MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

[redacted]

ACUERDO MINISTERIAL No. 025-2019

EL MINISTRO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

CONSIDERANDO:

Que, el numeral 1 del artículo 154 de la Constitución de la República del Ecuador confiere a las Ministras y Ministros de Estado, además de las atribuciones establecidas en la ley, la rectoría de las políticas del área a su cargo, así como la facultad de expedir acuerdos y resoluciones administrativas;

Que, el artículo 226 de la Constitución de la República indica que: "*Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución*";

Que, el artículo 227 ibídem dispone: *"La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación";*

Que, el inciso segundo del artículo 314 de la Constitución de la República, dispone que el Estado garantizará que los servicios públicos, prestados bajo su control y regulación, respondan a principios de obligatoriedad, generalidad, uniformidad, eficiencia, responsabilidad, universalidad, accesibilidad, regularidad, continuidad y calidad;

Que, el artículo 140 de la Ley Orgánica de Telecomunicaciones, dispone: "*Rectoría del sector. El Ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información es el órgano rector de las telecomunicaciones y de la sociedad de la información, informática, tecnologías de la información y las comunicaciones y de la seguridad de la información. A dicho órgano le corresponde el establecimiento de políticas, directrices y planes aplicables en tales áreas para el desarrollo de la sociedad de la información, de conformidad con lo dispuesto en la presente Ley, su Reglamento General y los planes de desarrollo que se establezcan a nivel nacional. Los planes y políticas que dicte dicho Ministerio deberán enmarcarse dentro de los objetivos del Plan Nacional de Desarrollo y serán de cumplimiento obligatorio tanto para el sector público como privado";*

Que, mediante Decreto Ejecutivo No. 8 de 13 de agosto de 2009, publicado en el Registro Oficial No. 10, de 24 de agosto de 2009, el Presidente de la República resolvió crear el Ministerio de Telecomunicaciones y de la Sociedad de la Información, como órgano rector del desarrollo de las Tecnologías de la Información y Comunicación, que incluye las telecomunicaciones y el espectro radioeléctrico;

Que, con Decreto Ejecutivo No. 5 de 24 de mayo de 2017, se suprime la Secretaría Nacional de la Administración Pública y se transfieren al Ministerio de Telecomunicaciones y de la Sociedad de la Información entre otras la atribución: *"b. Desarrollar y coordinar planes, programas o proyectos sobre gobierno electrónico que sean necesarios para su implementación*";

Que, conforme lo establece la Disposición General Segunda del referido Decreto Ejecutivo, *"El Ministerio de Telecomunicaciones y Sociedad de la Información gestionará y coordinará la*

implementación de políticas, planes, programas y proyectos de gobierno electrónico en las instituciones de la administración pública a través de las coordinaciones generales de gestión estratégica y las direcciones de tecnologías de la información, dependientes de estas o de quien haga sus veces";

Que, mediante Acuerdo Ministerial No. 011-2018, del 08 de agosto de 2018, se expide el Plan Nacional de Gobierno Electrónico 2018-2021; este instrumento muestra la situación actual del país en materia de gobierno electrónico, las acciones que serán ejecutadas en tres programas; Gobierno Abierto, Gobierno Cercano y Gobierno Eficaz y Eficiente. En el Capítulo 1. Fundamentos Generales, literal 5. Diagnóstico; se enfatiza que: "*Dentro de las iniciativas relevantes que ha implementado el gobierno entorno a la ciberseguridad se encuentra la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI)...*"

Que, mediante Decreto Ejecutivo No. 784 de 4 de junio de 2019, el Presidente de la República nombró al licenciado Andrés Michelena Ayala, como Ministro de Telecomunicaciones y de la Sociedad de la Información;

Que, en el Informe Técnico de 09 de septiembre de 2019, suscrito por el Subsecretario de Estado – Gobierno Electrónico, se recomienda: "*Expedir mediante Acuerdo Ministerial el Esquema Gubernamental de Seguridad de la Información -EGSI-, debido a la necesidad de gestionar la seguridad de la información acorde a la evolución normativa y tecnológica, ya que actualmente los riesgos en seguridad muestran continuos cambios, se desarrollan nuevas amenazas y se revelan vulnerabilidades e incidentes de seguridad que tienen efectos considerables en la sociedad*";

En ejercicio de las atribuciones que le confiere el numeral 1 del artículo 154 de la Constitución de la República, artículo 17 del Estatuto del Régimen Administrativo de la Función Ejecutiva;

ACUERDA

Artículo 1. - Expedir el Esquema Gubernamental de Seguridad de la Información -EGSI-, el cual es de implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, que se encuentra como Anexo al presente Acuerdo Ministerial.

