MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

Estudio comparativo entre instituciones públicas latinoamericanas referente a la aplicación del gobierno de la seguridad de la información.

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por las estudiantes:
Karol Dayanna GUILLÉN RIVAS
Clara Marisela VÉLIZ LOOR

Bajo la dirección de:
Raúl Vicente GONZALEZ CARRION

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
2019

Estudio comparativo entre instituciones públicas latinoamericanas referente a la aplicación del gobierno de la seguridad de la información.

Karol Dayanna GUILLÉN RIVAS[1]
Clara Marisela VÉLIZ LOOR[2]
Raúl Vicente GONZALEZ CARRION[3]

Resumen

El objetivo general del presente trabajo investigativo es realizar un estudio comparativo entre instituciones públicas latinoamericanas, referente a la seguridad de la información a nivel de gobierno, tomando como caso de estudio las instituciones ecuatorianas Senae y SRI. Su enfoque es cualitativo, con un alcance exploratorio-descriptivo; se realizó un análisis de la situación inicial sobre las directrices que propone el esquema gubernamental de seguridad de la información (en adelante EGSI) y el cumplimiento de estas en cada una de las Instituciones públicas en contraste con las mejores prácticas fundamentadas en estándares Internacionales enfocados en salvaguardar el activo más importante de los organismos como lo es la información, para posteriormente proponer mejores prácticas orientadas a la seguridad de la información, evaluadas por expertos en el área mediante la técnica de focus group; evidenciándose que la aplicación del EGSI no es suficiente para mantener una óptima gestión de seguridad de la información.

Palabras clave:	seguridad de la información, riesgo, estándar, amenaza, ciberseguridad.

Abstract

The general objective of this research work is to carry out a comparative study among Latin American public institutions, regarding the security of information at the government level, taking as a case study the Ecuadorian institutions Senae and SRI. Its approach is qualitative, with an exploratory-descriptive scope; An analysis of the initial situation was carried out on the guidelines proposed by the governmental information security scheme (hereinafter EGSI) and the compliance of these in each of the public institutions in contrast with the best practices based on international standards focused on safeguarding the most important asset of the organisms, such as information, to subsequently propose best practices oriented to information security, evaluated by experts in the area through the focus group technique; evidencing that the application of the EGSI is not enough to maintain an optimal management of information security.

Key words	Information security, risk, standard, threat, cybersecurity.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail correo kguillenr@uees.edu.ec
[2] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail correo cvelizl@uees.edu.ec
[3] Magíster en Administración de Sistemas de Información Empresarial. Docente de la Maestría en Auditoría en Tecnologías de la Información Universidad Espíritu Santo- Ecuador.

INTRODUCCIÓN

A nivel mundial las organizaciones públicas y privadas advierten su preocupación por el incremento de los casos de fuga de información, así lo establece el informe Data Threat Report 2018, en el cual se muestran indicadores que el 44% de las compañías dicen estar "muy" o "extremadamente" vulnerables ante la posibilidad de sufrir un incidente de este tipo, esta cifra con respecto al año anterior muestra un incremento del 14% (Ver Anexo 1).

La preocupación de las organizaciones frente a este problema no está infundada, debido a que estudios realizados por compañías reconocidas a nivel mundial, muestran cifras que respaldan dicha percepción con relación a la fuga de información, por ejemplo la Price Waterhouse Cooper en su estudio Ciberseguridad y privacidad: De la percepción a la realidad (2016), muestra que en países como México, el 87% de las empresas entre las públicas, privadas y civiles han tenido incidentes relacionados a la seguridad de la información. Por su parte Symantec demuestra también que el temor que tienen las organizaciones porque se filtre su información, está acorde a las causas por las cuales los cybercriminales cometen este tipo de delitos, en su informe de amenazas de la seguridad de internet (2018) indica que la principal razón de los incidentes de datos es el robo de información, siendo éste un poco más del 90%.

La Asociación Colombiana de Ingenieros de Sistemas (ACIS), que desde el 2008 realiza año a año un estudio con base en encuestas a nivel de toda Latinoamérica, con el fin de conocer el estado de la seguridad de la información en la región, en su XVIII Jornada Internacional de Seguridad Informática ACIS 2018 muestra que la temática de la seguridad de la información es la prioridad para las organizaciones y en lo referente a incidentes de seguridad, el 65% de los encuestados admitió haber tenido por lo menos un incidente en la seguridad de la información.

El impacto causado al infringir la seguridad en las organizaciones se traduce en pérdidas que pueden llegar a los cientos de miles de dólares. En el Reporte Anual de Ciberseguridad realizado por Cisco (2018), muestra que el 53% de los encuestados para la realización de dicho estudio, percibió un perjuicio financiero superior a los USD $500.000, entre las afectaciones se incluye la pérdida de ingresos, disminución de los clientes, decrecimiento de oportunidades y costos varios (Ver Anexo 2). Para contrarrestar estos riesgos las organizaciones han alcanzado una fuerte dependencia hacia los Sistemas de Información [en adelante SI] (Cavusoglu, Mishra, y Raghunathan, 2004; Ifinedo, 2009, 2011; Lebek, Uffen, Neumann, Hohler, y H. Breitner, 2014; Stanton, Stam, Mastrangelo, y Jolton, 2005). En relación a Ecuador, durante los últimos diez años, las organizaciones públicas han desarrollado mecanismos que promueven el aseguramiento de la información, que de acuerdo a la facultad concedida en la Constitución de la República es responsabilidad de ellas salvaguardarla (Lexisfinder, 2013).

Pero no es sólo el hecho de la institucionalidad como responsabilidad en pro de asegurar la información, sino es el comportamiento acompañado de procesos bien estructurados que como gestión de la organización no necesita centrarse en la cultura de seguridad como una percepción explícita, sino más bien la actitud de mostrar desde el jerárquico superior en cadena descendente hacia los subordinados, mediante la participación en operaciones de seguridad de la información, lo que influirá efectivamente en el cumplimiento de las reglas y prácticas de seguridad.

La gerencia tiene la autoridad de influir en otros empleados y tienen más probabilidades de triunfar en la superación de la resistencia y barreras culturales; cuando los empleados crean que la gestión se preocupa por la seguridad, se inclinarán por cooperar para mejorar la seguridad. Así pues, el papel de la administración y el compromiso de la Dirección es importante en el desarrollo de la Cultura organizacional y cambio cultural. Crear una cultura de seguridad dentro de la organización puede animar a los empleados a interesarse por la seguridad de la información y ayudar a dar forma a la seguridad de la información en la Organización (Al-Izki & Weir, 2016).En el Ecuador, con relación a la protección de la información pública y el acceso a ésta, se encuentra normada en la Ley Orgánica de Transparencia y Acceso de la Información, y específicamente en el artículo 10 de dicha ley, se indica que las instituciones públicas se encuentran obligadas a crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de

la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción (LOTAIP,2004). Adicionalmente, en el mismo artículo se responsabiliza a los servidores de dichas instituciones, que serán ellos quienes administren, manejen, archiven o conserven información pública, y las posibles irresponsabilidades que se llegaren a comprobar acarrearán consecuencias civiles, administrativas o penales a las que pudiera haber lugar.

En los últimos años las instituciones públicas ecuatorianas han sido sometidas al proceso de modernización, el cual ha consistido no solo en mejoras de infraestructura y equipos tecnológicos; sino también en el procesamiento electrónico de datos, con el fin de digitalizar todos los archivos impresos, libros, actas y demás documentación que puede corromperse con el pasar del tiempo, por ello es de gran importancia mantener a buen recaudo tanto la información almacenada en repositorios físicos como digitales, de manera que pueda estar accesible en cualquier momento, manteniendo su confiabilidad y disponibilidad.

Actualmente muchas de las entidades del sector público han puesto a disposición de los ciudadanos servicios en línea contribuyendo al gobierno electrónico, con el objetivo de ampliar y facilitar el acceso a sus servicios en el marco del proceso de simplificación de trámites alineados a su estrategia digital, así pues, a medida que los consumidores acuden a los proveedores de servicios en línea, muchas de estas mismas personas están cada vez más preocupados por el aspecto de seguridad de la utilización de estos sitios, ya que los artículos sobre ataques de hackers y pérdida de información personal privada contribuye a la posible pérdida de confianza de los usuarios; por ello las empresas deben autorregular su industrias en la provisión de entornos seguros, los gobiernos han promulgado un nivel mínimo en legislación para los sistemas seguros y proporcionar una mejor protección de los datos personales de los consumidores de información. Los países europeos tienen leyes que exigen la protección de datos personales y declarar que los proveedores de servicios en línea deben mantener sistemas informáticos seguros a través de una variedad de procesos técnicos y procesales (Kuzma, 2010).

En este contexto, es necesario conocer los riesgos a los que están expuestos, las vulnerabilidades y amenazas que enfrentan las organizaciones públicas con relación a la información digital que por su potestad poseen, por ello surge la importancia de realizar el presente trabajo investigativo, enfocado en un estudio comparativo entre instituciones estatales que están destinadas al servicio de la ciudadanía, por ende la información que manejan en su mayoría es pública, sin embargo sólo puede ser conocida por el ciudadano al que pertenece dicha información, por lo tanto se requiere los datos se mantengan a buen recaudo, conservando la integridad y confidencialidad de los mismos. Esta investigación pretende recomendar y aplicar mejores prácticas en pro de la mejora de la seguridad de la información en cada una de las Instituciones gubernamentales consideradas en este estudio, cuyo objetivo es minimizar el nivel del riesgo al que se encuentra expuesto la seguridad de la información de la Institución, y así ofrecer servicios de calidad con calidez.

MARCO TEÓRICO

Sistemas de Gestión de Seguridad de la Información

Un sistema de gestión de seguridad de la información en adelante (SGSI), se refiere a un conjunto de datos ordenados en poder de una institución que son de gran valor para la entidad, sea está en documentos físicos (papel), archivos digitales, repositorios electrónicos, en imágenes, email, entre otros (ISO, 2007).

El desarrollo y aplicación de los estándares tiene como objetivo apoyar tanto a las personas y empresas cuando adquieren productos y servicios, de manera que puedan aumentar su reputación al haber certificado su cumplimiento de las normas y ganar la confianza de sus clientes, ya que mejorará la calidad de sus productos y servicios ofrecidos (Disterer, 2013).

Orrego (2011) señala que una empresa puede tener implementando un SGSI, sin embargo, este sistema se puede mejorar mediante la inclusión de estándares y normas como ISO (Organización Internacional para la Estandarización), o midiendo el estado de maduración del SGSI a través de Cobit (Objetivos de Control para la Información y Tecnologías relacionadas) o ITIL (Biblioteca de Infraestructura de Tecnologías de la Información).

El SGSI se define de manera formal en la norma ISO 27001, donde están los estándares y mejores prácticas de seguridad de la información, el cual consiste en preservar la confidencialidad, disponibilidad e integridad de la información; así como de los sistemas involucrados dentro de la Organización (ISO, 2012).

ISO

La Organización Internacional para la Estandarización (ISO) la conforman representantes de los Organismos de Normalización nacionales (ONS), que produce Normas Internacionales industriales y comerciales, dichas normas se conocen como normas ISO, fue fundada en 1946 y está respaldada por 159 países. Disterer (2013) indica que, para la protección de los sistemas de información, las normas ISO 27000, ISO 27001 e ISO 27002 proporcionan objetivos de control, controles específicos, requisitos y directrices con los cuales la empresa puede reducir riesgos y evitar daños.

La norma ISO 27001 es la más utilizada y extendida que establece las bases para el establecimiento de un SGSI, esta norma incluye los requerimientos necesarios para la evaluación y el tratamiento de los riesgos de seguridad de la información; los cuales son genéricos y se procura que sean aplicables a todas las empresas, sin importar su tipo, tamaño o naturaleza (Avila, 2016); además Disterer (2013) señala que como punto principal para la planificación, implementación, operación, monitoreo continuo y la mejora de un ISMS (Information Security Management System) orientado a procesos, el enfoque debe estar alineado con el ciclo de PDCA (plan-do-check-act) como se puede apreciar en la figura 1.

