infecciones de virus.

j. **Política sobre sistemas de información del negocio**

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

El software utilizado por la Secretaría Nacional de Comunicación, que haya sido desarrollado o adquirido, estará regulado por las normas y reglamentos vigentes, dando cumplimiento a lo dispuesto por el Decreto Ejecutivo No. 1014 de 10 de abril de 2008, publicado en el Registro Oficial No. 322 de 23 de abril del mismo año sobre el uso del software libre en las Entidades de la Administración Pública Central.

Los usuarios y los administradores son responsables de todo software utilizado en las máquinas. Se les prohíbe a los usuarios instalar software no autorizado en equipos de la SECOM .

Se prohíbe a los usuarios la utilización de software que ha sido descargado desde Internet o desde otra red que no pertenece a SECOM. Sin embargo, si se requiere dicho software para fines institucionales, los usuarios son responsables de usarlo según instrucciones de la Institución y de obtener la aprobación administrativa de la necesidad.

La DTIC aplicará el marco de desarrollo ágil SCRUM para implementarlo en todos los sistemas a desarrollar, de manera que se mejore notablemente la calidad y el tiempo de desarrollo de los sistemas.

La Dirección de Tecnologías de la Información es el único autorizado para instalar software. Si un usuario detecta algo anormal dentro de su computador, tiene la obligación de notificarlo en forma inmediata al Soporte Técnico.

Los funcionarios de la Dirección de Tecnologías de la Información tienen el derecho de auditar el contenido de una computadora en cualquier momento. Esta auditoría, de resultar satisfactoria,

deberá ser recibida conforme por el usuario quien, a partir de ese momento, se convierte en el único responsable por el software y datos que haya en la computadora. Para determinar qué software debe estar o no en su computadora, el usuario puede consultar a la Dirección de Tecnologías de la Información.

Cada computadora nueva tendrá una certificación de la Dirección de Tecnologías de la Información de que cuenta sólo con el software autorizado y correcto, pudiendo ser verificado por el usuario quien, a partir de ese momento, será el único responsable del contenido de su computadora.

Ningún usuario está autorizado a comprar software sin seguir el procedimiento de compras de la institución definido en el Instructivo Interno de Contratación Pública.

Bajo ninguna circunstancia podrá residir en una computadora ninguna pieza de software o hardware que no tenga la respectiva licencia de uso o prueba de compra.

Los usuarios no pueden copiar material protegido bajo las leyes de protección de derechos de autores ni facilitar a otros el hacer esas copias.

Mantenimiento de Aplicaciones

Se realizará un análisis de las aplicaciones vigentes y se ordenarán en base a prioridad para realizar el mantenimiento, así como también la elaboración puesta en marcha de planes de mejora de las mismas.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Transaccionalidad de los sistemas

En el desarrollo de los sistemas se tomará en cuenta la transaccionalidad y la integridad referencial de manera que no exista pérdida de información y ésta sea confiable.

k. **Política de control de calidad**

Se implementará una fase de control de calidad de software en la cual deberán realizarse pruebas de rendimiento, seguridad y robustez de las aplicaciones desarrolladas.

Los sistemas de comunicación, incluyendo la red de datos, las computadoras, el correo electrónico, archivos y bibliotecas residentes en computadoras, la navegación por el Internet y los sistemas de telefonía empleados en la SECOM, son propiedad o derechos de la Institución, y sólo pueden ser usados para fines de negocio o asuntos de interés de la SECOM.

La SECOM provee un sistema regulado de electricidad que es exclusivo para el uso de los sistemas electrónicos, el personal no podrá hacer uso de este servicio para conectar ningún artefacto eléctrico que no haya sido aprobado por Dirección de Tecnologías de la Información como, por ejemplo: cafeteras, impresoras, equipos de audio y/o video, etc.

l. **Política para el manejo de la información**

Aunque se suministren códigos de seguridad a los empleados y su uso es requerido para el acceso a las distintas plataformas y sistemas, la Institución mantiene su derecho de revisar los sistemas, y

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

para la Institución, los usuarios no pueden asumir que los mensajes e información dentro de los sistemas son personales y de su propiedad.

El intento de los usuarios por proteger esa información, aunque sea creada, almacenada, enviada o recibida por ellos, no genera el derecho de privacidad o pertenencia. Una vez que la información entre a los sistemas de la SECOM , ésta puede ser extraída o restaurada por un funcionario autorizado usando cualquiera de los diferentes mecanismos con que cuenta la Institución, si el caso lo requiere.

Bajo ninguna circunstancia, los usuarios pueden usar los sistemas de comunicación de la Institución para transmitir material ofensivo o ajeno a la razón de ser de la misma. Cualquier material de este tipo puede ser interpretado como acoso, y puede inducir a la creación de un ambiente de trabajo hostil o puede constituirse en discriminación sexual, religiosa, de género, racial o étnica o crear una tendencia. Más aún, los sistemas de la Institución no pueden ser usados para transmitir este tipo de información a entidades o personas ajenas al SECOM, salvo autorización expresa. La transmisión no autorizada de información de la SECOM puede ser interpretado como facilitación ilegal o actividad inmoral o no ética.

La SECOM tiene el derecho de, en cualquier momento, remover de cualquier sistema propiedad de la SECOM , todo tipo de información que considere no es de interés de la Institución.

Es responsabilidad de los usuarios el mantener la confidencialidad y secreto de los códigos de seguridad que se le asignen para el desempeño de sus funciones.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

m. **Política para intercambio de información**

A pesar de que los programas de software de mensajería instantánea e intercambio de archivos pueden mejorar la productividad, presentan vulnerabilidades especiales que pueden aumentar significativamente el riesgo para los activos de información de la SECOM . Debido a que esta tecnología dificulta la eliminación de virus y otra clase de códigos malintencionados, y conscientes de que esto permite la introducción de canales de apoyo que pueden sortear las medidas de seguridad, abre nuevas vías para el ataque de redes, aplicaciones y recursos de información comercial fundamental. Por lo tanto, la instalación, la configuración y el uso de estos sistemas requieren atención especial de la Dirección de Tecnologías de la Información.

Consideraciones de privacidad

El usuario autoriza al SECOM el derecho de controlar el contenido y tráfico y de proteger los recursos informáticos y de red para todas las actividades que utilicen la mensajería electrónica o los recursos informáticos y de red de la SECOM. El propósito de este control o esta protección incluye la determinación de cumplimiento de todas las s institucionales. Dicho control o dicha protección respetará los derechos de privacidad de los usuarios, y también el cumplimiento de las leyes nacionales.

Todos los sistemas o las aplicaciones que procesan o almacenan información fundamental de la SECOM deberán cumplir los requisitos de seguridad de información en todas las fases del ciclo de desarrollo.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Esta normativa se aplica a sistemas y aplicaciones sin importar dónde o por quién son desarrollados o implementados.

En la memoria técnica de los sistemas y aplicaciones se determinará si aplica o no la vida útil y el tiempo respectivo.

n. **Políticas para Análisis y especificaciones de los requisitos de seguridad**

Se deberá determinar, previo al desarrollo de los requisitos y especificaciones de seguridad, el propietario de la información y la valoración de la información almacenada, procesada y comunicada por el sistema.

Se deberá realizar un análisis y una especificación exhaustiva de los requisitos de seguridad en todos los sistemas y todas las aplicaciones nuevas o las actualizaciones importantes de sistemas existentes.

El análisis deberá identificar todos los requisitos válidos en seguridad y áreas relacionadas con la seguridad, como:

Los requisitos y las especificaciones de seguridad de los sistemas o las aplicaciones deben cumplir con las normas o mejores prácticas de configuración de tecnologías y sistemas.

Los requisitos y las especificaciones de seguridad de los sistemas o las aplicaciones deben exigir la interoperabilidad con todas las fuentes y servicios de información con los que debe interactuar.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Los requisitos y las especificaciones de seguridad de los sistemas o las aplicaciones deben asegurar la integración con los servicios de seguridad existentes, cuando sea apropiado.

Se deberán realizar evaluaciones adicionales de seguridad ante cualquier cambio del sistema o la aplicación.

- Confidencialidad
- Autenticación
- Autorización
- Gestión

Verificación de seguridad

Todos los sistemas o todas las aplicaciones nuevas o existentes deben ser probadas en un ambiente separado para comprobar su estabilidad e identificar cualquier interacción imprevista con los sistemas existentes, antes de ser introducidos en el ambiente de producción u operaciones.

Se deberán probar la integridad de la seguridad y la verificación operativa de todos los sistemas o todas las aplicaciones nuevas, de acuerdo con los requisitos y las especificaciones, con anterioridad a la disponibilidad general.

Desarrollo y prueba

Los servidores o ambientes en los cuales se desarrollan los sistemas o las aplicaciones no serán utilizados para actividades de pruebas o producción.

Durante las pruebas de aceptación y las pruebas operativas formales, se deberán utilizar todas las características y funciones de seguridad.

POLÍTICA DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA
Versión: 1.0

Antes de lanzar un nuevo sistema o realizar una actualización de un sistema existente de uso general, se realizarán pruebas para asegurar que el nuevo sistema o la nueva aplicación no afecten negativamente a los sistemas existentes.

Los sistemas o las aplicaciones nuevas (o las actualizaciones grandes de los existentes) serán aprobadas para su uso en la Institución por la Dirección de Tecnologías de la Información.

Ejecución

Los sistemas y las aplicaciones de producción u operación serán ejecutados y administrados de acuerdo con las mejores prácticas para la protección de los activos de información de la SECOM.

Continuidad del servicio

Se deberá diseñar un plan de Contingencia para recuperar los servicios existentes en caso de que la introducción de un sistema nuevo o evento causara la interrupción o degradación del servicio.

Se deberá diseñar un plan de contingencia específico antes del lanzamiento de un nuevo sistema para asegurar la continuidad del servicio. Este plan será adicional a la memoria técnica del sistema.

MODELO DE ACUERDO DE NIVEL DE SERVICIO (SLA)

PROVEEDOR. - CLIENTE

Modelo de Acuerdo de Nivel de Servicio

CONTENIDO

Modelo de Acuerdo de Nivel de Servicio

Acuerdo de Niveles de Servicio[7]

1.1. Definiciones y Objetivos

El presente acuerdo tiene como finalidad:

- Definir el Acuerdo de Niveles de Servicio (SLA) "Service Level Agreement" entre el CLIENTE y PROVEEDOR, el cual describe los objetivos de desempeño y disponibilidad.
- Proporcionar una mayor visibilidad y conocimiento de los **Servicios ABC** que demanda el CLIENTE para su negocio.
- Conocer los alcances, limitaciones y responsabilidades tanto del CLIENTE, como de PROVEEDOR

Los objetivos de desempeño y disponibilidad serán los parámetros medibles de la relación CLIENTE - PROVEEDOR, y podrán estar sujetos a revisiones continuas.

1.2. Relación CLIENTE – PROVEEDOR

El SLA descrito en este documento establece un acuerdo entre el CLIENTE y PROVEEDOR, a través de la provisión de canales para el Servicio de Internet y/o enlaces de datos y cuyo sistema servirá para la implementación de los servicios contratados para uso exclusivo del CLIENTE.