Artículo 2. – Las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, realizarán la Evaluación de Riesgos sobre sus activos de información críticos y diseñarán el plan para el tratamiento de los riesgos de su Institución, utilizando como referencia la "GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN" que es parte del Anexo del presente Acuerdo Ministerial, previo a la actualización o implementación de los controles de seguridad.

Artículo 3. – Recomendar a las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, utilicen como guía las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.

Artículo 4. - Las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, actualizarán o implementarán el Esquema Gubernamental de Seguridad de la Información EGSI en un plazo de doce (12) meses contados a partir de la publicación del presente Acuerdo Ministerial en el Registro Oficial.

La Evaluación de Riesgos y el plan para el tratamiento de los riesgos de cada Institución se realizarán en un plazo de cinco (5) meses y la actualización o implementación de los controles del Esquema Gubernamental de Seguridad de la Información (EGSI) se realizarán en un plazo siete (7) meses.

La actualización o implementación, se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información.

Artículo 5. – La máxima autoridad designará al interior de su Institución, un Comité de Seguridad de la Información (CSI), que estará integrado por los responsables de las siguientes áreas o quienes hagan sus veces: Talento Humano, Administrativa, Planificación y Gestión Estratégica, Comunicación Social, Tecnologías de la Información, Unidades Agregadores de Valor y el Área Jurídica participará como asesor.

El Comité de Seguridad de la Información tiene como objetivo, garantizar y facilitar la implementación de las iniciativas de seguridad de la información en la institución.

Los Comités en la primera convocatoria definirán su agenda y su reglamento interno.

Artículo 6.- El Comité de Seguridad de la Información, tendrá las siguientes responsabilidades:

a) Gestionar la aprobación de la política y normas institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la Institución.

b) Realizar el seguimiento de los cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

c) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto.

d) Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI.

e) Promover la difusión de la seguridad de la información dentro de la institución.

f) Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.

g) El comité deberá convocarse bimensualmente o cuando las circunstancias lo ameriten, se deberá llevar registros y actas de las reuniones.

h) Informar a la máxima autoridad los avances de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

i) Reportar a la máxima autoridad las alertas que impidan la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

j) Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

Artículo 7. – El Comité de Seguridad de la Información (CSI) designará al interior de su Institución a un funcionario como Oficial de Seguridad de la Información (OSI).

El Oficial de Seguridad debe tener conocimiento en Seguridad de la Información y Gestión de Proyectos, podrá ser si existiere el responsable de la Unidad de Seguridad de la Información, se recomienda que no pertenezca al área de Tecnologías de la Información.

Artículo 8.- El Oficial de Seguridad de la Información tendrá las siguientes responsabilidades:

a) Identificar todas las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI.

b) Generar propuestas para la elaboración de la documentación esencial del Esquema Gubernamental de Seguridad de la Información (EGSI).

c) Asesorar a los funcionarios en la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas.

d) Elaborar el Plan de concienciación en Seguridad de la Información basado en el Esquema Gubernamental de Seguridad de la Información (EGSI).

e) Elaborar un plan de seguimiento y control de la implementación de las medidas de mejora o acciones correctivas.

f) Coordinar la elaboración del Plan de Continuidad de Seguridad de la Información.

g) Orientar y generar un procedimiento adecuado para el manejo de los incidentes de seguridad de la información presentados al interior de la institución.

h) Coordinar la gestión de incidentes de seguridad con nivel de impacto alto a través de otras instituciones gubernamentales.

i) Mantener la documentación de la implementación del EGSI debidamente organizada.

j) Verificar el cumplimiento de las normas, procedimientos y controles de seguridad institucionales establecidos.

k) Informar al Comité de Seguridad de la Información, el avance de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), así como las alertas que impidan su implementación.

l) Previa la terminación de sus funciones el Oficial de Seguridad realizará la transferencia de la documentación e información de la que fue responsable al nuevo Oficial de Seguridad, en caso de ausencia, al Comité de Seguridad de la Información.

DISPOSICIONES GENERALES

PRIMERA. - Se designa al Subsecretario de Estado - Gobierno Electrónico o su delegado, para que en representación del Ministro de Telecomunicaciones y de la Sociedad de la Información, pueda emitir

oficios, comunicaciones y cualquier otro documento que permita la implementación, control y seguimiento del Esquema Gubernamental de Seguridad de la Información- EGSI.

SEGUNDA. - El Ministerio de Telecomunicaciones y de la Sociedad de la Información, a través de la Subsecretaría de Estado - Gobierno Electrónico, una vez finalizado el plazo fijado para la implementación, realizará la evaluación del cumplimiento del EGSI basado en los criterios establecidos en el Plan de Evaluación que para el efecto se elabore.

Durante el proceso de implementación del EGSI, las instituciones reportarán el avance mediante el Sistema de Gestión por Resultados (GPR) u otras herramientas que se implemente para el efecto.