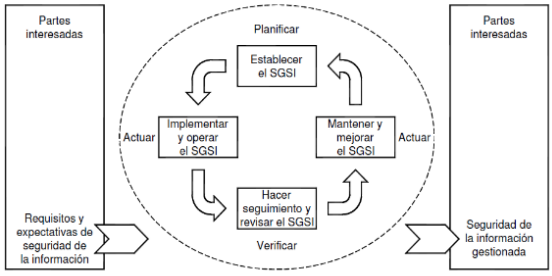


Figura 1. Modelo PDCA aplicado a los procesos de SGSI.
Fuente: (ICONTEC, 2006)

COBIT

Lainhart (2000) señala que COBIT (Objetivos de Control para la Información y Tecnologías relacionadas) posiblemente es el marco de control más apropiado para ayudar a una organización a asegurar la alineación entre el uso de la tecnología de la información (TI) y sus objetivos comerciales, ya que pone énfasis en las necesidades de la empresa y que se cumpla con cada objetivo de control, estos controles son actividades que se llevan a cabo para mitigar los riesgos o reducirlos a un nivel que se considere aceptable.

El marco COBIT 5 diseñado por ISACA es la innovadora herramienta de gobierno de TI que ayuda a comprender y gestionar los riesgos asociados con la información y la TI, cuenta con 37 procesos donde cada uno de ellos contiene prácticas de gobierno o de administración y 5 dominios: el dominio de gobierno posee 5 procesos y en cada uno se detallan las prácticas para evaluar, dirigir y monitorear (EDM) y los 4 dominios de administración que se encuentran alineados en planificar, construir operar y monitorear (PBRM); como se puede apreciar en la figura 2 se construye bajo 5 principios que optimizan la inversión en tecnologías de la información así como el uso en beneficio de las partes interesadas, permitiendo a la Institución construir un marco efectivo de Gobierno y administración (Isaca, 2012).

Figura 2: *Principios de COBIT 5*
Fuente: (ISACA, 2012)

ITIL

La Biblioteca de Infraestructura de Tecnologías de la Información (ITIL) fue desarrollada a finales de 1980, pertenece a la OGC (Oficina de Comercio del Gobierno Británico), pero es de libre uso; proporciona una descripción detallada de los procesos más importantes que debe llevar una organización en temas de Tecnologías de la Información y estos se adaptan en función de cada organización, sin importar el sector o tamaño de la empresa; por lo que ITIL

especifica un método sistemático que garantiza la calidad de los servicios de TI (López, 2017).

Hoy en día ITIL se ha convertido en un estándar reconocido y utilizado a nivel mundial por todas las Organizaciones que desean auditar y certificar sus capacidades en gestión del servicio; así pues, mientras que la norma ISO/ IEC 2000 se debe cumplir y mantener, ITIL proporciona una estructura de conocimiento útil para cumplir el estándar (Office of Government Commerce, 2010).

A continuación, en la figura 3 se puede observar el núcleo de ITIL, el cual contiene una guía de mejores prácticas aplicables a todo tipo de Organización que proporcionen servicios para un negocio que consta de: estrategia, diseño, transición, operación y mejora continua del servicio.

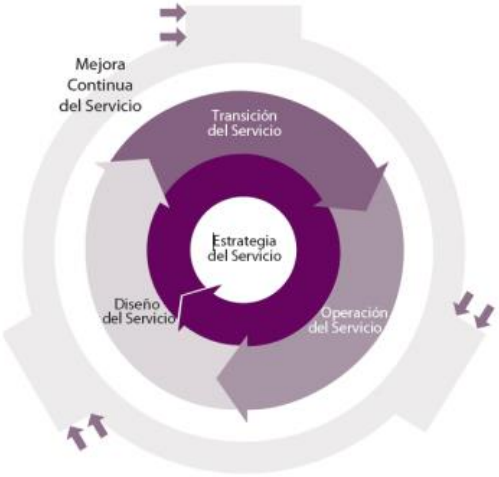


Figura 3. Núcleo de ITIL
Fuente: (Office of Government Commerce, 2010)

RFC 2196

El estándar RFC2196 también es un estándar usado para la ejecución y mejora en la seguridad de la información. Entre las características y componentes más relevantes es importante el establecimiento de la puesta en marcha mediante procedimientos descritos de administración de sistemas, la difusión de guías sobre el uso aceptable de los recursos informáticos o por medio de la practicidad de métodos que sean conveniente para cada caso; debe permitir que en la implantación; se obligue al cumplimiento de las actividades vinculadas mediante herramientas de seguridad; que permita la detección de fugas o errores; y establecer de forma clara cuáles son las áreas responsables de los usuarios, administradores y dirección, y en cualquier eventualidad que exista poder determinar a un responsable. A continuación, se describen en resumen los componentes en los cuáles RFC-2196 se basa y donde se establecen directrices para la política de seguridad de la información (RFC2196, 2018):

- Evaluación de riesgos
- Identificación de los activos:
    - Hardware
    - Software
    - Datos
    - Personas
    - Documentación
    - Suministros
- Identificación de las amenazas
- Políticas de seguridad
    - ¿Qué es una política de seguridad y por qué tener una?
        - Definición de una política de seguridad
        - Propósitos de una política de seguridad
        - ¿Quién debería participar cuando se formule la política?
    - ¿Qué hace una buena política de seguridad?
    - Mantener la política flexible
- Arquitectura
    - Planes de seguridad completamente definidos
    - Separación de servicios
    - Denegar todo / Permitir todo
    - Identificar necesidades reales de servicios
    - Configuración de red y servicio
        - Protegiendo la infraestructura
        - Protegiendo la red
        - Protegiendo los Servicios
        - Protección de la protección
- Servicios y procedimientos de seguridad.
- Autenticación
- Confidencialidad
- Integridad
- Autorización
- Acceso
- Auditoría
- Asegurando copias de seguridad
- Manejo de incidentes de seguridad
- Notificación y Puntos de Contacto
- Identificación de un incidente
- Manejo de un incidente
- Contención
- Responsabilidades

Marco legal y jurídico respecto a la seguridad de la información en Latinoamérica.

Sánchez & Rojas (2012) señalan que en algunos países del mundo existe la motivación de implantar normas, leyes o procedimientos que establezcan los términos, aprobaciones y sanciones pertinentes referentes al uso apropiado de los datos almacenados en los distintos sistemas de información; principalmente en la información clasificada como sensible, en donde se busca mantener su disponibilidad, integridad y confidencialidad. Teniendo en cuenta que cuanto más grande es el desarrollo de una sociedad, existe mayor dependencia hacia la tecnología; por lo tanto, existe un alto índice de vulnerabilidad y riesgo de que ocurran incidentes de seguridad de la información (Borbúa, Herrera & Reyes, 2017).

El marco del consejo de defensa suramericano (en adelante CDSA) anualmente promueve realizar un plan de acción en el que se desarrollen políticas de defensa, cooperación militar, acciones humanitarias y operaciones de paz, industria, tecnología, formación y capacitación, conformando un grupo de trabajo que busca "establecer una política y mecanismos regionales para hacer frente a las amenazas cibernéticas e informáticas en el ámbito de la defensa". A continuación, se enfatiza en el estatuto y normas que rigen en el Sistema de Defensa Nacional de tres países que integran el CDSA: Colombia, Argentina y Brasil en procura de la seguridad de la información (Justribó, 2014).

Colombia

En el año 2011 el gobierno colombiano aplicó el Consejo Nacional de Política Economía Social (CONPES 3701), basada en los lineamientos de política en temas de ciberseguridad y ciberdefensa de Colombia, cuyos aspectos técnicos están a cargo de tres instituciones: El Centro Cibernético Policial (CCP), Comando Conjunto Cibernético (CCOC) y el colCERT (Equipo de Respuesta a Emergencias Informáticas de Colombia) entidad coordinadora a nivel nacional que supervisa todos los aspectos de la Ciberseguridad y la Ciberdefensa; colocando a Colombia como pionero en Latinoamérica en temas de ciberseguridad y ciberdefensa, al 2016 el Gobierno Nacional emite el CONPES 3854 incluye la gestión de riesgos como uno de los temas más importantes en seguridad digital (Cáceres, 2017).

El Decreto 1704 (2012), hace referencia a la cooperación y el intercambio de información entre el sector privado y autoridades del gobierno, en donde se establecen los lineamientos a seguir por los proveedores de redes y telecomunicaciones con el objetivo de salvaguardar, oportuna y eficazmente la labor de las autoridades nacionales; un claro ejemplo de ello fue la colaboración de países como: Argentina, Brasil, Chile, Costa Rica, Ecuador, Uruguay, Venezuela y España con las autoridades nacionales de Colombia auspiciados por el Grupo de Trabajo Latinoamericano Sobre Delitos Tecnológicos de INTERPOL, con el objetivo de identificar usuarios que intercambiaban y distribuían contenido de pedofilia online (Leiva, 2015).

Argentina

Mediante Decreto 1028 en el 2003, se le confiere a la Oficina Nacional de Tecnologías de la Información (ONTI), el compromiso de comprender y acoplar las directrices en temas de protección de datos y privacidad y seguridad de la información digital, así con disposición administrativa N° 669 del 2004 resultó el primer y un gran avance en materia de seguridad de la información, implantando la "Política de Seguridad Modelo", que fue reemplazada mediante la Disposición ONTI N° 3/2013; complementando mediante Resolución N° 351 del 2014 el Ministerio de Defensa creó el Comando Conjunto de Ciberdefensa encargado de la ciberdefensa (Justribó, 2014).

Borghello & Temperini (2013) en simposio Argentino de Informática y Derecho, señala que mediante decisión Administrativa 669/2004, se determina en artículo 1° que "los organismos del Sector Público Nacional comprendidos en los incisos a) y c) del artículo 8° de la Ley N° 24.156 y sus modificatorias, deberán dictar o bien adecuar sus políticas de seguridad de la información a la Política de Seguridad Modelo, dentro del plazo de CIENTO OCHENTA (180) días de aprobada ésta última".

En Resolución 1107-E/2017 se crea el comité de respuestas a incidentes de seguridad informática, formando parte del ministerio de seguridad, en el que se indica textualmente que las funciones del comité serán: "Proteger los activos de información de su comunidad objetivo y promover la conciencia en materia

de seguridad de la información, intentando reducir la probabilidad y la gravedad de los incidentes que puedan comprometer significativamente la seguridad de los sistemas y redes respondiendo de manera rápida y eficaz, reactiva y proactivamente" (ESET, 2017).

Brasil

La normativa a nivel Nacional que reconoce el derecho de acceso a la información pública se encuentra en la Ley 12.527/2011 de la LAI (Ley de Acceso a la Información), cuyo alcance es que toda información de gobierno es pública; por lo tanto, puede ser solicitada por los ciudadanos, siendo está clasificada por: información pública, reservada, secreta y ultra secreta (Contraloría General de la Unión, 2016).

Leiva (2015) señala que existe un acuerdo entre la Policía Federal (más adelante DPF) y Microsoft, en el que Microsoft le proporciona al DPF la información del registro de usuarios de sus servicios, cuando éste le solicita a través de un formulario electrónico, además las autoridades indican que Brasil tiene un sector que desarrolla software de ciberseguridad personalizadas tanto para entidades privadas como públicas; además, la política de seguridad de la información que pertenece a las Agencias de la Administración Pública Federal es otro mecanismo de seguridad de gran importancia, cabe recalcar que la RENASIC (Red Nacional de Seguridad de la Información y Criptografía) funciona como el ente de intercambio de información bajo la coordinación del Gabinete de Seguridad Institucional de la Presidencia de la República (Justribó, 2014).