1.3. Grupos de Trabajo

Cada una de las partes establecerá un Grupo de Trabajo, cuyas tareas serán:

1.3.1. Implementar la solución demandada, lo cual comprende:

- Instalar y configurar el equipamiento para los enlaces contratados.
- Activar los enlaces contratados, utilizando la tecnología que mejor relación costo-beneficio ofrezca para cada localidad en particular.

[7] Referencia del SLA tomado de la Corporación Nacional de Telecomunicaciones CNT E.P.

1.3.2. Administrar la solución, lo cual comprende:

- Cuidar de que los enlaces contratados y equipos de comunicación se hallen trabajando dentro de los parámetros y rangos de utilización apropiados para garantizar el servicio.
- Planificar cambios y crecimientos, de tal forma que cualquier variación a una topología no implique degradación del servicio a los usuarios de la red, no afecte a otras áreas de la red y no genere costos indirectos en otras plataformas tecnológicas.
- Ofrecer soluciones alternas y/o de contingencia, para superar problemas en el o los enlaces contratados o equipos de comunicación.
- Realizar el mantenimiento preventivo y correctivo, tanto de los enlaces contratados, como del equipamiento de comunicación.

1.4. Condiciones de Servicio

Se define como **servicio** a la solución informática o de telecomunicaciones que el cliente contrate a PROVEEDOR y que se encuentra dentro de las órdenes de servicio anexas al contrato, las cuales pueden abarcar, entre otros, servicios de datos, Internet, telefonía, data center.

Las Condiciones de Servicio que se aplican a los servicios contratados se indican en la siguiente tabla:

Id	Denominación	Condiciones de Servicio
1.4.1	**TIEMPO DE INSTALACIÓN**	
1.4.2	Límites de Responsabilidad	
1.4.3	Interfaces	
1.4.4	Seguridad	
1.4.5	Confidencialidad	
1.4.6	Actualizaciones y Cambios	

Modelo de Acuerdo de Nivel de Servicio

Id	Denominación	Condiciones de Servicio
1.4.7	Desempeño de la Red	
1.4.8	Escalamiento de un problema	

1.5. Niveles de Servicio

PROVEEDOR deberá cumplir con los Niveles de Servicio detallados en la siguiente tabla.

Id	Denominación	Niveles de Servicio
1.5.1	Disponibilidad de servicio	Se entiende como "**disponibilidad**" al tiempo medido en horas, que el canal está en servicio, con los parámetros anotados en este numeral. La disponibilidad será medida mensualmente, considerando los valores de cada uno de los servicios de datos y/o Internet (considerando el enlace de backup en caso de tenerlo) contratados (SI SE DEBE RECALCAR QUE ES DE FORMA INDEPENDIENTE). Según el resultado de esta medida se definirá el Valor Mensual a Pagar, conforme a lo expresado en el numeral 1.5.5 de esta tabla. La disponibilidad (D) mínima mensual contratada es: XX % y XX % El valor de disponibilidad se calculará con la siguiente expresión: $$D = \left(1 - \frac{TI - TM}{TT}\right) * 100$$ Donde:

Modelo de Acuerdo de Nivel de Servicio

Id	Denominación	Niveles de Servicio
		D (%) = Disponibilidad mensual del enlace, expresado como un porcentaje. **TI** (horas) = Tiempo Indisponible, tiempo que el servicio estuvo indisponible o fuera de servicio en horas durante el mes. Este tiempo inicia desde el momento del reporte realizado por el cliente, y la recepción del Número de Caso **TT** (horas) = Tiempo Total, tiempo total de horas en un mes. Este valor es fijo, y dependiendo del mes, será igual a: • 672 horas (28 días). • 696 horas (29 días). • 720 horas (30 días). • 744 horas (31 días). **TM** (horas) = Tiempo de Mantenimiento, tiempo que el enlace estuvo fuera de servicio debido a mantenimientos preventivos planificados por la PROVEEDOR y previamente aceptados por el CLIENTE; o a cualquiera de los motivos considerados como caso fortuito o fuerza mayor siempre que tales eventos, según lo establecido en el artículo 30 del Código Civil Ecuatoriano, impidan que de forma continua las partes cumplan sus obligaciones contractuales, sin derecho a reclamo de indemnización alguna entre las partes, sin perjuicio de que, también se produzcan los eventos que se indican a continuación:" Desastres naturales, atentados, hurto, vandalismo, accidente, incendio, alteración del orden público, etc, que afecten las instalaciones, equipos y/o facilidades de PROVEEDOR
1.5.3	Horario de Soporte Técnico.	PROVEEDOR cuenta con un Centro de Servicio Técnico, en el cual se encuentre laborando el personal con la experiencia y el conocimiento necesario, de tal manera que puedan brindar el soporte apropiado al CLIENTE para superar cualquier inconveniente o problema en los canales. Este horario es de: **7x24x365**.

Modelo de Acuerdo de Nivel de Servicio

Id	Denominación	Niveles de Servicio
1.5.4	MTTR Y MTBF	PROVEEDOR ofrece un tiempo promedio de recuperación ante fallas del enlace (MTTR - mean time to recovery) del canal de datos de: X horas. Los tiempos indicados anteriormente se toman bajo las siguientes consideraciones: • Este tiempo inicia desde el momento del reporte realizado por el CLIENTE, y la recepción del Número de Caso (notar numeral 1.4.8 de este documento). • En este tiempo se contempla el período de diagnóstico y solución del problema. • No está considerado el tiempo de movilización, en caso de ser requerido (ver numeral 1.5.1) • Para asegurar los lapsos mencionados, PROVEEDOR indicará, en el momento del reporte, el personal que va a dar solución al problema, de tal manera que se generen los permisos apropiados para el acceso a las instalaciones del CLIENTE. PROVEEDOR ofrece un tiempo promedio entre fallas del enlace (MTBF - mean time between failure) de 120 días.
1.5.5	Valor a pagar	El valor mensual a pagar por el CLIENTE a PROVEEDOR por cada enlace se calculará basándose en la siguiente fórmula: VALOR A PAGAR = VALOR MENSUAL * FCS DESCUENTO: Si por causas atribuibles a PROVEEDOR y salvo caso fortuito o fuerza mayor, existiera una disponibilidad inferior a la ofertada en este SLA, PROVEEDOR se compromete a descontar del valor mensual contratado, por concepto de multa el valor a describirse a continuación:

Modelo de Acuerdo de Nivel de Servicio

<table>
<tr><th>Id</th><th>Denominación</th><th>Niveles de Servicio</th></tr>
<tr><td></td><td></td><td>
Para el XX%
<table>
<tr><th colspan="2">% DISPONIBILIDAD</th><th rowspan="2">Factor de Calidad del Servicio (FCS)</th></tr>
<tr><th>DESDE</th><th>HASTA</th></tr>
<tr><td>100.00</td><td>99.80</td><td>1.00</td></tr>
<tr><td>99.79</td><td>99.30</td><td>0.98</td></tr>
<tr><td>99.29</td><td>93.00</td><td>0.92</td></tr>
<tr><td>92.99</td><td>75.00</td><td>0.80</td></tr>
<tr><td>74.99</td><td>00.00</td><td>0.00</td></tr>
</table>
Para el XX%
<table>
<tr><th colspan="2">% DISPONIBILIDAD</th><th rowspan="2">Factor de Calidad del Servicio (FCS)</th></tr>
<tr><th>DESDE</th><th>HASTA</th></tr>
<tr><td>100.00</td><td>99.60</td><td>1.00</td></tr>
<tr><td>99.59</td><td>99.00</td><td>0.98</td></tr>
<tr><td>98.99</td><td>93.00</td><td>0.92</td></tr>
<tr><td>92.99</td><td>75.00</td><td>0.80</td></tr>
<tr><td>74.99</td><td>00.00</td><td>0.00</td></tr>
</table>
</td></tr>
</table>

Id	Denominación	Niveles de Servicio
		NOTA: En casos donde la contratación de servicios sea menor a un mes, se tomará como referencia para aplicación de multas el tiempo indisponible de la tabla.
1.5.6	Provisión de nuevos servicios	Para nuevos servicios o ampliaciones solicitados por el CLIENTE, PROVEEDOR deberá cumplir con los siguientes valores máximos: • Entrega de factibilidad y cotización: X días, a partir de la solicitud escrita (aplica el uso de correo electrónico) • Entrega de un nuevo enlace o servicio: de X a X (días laborables), a partir de la aceptación escrita de la cotización y dependiendo de la solución. Todos los servicios serán sujetos a disponibilidad y factibilidad técnica. • Una vez realizado una ampliación, los costos se reflejarán en la nueva facturación mensual.

1.6. Personal de Escalamiento

Los puntos de contacto entre el CLIENTE (o quien este defina) y PROVEEDOR se indican a continuación.

CLIENTE:

Nivel	Punto de Escalamiento	Región	Teléfono
Nivel 1			
Nivel 2			
Nivel N			

Modelo de Acuerdo de Nivel de Servicio

PROVEEDOR:

Nivel	Punto de Escalamiento	Región	Teléfono
Nivel 1			
Nivel 2			
Nivel N			

CLIENTE **PROVEEDOR**

1.7. SEGURIDAD: RESPONSABILIDAD DE PROVEEDOR Y DEL CLIENTE

Responsabilidades de PROVEEDOR:

PROVEEDOR no realizará ninguna actividad en contra de la seguridad de la red del cliente, así como los datos que en ella circulen,

Modelo de Acuerdo de Nivel de Servicio

Responsabilidades del cliente:

a) Uso ilegal:
Los servicios de PROVEEDOR no deben ser usados para fines ilegales o en soporte de actividades ilegales. PROVEEDOR se reserva el derecho a cooperar con las autoridades legales y/o terceras partes afectadas en la investigación de cualquier crimen o acción ilegal.

b) Perjuicio a menores de edad:
El uso de servicios de PROVEEDOR para perjudicar, o intentar perjudicar, a menores de edad de cualquier modo, incluyendo, pero no limitándose, a la pornografía infantil.

c) Amenazas:
El uso de servicios de PROVEEDOR para transmitir cualquier material (por e-mail, subida de archivos, alojamiento u otros) que amenace o aliente el daño físico o destrucción de la propiedad.

d) Hostigamiento:
El uso de servicios de PROVEEDOR para transmitir cualquier material (por e-mail, subida de archivos, alojamiento u otros) que hostigue a un tercero.

e) Actividad fraudulenta:
El uso de los servicios de PROVEEDOR para realizar ofrecimientos fraudulentos para vender o comprar productos, objetos o servicios, o para ejecutar cualquier tipo de estafa financiera.

f) Falsificación o imitación de persona:
Está prohibido agregar, remover o modificar información identificadora en la red, en un esfuerzo de engañar o confundir. Está prohibido el intentar reemplazar a otra persona utilizando su información identificadora. El uso de e-mails anónimos o de nicknames (apodos) no constituye imitación de persona.

g) E-mail comercial no solicitado / E-mail masivo no solicitado (SPAM):
El uso de servicios de PROVEEDOR para el envío de e-mails comerciales o masivos no solicitados está expresamente prohibido. Violaciones de este tipo resultarán en la finalización inmediata del servicio.