Ecuador

Esquema Gubernamental de Seguridad de la Información

La Secretaria Nacional de Administración Pública (en adelante SNAP) mediante Registro Oficial Suplemento 88 de 25-sep-2013 emitió el acuerdo Ministerial 166 del esquema gubernamental de seguridad de la información (en adelante EGSI), en la que acuerda en su Artículo 1 "Disponer 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" y en su Artículo 2 donde indica que las entidades de la administración Pública deberán implementar en un plazo de 18 meses el Esquema Gubernamental de Seguridad de la Información (EGSI), de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información; cabe señalar que existen 749 hitos entre los cuales se desglosan los prioritarios u obligatorios y además los opcionales que deben ser implementados por las instituciones estatales (Lexisfinder, 2013).

Mediante Decreto Ejecutivo Nro. 5, suscrito el 24 de mayo del 2017, el Presidente de la República del Ecuador, en funciones, suprimió la SNAP, y transfirió las atribuciones que le correspondían a varias entidades; una de ellas es el Ministerio de Telecomunicaciones y de la Sociedad de la Información (en adelante Mintel), de acuerdo con el Decreto mencionado a partir del 1 de agosto del 2017, esta Secretaría de Estado está a cargo de gestionar todos los trámites vinculados a la Subsecretaría de Gobierno Electrónico, que tiene a su cargo las siguientes competencias (Mintel, 2017):

1. Gestionar la política y directrices emitidas para la gestión de la implementación del Gobierno Electrónico; y,
2. Desarrollar y coordinar planes, programas y proyectos sobre Gobierno Electrónico, que sean necesarios para su implementación.

La autoevaluación del EGSI se llevó a cabo por varias entidades de la función ejecutiva, en el que el 85.34% de las instituciones reportaron un buen nivel de cumplimiento en la autoevaluación; para corroborar estos datos reportados por las instituciones, MINTEL realizó la evaluación a 55 entidades de las que solo el 16.36% obtuvo un resultado bueno en el cumplimiento del EGSI, el 65,45% logró un resultado regular; mientras, que el 7,27% obtuvo una calificación mala, y el 10,91%, muy mala, tal como se lo puede apreciar en la figura 4 a continuación:

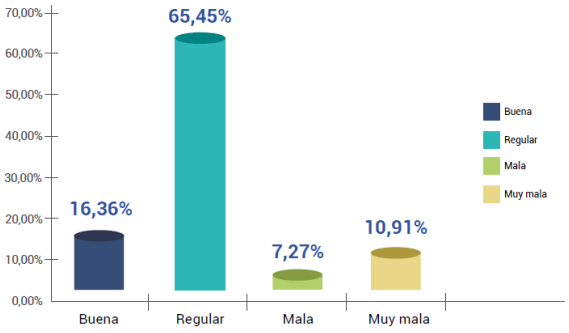


Figura 4. Cumplimiento del EGSI en las Instituciones Públicas
Fuente: (MINTEL, 2017)

LOTAIP

La Ley Orgánica de Transparencia y Acceso a la Información Pública (por sus siglas LOTAIP) en su artículo 1 señala el principio de publicidad de la Información Pública, en la que indica que el Estado garantiza a las personas el derecho de acceso a la información pública; este artículo entra en concordancia con el Articulo 18 de la Constitución de la República del Ecuador, la Ley Orgánica de la Contraloría General del Estado en sus artículos 46, 49, 76, 80 y 81, y Código Orgánico de Planificación Finanzas Públicas en su artículo 174. (Lexis, 2004)

Constitución de la República del Ecuador

En la Constitución de la república del Ecuador en su artículo 18 numeral 2 indica: "Todas las personas, en forma individual o colectiva, tienen derecho a:
Acceder libremente a la información generada en entidades públicas, o en las privadas que manejan 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" (Constituyente, 2008).

Normas de Control interno de la Contraloría General del Estado

En las normas de control interno de la Contraloría General del Estado en su artículo 410-10 indica:

"410-10 Seguridad de tecnología de información
La Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:

1. Ubicación adecuada y control de acceso físico a la Unidad de Tecnología de Información y en especial a las áreas de: servidores, desarrollo y bibliotecas.
2. Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado.
3. En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación.
4. Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización.
5. Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.
6. Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire controlado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros;
7. Consideración y disposición de sitios de procesamiento alternativos.
8. Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana (Contraloría General del Estado, 2009).

A continuación, en la tabla 1 se muestran a manera de resumen las normativas o estándares que aplican algunos Países de Latinoamérica respecto a la seguridad de la información:

Tabla 1
Estándares de seguridad de la información aplicados en Países de Latinoamérica

PAÍS	ESTANDAR/NORMA SEGURIDAD DE LA INFORMACIÓN	BASE LEGAL	INSTITUCIONES QUE INTERVIENEN	LINK
ECUADOR	EGSI (Basado en la INEN ISO/IEC 27002)	ACUERDO N° 166	MINTEL INEN (Instituto Ecuatoriano de Normalización)	https://www.politica.gob.ec/wp-content/uploads/2017/04/EGSI.pdf

PAÍS	ESTANDAR/NORMA SEGURIDAD DE LA INFORMACIÓN	BASE LEGAL	INSTITUCIONES QUE INTERVIENEN	LINK
COLOMBIA	SGSI NTC-ISO/IEC 27001 MSPI (MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN)	Decreto 1078 de 2015	MINTIC (Ministerio de Tecnologías de la Información y las Comunicaciones) ICONTEC (Instituto Colombiano de Normas Técnicas y Certificación)	http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf
ARGENTINA	ISO/IRAM 17799 ETAP (Estándares Tecnológicos para la Administración Pública)V23	Decreto N° 2645/2014 (PRICNICPIOS DEL SISTEMA DE DEFENSA) Resolución MD N° 781/2015 (POLITICA DE SEGURIDAD)	IRAM (Instituto Argentino de Normalización)	https://www.scribd.com/document/62568152/Argentina-Iso-17799
PERÚ	NTP ISO/IEC 17799: 2007 EDI	Decreto Nº 1412/2018 Resolución Nº 004-2016-PCM	OGTI (Oficina General de Tecnologías de la Información) ONGEI (Oficina Nacional de Gobierno electrónico e Informática)	http://spij.minjus.gob.pe/Graficos/Peru/2007/agosto/25/RM-246-2007-PCM_25-08-07.pdf
MÉXICO	SGSI NMX-I-27001-NYCE-2009	Ley Orgánica de la Administración Pública Federal Arts. 34 fracciones XIII y XXXI	Dirección General de Normas Normalización y Certificación Electrónica, A.C.(NYCE)	http://www.jmcti.org/kaigai/Latin/2010/2010_03/2010_03_M01.pdf
CHILE	PNCS (POLITICA NACIONAL DE CIBERSEGURIDAD)	Ley Nº 19.223 Ley Nº20.285 Decreto D.S. Nº1/2015	CSIRT (Seguridad de la Red de Conectividad del Estado) CICS (Comité Interministerial sobre Ciberseguridad) MTT (Ministerio de Transportes y Telecomunicaciones) MISP (Ministerio del Interior y Seguridad Pública)	https://www.ciberseguridad.gob.cl/media/2018/06/PNCS_Chile_ES_FEA.pdf
URUGUAY	Marco de Ciberseguridad de AGESIC	Ley 18.331	Todas las instituciones del Estado de Uruguay	https://www.agesic.gub.uy/innovaportal/file/5823/1/marco-de-ciberseguridad-4.0-completo.pdf

Fuente: *Elaboración propia, 2019*

Gestión de la Seguridad de la información a nivel de Latinoamérica

Eset (2018) en su página oficial publicó el Eset Security Report Latinoamérica 2018, en el que muestra un informe de la perspectiva actual de seguridad de la información en las empresas de Latinoamérica, tomando como referencia a partir del año 2015 al 2017, donde refleja un aumento de empresas que cuentan con un área de gestión de seguridad tal como se puede apreciar en la siguiente figura:

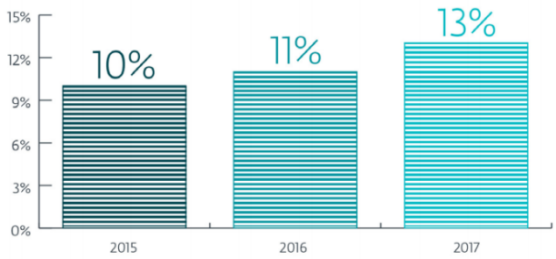


Figura 5. Empresas en Latinoamérica que cuentan con un área de gestión de seguridad
Fuente: (Eset, 2018)

De acuerdo a los datos publicados por Eset en el año 2017 hubo una reducción del presupuesto en las empresas para inversión en materia de seguridad, se presentan grandes expectativas a futuro en temas de concientización en el que el usuario cumple un rol fundamental, dicho estudio indica que más del 75% de las empresas ejecutan acciones de seguridad periódicamente y un 11% piensa implementarlas; es importante indicar que el término seguridad no solo se refiere a la aplicación de controles basados en tecnología, sino también a las políticas, estándares, normativas, plan de gestión y/o auditorías que reflejen cual el estado de la seguridad de la empresa, en la figura 6 se muestran los niveles de implementación de los controles basados en seguridad.

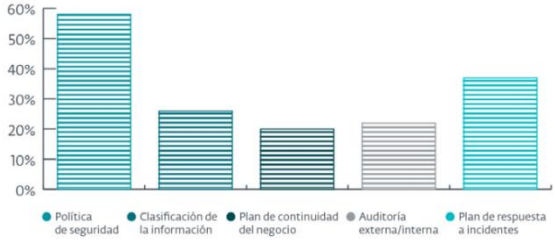


Figura 6. Adopción de controles basados en gestión
Fuente: (Eset, 2018)

Como se puede apreciar en la figura 6, la política de seguridad es una parte fundamental que toda empresa debe cumplir como parte de la seguridad de la información, sin embargo, es necesario desarrollar una cultura de seguridad y concientizar tanto al personal interno como externo de la institución sobre el uso y aplicación de la misma, de manera que se pueda lograr resultados más efectivos, contribuyendo a mantener a buen recaudo el activo más importante de la Institución como lo es la información.

Olmedo & Gavilánez (2018) señalan que el delito cibernético que golpeó últimamente a Latinoamérica, afectando grandemente a Ecuador, fue Pokémon GO, en la que los usuarios instalaban otras versiones de la aplicación, al no poder instalar la aplicación oficial que contenía un sistema de seguridad de la información; los países Latinoamericanos en su gran mayoría buscan implementar o reforzar la protección de datos y la privacidad, sin embargo no cuentan con los recursos necesarios, a pesar del gran esfuerzo y colaboración por parte del gobierno en reforzar la infraestructura, implementación de normativas, centros de protección, entre otros; aún queda mucho por hacer en el ámbito de seguridad informática.

Por su parte Deloitte (2016) realizó una encuesta sobre las tendencias en gestión de seguridad de la información y ciberriesgos en Latinoamérica, en el que de acuerdo a los resultados obtenidos en la encuesta en los últimos dos años cada cuatro de diez Organizaciones se han visto afectadas por una brecha de seguridad, por lo que los desafíos más grandes para las empresas en Latinoamérica, resaltan la implementación de capacidades de monitoreo de riesgos, brechas de seguridad de la información y respuesta ante incidentes; los países participes en este estudio fueron 13, entre ellos: Argentina, Chile, Colombia, Costa Rica, Ecuador, El salvador, Guatemala, México, entre otros, con 89 Organizaciones y 7 Industrias o sectores diferentes, dicho estudio reflejo los siguientes resultados:

- El 16% de las Organizaciones no cuenta con un ejecutivo responsable de gestionar los ciberriesgos y seguridad de la información.
- El 51% de ejecutivos de ciberriesgos y seguridad de la información, consideran que el principal obstáculo que tienen para desarrollar su estrategia es la falta de suficientes recursos.
- El 35% de las Organizaciones no cuenta con un tablero de control.
- El 39% de las Organizaciones no mide el retorno de la inversión en ciberriesgos y seguridad de la información.
- El 51% de las Organizaciones indicaron que han implementado como medida, sensibilizar y capacitar sobre las políticas y recomendaciones acerca de la privacidad de datos, sin embargo, tal como reporta en su publicación Deloitte (2016) en Latinoamérica, aún falta desarrollar capacidades para identificar y clasificar la información, de manera que se garantice la privacidad de los datos personales.

La Agencia de Gobierno electrónico y Sociedad de la Información y del Conocimiento de Uruguay (AGESIC) contemplando el desarrollo del gobierno electrónico en lo que respecta a las administraciones públicas ha identificado los temas centrales como el acceso a la información pública, la protección de datos personales, firmas electrónicas y un marco

general que consagra el derecho de un ciudadano a ser capaz de interactuar con el gobierno por medios electrónicos y la obligación de las entidades gubernamentales de trabajar juntas, siendo lo más importante la creación de un marco institucional como factor clave para llevar la sostenibilidad a las políticas públicas conformadas por los canales normativos descritos anteriormente manteniendo la autoridad legal a nivel del todo el territorio nacional que cubre aspectos como la seguridad de la información, el uso de la información, recursos del gobierno, intercambio de información entre entidades públicas, entre otras (Navarro, 2011).

Es importante señalar que para reducir en la medida de lo posible estas cifras, es necesario identificar el activo de la información y clasificarlo, de acuerdo a las evaluaciones realizadas revisar las amenazas que puedan llegar a materializarse en algún momento y puedan dañar la información; por ello, es recomendable tomar acciones, implementar planes de contingencia y de continuidad, establecer controles de seguridad, realizar mejora a los procedimientos, monitoreo continuo y concientizar al personal; las vulnerabilidades, riesgos y amenazas han ido en aumento en todas las partes del mundo, los malware y riesgo de la seguridad digital han ido a la par con el proceso de desarrollo; el enfoque principal de las Instituciones ha sido Gestionar los riesgos de ciberseguridad, en este ámbito Colombia ha sido uno de los Países considerado como líder de la ciberseguridad en Latinoamérica, tomando como estrategia en las fuerzas del estado, desarrollar actividades centralizadas (Linares, 2018).

Instituciones públicas seleccionadas para el caso de estudio.

El Servicio de Rentas Internas (más adelante SRI) nació el 2 de diciembre de 1997 basándose en los principios de justicia y equidad, por la esquivación tributaria, debido a la ausencia de la cultura tributaria; cuya misión es gestionar la política tributaria, asegurando la recaudación destinada al fomento de la cohesión social. Destacándose al ser una institución autónoma en la definición de políticas y estrategias de gestión que han permitido que se maneje con equilibrio, transparencia y firmeza en la toma de decisiones, aplicando de manera transparente tanto sus políticas como la legislación tributaria (Servicio de Rentas Internas, 2018). A diferencia del Servicio Nacional de Aduana del Ecuador (en adelante Senae), ésta última institución es más antigua, conociéndose sus primeras competencias alrededor de 1830, sus facultades hasta ese entonces estaban basadas únicamente en el traslado de personas y los vehículos en los cuales se movilizaban. En la actualidad Senae es una empresa estatal, autónoma y moderna, orientada al servicio. Es parte activa del quehacer nacional e internacional, siendo facilitadores del Comercio Exterior, con un alto nivel profesional, técnico y tecnológico. Adicionalmente, la misma está en constante innovación, y perfeccionamiento de los procesos, con el objetivo de brindar la mejor calidad en el servicio al usuario (Servicio Nacional de Aduana del Ecuador, 2018).

El Servicio de Rentas Internas a partir del año 2000, entró en un proceso de evolución, con enfoque hacia la incorporación de la tecnología para mejorar los procesos, la atención a la ciudadanía y la agilización en trámites. En cumplimiento a lo dispuesto por la SNAP en el acuerdo Ministerial 166, el SRI implementó las directrices prioritarias establecidas en el EGSI, así como las actividades que se encuentran establecidas en el mencionado acuerdo; esto reducirá significativamente amenazas, riesgos y vulnerabilidades relacionadas a la gestión de la información, tanto física como electrónica que procesa la Institución. Así mismo, contribuirá al proceso de mejora continua, incrementando la cultura de los servidores públicos en manejo de la información que utilizan para cumplir sus roles y actividades asignadas. Tal como lo señala el informe de gestión del SRI que comprende el periodo de enero a diciembre del 2017 constan con la matriz de riesgo de seguridad de la información, tomando como base la Norma Técnica Ecuatoriana INEN-ISO/IEC 27005 y sus anexos, conforme lo establece el EGSI (Servicio de Rentas Internas, 2018).

En referencia al Estado Colombiano la viceministra general encargada de las funciones del Despacho del Ministro de Tecnologías de la Información y las Comunicaciones (más adelante MINTIC), María Carolina Hoyos Turbay (2015) mediante Decreto 1078 expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, el cual abarca la estrategia de Gobierno en línea, cuyo objetivo es definir los lineamientos y plazos de estrategia, con el fin de contribuir a la construcción de un Estado abierto, transparente y participativo. El MINTIC

establece un modelo de seguridad y privacidad de la información (en adelante MSPI) en el marco de la estrategia de gobierno en línea vs. 3.0.2 cuya última actualización fue en Julio del 2016, que debe ser adoptado por las entidades públicas de orden Nacional y territorial, así como proveedores de servicio en línea (MINTIC, 2016).

El MSPI es un modelo de evaluación del Gobierno en Línea, cuya herramienta fue diseñada para medir el nivel de madurez y mejorar los estándares de seguridad de la información en el sector gubernamental, el cual está basado en la norma ISO 27001 vs. 2013, en cumplimiento al Decreto 1078, con el fin de garantizar la privacidad de los funcionarios y ciudadanos de acuerdo a la normativa Colombiana, este modelo consta de cinco fases que comprenden la fase de diagnóstico, planificación, implementación, gestión y mejora continua; cada una de estas fases proporcionan instrumentos o guías para crear un SGSI adecuado para las Instituciones, tal como se observa en la siguiente figura:

Figura 7. MSPI
Fuente: (MINTIC, 2016)

La Dirección de Impuestos y Aduanas Nacionales (en adelante DIAN) es la entidad Colombiana que nació de la fusión de la Dirección de impuestos Nacionales y la Dirección de Aduanas Nacionales en 1993, cuyo propósito es garantizar la seguridad fiscal, la administración y control al debido cumplimiento de las obligaciones tributarias, aduaneras y cambiarias, así como la facilitación de las operaciones de comercio exterior en condiciones de equidad, transparencia y legalidad; en la actualidad Tiene 50 direcciones seccionales, 30 de Impuestos y Aduanas, 6 de Aduanas, 7 de Impuestos y 7 Direcciones Seccionales Delegadas de Impuestos y Aduanas (DAPRE, 2017).

La DIAN es una Institución que abarca muchas direcciones, por lo tanto, involucra grandes cantidades de dinero en recaudación de impuestos, por ello debe ser transparente y legitima ante los contribuyentes. Sin embargo, tal como lo pública el medio de comunicación "*semana*" en noviembre del 2013, la DIAN se ha visto envuelta en temas conflictivos y de corrupción, como es el caso de la falta de sistemas de control que eviten que un funcionario mal intencionado pueda eliminar las deudas de los contribuyentes, colaborando a evadir la recaudación o desviando los recursos del estado a cuentas falsas; por cuanto, es necesario implementar en la Institución sistemas informáticos robustos, que refuercen la seguridad de la institución y así evitar las conocidas caídas del sistema cuando ingresan ciertos cargamentos (Semana, 2013).

Es por ello, que las autoridades de conformidad con la norma técnica alineada a las directrices entregadas por MINTIC a través del Modelo de Seguridad y Privacidad de la Información, regulada en el Decreto 1078, el Ministerio de Hacienda y Crédito Púbico en Decreto 2184 del 23 de diciembre del 2017 dispone crear la oficina de seguridad de la información para la DIAN (Cárdenas & Caballero, 2017). Por lo que, en el código de buen gobierno y de ética de la Unidad Administrativa Especial DIAN (2016), en el literal 3.3.2 se detallan las Políticas Específicas para el sistema de gestión de seguridad de la información, en el que se indica que: "La Dirección de Impuestos y Aduanas Nacionales - DIAN protege la información creada, procesada, transmitida o resguardada por sus procesos de negocio y activos de información que hacen parte de los mismos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia" (DIAN, 2016); la información se encuentra clasificada como Reservada y Clasificada según su contenido, tal como se puede observar en el Anexo 3.

Por otra parte, el Gobierno de Chile mediante Decreto Supremo N° 83/03.06.04 del Ministerio Secretaría General de la Presidencia aprobó la norma técnica Chilena

ISO 27001/2013, la cual debe ser aplicado por las Instituciones Estatales, con el objetivo de salvaguardar los activos de información y mantener la continuidad del negocio. En atención a lo dispuesto en el mencionado Decreto, el Servicio Nacional de Aduanas (2018) encargado de la Fiscalización del ingreso y salida de mercancías del País Chileno mediante resolución exenta N° 2782 publicada el 22 de junio del 2018 y sumillada por el Director Nacional de Aduanas, Claudio Sepulveda Valenzuela en la que se realizan mejoras a la política general de la seguridad de la información, el cual debe ser cumplido estrictamente por todos los funcionarios de la Institución.

Como parte del proceso de modernización, el Servicio Nacional de Aduanas implementó el sistema de selección de cargas (CTS), este software es una herramienta automática cuyos datos electrónicos facilitan a los funcionarios de Aduanas identificar cargas peligrosas, siendo ésta una herramienta fundamental para analizar los tramites de importación, exportación y transbordos de la mercancía que entra y sale del país Chileno, de manera que se pueda identificar las cargas de alto riesgo de una forma más eficiente, efectiva y oportuna (Aduanas Chile, 2017).

METODOLOGÍA

Este trabajo investigativo aplica una metodología con enfoque cualitativo, en el que se realiza un estudio comparativo entre dos Instituciones públicas Senae y SRI en cuanto al nivel de seguridad de la información que manejan en referencia a Instituciones símiles a nivel Latinoamericano; para identificar el nivel de aplicación del EGSI a través del check list, herramienta que permitirá identificar los controles existentes en las Instituciones y evaluar el nivel de cumplimiento del mismo, para posteriormente recomendar buenas prácticas aplicables en ambas entidades con el objetivo de salvaguardar el activo más importante de la Institución como es la información.

Las Instituciones Públicas analizadas en este estudio: Senae y SRI, tal como se lo indico anteriormente, se basan en el EGSI en el cual refiere en su artículo 1 el uso obligatorio de las Normas técnicas Ecuatorianas NTE INEN-ISO/IEC 27000; en base a esto el SRI ha cumplido hasta el año 2018 con todos los hitos obligatorios (311) que se especifican en dicho acuerdo, por su parte el Senae tiene en la actualidad actividades en ejecución de dicho esquema y de acuerdo al nivel de cumplimiento posee aproximadamente un 70% de ejecución de los hitos prioritarios, este dato fue ponderado de los resultados de la evaluación del check list realizado al personal directivo de TI (ver anexo), calificando con un nivel de cumplimiento como: ALTO, MEDIO o BAJO, además otro método utilizado fue la observación y entrevista para el levantamiento de información que no fue posible obtener a través del check list.

La primera fase de la metodología fue realizar el check list a los directivos de TI en ambas Instituciones, se incluyeron sólo los 2 primeros hitos que hacen referencia a la política y organización de la seguridad de la información; luego se realizó la entrevista al oficial de seguridad de la información y por último se constató que cumplan con los lineamientos indicados en el EGSI, enfocados en la seguridad de la información.

El objetivo principal de este estudio comprende en la propuesta de mejores prácticas en procura de la seguridad de la información de las Instituciones seleccionadas, para ello se elaboró un grupo focal con expertos en el área de seguridad de la información, en el que se presentaron los casos de estudios y análisis de la propuesta, el cual permitirá realizar un análisis contemplando las variables que se han obviado en la implementación del esquema actual relacionado a la seguridad de la información digital y potenciales riesgos que deberán ser mitigados de acuerdo a la propuesta de mejores prácticas.