El CLIENTE que aloje sitios o servicios en nuestros servidores y que acepte personas que realizan envíos masivos (spammers) que provoquen que las IP's de PROVEEDOR estén listadas en cualquier base de datos de spam, será removido como cliente. El servicio no será reconectado hasta que el CLIENTE acuerde remover cualquier y todos los restos del material spam inmediatamente después de la reconexión y permita a la empresa el acceso a sus servicios para confirmar que el material ha sido completamente removido. De darse una segunda violación, resultará en la inmediata y permanente eliminación del servicio de nuestra red, sin previa notificación.

Modelo de Acuerdo de Nivel de Servicio

h) Bombardeo de E-mails y noticias:
Intentos malignos para impedir el uso a otra persona del servicio de correo electrónico o noticias, resultará en la inmediata remoción del servicio contratado.

i) Falsificación de E-mails y mensajes:
Falsificar cualquier mensaje, completa o parcialmente, de cualquier transmisión electrónica, originada o transitando a través de nuestros servicios es una violación de estas PUA.

j) **Accesos no autorizados:**
El uso de los servicios de PROVEEDOR para acceder, o intentar acceder, a las cuenta de otros, o penetrar, o intentar penetrar, medidas de seguridad de PROVEEDOR u otro software o hardware de otra entidad, sistemas de comunicaciones electrónicas o sistemas de telecomunicaciones, ya sea que la intrusión resulte o no en la corrupción o perdida de información, está expresamente prohibida y el servicio será inmediatamente cancelado.

k) Infracción en la marca registrada y derechos de autor:
El uso de los servicios de PROVEEDOR para transmitir cualquier material que viole derechos de autor, marca registrada, patentes, secreto comercial u otros derechos de propiedad de una tercera parte, incluyendo, pero no limitándose, a la copia no autorizada de material con derechos de autor, la digitalización y distribución de fotografías de revistas, libros u otras fuentes con derechos de autor, y la transmisión no autorizada de software con copyright.

l) Recolección de información personal:
El uso de los servicios de PROVEEDOR para obtener o intentar obtener información personal de terceras personas sin su conocimiento o consentimiento.

m) Discontinuidades en la red y actividad no amistosa:
El uso de los servicios de PROVEEDOR para cualquier actividad que afecte la habilidad de otras personas o sistemas para utilizar nuestros servicios o Internet. Esto incluye ataques de "denegación de servicios" (DOS – Denial of Service) contra otras redes de Hosting o usuarios particulares. La interferencia o interrupción de otras redes, servicios o equipamiento está terminantemente prohibida.

Es responsabilidad del cliente asegurarse que su sitio esté configurado de una forma segura. Un cliente no debe permitir que su sitio este configurado de tal forma que le permita a una tercera parte la posibilidad de usar su red para un fin ilegal o inapropiado. La entrada no autorizada y/o el uso del sistema de otra compañía o individuo, resultará en la inmediata finalización de la cuenta.

Modelo de Acuerdo de Nivel de Servicio

PROVEEDOR no tolerará que ningún cliente intente acceder a las cuentas de otros clientes, o penetrar medidas de seguridad de otros sistemas, ya sea que la intrusión resulte o no en la corrupción o perdida de información.

n) Fraude:
Implica una declaración conscientemente engañosa o tergiversada realizada con la intención que la persona que la reciba actúe conforme a ello.

o) Distribución de Virus:
La distribución intencional de software que intente o cause daños, hostigamiento o molestia a personas, información y/o sistemas de computación están prohibidos. Semejante agravio resultará en la finalización del servicio contratado.

p) Responsabilidad por terceras partes:
Los clientes de PROVEEDOR son responsables y deberán dar cuenta por las actividades de terceras partes, que utilicen sus servicios, y violen esta guía creada como políticas de uso aceptable.

Bitácora de Respaldo

	Dirección de Tecnologías de la Información y Comunicación	**Versión 01**
	Bitácora de Respaldos y Restauraciones	**Fecha de Emisión:**
		Página 1 de 1
		Ticket asociado:

Edificio:		**Ubicación:**	
Funcionaria (o) solicitante:	**Área:**		
Cargo:	**Nombre Equipo:**	**Ubicación en el servidor:**	

FECHA DE GENERACION RESPALDO	TAMAÑO	UBICACIÓN FÍSICA	FECHA RESTAURACIÓN	FUNCIONÓ?	OBSERVACIONES
		DATASTORE		SI	

Firma:

Nombre Funcionaria(o):

Cargo:

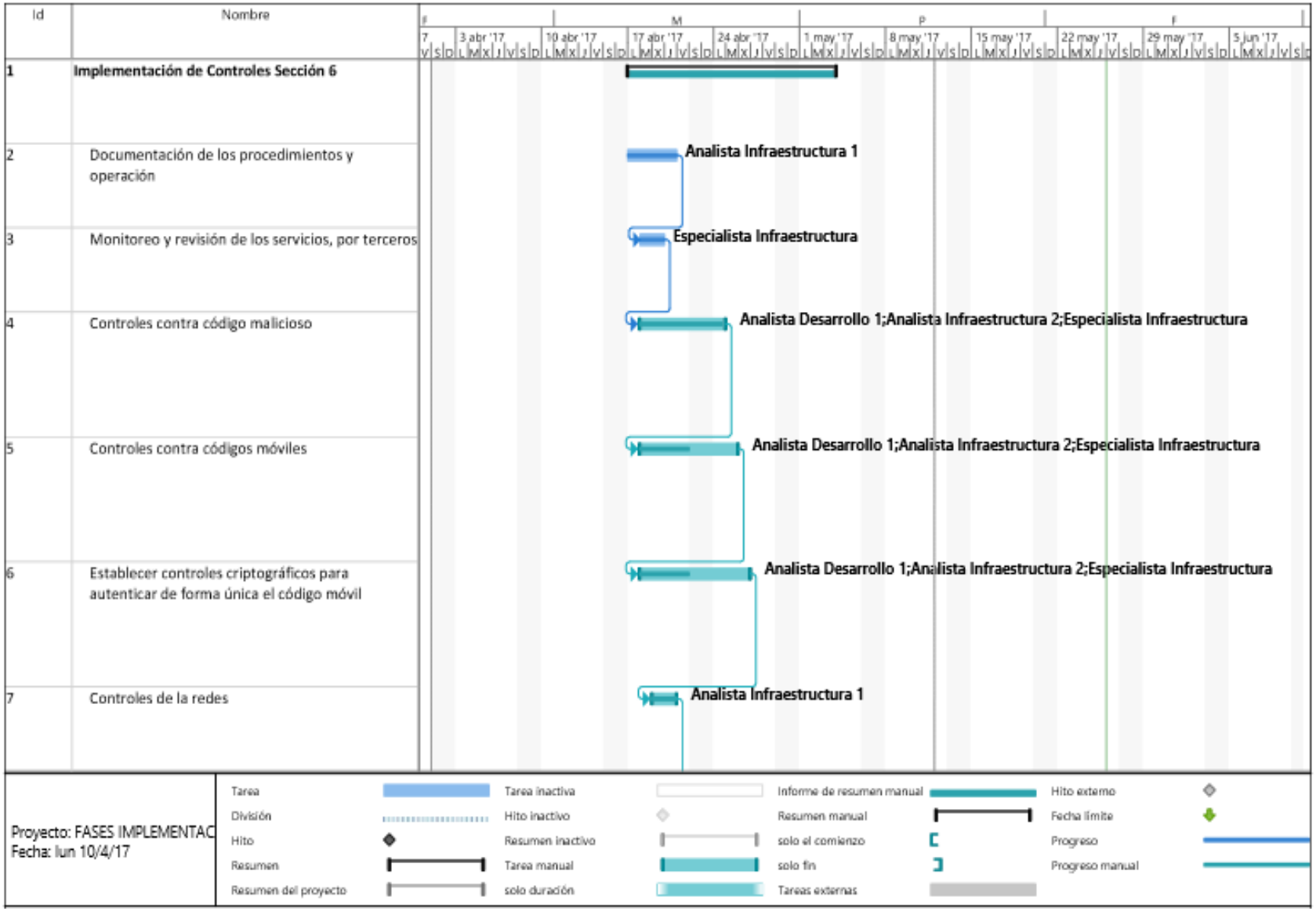
Detalle de Cronograma de Implementación

Id	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos
1	**Implementación de Controles Sección 6**	**19 días**	**lun 17/4/17**	**jue 11/5/17**	
2	Documentación de los procedimientos y operación	19 días	lun 17/4/17	jue 11/5/17	Analista Infraestructura 1
3	Monitoreo y revisión de los servicios, por terceros	2 días	mar 18/4/17	mié 19/4/17	Especialista Infraestructura
4	Controles contra código malicioso	5 días	mar 18/4/17	lun 24/4/17	Analista Desarrollo 1;Analista Infraestructura 2;Especialista Infraestructura
5	Controles contra códigos móviles	5 días	mar 18/4/17	mar 25/4/17	Analista Desarrollo 1;Analista Infraestructura 2;Especialista Infraestructura
6	Controles de la redes	2 días	mié 19/4/17	jue 20/4/17	Analista Infraestructura 1
7	Seguridad de los servicios de la red	2 días	vie 21/4/17	lun 24/4/17	Analista Infraestructura 2
8	Gestión de los medios removibles	1 día	lun 24/4/17	mar 25/4/17	Especialista de Soporte
9	Procedimiento para el manejo de la información	2 días	mar 25/4/17	mié 26/4/17	Especialista Infraestructura;Especialista de Soporte;Especialista Desarrollo
10	Seguridad de la documentación del sistema	2 días	mar 25/4/17	jue 27/4/17	Especialista de Soporte;Especialista Desarrollo;Especialista Infraestructura
11	Políticas y procedimientos para el intercambio de información	2 días	jue 27/4/17	vie 28/4/17	Especialista de Soporte;Especialista Desarrollo;Especialista Infraestructura
12	Mensajería electrónica	1 día	mar 25/4/17	mar 25/4/17	Analista Infraestructura 2
13	Sistemas de Información del Negocio	2 días	mar 2/5/17	mié 3/5/17	Especialista de Soporte;Especialista Desarrollo;Especialista Infraestructura
14	Transacciones en línea	1 día	mié 26/4/17	mié 26/4/17	Analista Infraestructura 2
15	Protección del registro de la información	1 día	mar 25/4/17	mar 25/4/17	Analista Infraestructura 1;Analista Desarrollo 1