Evaluación de cumplimiento del EGSI a las Instituciones del caso de estudio

Para la evaluación de cumplimiento del EGSI, se consideraron las 2 primeras directrices del acuerdo ministerial 166 que se enfocan en la seguridad de la información; a continuación, en la tabla 2 se detalla en cada uno de los puntos el análisis realizado en las dos Instituciones del caso de estudio Senae y SRI, en el que se establece el nivel de cumplimiento del EGSI para cada ítem:

Tabla 2
Cumplimiento EGSI en SRI y Senae

Porcentaje de cumplimiento de seguridad de la información en Instituciones Públicas del Caso de Estudio SENAE y SRI		
EGSI	**%**	**OBSERVACIONES**
1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		
1.1. Documento de la Política de la Seguridad de la Información.	SRI: 100% Senae: 70%	La política de seguridad de información implementada en las dos instituciones se enmarca a nivel general, sin especificaciones especiales para los departamentos de TI, es decir que es una política generalizada para todas las áreas ya sea en planta central como en las unidades descentralizadas que estas instituciones poseen a nivel nacional. Con relación a Senae, la Política de Seguridad de la Información no ha sido difundida en su totalidad, el conocimiento de la misma lo poseen los servidores que se encuentran ubicados en planta central (Guayaquil) y en las unidades descentralizadas existe desconocimiento de dicha política. Cabe destacar que se verificó que Dirección Nacional de Tecnología del SRI mantiene lineamientos y/o propios para cada proceso o subproceso que realizan de acuerdo al tipo de información que se ha clasificado y clasificado por el Departamento de Seguridad Institucional de dicha entidad.
1.2 Revisión de la Política	SRI: 100% Senae: 50%	La política de seguridad de la información del SRI se mantiene en constante revisión, siendo ésta adecuada a las necesidades que las áreas de la institución, así lo requieran; sin embargo, la política de seguridad de información del Senae se encuentra en etapa de actualización y reestructuración, debido a que de acuerdo a los nuevos procesos que han sido implementados en la institución, éstos dejan obsoleta a la política que hasta finales de 2017 estaba implementada.
2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
2.1. Compromiso de la máxima autoridad de la institución con la seguridad de la información	SRI: 100% Senae: 70%	El compromiso por parte de la máxima autoridad en el SRI se ha consolidado durante los últimos diez años, siendo una responsabilidad heredada desde la Dirección General hasta las coordinaciones, las cuales permite que la responsabilidad sea generalizada. En el caso de Senae se dispuso desde el año 2017 por parte de la Dirección General el compromiso no sólo de la máxima autoridad, sino también de sus delegados con el fin de que la responsabilidad que se enmarca en lo relacionado a la seguridad de la información se institucionalice, sin embargo se evidenció que existe desconocimiento y falta de compromiso por parte de los servidores, que no se encuentran sensibilizados con esta problemática.
2.2. Coordinación de la Gestión de la Seguridad de la Información	SRI: 95% Senae: 45%	Mediante coordinación interna usando memorandos físicos y el sistema de Gestión Documental Quipux se gestionó por parte de las máximas autoridades la directriz del EGSI que indica las coordinaciones necesarias para que la Gestión de la Seguridad de la Información sea efectiva, mediante las herramientas anteriormente indicadas se establecieron los nombres de los servidores que integran el comité de cada institución y el oficial designado. Es importante mencionar que en relación al Senae han existido cambios de los directivos desde la fecha del

Porcentaje de cumplimiento de seguridad de la información en Instituciones Públicas del Caso de Estudio SENAE y SRI		
EGSI	**%**	**OBSERVACIONES**
		levantamiento de la información (año 2017) hasta la presentación del presente artículo, estos cambios de autoridades y por ende de los equipos de trabajo podrían generar discontinuidad en el seguimiento y monitoreo de las directrices que dispone el EGSI, al ser cambiante el oficial de cumplimiento dentro de la institución, por lo que el mismo deberá entrar en una curva de aprendizaje antes de poder evaluar y coordinar con las áreas involucradas el cumplimiento del actual esquema.
2.3 Asignación de responsabilidades para la seguridad de la información	SRI: 100% Senae: 50%	En las dos Instituciones se cuenta con un oficial designado para el EGSI y el delegado de TI, sin embargo tal como se describió en la observación de la directriz anterior, es necesario que el oficial de cumplimiento sea transversal en su gestión indiferente de las autoridades en curso, para evitar atrasos o deficiencias por desconocimiento de los procesos y de las áreas agregadoras de valor que son las principales generadoras de la información que se maneja en la institución.
2.4 Proceso de autorización para nuevos servicios de procesamiento de la información	SRI: 95% Senae: 40%	En el SRI existe un proceso de autorización para signar un custodio o responsable para cualquier nuevo servicio o área de negocio que exista o que se requiera implementar, estos responsables están definidos a nivel técnico brindando soporte a nivel de TI y también existen responsables a nivel de conocimiento del área o proceso relacionado al negocio de la entidad gubernamental, para definir a los responsables técnicos como de negocio, el Departamento de Inteligencia de la Información levanta la necesidad de la información de forma detallada y de acuerdo al uso transversal o vertical que tenga dicha información coordina con los procesos y las responsabilidades. El detalle de los responsables con el servicio o área de negocio es transparente para todos los servidores de la institución, con el fin que puedan acceder mediante mecanismos de autorización a la información o servicios que custodian, sin embargo, en la evaluación de este ítem se pudo identificar, que la difusión de este proceso como la actualización de los responsables en la intranet de la institución, no estaría actualizado, lo que muchas veces ocasiona confusión en los usuarios. En el Senae los mecanismos de autorización son básicos y poco documentados, o archivados de forma manual lo que impide tener la trazabilidad y verificación posterior de las autorizaciones a accesos.
2.5. Acuerdos sobre Confidencialidad	SRI: 95% Senae: 70%	En el SRI desde hace aproximadamente diez años se maneja acuerdos de confidencialidad y de exclusividad laboral, los mismos que se sociabilizan con las personas antes inclusive que sean servidores públicos del SRI, el estricto cumplimiento de lo que estipula dicho acuerdo es competencia del Departamento de Seguridad Institucional del SRI. En relación al Senae este tipo de acuerdo de confidencialidad se puso en práctica a partir del 2017; sin embargo, el 30% de los empleados no colaboraron con la aceptación del mismo, aduciendo que dichos acuerdos vulneran sus derechos porque los mismos establecen las sanciones en el caso que se determine alguna irresponsabilidad.
2.6 Contacto con las autoridades	SRI: 95% Senae: 95%	Tanto en el Senae como en el SRI se cumple con el literal c), en el cual se especifica que es necesario identificar y mantener los contactos de los proveedores de servicios, principalmente con aquellos relacionados a telecomunicaciones e internet.
2.7 Contactos con	SRI: 5%	En el análisis del cumplimiento de este ítem, se determinó que

Porcentaje de cumplimiento de seguridad de la información en Instituciones Públicas del Caso de Estudio SENAE y SRI		
EGSI	**%**	**OBSERVACIONES**
grupos de interés especiales	Senae: 5%	ninguna de las instituciones poseía documentación para respaldar que existe efectivamente un monitoreo constante de alertas a nivel de organizaciones similares dentro y fuera del país y que los oficiales de cumplimiento se comuniquen entre entidades públicas con el fin de mantenerse informados acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.
2.8 Revisión independiente de la seguridad de la Información	SRI: 95% Senae: 0%	En el SRI se mantiene en portafolio de proyectos iniciativas que encaminadas a realizar auditorías internas en relación al diagnóstico y determinación de riesgos asociados a la seguridad de la información, sin embargo no se han podido ejecutar debido a la falta de presupuesto en la entidad, en el caso del Senae no se evidenció en el portafolio del proyecto ninguna iniciativa relacionada a esta temática.
2.9 Identificación de los riesgos relacionados con las partes externas	SRI: 100% Senae: 75%	En el SRI si se cumple con esta directriz, debido a que se presentó documentación y la matriz de sujetos y entidades externas de contratos de servicios con esta institución, adicionalmente para todo tipo de estos servicios existe la documentación de respaldo, ya sean éstos, acuerdos interinstitucionales o acuerdo públicos-privados que son autorizados por las máximas autoridades o su delegado. En el caso de Senae existen ciertas deficiencias porque no se determinan claramente las responsabilidades desde las partes externas cuando se evidencien deficiencias o incumplimientos, debido a que estos acuerdos están desactualizados desde la fecha que se contrataron los servicios.
2.10 Consideraciones de la seguridad cuando se trata con ciudadanos o clientes	SRI: 100% Senae: 85%	En el caso de estudio del SRI, es muy notable que la consideración de seguridad hacia los contribuyentes está en un grado de madurez muy alto, inclusive a nivel nacional esta entidad ha tenido menciones honoríficas en relación a otras entidades públicas porque los servicios que han brindado son de alta calidad y calidez. En el caso del Senae desde el 2010 se decretó el uso y administración de la VUE (Ventanilla Única del Ecuador) a dicha entidad, la misma permite unificar los requerimiento de los ciudadanos en una sola ventanilla única virtual, conectada con todos los ministerios facilitando la intercomunicación y con las seguridades que presta a los OCE (Operadores de Comercio Exterior), cabe destacar que desde el 2012 dicho sistema se encuentra implementado y en constante mejora enfocado en las facilidades y aseguramiento al ciudadano.
2.11 Consideraciones de la seguridad en los acuerdos con terceras partes	SRI: 100% Senae: 75%	En Senae los acuerdos (notas reversales) realizados con terceras partes no están continuamente en revisión, por lo que en el transcurso de los años se vuelven obsoletos para los servicios que se prestan entre las partes. En el caso del SRI existe el Departamento de Inteligencia de la Información que mantiene su plan actual enfocado a las necesidades de información que posee el SRI a todo nivel y se actualizan dichas notas reversales anualmente o cuando la necesidad así lo determine.

Fuente: *Elaboración propia, 2019*

ANÁLISIS DE RESULTADOS

Con base a la evaluación realizada para verificar el cumplimiento del EGSI en las Instituciones del SRI y Senae, se procedió a elaborar las buenas prácticas recomendadas en referencia a varios estándares y normas de seguridad como lo son: NIST SP 800-53, NIST SP 800-30, ISO 27005, ISO 27033, ISO 15408 y RFC2196, estas buenas prácticas que se recomiendan a ambas Instituciones fueron

validadas por expertos en la materia de seguridad de la información Nacionales y Extranjeros (ver Anexo 4), mediante la realización de un focus group.

Buenas prácticas recomendadas a las Instituciones del Caso de estudio.