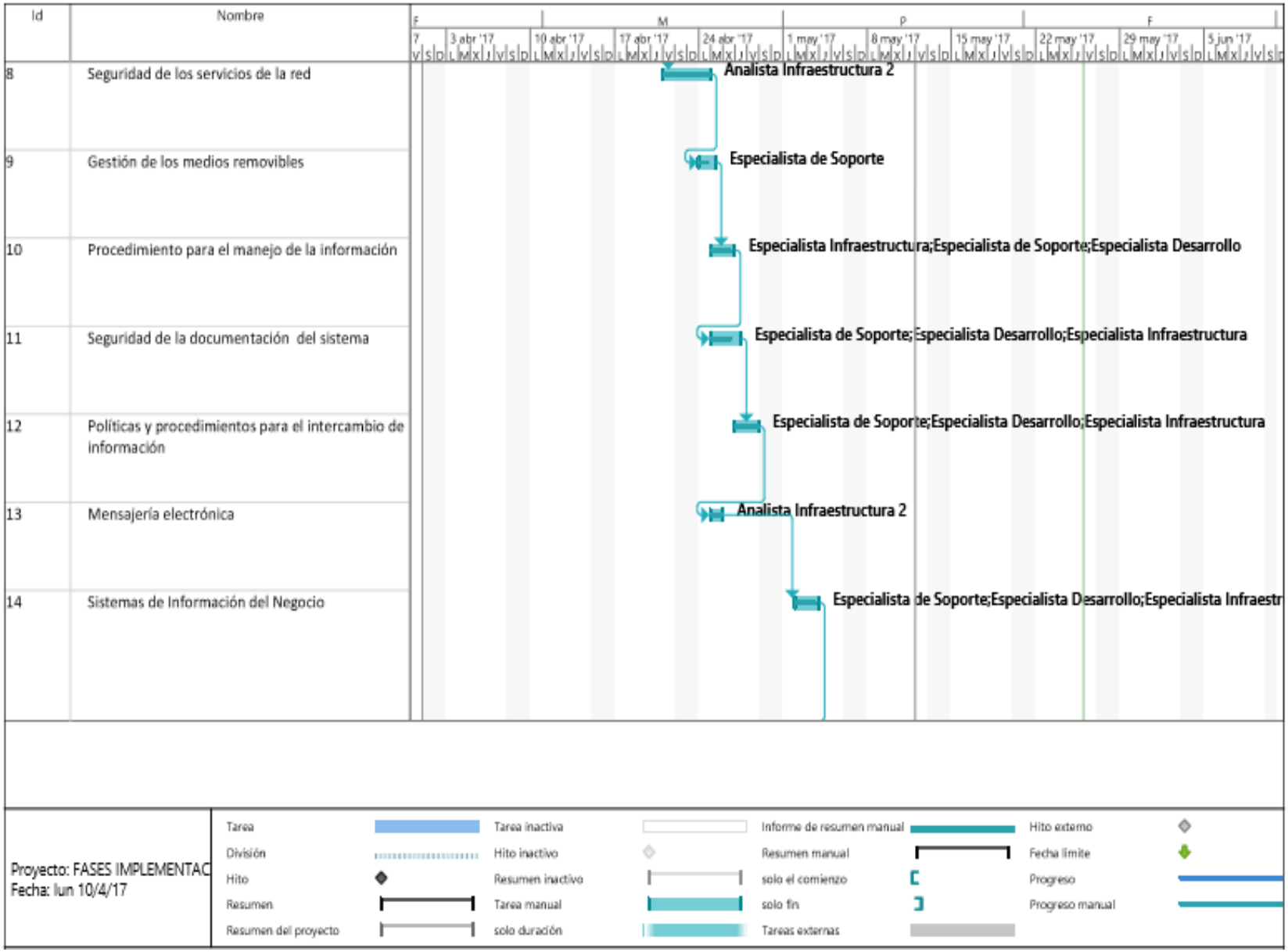
Detalle de Cronograma de Implementación

Id	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos
16	**Implementación de Controles Sección 7**	**5 días**	**vie 28/4/17**	**jue 4/5/17**	
17	Control de acceso	1 día	vie 28/4/17	vie 28/4/17	Analista Infraestructura 1;Especialista Desarrollo
18	Registro de usuarios	1 día	mar 2/5/17	mar 2/5/17	Analista Infraestructura 2;Analista Desarrollo 1
19	Gestión de privilegios	1 día	mié 3/5/17	mié 3/5/17	Analista Infraestructura 2
20	Gestión de contraseñas para usuarios	1 día	mié 3/5/17	mié 3/5/17	Analista Desarrollo 1;Analista Infraestructura 1
21	Revisión de los derechos de accesos de los usuarios	1 día	jue 4/5/17	jue 4/5/17	Analista Infraestructura 2
22	Uso de contraseñas	1 día	jue 4/5/17	jue 4/5/17	Especialista Desarrollo;Especialista Infraestructura
23	**Implementación de Controles Sección 8**	**5 días**	**vie 5/5/17**	**jue 11/5/17**	
24	Análisis y especificaciones de los requerimientos de seguridad	1 día	vie 5/5/17	vie 5/5/17	Especialista de Soporte;Especialista Infraestructura
25	Control de procesamiento interno	1 día	lun 8/5/17	lun 8/5/17	Especialista de Soporte;Especialista Desarrollo;Especialista Infraestructura
26	Integridad del mensaje	1 día	lun 8/5/17	mar 9/5/17	Analista Desarrollo 1;Analista Infraestructura 1
27	Fuga de información	1 día	mar 9/5/17	mar 9/5/17	Especialista de Soporte;Especialista Desarrollo;Especialista Infraestructura
28	Control de las vulnerabilidades técnicas	2 días	mié 10/5/17	jue 11/5/17	Especialista de Soporte;Especialista Desarrollo;Especialista Infraestructura