C1. Relevar lo considerado por las propias instituciones como supuestos riesgos a los que podrían estar expuestos, las amenazas identificadas y las políticas vigentes, cada documento deberá tener una subclasificación de acuerdo a ponderaciones por todos los activos que posee la institución (principalmente la información y la subcategorización por importancia de ésta, en relación al proceso que la genera o que la consume). Este primer punto, permite tener el diagnóstico de las entidades de estudio.
C2. Definir dentro de la política, la frecuencia con la que deben realizarse las copias de seguridad en cada Institución.
C3. Realizar respaldos de seguridad periódicamente y almacenarlos en repositorios adecuados y seguros.
C4. Identificar y evaluar el nivel de riesgo al que se encuentra expuesto la seguridad de la información Institucional.
C5. En correspondencia a los riesgos evidenciados a los que está expuesta la información, se evidenciaron áreas críticas de cada institución que manejan información confidencial/reservada, que necesita un tratamiento diferente; para estos casos se recomienda arquitecturas de correo electrónico de Internet.
C6. Definir un plan estratégico de tratamiento del riesgo en base a la evaluación realizada de acuerdo a las necesidades de la Institución.
C7. Implementar en las áreas más críticas de la Entidad, un control de riesgos que genere una alerta al oficial de seguridad de la información, sobre la vulnerabilidad encontrada o el intento de vulnerabilidad de la seguridad.
C8. Realizar monitoreo y seguimiento continuo de los riesgos evaluados, de manera que las Instituciones puedan utilizar los resultados de dicha evaluación para renovar y reforzar la estrategia de gestionar los riesgos.
C9. Documentar los controles implementados para el tratamiento del riesgo, así como los resultados obtenidos de la evaluación del riesgo realizado.
C10. Mantener una constante revisión de la política, de manera que se puedan realizar mejoras continuas y reforzar el nivel de seguridad.
C11. En el caso del Senae se debe definir los accesos y privilegios, de manera que se registre un control y monitoreo constante a la red de datos, dispositivos dentro de la red o equipos externos fuera del dominio Institucional.
C12. Establecer mensajes de alertas que notifiquen advertencias sobre el uso autorizado del sistema y módulos de información sensibles, así como confirmaciones de acceso exitoso o erróneo a los sistemas.
C13. Se debe definir las áreas de responsabilidad tanto para los usuarios y administradores, así como establecer las sanciones que correspondan.
C14. Definir una política en donde se establezcan las responsabilidades de contingencia del personal operativo y administrativo y en caso de detectar una intrusión, tener conocimiento de cómo actuar y a quién contactar.
C15. En el caso de Senae se debe establecer una política de autenticación de contraseñas, así como la complejidad de la misma, en donde se indique la periodicidad con la que esta debe ser cambiada, notificando y llevando un registro de los cambios realizados.
C16. En el caso de Senae se debe establecer una política de disponibilidad de recursos, que en caso de existir un corte de servicio sea por mantenimiento o fallas del sistema, se especifique el tipo de incidente, la afectación y tiempo aproximado de inactividad o interrupción del servicio.
C17. Definir una política en donde se establezca que en caso de infracciones de privacidad y seguridad sean éstas internas o externas, se establezca el nivel de responsabilidad de los custodios tanto del sistema como de los oficiales de seguridad, que a su vez reporten de forma clara y precisa los sucesos indicados, con el fin de determinar a quién debe reportarse el respectivo informe indicando los sucesos, pudiendo evitar una posible violación de accesos.
C18. Definir una política de validación del servicio, dicha política tendrá como base los requerimientos de seguridad de manera primordial, cuya finalidad es que se verifique la calidad del desarrollo de los

sistemas antes de pasar a producción desde el ámbito de funcionalidad sin descuidar la seguridad.

C19. Realizar evaluaciones constantes en todas las fases de desarrollo, producción y aplicación por usuarios finales de un sistema o producto, para así llevar un registro de los cambios y mejoras realizadas y el cumplimiento de éstos de acuerdo a los requisitos de seguridad; la información relevada durante la evaluación deberá estar debidamente documentada con los hallazgos.

C20. Durante la evaluación, el evaluador deberá determinar que la especificación funcional sea una exacta y completa instanciación de los requisitos funcionales de seguridad del objetivo de evaluación.

C21. La flexibilidad en el concepto de la seguridad arquitectónica como política, permite su estabilidad en el tiempo, siendo independiente del hardware o software utilizado y la actualización de la misma debe estar claramente explicada. Se deben considerar todos los aspectos, inclusive el traspaso de información clave de acuerdo a las funciones de los sujetos que hacen parte de la organización.

C22. Desde la funcionalidad hasta la implementación, el diseño y desarrollo debe estar orientado a la seguridad de la red, incluyendo la provisión de una visión general de la seguridad de la red, definiciones relacionadas, y orientación sobre cómo identificar y analizar los riesgos de seguridad de la red y luego definir los requisitos de seguridad de la red.

C23. La seguridad de la red debe ser customizado de acuerdo a las necesidades de la entidad y es importante que para todo el personal que participa en la planificación, diseño e implementación de los aspectos arquitectónicos de la red, esté empoderado de los temas de seguridad en redes, mediante responsabilidades definidas documentalmente en políticas o manuales que sean explícitos en la definición de funciones y sanciones.

C24. Para cada institución se debe definir un mantenimiento enfocado a la mejora constante y continuidad del negocio, basándose en las evaluaciones ya realizadas, de tal manera que el evaluador continúe cumpliendo con sus actividades de seguridad a medida que se realizan cambios en el objetivo de evaluación o en su entorno.

De acuerdo a las revisiones realizadas por los expertos en el focus group con fecha 30 de enero del 2019 el Ing. Alberto Pazmiño enfatizó que existe la necesidad de que las recomendaciones indicadas anteriormente sean aterrizadas en el mejoramiento de esa deficiencia evidenciada durante el análisis de resultados; por ello, acogiendo sus observaciones, en la tabla 3 se detallan los mecanismos que se sugieren implementar para poder reforzar el nivel de seguridad de la información en las Instituciones del caso de estudio.

Tabla 3

Mecanismos asociados a los códigos de buenas prácticas

Códigos asociados	**Mecanismo a implementar**
C1, C10	**BP1.** Establecer un plan de sensibilización de seguridad de la información
C2, C5, C6, C7, C8, C9	**BP2.** Sistemas de Gestión de Riesgos de Seguridad de la información
C3, C4	**BP3.** Asociarlo al perfil de puestos y definirlo como una actividad
C11, C12, C13, C14, C15, C16, C17, C23	**BP4.** Estatuto Orgánico por Procesos, políticas y reestructurar el departamento de TI (QA, Soporte, Redes, Seguridad, Desarrollo)
C18, C19, C20, C21, C22, C23	**BP5.** SSDLC (Ciclos de Vida de Software Seguro), aplicar seguridad en cada etapa del desarrollo
C24	**BP6.** Sistema PHVA (Ciclo de mejora continua enfocado a la seguridad de la información)

Fuente: *Elaboración propia, 2019*

CONCLUSIONES

El presente trabajo investigativo tiene como objetivo principal proponer mejores prácticas en procura de la seguridad de la información para las instituciones ecuatorianas Senae y SRI, para lo cual se realizó un focus group con expertos en el área de seguridad de la información, en el que se presentaron los casos de estudios y análisis de la propuesta, validando las buenas prácticas recomendadas.

En base a los estudios realizados se pudo evidenciar que a pesar de que ha existido una

reducción del presupuesto en las instituciones para invertir en temas de seguridad, más del 75% de las empresas a nivel de Latinoamérica ejecutan acciones de seguridad periódicamente, esto se refiere a la aplicación de políticas, estándares, normativas o planes de gestión; sin embargo, es necesario reforzar los controles y concientizar al personal en temas de seguridad de la información.

A nivel de Latinoamérica la mayoría de las instituciones se esfuerzan por cumplir con las normativas establecidas y no solo basta con tener una política de seguridad, sino verificar que abarca esa política, de ahí surge la necesidad de desarrollar una cultura de seguridad y contar con el compromiso de las autoridades de manera que exista una buena gestión de seguridad de la información.

La información que manejan las entidades diariamente están expuestas a riesgos, pudiendo tener un impacto considerable y llegar a afectar la disponibilidad, confidencialidad e integridad de la información; por ello se debe realizar una adecuada gestión y medición de los riesgos, de acuerdo al entorno y clasificación de la información de cada institución, de manera que se pueda identificar el impacto que tendrían estos riesgos sobre la institución.

En base a los resultados obtenidos en la evaluación a las entidades del caso de estudio, es notorio la falta de cumplimiento de las directrices establecidas en el EGSI por parte de Senae en comparación con el SRI; por lo cual en el presente documento se detallan las buenas prácticas recomendadas en función de la seguridad de la información aplicables a ambas Instituciones, y de ser el caso a cualquier institución pública que requiera reforzar su nivel de seguridad.

Concluyendo así en base a los resultados obtenidos en dicho estudio, que las instituciones a nivel de gobierno no solo deberían basarse en el cumplimiento del EGSI, sino también reforzar su nivel de seguridad con la aplicación de otro estándar o normativa de seguridad que brinde la robustez necesaria, de acuerdo a las actividades y clasificación de la información de cada entidad; esto último fue enfatizado en recomendar por parte de los expertos partícipes del focus group.

FORTALEZAS Y LIMITACIONES

La fortaleza principal del presente estudio de investigación fue la apertura brindada por ambas instituciones para poder realizar el estudio, levantamiento de información y entrevistas, así como también el apoyo por parte de los directivos de TI y responsables de áreas que colaboraron en la obtención de la información y aclaración de inquietudes presentadas a lo largo del trabajo realizado.

La limitación presentada fue la negatividad y rechazo que presentaron algunas entidades gubernamentales en las que se presentó la solicitud para poder realizar el trabajo investigativo con más instituciones del gobierno, por lo que sólo tuvimos la aceptación por parte del Senae y SRI.

FUTURAS LÍNEAS DE INVESTIGACIÓN

Considerando que el Servicio de Rentas Internas y el Servicios Nacional de Aduana del Ecuador, están en un proceso de fusión, que consolidará las administraciones tributarias a nivel nacional, será necesario que los mecanismos en relación a la seguridad de la información que en la actualidad son implementados por las instituciones de estudio deberán homologarse, por lo que es preponderante realizar un estudio posterior, el mismo que puede estar basado en las líneas de acción que se proponen en el presente artículo.

RECOMENDACIONES

En correspondencia al análisis realizado y de acuerdo a las conclusiones que se han evidenciado en los resultados del presente estudio, se recomienda que previamente a implementar los mecanismos propuestos en la Tabla N° 3, se evalué al interno de cada institución con los encargados de las áreas responsables y relacionadas, el impacto que significará el desarrollo y la puesta en marcha de cada una de las propuestas de cambio o reformulación de nuevas prácticas y priorizar de acuerdo al riesgo que representa la no implementación de estas mejores prácticas, para cada organismo estatal.

En relación a los resultados del presente estudio y de acuerdo a las consideraciones efectuadas en el focus group por los expertos en el área de seguridad de la información, se recomienda a las instituciones de estudio y en general a todas las instituciones que deseen implementar mecanismos en Gestión de Seguridad de la Información, que inicialmente se realice un proceso de concientización que

abarque a todas las áreas de negocio y posterior a este proceso de acuerdo al impacto de los riesgos se analice la pertinencia de efectuar los demás controles.

La información es uno de los activos más importantes de la institución, por ello es fundamental que las autoridades o los responsables de los organismos estatales estén comprometidos con los mecanismos necesarios que implica tener una buena gestión de seguridad de la información, por ello es preponderante que la seguridad de la información sea vista como una inversión la misma que apalanca a todos los procesos y no como un costo adicional; es por esto que en base al estudio realizado se recomienda un reforzamiento en los controles sumado a la motivación de los funcionarios y que éstos sientan que son parte importante de esta gestión con el acompañamiento adecuado de los empleados de las áreas responsables como lo es Tecnología de la Información y Planificación y siempre alineados al cumplimiento de la normativa, de manera que todos se involucren y se responsabilicen por los riesgos a los que está expuesta la información.

Se evidenció que en ambas instituciones se cumple con la política de seguridad, sin embargo, se recomienda que el oficial de seguridad de la información designado evalué la política de forma íntegra y analicé si la misma sólo es un ítem adicional para cumplir las directrices del EGSI, a esto se le denomina compromiso. Adicionalmente es importante que se resuelva mediante talleres de trabajo a nivel institucional si realmente la política involucra todos los aspectos de la entidad considerando la actualización continua de la misma con los respaldos o documentación necesaria que permita el seguimiento de las mejoras realizadas.

Se sugiere a las Instituciones del caso de estudio, considerar las buenas prácticas recomendadas en este trabajo, pudiendo ser aplicables a todas las instituciones públicas ecuatorianas que se rigen en el EGSI; de manera que se pueda reforzar el nivel de seguridad de la información con las recomendaciones antes indicadas y que no están contempladas en el EGSI.

Referencias Bibliográficas

Thales (2018). Data Threat Report, (pp. 8). Retrieved from https://dtr.thalesesecurity.com/.