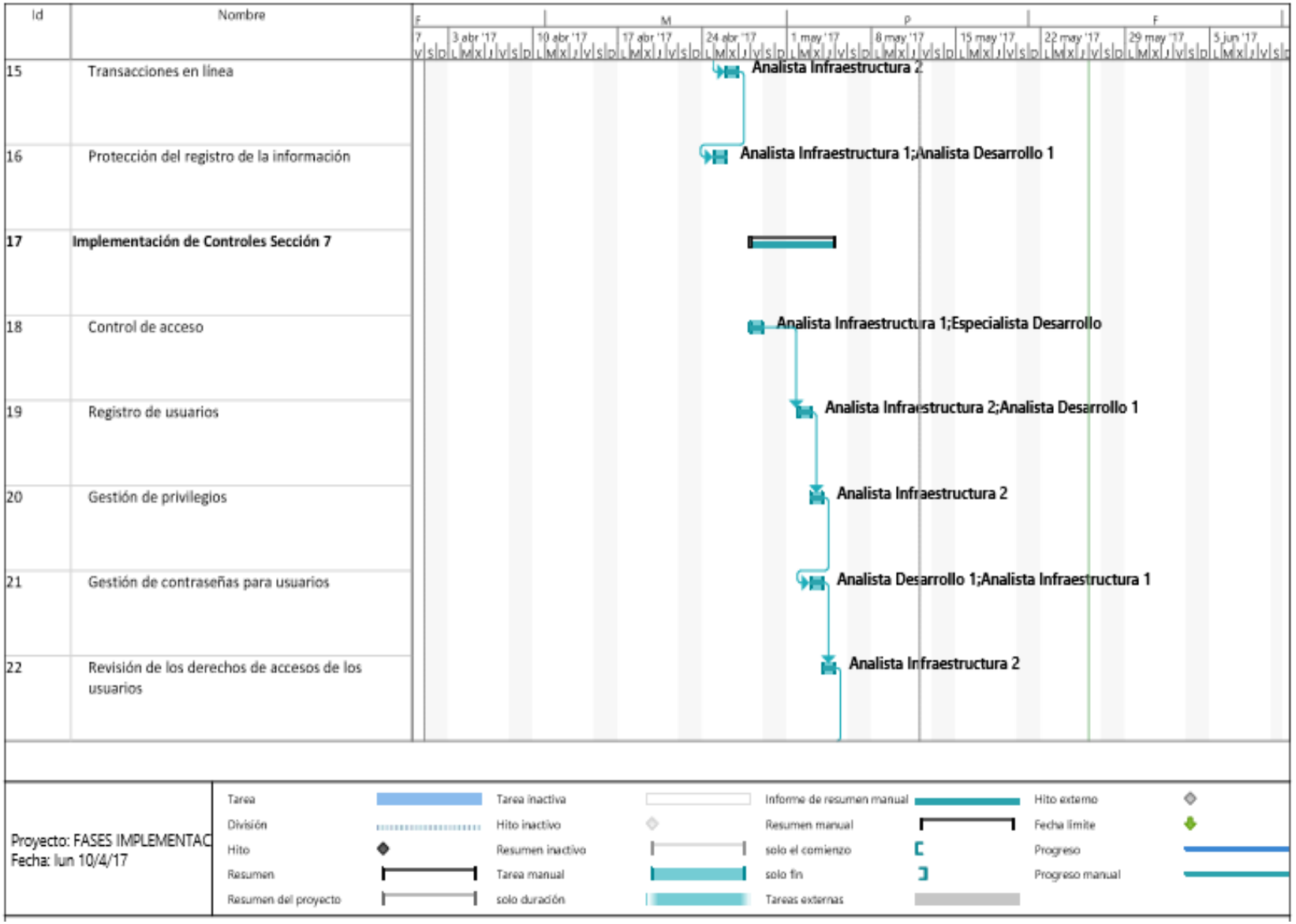
Detalle de Cronograma de Implementación



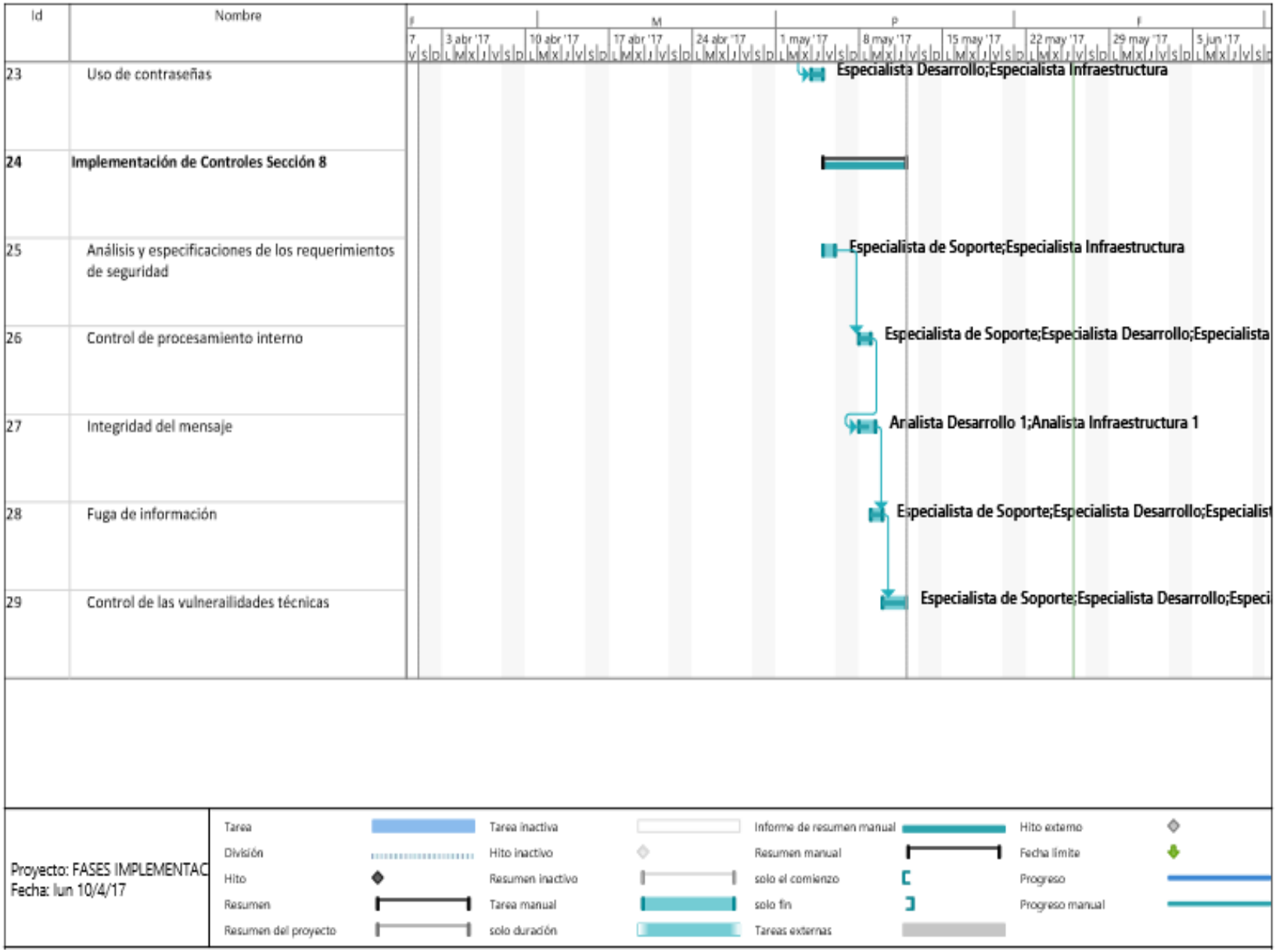
Detalle de Cronograma de Implementación



Detalle de Cronograma de Implementación



Detalle de Cronograma de Implementación



Plan de Auditoría SGSI
Versión 1.0 / Dic2016

Institución	**SECRETARÍA NACIONAL DE COMUNICACIÓN (SECOM)**	
Dirección de la organización auditada	**DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN**	
Representante de la Dirección	**Director de TIC's**	
Tipo de Revisión		
☐ Pre-Revisión	Revisión para Certificación ☐ Etapa 1 o ☒ Etapa 2	Re certificación ☐ Etapa 1 o ☐ Etapa 2
☐ Seguimiento ( )	Otros :	
Responsable auditoría	María Belén Jiménez (MBJA)	
Objetivos de la auditoría	Para Revisión etapa 1 (marcar todo) ☐ revisar la documentación del sistema de gestión. evaluar la ubicación y las condiciones específicas del sitio e intercambiar información con el personal ☐ revisar el estado de la SECOM y su grado de compresión de los requisitos de la norma, en particular en lo que concierne a la identificación de aspectos clave o significativos del desempeño procesos, objetivos y funcionamiento del sistema de gestión; ☐ recopilar la información necesaria correspondiente al alcance del sistema de gestión, a los procesos y a las ubicaciones de la SECOM, así como a los aspectos legales y reglamentarios relacionados y su cumplimiento (por ejemplo, aspectos de calidad, ambientales, legales del funcionamiento de la SECOM, los riesgos asociados, etc.); Para Revisión etapa 2 (marcar todo)	

	☒evaluar el grado de implementación, incluyendo su eficacia del Sistema de gestión. Para Revisión de seguimiento (marcar todo) ☐ evaluar el mantenimiento del sistema de gestión y mejoramiento continuo de su eficacia.
Alcance de la revisión	Evaluar y comprobar el cumplimiento de controles implementados en el Sistema de Gestión de Seguridad de la Información diseñado en la SECOM.
Criterio de revisión & Documentos de referencia	NTE INEN-ISO/IEC 27001 Acuerdo Ministerial No. 166 Documentación de la SECOM para su SGSI
Idioma	Español

Declaración de Confidencialidad Todas las informaciones evidenciadas durante la realización de esta revisión serán tratadas en estricta confidencialidad, y no serán reveladas a un tercero sin el consentimiento escrito de la SECOM, excepto a las autoridades de acreditación para su evaluación del Sistema de Gestión de la Seguridad.

_____ _____

Representante de la Dirección Fecha

	Requerimientos de Sistema de Gestión de Seguridad de la Información **ISO 27001** **Equipo para Revisión:** **María Belén Jiménez (MBJA)**	Requisitos Generales	Establecimiento del SGSI	Implementación y Operación del SGSI	Seguimiento y revisión del SGSI	Mantenimiento y mejora del SGSI	Generalidades de Requisitos de documentación	Control de Documentos	Control de registros	Compromiso de la dirección	Provisión de recursos	Formación, concienciación	Auditoría Interna del SGSI	Revisión por la dirección	Mejora continua	Acción correctiva	Acción Preventiva
Hora:	**Procesos de la SECOM**																
08:30	Reunión de Apertura																
09:00	Gestión de la Dirección ***(Política de Seguridad / Aspectos organizativos de la seguridad de la Información, Cumplimiento)*** (MBJA)	X	X	X	X	X				X				X			
10:00-16:30	Gestión de la Seguridad de la Información ***(Política de Seguridad / Aspectos organizativos de la seguridad de la Información / Gestión de Activos, Control de Acceso, Gestión de Incidentes de la Seguridad de la Información)*** (MBJA)	X	X	X	X	X	X		X		X		X		X	X	X

Día #1																	
09:00-16:30	Gestión de Comunicaciones y Operaciones ***(Gestión de Comunicaciones y Operaciones)*** (MBJA)	X	X	X	X	X											

Día #2																	
09:00-16:30	Control de Accesos ***(Control de Accesos)*** (MBJA)	X	X	X	X	X											

Día #3																	
09:00-16:30	Desarrollo y Mantenimiento de Aplicaciones ***(Adquisición, desarrollo y mantenimiento de los sistemas de información)*** (MBJA)	X	X	X	X	X											

Día #4																	
09:00	Revisión de hallazgos y preparación de las conclusiones e Informe de revisión																
15:30	Reunión de Cierre de la Revisión																

Solo para Auditor/Encargado de Revisión

Tenga en cuenta para el plan de Auditoría y su realización
Para toda la Auditoría, el recorrido es obligatorio, puede ayudar al desarrollo de la Auditoría.
Registre y mencione el sitio o proyecto a visitar.

Para la Auditoría Etapa 1

La Auditoría etapa 1 debe realizarse:

a) Al sistema de documentación de la SECOM
b) Evaluación del sitio de la SECOM y condiciones específicas de sitios y discutir con el personal de la SECOM para determinar la preparación de la Auditoría etapa 2
c) revisión del estado de la SECOM y entendimiento relacionado con los requerimientos de la norma, en particular con la identificación del desempeño clave o aspectos/impactos claves, peligros/riesgos, amenazas en cadena de suministro/riesgos, peligros en inocuidad de alimentos/riesgos, procesos, objetivos y operación del Sistema de Gestión
d) Recolectar información necesaria acerca del alcance del sistema de gestión, procesos, sitio(s) de la SECOM, aspectos regulatorios, legislación y cumplimientos (ejemplos, calidad, ambiental, aspectos legales de la operación, productos/servicio de la SECOM, riesgos asociados, etc)
e) Toda duda y hallazgos negativos considerados en la etapa 1 que podría clasificar como no conformidad debe ser verificado y confirmado durante la etapa 2 y registrar sus evidencias.
f) Revisar la asignación de recursos para la Auditoría de etapa 2 y ponerse de acuerdo con el SECOM en sus detalles
g) Proveer un enfoque para plan de la Auditoría etapa 2 mediante el grado de comprensión del sistema de gestión de la SECOM y operaciones en sitio en el contexto de los posibles aspectos significantes
h) Evaluar si las Auditorías internas y revisión por la dirección son planeadas y realizadas, y si el grado de implementación del sistema de gestión es sostenible y está listo para la Auditoría etapa 2
i) Las razones de aceptación de exclusiones aplicables para ISO 27001 debe ser registradas

Para la mayoría de Sistemas de Gestión, se recomienda que por lo menos una parte de Auditoría de etapa 1 se realice en la instalación de la SECOM para obtener los objetivos arriba descritos.

Para Auditoría Etapa 2

El propósito de la Auditoría Etapa 2 es evaluar el grado de implementación, mantenimiento y mejora continua del sistema de Gestión de la SECOM incluyendo su eficacia. La Auditoría Etapa 2 se debe realizar en el(los) sitio(s) de la SECOM. Deben incluir, por lo menos, los siguientes aspectos:

a) Información y evidencia de conformidad a todos los requerimientos de la norma del sistema de gestión aplicable u otro documento normativo
b) Desempeño de monitoreo, medición, reporte y revisión de objetivos y metas de desempeño claves (consistente con

las expectativas del estándar del Sistema de gestión aplicable u otro documento normativo)

c) El sistema de gestión de la SECOM y desempeño respecto al cumplimiento legal
d) Control operacional de los procesos de la SECOM
e) Auditoría interna y revisión por la dirección
f) Responsabilidad de manejo para la política de seguridad de la SECOM
g) Vínculos entre los requerimientos normativos, política, desempeño de objetivos y metas (consistente con las expectativas del estándar del Sistema de Gestión aplicable u otro documento normativo), requerimientos legales aplicables, responsabilidades, competencia del personal, operaciones, procedimientos, datos de desempeño, hallazgos y conclusiones de auditoría interna
h) Las razones de aceptación de exclusiones aplicables para ISO 27001 debe ser registrado.
i) Las razones de aceptación del alcance deben ser registrado.
j) Toda duda y hallazgos negativos considerados en la etapa 1 que podría clasificar como no conformidad. Debe ser verificado y confirmado durante la etapa 2 y registrar sus evidencias.

Para Auditoría de Seguimiento solamente, se debe considerar lo siguiente:

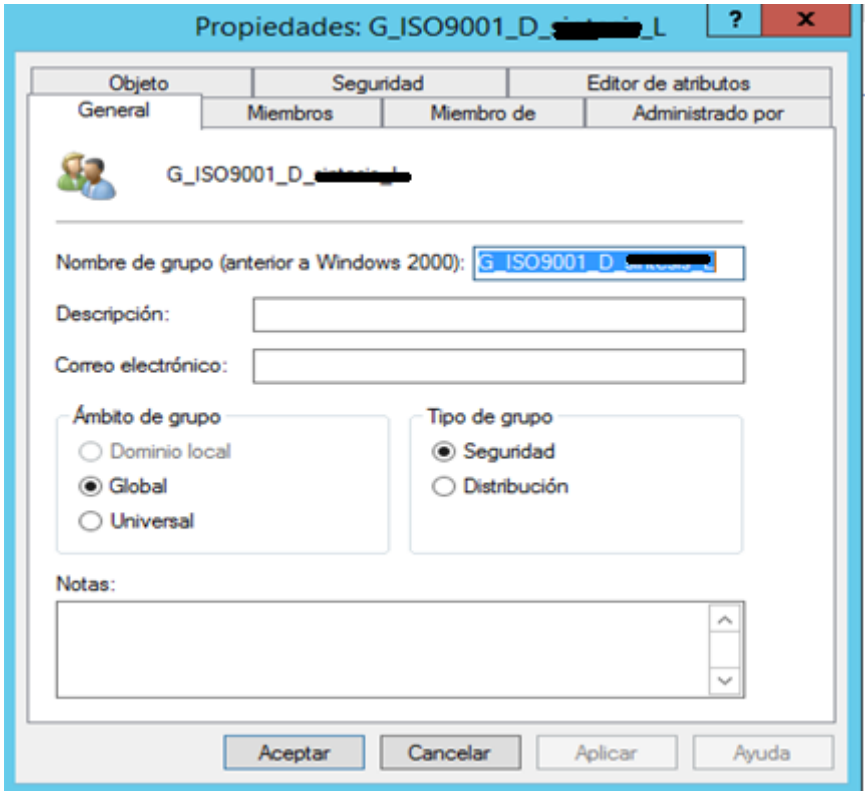
a) Auditorías internas y revisión por la dirección
b) Revisión de acciones tomadas de no conformidades identificadas durante la Auditoría previa
c) Tratamiento de quejas
d) Eficacia del Sistema de Gestión respecto al logro de objetivos de la SECOM ya certificado
e) Progreso de atividades planeadas para logro de majora continua
f) Continuo control operacional
g) Revisión de cualquier cambio
h) **Uso de marcas y logos, cualquier referencia de certificación**.

Para Auditoría de Recertificación solamente, Se deben incluir los siguientes aspectos en el plan de Auditoría:

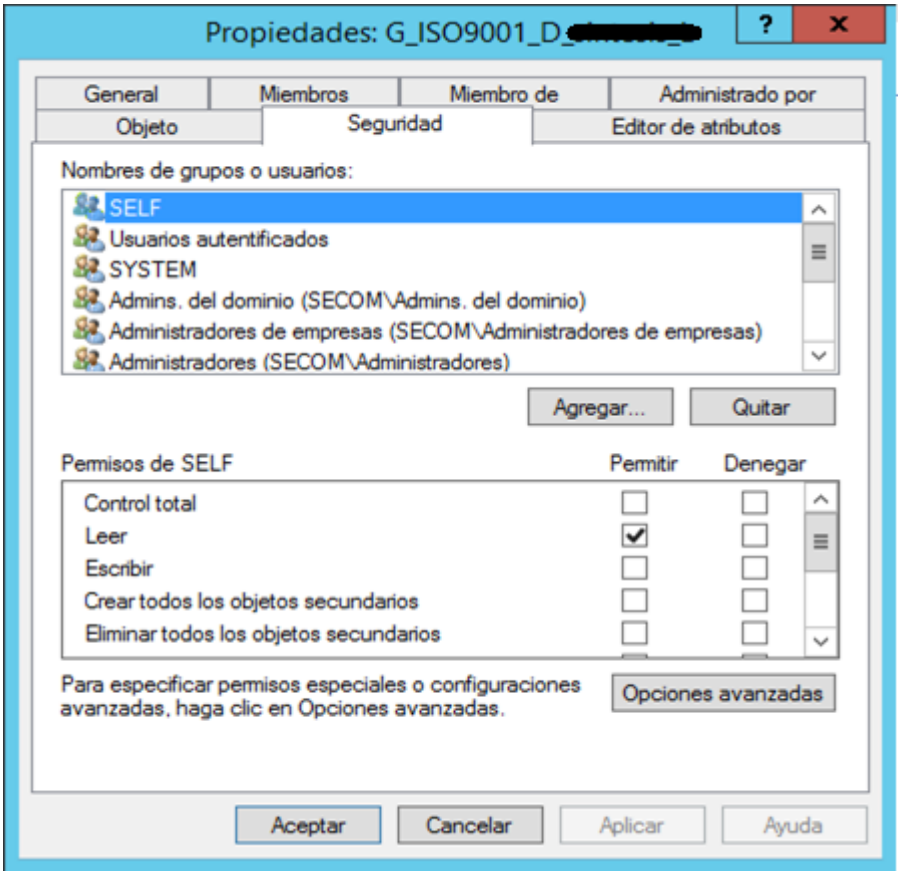
a) Revisión de la eficacia del Sistema de Gestión en su totalidad con respecto a los cambios internos y externos y su continua aplicación al alcance de certificación
b) revisar el compromiso de la compañía a mantener la eficacia del sistema de Gestión para mejorar el desempeño en general
c) revisar la operación del Sistema de Gestión certificado que contribuye al logro de los objetivos y política
d) verificar acciones tomadas basadas en quejas, reclamos y apelaciones

Pruebas Técnicas Medición de Eficacia

Validación Implementación y Operación de Plan de Tratamiento de Riesgos	
Posterior al levantamiento documental se ha ejecutado una serie de pruebas técnicas para validad la efectividad de los controles.	
Datos vinculados	
Activo Tecnológico en prueba:	Equipo de almacenamiento, servidores NAS, discos externos, repositorio digital
Tipo de prueba:	Escaneo de puertos / Vulnerabilidades / Manejo de Sesiones / Escalamiento de privilegios / Ataques de Autenticación
Dirección Vinculada:	Informes Gubernamentales
Producto Crítico:	Mensajes comunicacionales / Cadenas informativas en radio y televisión.
Ejecución	
Sobre Confidencialidad / Integridad / Disponibilidad	
Aplicación	
Gestión de Privilegios	



Pruebas Técnicas Medición de Eficacia



Gestión de Contraseñas

Directivas de cuenta/Directiva de contraseñas	ocultar
Directiva	**Configuración**
Exigir historial de contraseñas	5 contraseñas recordadas
Las contraseñas deben cumplir los requisitos de complejidad	Habilitado
Longitud mínima de la contraseña	7 caracteres
Vigencia máxima de la contraseña	45 días
Vigencia mínima de la contraseña	1 días

Directivas de cuenta/Directiva de bloqueo de cuenta	ocultar
Directiva	**Configuración**
Duración del bloqueo de cuenta	5 minutos
Restablecer recuentos de bloqueo de cuenta tras	5 minutos
Umbral de bloqueo de cuenta	20 intentos de inicio de sesión no válidos

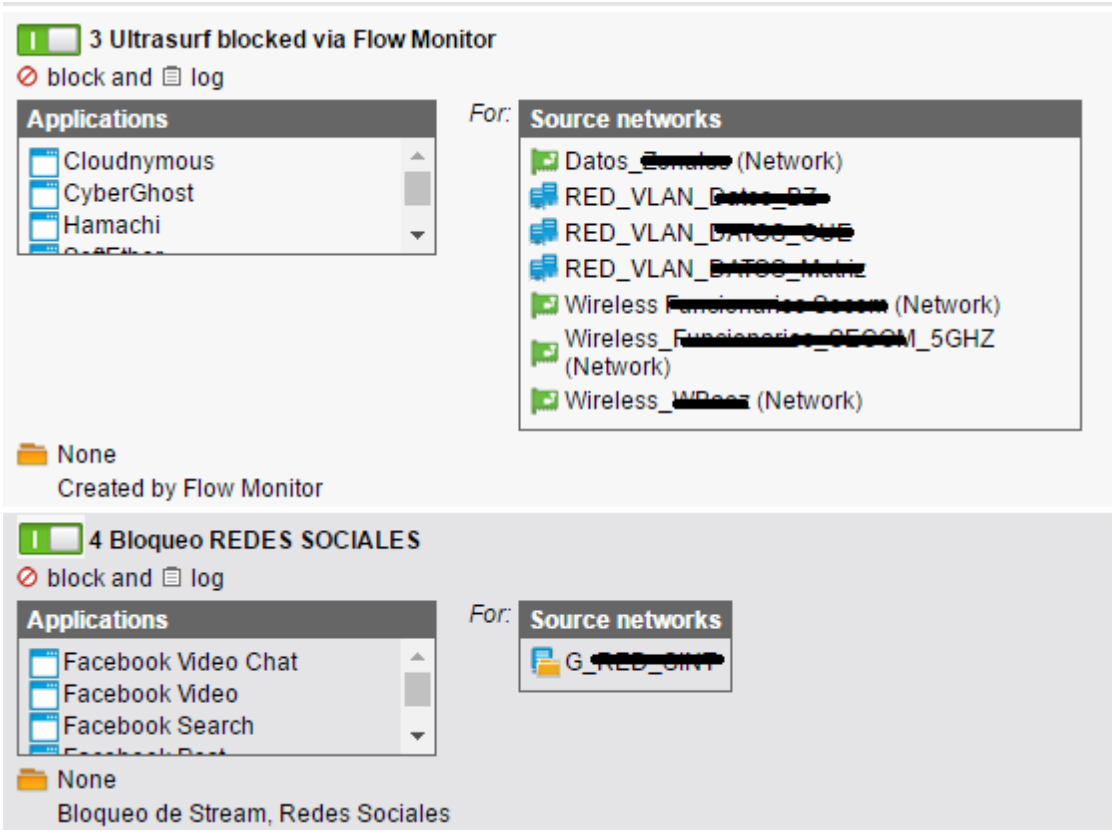
Directivas locales/Directiva de auditoría	ocultar
Directiva	**Configuración**
Auditar eventos de inicio de sesión	Errores
Auditar eventos de inicio de sesión de cuenta	Aciertos, errores
Auditar eventos del sistema	Aciertos, errores

Plantillas administrativas	ocultar
Definiciones de directiva (archivos ADMX) recuperadas del equipo local.	