Price Waterhouse Cooper (2016). Ciberseguridad y privacidad: de la percepción a la realidad, (pp. 6) Retrieved from https://www.pwc.com

Symantec (2018). Internet Security Threat Report 23, (pp. 26) Retrieved from https://www.symantec.com

Cisco (2018). Reporte Anual de Ciberseguridad, (pp. 49) Retrieved from https://www.cisco.com/

Asociación Colombiana de Ingenieros de Sistemas –ACIS– (2018). XVIII Jornada Internacional de Seguridad Informática ACIS 2018, (pp. 49) Retrieved from http://acis.org.co/revista147/content/xviii-encuesta-nacional-de-seguridad-informatica-evolucian-del-perfil-del-profesional-de-seguridad-digital

Secretaría de la Administración Pública, Gobierno Nacional de la República del Ecuador (2014). Plan de Gobierno Electrónico v2.0 2016-2017 (pp. 9) Retrieved from https://www.gobiernoelectronico.gob.ec/wp-content/uploads/downloads/2016/11/Plan-Gobierno-Electro%CC%81nico-Final.pdf

ISO (2007). Sistema de Gestión de Seguridad de la Información (SGSI). Retrieved from http://www.iso27000.es/

Orrego, V. M. (2011). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. Revista Pensamiento Americano, 4(6), 21-23. http://www.coruniamericana.edu.co/publicaciones/ojs/

ISO (2012). ISO 27000. Que es un SGSI. Recuperado de: http://www.iso27000.es/sgsi

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 4(02), 92. https://file.scirp.org/pdf/JIS_2013042311130103

Ávila, A. (2016). Diseño de un prototipo de gestión de seguridad de la información para instituciones educativas. Obtenido de https://repository.upb.edu.co/bitstream/handle/20.500.11912/2763

Lainhart, J. (2000). COBIT™: A methodology for managing and controlling information and information technology risks and vulnerabilities. 14 (s-1), 21-25. Retrieved from http://pingitsystems.com/PDF/Article

ISACA (2012). COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. http://www.isaca.org/cobit/Documents

López, D. (2017). Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000. Revista Tecnológica-ESPOL, 30(1). http://rte.espol.edu.ec/index.php/tecnologica/article

ICONTEC (2006). NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA. Retrieved from https://www.serviciocivil.gov.co

Office of Government Commerce. (2010). Mejora continua del servicio. The Stationery Office.Retrieved from https://books.google.com.ec/

RFC2196. Network Working Group. Site Security Handbook. Internet Engineering Task Force [En línea, p. 4]. https://www.ietf.org/rfc/

Lexisfinder (2013), Esquema Gubernamental de seguridad de la información EGSI. pag. 2. disponible en: http://www.planificacion.gob.ec/

LOTAIP, Ley Orgánica de Transparencia y

Acceso a La Información Pública (2004). Acceso a la información pública. Registro Oficial, 337.

Currall, J. (2006). Security and the digital domain.

Kuzma, J. (2010). European digital libraries: Web security vulnerabilities. Library Hi Tech, 28(3), 402-413.

Al-Izki, F., & Weir, G. R. (2016). Management attitudes toward information security in Omani public sector organisations. In Cybersecurity and Cyberforensics Conference (CCC), 2016 (pp. 107-112). IEEE

Constituyente (2008). Constitución de la República del Ecuador. Disponible en: http://www.funcionjudicial.gob.ec/

Contraloría General del Estado (2009), NORMAS DE CONTROL INTERNO DE LA CONTRALORIA GENERAL DEL ESTADO. Disponible en: https://www.oas.org/juridico/PDFs/

Servicio de Rentas Internas (2018). Ecuador. Recuperado de http://www.sri.gob.ec/web/

Servicio Nacional de Aduana del Ecuador (2018). Ecuador. Recuperado de https://www.aduana.gob.ec/

Calero (2018). Usando Oracle 12c en Docker sobre Windows 10. Oracle. Recuperado de http://www.oracle.com/technetwork/es/articles/

Valdés, E. (2009). Tendencias de la Auditoria Informática. Ingenium, 4(8), 69-98. Retrieved from http://revistas.usc.edu.co

Sánchez, G. & Rojas, I. (2012). Leyes de protección de datos personales en el mundo y la protección de datos biométricos–Parte I. Retrieved from https://revista.seguridad.unam.mx

Borbúa, R., Herrera, L. & Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 31-45.

Cáceres, J. (2017). Colombia, estrategia nacional en ciberseguridad y ciberdefensa. AIR & SPACE POWER JOURNAL, pp. 86-87. Retrieved from https://www.airuniversity.af.mil/

Leiva, E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en Enfoque Top-Down desde una visión global a una visión local. Revista Latinoamericana de Ingeniería de Software, 3(4), 161-176.

Justribó, C (2014). Ciberdefensa: una visión desde la UNASUR. Instituto de Relaciones Internacionales. Retrieved from http://hdl.handle.net/10915/44716

ESET (2017). Welivesecurity. Comité de respuestas a incidentes de seguridad informática- Argentina. Retrieved from https://www.welivesecurity.com/

Borghello, C. & Temperini, M. (2013). Ciberseguridad Nacional Argentina: Cracking de Servidores de la Administración Pública. In Simposio de Informática y Derecho. pp. 36.

Contraloría General de la Unión (2016). Transparencia Pública en Brasil: Mecanismos de Verificación. Secretaria de Transparencia y Prevención de la Corrupción. Retrieved from http://www.cpccs.gob.ec/

Lexis (2004). LEY ORGANICA DE TRANSPARENCIA Y ACCESO A LA INFORMACION PUBLICA. Registro Oficial Suplemento 337 del 18 de mayo del 2004. Retrieved from http://www.oas.org/

DAPRE (2017). Gobierno de Colombia. Noticias Presidencia de la República. Retrieved from http://es.presidencia.gov.co/

Hoyos, M (2015) Ministerio de Tecnologías de la Información y las Comunicaciones. República de Colombia. Decreto 1078 de 2015. Publicado el 26 de mayo del 2015. Retrieved from https://www.mintic.gov.co/

Cárdenas, M & Caballero, L. (2017) Ministerio de Hacienda y Crédito Público. República de Colombia. Decreto Número 2184. Publicado el 23 de diciembre del 2017. Retrieved from http://es.presidencia.gov.co/normativa

DIAN (2016). CÓGIGO DE BUEN GOBIERNO Y DE ÉTICA. UNIDAD ADMINISTRATIVA ESPECIAL DIRECCIÓN DE IMPUESTOS Y ADUANAS NACIONALES – DIAN. PROCESO INTELIGENCIA CORPORATIVA. Retrieved from https://www.dian.gov.co/dian

Servicio de Rentas Internas (2018). Informe de Gestión Enero- diciembre 2017. Dirección Nacional de Planificación y Gestión Estratégica. Retrieved from www.sri.gob.ec/.

MINTIC (2016). Modelo de Seguridad y Privacidad de la información. Ministerio de Tecnologías de la Información y las Comunicaciones. Retrieved from https://www.mintic.gov.co/gestionti

Servicio Nacional de Aduanas (2018). Política General de la Seguridad de la Información. Retrieved from https://www.aduana.cl/aduana

Aduanas Chile (2017). Aduana implementa software para enfrentar riesgos del Comex. Gobierno de Chile. Retrieved from https://www.aduana.cl/

Semana (2013). Cruzada contra la corrupción en la Dian. Publicada el 23 de noviembre del 2013. COPYRIGHT © 2018 PUBLICACIONES SEMANA S.A. Retrieved from https://www.semana.com/

Mintel (2017). Libro blanco de la sociedad de la información y del conocimiento. © Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL). Retrieved from https://www.telecomunicaciones.gob.ec/

ESET (2018)® Eset Security Report Latinoamérica 2018. Retrieved from https://www.welivesecurity.com/

Deloitte (2016) © La Evolución de la Gestión de Cyber Riesgos y Seguridad de la Información. Encuesta 2016 sobre Tendencias de Cyber Riesgos y Seguridad de la Información en Latinoamérica. Retrieved from https://www2.deloitte.com/ec

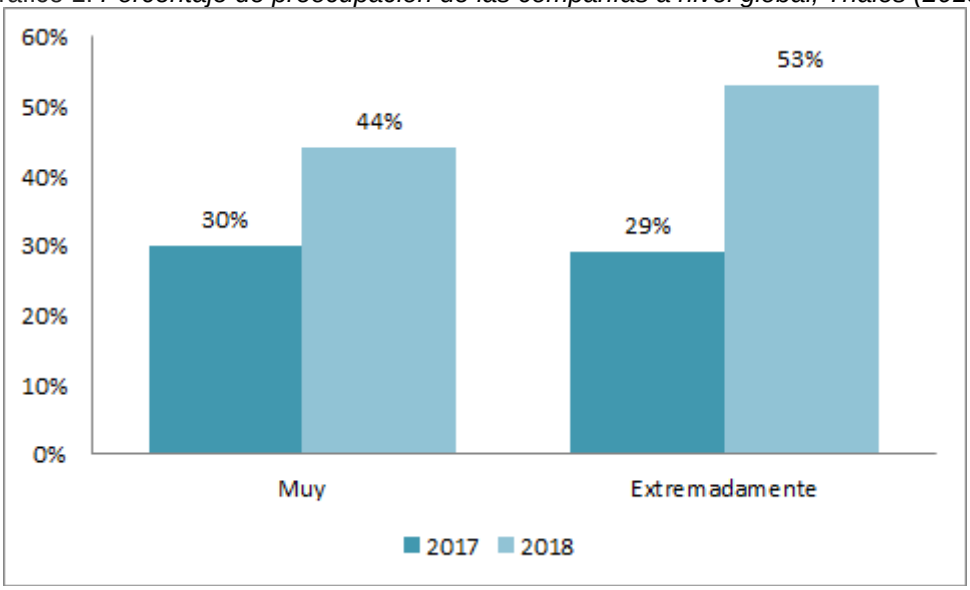
Olmedo, J. & Gavilánez, F. (2018). Análisis de los Ciberataques realizados en América Latina. INNOVA Research Journal, 3(9), 180-189.

Navarro, J. (2011). Cyber regulation in Latin America and the Caribbean. Corporate Author(s):: NU. CEPAL; Date Issued: 2011-06; Serie: Newsletter eLAC; No. 15; 12 p.; ilus.

Linares, Y. (2018). ¿Cómo estamos en ciberseguridad nacional e internacional, su gestión de riesgos y tendencias? Retrieved from http://repository.unipiloto.edu.co/bitstream

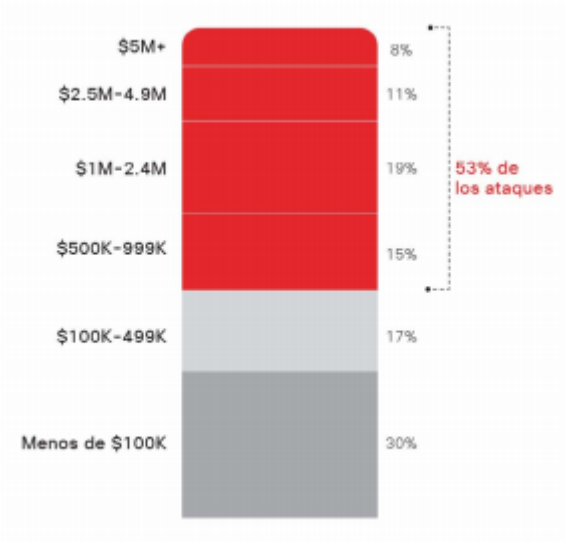
Anexo 1. NIVELES DE VULNERABILIDAD FRENTE A AMENAZAS DE DATOS.

Gráfico 1. *Porcentaje de preocupación de las compañías a nivel global, Thales (2018)*



Anexo 2. COSTO DE ATAQUES.

Gráfico 2. *Costo de Ataques, Reporte Anual, Cisco (2018)*



Anexo 3. INDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA.