Componentes de Windows/Explorador de juegos		ocultar
Directiva	**Configuración**	**Comentario**
Desactivar el seguimiento del último tiempo de juego en la carpeta Juegos	Habilitado	
Desactivar la actualización de juegos	Habilitado	
Desactivar la descarga de información sobre juegos	Habilitado	

Pruebas Técnicas Medición de Eficacia

Gestión Contra Código Malicioso



Pruebas Técnicas Medición de Eficacia

Default content filter action [This is the default content filter action profile]

Mode:	Blacklist
Blocked Categories	CriminalActivities Anonymizers SPAM Nudity
Warned Categories	Drugs
Blocked Sites	http://www.freecamsexposed.com/ ^https?://[A-Za-z0-9.-]*\.typeform\.com/ directtv Spam correo
Allowed Sites	http://www.longisland.com/ Webmail Presidencia
Uncategorized sites are	allowed
Spyware is	blocked
Blocked file extensions	com, bat, vbx, hta, inf, jse, wsh, vbs, vbe, lnk, chm, pif, reg, scr, cmd

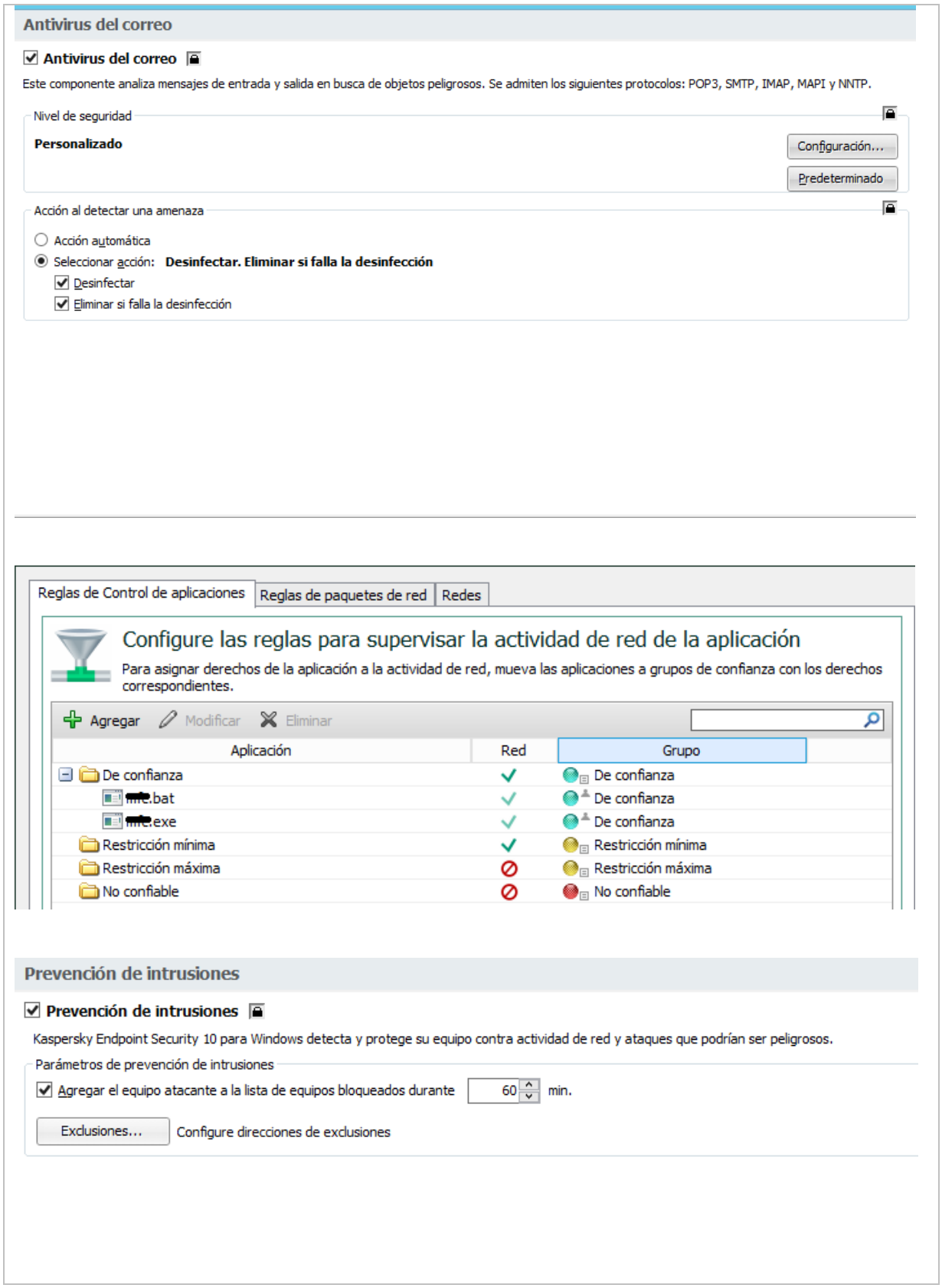
Default content filter block action [This is the default content filter block action profile]

Mode:	Whitelist
Uncategorized sites are	blocked

Filtro Sin Redes/Streaming

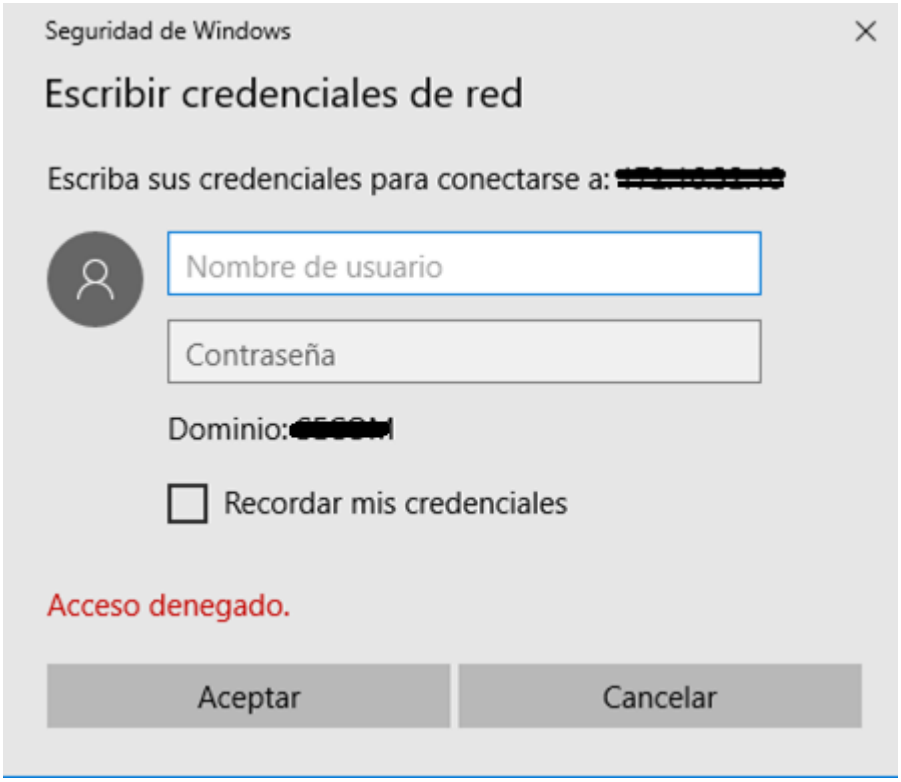
Mode:	Blacklist
Blocked Categories	GamesGambles Stream Video CriminalActivities Nudity Stream Audio Redes Sociales
Warned Categories	Drugs
Uncategorized sites are	allowed
Spyware is	blocked

Pruebas Técnicas Medición de Eficacia

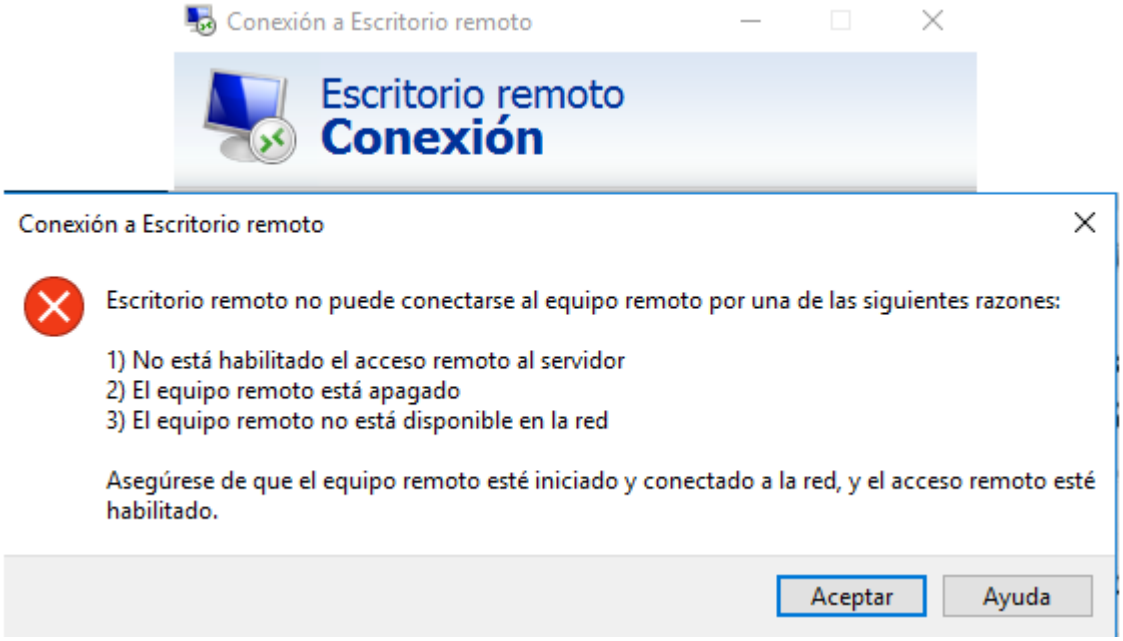


Pruebas Técnicas Medición de Eficacia

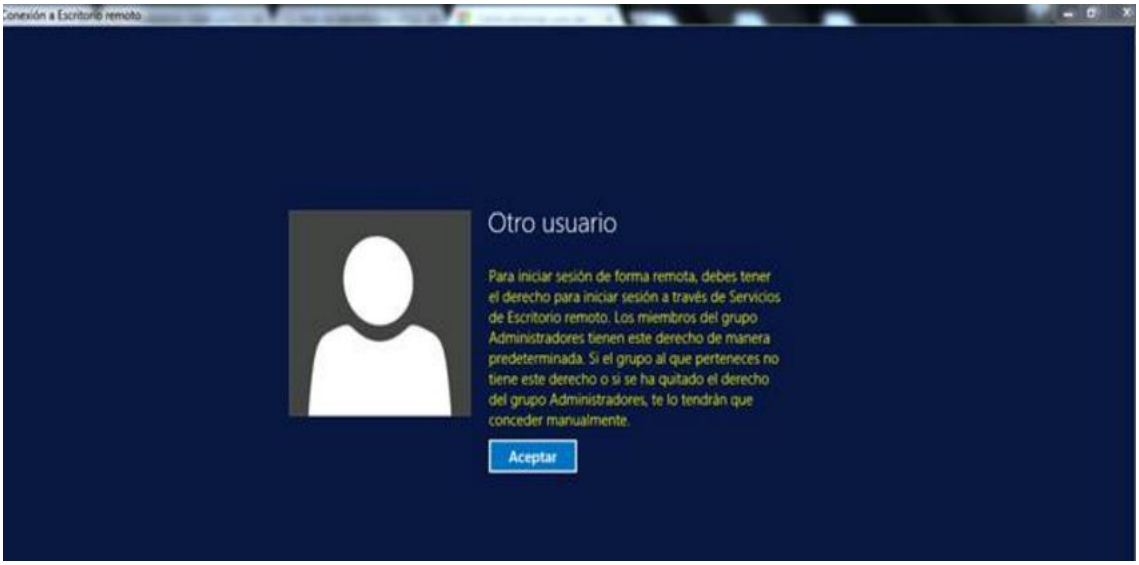
Pruebas
Gestión de Privilegios



Pruebas Técnicas Medición de Eficacia



Gestión de Contraseñas



Pruebas Técnicas Medición de Eficacia

Gestión Contra Código Malicioso

Pruebas Técnicas Medición de Eficacia

Nombre de grupo	Nombre del equipo	Objeto detectado	Ruta al archivo	Tipo de objeto	Acción	Cuenta	Aplicación
Servidores	[redacted]	not-a-virus:RiskTool.Win32.HackKMS.d	C:\Windows\System32\KMSServer.exe	otra aplicación	Object deleted. Object name: C:\Windows\System32\KMSServer.exe	[redacted]	Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition
Servidores	[redacted]	not-a-virus:RiskTool.Win32.HackKMS.d	C:\Windows\System32\KMSServer.exe	otra aplicación	Object deleted. Object name: C:\Windows\System32\KMSServer.exe	[redacted]	Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition
Servidores	[redacted]	not-a-virus:RiskTool.Win32.HackKMS.d	C:\Windows\System32\KMSServer.exe	otra aplicación	Object deleted. Object name: C:\Windows\System32\KMSServer.exe	[redacted]	Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition
Servidores	[redacted]	not-a-virus:RiskTool.Win32.HackKMS.d	C:\Windows\System32\KMSServer.exe	otra aplicación	Object deleted. Object name: C:\Windows\System32\KMSServer.exe	[redacted]	Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition

Resultados

De conformidad con las pruebas efectuadas se determina que los controles aplicados en gran medida cumplen con sus objetivos, obteniendo lo siguiente:

Control	% Cumplimiento
Implementación de Controles Sección 6	97
Implementación de Controles Sección 7	100
Implementación de Controles Sección 8	94,6

Declaración de Confidencialidad Todo lo evidenciado durante las pruebas será tratado en estricta confidencialidad, y no será revelado a un tercero sin el consentimiento escrito de la SECOM, excepto a las autoridades de acreditación para su evaluación del Sistema de Gestión de la Seguridad.