Gráfico 3. DIAN (2016)

DIAN

ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA

Actualización: Diciembre de 2016

Código TRD	Tipo de Activo de Información	Nombre o título de la Categoría de Información	Descripción del contenido de la Categoría de Información	Idioma	Medio de conservación y/o soporte	Formato Electrónico	Calificación de la Información	Fecha de Generación de la Información (AAAA/MM/DD)	Nombre del responsable producción de la información	Nombre del responsable de la información	Objetivo legítimo de la excepción	Fundamento constitucional o legal	Fundamento jurídico de la excepción	Excepción Total o Parcial	Fecha de la calificación (AAAA/MM/DD)	Plazo de la clasificación o reserva
1-532	Información	1-ACTAS	1-532-Actas de Reunión	Español	Físico y Electrónico	Varios	Clasificada	Por Demanda	Transversal (todas las dependencias)	Funcionario a cargo de la Gestión documental	Art.18-Clasificada por ser secreto comercial, industrial y profesional.	Ley 1712 de 2014		Parcial	2016/10/07	Ilimitada
1-556	Información	1-ACTAS	1-556-Actas de Inspección Física	Español	Físico y Electrónico	Base de datos	Clasificada	Por demanda condicionada a aprobación DIAN	Dirección Seccional	Dirección Seccional	Art.18-Clasificada por ser secreto comercial, industrial y profesional.	Ley 1712 de 2014		Total	2016/12/31	Ilimitada
1-644	Información	1-ACTAS	1-644-Actas de Visita a Contribuyentes	Español	Físico y Electrónico	Documento de texto	Reservada	Permanente	DGF - SGOC - SGFI	DGF - SGOC - SGFI	Art.19-Reservada (Inf. del debido proceso y la igualdad de las partes en los procesos judiciales)	Art. 583 E.T., Ley 1581 de 2012 - Ley de protección de datos personales, Art. 15 C.P/C.		Total	2016/09/31	15 años (Art. 22 Ley 1712 de 2014)
1-691	Información	1-ACTAS	1-691-Actas de Comité de Denuncias	Español	Físico y Electrónico	Documento de texto	Reservada	Diaria	DGF - COyPLA	DGF - COyPLA	Art.19-Reservada (Inf. del debido proceso y la igualdad de las partes en los procesos judiciales)	Art. 11 Ley 526 de 1999 (reserva de la información)		Total	2016/09/31	15 años (Art. 22 Ley 1712 de 2014)
1-712	Información	1-ACTAS	1-712-Actas de Comité Triple A	Español	Físico		Reservada	Por demanda	DGA - Desp.	DGA - Desp.	Art.19-Reservada (Inf. de la estabilidad macroeconómica y financiera del país)	Ley 1712 de 2014		Total	2016/09/31	15 años (Art. 22 Ley 1712 de 2014)
1-717	Información	1-ACTAS	1-717-Actas de Comité Técnico de Programas y Campañas de Control	Español	Físico y Electrónico	Documento de texto	Clasificada	Permanente	DGF - Desp.	DGF - Desp.	Art.18-Clasificada por ser secreto comercial, industrial y profesional.	Ley 1712 de 2014		Parcial	2016/09/31	Ilimitada
1-718	Información	1-ACTAS	1-718-Actas de Visita	Español	Físico y Electrónico	PDF	Clasificada	Permanente	SGRA	SGRA	Art.18-Clasificada por derecho a la intimidad (no consentimiento en revelación de datos personales o privados)	Ley 1712 de 2014		Parcial	2016/09/31	Ilimitada
1-755	Información	1-ACTAS	1-755-Actas de Reparto - Distribución interna para la atención a los derechos de petición, consultas y solicitudes de información	Español	Físico		Clasificada	Diaria	DGI - SGAC - CAR	DGI - SGAC - CAR	Art.18-Clasificada por ser secreto comercial, industrial y profesional.	Ley 1712 de 2014		Total	2016/10/07	Ilimitada
3-0	Información	3-AUTOS	Auto Comisorio formato 1090	Español	Físico y Electrónico	Documento de texto	Reservada	Permanente	DGA - SGRA	DGA - SGRA - CS	Art.19-Reservada (Inf. del debido proceso y la igualdad de las partes en los procesos judiciales)	Ley 1712 de 2014		Parcial	2016/09/31	15 años (Art. 22 Ley 1712 de 2014)
3-0	Información	3-AUTOS	Auto de Apertura de Expedientes (plantilla)	Español	Físico y Electrónico	Documento de texto	Reservada	Permanente	DGA - SGRA	DGA - SGRA - CSRA	Art.19-Reservada (Inf. del debido proceso y la igualdad de las partes en los procesos judiciales)	Ley 1712 de 2014		Parcial	2016/09/31	15 años (Art. 22 Ley 1712 de 2014)
3-0	Información	3-AUTOS	Auto de desgloce (plantilla)	Español	Físico y Electrónico	Documento de texto	Reservada	Permanente	DGA - SGRA	DGA - SGRA - CSRA, CS	Art.19-Reservada (Inf. del debido proceso y la igualdad de las partes en los procesos judiciales)	Ley 1712 de 2014		Parcial	2016/09/31	15 años (Art. 22 Ley 1712 de 2014)
3-0	Información	3-AUTOS	Auto de reconocimiento o de no reconocimiento de personería jurídica. (plantilla)	Español	Físico y Electrónico	Documento de texto	Reservada	Permanente	DGA - SGRA	DGA - SGRA - CS	Art.19-Reservada (Inf. del debido proceso y la igualdad de las partes en los procesos judiciales)	Ley 1712 de 2014		Parcial	2016/09/31	15 años (Art. 22 Ley 1712 de 2014)
3-0	Información	3-AUTOS	Auto de reconstrucción de expedientes (plantilla)	Español	Físico y Electrónico	Documento de texto	Reservada	Permanente	DGA - SGRA	DGA - SGRA - CSRA	Art.19-Reservada (Inf. del debido proceso y la igualdad de las partes en los procesos judiciales)	Ley 1712 de 2014		Parcial	2016/09/31	15 años (Art. 22 Ley 1712 de 2014)
3-0	Información	3-AUTOS	Auto de reliquidación de expedientes (plantilla)	Español	Físico y Electrónico	Documento de texto	Reservada	Permanente	DGA - SGRA	DGA - SGRA - CSRA, CS	Art.19-Reservada (Inf. del debido proceso y la igualdad de las partes en los procesos judiciales)	Ley 1712 de 2014		Parcial	2016/09/31	15 años (Art. 22 Ley 1712 de 2014)
3-0	Información	3-AUTOS		Español	Físico y Electrónico	Documento de texto	Reservada	Semanal	DGF - SGFT, SGFA, SGOC, SGFI	DGF - Despacho	Art.19-Reservada (Inf. del debido proceso y la igualdad de las partes en los procesos judiciales)	Ley 1712 de 2014		Total	2016/09/31	15 años (Art. 22 Ley 1712 de 2014)
11-17	Información	11-CONCEPTOS JURÍDICOS	11-17-Conceptos Jurídicos Cambiarios	Español	Físico y Electrónico	PDF	Reservada	Mensual	DGF - SGOC	DGF - SGOC	Art.19-Reservada (Inf. del debido proceso y la igualdad de las partes en los procesos judiciales)	Ley 1712 de 2014		Total	2016/09/31	15 años (Art. 22 Ley 1712 de 2014)
13-652	Información	13-CONSECUTIVOS DE COMUNICACIONES OFICIALES	13-652-Consecutivos de Comunicaciones Oficiales Externas	Español	Físico y Electrónico	Documento de texto	Clasificada	Permanente	Transversal (todas las dependencias)	Funcionario a cargo de la Gestión documental	Art.18-Clasificada por derecho a la intimidad (no consentimiento en revelación de datos personales o privados)	Ley 1712 de 2014		Parcial	2016/06/14	Ilimitada
13-653	Información	13-CONSECUTIVOS DE COMUNICACIONES OFICIALES	13-653-Consecutivos de Comunicaciones Oficiales Internas	Español	Físico y Electrónico	Documento de texto	Clasificada	Permanente	Transversal (todas las dependencias)	Funcionario a cargo de la Gestión documental	Art.18-Clasificada por derecho a la intimidad (no consentimiento en revelación de datos personales o privados)	Ley 1712 de 2014		Parcial	2016/06/14	Ilimitada
16-375	Información	16-CUENTAS	16-375-Cuentas Fiscales	Español	Físico y Electrónico	Documento de texto	Clasificada	Mensual	Dirección Seccional	DGI - SGRyC - CCFR	Art.18-Clasificada por derecho a la intimidad (no consentimiento en revelación de datos personales o privados)	Art. 583 E.T.		Total	2016/06/14	Ilimitada
18-53	Información	18-DECLARACIONES ADUANERAS	18-53-Documentos de Vuelo y Transporte	Español	Electrónico	Base de datos	Clasificada	Por demanda	Transportador y/o Agente de Carga Intral	DGA	Art.18-Clasificada por ser secreto comercial, industrial y profesional.	Ley 1712 de 2014		Total	2016/12/31	Ilimitada
18-377	Información	18-DECLARACIONES ADUANERAS	18-377-Manifiestos de Carga	Español	Electrónico	Base de datos	Clasificada	Por demanda	Transportador	DGA	Art.18-Clasificada por ser secreto comercial, industrial y profesional.	Ley 1712 de 2014		Total	2016/12/31	Ilimitada
19-0	Información	19-DERECHOS DE PETICIÓN	Quejas y Reclamos, Consultas Administraciones Seccionales	Español	Físico y Electrónico	Varios	Clasificada	Por Demanda	Varias dependencias	DGI - SGAC-CSQRyS, Superior jerárquico de la dependencia	Art.18-Clasificada por derecho a la intimidad (no consentimiento en revelación de datos personales o privados)	Ley 1712 de 2014		Parcial	2016/06/14	Ilimitada

Anexo 4. EXPERTOS PARTICIPES DEL FOCUS GROUP

Nombres	Perfil
Ing. Alberto Pazmiño	Nacionalidad: ecuatoriana CISM, CISA, ITIL V3, COBIT F, Asesor en gestión y seguridad de TIC's en Self-employed Teléfono 0999024446 lapazmino@puce.edu.ec
Ing. Vargas Nolivos Hernán Patricio	Nacionalidad: ecuatoriana Ingeniero en Sistemas. Docente en Gestión de Bases de Datos en la Universidad Técnica de Manabí. Gerente General en SERVITECNO Y COMPUTERS S.A Teléfono 0967064671 hvargas@utm.edu.ec
Ing. Asitimbay Castro Jorge Luis	Nacionalidad: ecuatoriana Ingeniero en Sistemas, Magíster en Seguridad Informática. Director de TI en BCM. Experiencia en el sector de la Seguridad Informática en aspectos relacionados con Manejo de Firewalls, Antivirus, Seguridad en Servidores, Vulnerabilidades de Seguridad, Seguridad en Redes, Seguridad informática basada en Normativas Teléfono 0999179970 asitimbaycastro@yahoo.com
Ing. Marcos Hernán Martínez	Nacionalidad: Argentina Ingeniero en Sistemas. Consultor Informático en Adamo S.A. Auditor Interno 27001 TUV RHEINLAND Desarrollador de soluciones web, capacitador y soporte técnico (nivel 1, 2 y 3) Lenguajes de programación: c# jquery, javascrispt, html5, bootstrap, php 7 y otros mhernanmartinez@gmail.com
Ing. Darío Salgado	Nacionalidad: ecuatoriana Analista de Seguridad Informática Dirección General de Registro Civil, Identificación y Cedulación Capacitaciones: Oficial de Seguridad de la Información Manejo incidentes de seguridad de la información Informática Forense Hacking Ético y Defensa en profundidad Ethical hacking y test de penetración dario.salgado.08@gmail.com
Ing. Edgar Alfonso Godoy	Nacionalidad: colombiana CISSP, CISM, LA 27001, IMPLEMENTADOR LIDER 27001, IMPLEMENTADOR LIDER 27003, LA 22301 GESTOR CYBERSECURITY ISO 27032, RISK MANAGER ISO 31000, CEH, CRISC, ECIH, COBIT5 FC, ITIL FC, CCNA SECURITY, TOGAF 9 CERTIFIED, CERTIFIED ARCHIMATE 3, NSE4 FORTINET, IPV6 CSE , IPV6 CNE Consultor en Seguridad de la Información Magíster en Seguridad de la Información NDV Móvil 3005821212 edgar.godoy@ndv.com.co