______________________________ __________________

Representante de la Dirección Fecha

Nota del Auditor

Institución	**SECRETARÍA NACIONAL DE COMUNICACIÓN (SECOM)**		
Dirección de la organización auditada	**DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN**		
Nombre del Representante de la dirección	Director de TIC's	**Tipo de Auditoría**	**Certificación** ☒ **Etapa 2** ☐ **Seguimiento (….)** **Recertificación** ☐ **Etapa 2**
Responsable auditoría	**María Belén Jiménez (MBJA)**		

Tipo: **OM** = Oportunidad de Mejora / **NC** = No Conformidad. (**+** = Mayor / **-** = Menor) **OK**= Conforme

Proceso/ área	**Requerimiento /elementos**	**Nota / Evidencia**	**Tipo (OK/OM/NC)**
Revisión Documental	Requisitos Generales	A través de la documentación entregada por la SECOM se evidencia que tienen implementado un Sistema de Gestión para la Seguridad de la Información.	OK
	Creación y Gestión del SGSI		
		Se evidencia el alcance, objetivos y límite del SGSI para SECOM.	OK
		Se evidencia el levantamiento de activos de la información.	OK

Nota del Auditor

Proceso/ área	**Requerimiento /elementos**	**Nota / Evidencia**	**Tipo (OK/OM/NC)**
		Menciona la metodología utilizada para la evaluación de los riesgos, y se evidencian los criterios de aceptación y la fijación de niveles de riesgos.	OK
		Existe la matriz de riesgos se identifican las amenazas a que están expuestas los activos, vulnerabilidades bajo las que podrían actuar las amenazas.	OK
		Existe la matriz de riesgos y se evidencia un análisis completo sobre la probabilidad que estos ocurran.	OK
		Se evidencia el plan del tratamiento de riesgos.	OK
		No se evidencia la aprobación de la Dirección al informe de la evaluación de riesgos realizada.	NC-
		No se evidencia la aprobación de la Dirección para la implementación y operación del SGSI	NC-
		Existe el documento de declaración de aplicabilidad y se encuentran definidos todos los controles que se exceptúan.	OK

Nota del Auditor

Proceso/ área	**Requerimiento /elementos**	**Nota / Evidencia**	**Tipo (OK/OM/NC)**
	Implementación y Operación del SGSI		OK
Sistema de Gestión de Seguridad de la Información		Los controles que se involucran con la Sección 6. de la norma se han cumplido en su totalidad	OK
		Los controles que se involucran con la Sección 7. de la norma se han cumplido en su totalidad	OK
		Los controles que se involucran con la Sección 8. de la norma se han cumplido en su totalidad	NC+
	Auditorías		
		Existe identificado un esquema de auditorías para el SGSI implementado.	OK

Reporte de Auditoría

Institución	**SECRETARÍA NACIONAL DE COMUNICACIÓN (SECOM)**		
Dirección de la organización auditada	**DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN**		
Nombre del Representante de la dirección	Director de TIC's	**Tipo de Auditoría**	**Certificación** ☒ **Etapa 2** ☐ **Seguimiento (…)** **Recertificación** ☐ **Etapa 2**
Responsable auditoría	**María Belén Jiménez (MBJA)**		
Fecha de Auditoría desde / hasta	**Mayo 2017**		
Toda la información evidenciada durante esta auditoría será tratada en absoluta confidencialidad y no será revelada a un tercero sin consentimiento escrito del cliente, excepto a las autoridades de acreditación para la evaluación de la SECOM. Este reporte es confidencial y su distribución es limitada al equipo auditor, representante de la Dirección Auditada.			

1. Objetivos de Auditoría

- Verificar si el sistema de gestión de seguridad es conforme a todos los requerimientos de la ISO 27001.
- Evaluar la implementación y la eficacia del SGSI de la organización auditada
- Verificar el mantenimiento y la mejora continua del SGSI de la SECOM.
- Evaluar si el SGSI es capaz de lograr los objetivos y política(s) definidas por la SECOM

2. Hallazgos de Auditoría

¿La SECOM ha demostrado la implementación, mantenimiento y mejora continua de su SGSI?	☒ Sí	☐ No
¿La SECOM ha realizado la medición, análisis y acciones de mejora para lograr objetivos y metas claves de desempeño y política(s) del SGSI?	☒ Sí	☐ No
¿El programa de auditoría interna ha sido completamente implementado y funciona como una herramienta de mantenimiento y mejora de la eficacia del SGSI?	☒ Sí	☐ No
¿La revisión por la dirección asegura la conveniencia, adecuación y la eficacia continua del SGSI?	☒ Sí	☐ No

Reporte de Auditoría

¿El sistema de gestión demostró el cumplimiento mayoritario de los requerimientos de la ISO 27001?	☒ Sí	☐ No

3. Conclusiones de Auditoría

Se realizó la auditoría basada en los procesos, enfocado en objetivos/riesgos/aspectos significativos requeridos por la(s) norma(s).

Los métodos de auditoría usados fueron entrevistas, observaciones de actividades y revisión de documentos y registros.

La estructura de la auditoría fue acorde con el plan de auditoría anexo.

Se concluye que la SECOM:

☒ ha ☐ no ha	Implementado, mantenido y mejorado en gran medida su SGSI de acuerdo con los requerimientos de la ISO 27001 y demostrado la capacidad del sistema de satisfacer el alcance propuesto, la política y objetivos de la organización.

Número de no conformidades identificadas:	**1**	**Mayor**	**2**	**Menor**

Las no conformidades mencionadas deben ser tratadas mediante el proceso de acciones correctivas.

Todas las no conformidades identificadas deben ser tratadas inmediatamente y se deben poner en conocimiento del Director de Tecnologías de la Información y Comunicación las acciones tomadas lo más pronto posible ya que el plazo máximo de cierre de No conformidad detectada es de 90 días calendario a partir de la reunión de cierre.

Reporte de Auditoría

4. Resumen:		
¿Es requerida una auditoría complementaria (follow-up) o limitada (adicional) para verificar las acciones correctivas y correcciones eficaces?	☒ Sí	☐ No

5. Observaciones en General

Continuar con la revisión del SGSI y mejorar aspectos de documentación.
Corregir las no conformidades detectadas.

Nombre del Responsable de la Auditoría Fecha

Nombre del Responsable de la Dirección Fecha

Institución	**SECRETARÍA NACIONAL DE COMUNICACIÓN (SECOM)**
Representante de la Dirección	**Director de TIC's**
Informe de No conformidad Detectada	
Tipo de No Conformidad	Mayor ☒ Menor ☐
Responsable del informe	María Belén Jiménez (MBJA)
Hallazgo	
En su mayoría los controles del SGSI seleccionados se encuentran implementados sin que algunos de estos tengan una correcta descripción o documentación.	
Análisis de la Causa Raíz	
Miembros del área de Desarrollo que participan en la implementación de los controles han dilatado las actividades debido a asignaciones de nuevas tareas no asociadas con el plan de implementación del SGSI.	
Acción Correctiva	
Documentar adecuadamente los controles de la Sección 8.	

Declaración de Confidencialidad Todas las informaciones evidenciadas durante la realización de esta revisión serán tratadas en estricta confidencialidad, y no serán reveladas a un tercero sin el consentimiento escrito de la SECOM, excepto a las autoridades de acreditación para su evaluación del Sistema de Gestión de la Seguridad.

_____ _____

Representante de la Dirección Fecha

Institución	**SECRETARÍA NACIONAL DE COMUNICACIÓN (SECOM)**
Representante de la Dirección	**Director de TIC's**
Informe de No conformidad Detectada	
Tipo de No Conformidad	Mayor ☐ Menor ☒
Responsable del informe	María Belén Jiménez (MBJA)
Hallazgo	
No se evidencia la aprobación de la Dirección al informe de la evaluación de riesgos realizada.	
Análisis de la Causa Raíz	
Existe tema de transición dentro de la institución, por lo que el responsable del área no cuenta con tiempo para revisión de documentación final y posterior aprobación de la misma.	
Acción Correctiva	
Delegar rol aprobador a otro funcionario para recopilación de firmas	

Declaración de Confidencialidad Todas las informaciones evidenciadas durante la realización de esta revisión serán tratadas en estricta confidencialidad, y no serán reveladas a un tercero sin el consentimiento escrito de la SECOM, excepto a las autoridades de acreditación para su evaluación del Sistema de Gestión de la Seguridad.

_____ _____

Representante de la Dirección Fecha

Informe de No Conformidad Versión 1.0 / Dic2016

Institución	**SECRETARÍA NACIONAL DE COMUNICACIÓN (SECOM)**
Representante de la Dirección	**Director de TIC's**
Informe de No conformidad Detectada	
Tipo de No Conformidad	Mayor ☐ Menor ☒
Responsable del informe	María Belén Jiménez (MBJA)
Hallazgo	
No se evidencia la aprobación de la Dirección para la implementación y operación del SGSI	
Análisis de la Causa Raíz	
Existe tema de transición dentro de la institución, por lo que el responsable del área no cuenta con tiempo para revisión de documentación final y posterior aprobación de la misma.	
Acción Correctiva	
Delegar rol aprobador a otro funcionario para recopilación de firmas	

Declaración de Confidencialidad Todas las informaciones evidenciadas durante la realización de esta revisión serán tratadas en estricta confidencialidad, y no serán reveladas a un tercero sin el consentimiento escrito de la SECOM, excepto a las autoridades de acreditación para su evaluación del Sistema de Gestión de la Seguridad.

_____ _____

Representante de la Dirección Fecha