TERCERA. - El Ministerio de Telecomunicaciones y de la Sociedad de la Información, a través de la Subsecretaría de Estado - Gobierno Electrónico, deberá elaborar hasta el 31 de enero de cada año un *"Plan de Evaluación"* una vez finalizado el plazo de implementación del EGSI, que será socializado a las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.

CUARTA. - En caso de no ser posible la implementación de controles establecidos en el EGSI, deberá ser justificado técnicamente y comunicado a la Subsecretaría de Estado – Gobierno Electrónico, del Ministerio de Telecomunicaciones y de la Sociedad de la Información, para su análisis y aprobación.

QUINTA. - Los Oficiales de Seguridad de la Información de las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, actuarán como contrapartes del Ministerio de Telecomunicaciones y de la Sociedad de la Información en la actualización e implementación del EGSI, quienes reportarán a través del sistema Gobierno por Resultados (GPR).

SEXTA. - Las instituciones deberán remitir hasta el 31 de enero de cada año un *"Informe de cumplimiento de la Gestión de Riesgos"* debidamente suscrito por la máxima autoridad, a la Subsecretaria de Estado - Gobierno Electrónico del Ministerio de Telecomunicaciones y de la Sociedad de la Información.

SÉPTIMA. - Es responsabilidad de la máxima autoridad de cada institución gestionar la implementación de esta normativa asignando los recursos necesarios.

DISPOSICIONES TRANSITORIAS

PRIMERA. - La designación de Oficial de Seguridad de la Información deberá ser comunicada al Subsecretario de Estado - Gobierno Electrónico o su delegado, del Ministerio de Telecomunicaciones y de la Sociedad de la Información dentro del plazo de treinta (30) días posteriores a la publicación del presente Acuerdo Ministerial en el Registro Oficial.

En el caso de cambio de Oficial de Seguridad de la Información, deberá comunicarse de forma inmediata a la misma autoridad.

SEGUNDA. - Para efectivizar el control y seguimiento del EGSI el Subsecretario de Estado - Gobierno Electrónico o su delegado, del Ministerio de Telecomunicaciones y de la Sociedad de la Información en un plazo de sesenta (60) días desde la publicación del presente Acuerdo Ministerial en el Registro Oficial, creará indicadores de gestión e implementación del Esquema Gubernamental de Seguridad de la Información -EGSI-, en el sistema Gobierno por Resultados (GPR).

TERCERA. - El Subsecretario de Estado - Gobierno Electrónico o su delegado, del Ministerio de Telecomunicaciones y de la Sociedad de la Información, en un plazo de sesenta (60) días a partir de la publicación del presente Acuerdo Ministerial en el Registro Oficial, emitirá el formato en el cual las instituciones presentarán el *"Informe de cumplimiento de la Gestión de Riesgos"*.

CUARTA. - El Subsecretario de Estado - Gobierno Electrónico o su delegado, del Ministerio de Telecomunicaciones y de la Sociedad de la Información, en un plazo de noventa (90) días a partir de la publicación del presente Acuerdo Ministerial en el Registro Oficial, emitirá los lineamientos para el seguimiento y control de la implementación del Esquema Gubernamental de Seguridad de la Información -EGSI-.

DISPOSICIÓN DEROGATORIA ÚNICA

Deróguese el Acuerdo Ministerial No. 166, publicado en el Registro Oficial Suplemento No.88 de 25 de septiembre de 2013 y los artículos 11, 12, 13 y 15 del Acuerdo Ministerial No. 1606 publicado en Registro Oficial 776 de 15 de junio del 2016.

El presente Acuerdo Ministerial entrará en vigencia a partir de su publicación en el Registro Oficial.

Dado en el Distrito Metropolitano de Quito, a 20 de septiembre de 2019.

Lcdo. Andrés Michelena Ayala
MINISTRO DE TELECOMUNICACIONES
Y DE LA SOCIEDAD DE LA INFORMACIÓN

MM/ MS/ OC/ GB/ ED/ LG/ BC

ANEXO

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION (EGSI)

Versión 2.0

"El Sistema de Gestión de Seguridad de la Información de las Instituciones Públicas de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva -APCID-"

INTRODUCCIÓN

Los avances de las Tecnologías de la Información y Comunicación (TIC) han ocasionado que los gobiernos otorguen mayor atención a la protección de sus activos de información con el fin de generar confianza en la ciudadanía, en sus propias instituciones y minimizar riesgos derivados de vulnerabilidades y amenazas informáticas.

El presente documento, denominado Esquema Gubernamental de Seguridad de la Información (EGSI), está basado en las normas técnicas ecuatorianas *"INEN ISO/IEC 27000"*, para la Gestión de la Seguridad de la Información y está dirigido a las Instituciones de la Administración Pública Central e Institucional y que depende de la Función Ejecutiva – APCID -.

El EGSI establece un conjunto de recomendaciones para la Gestión de la Seguridad de la Información y ejecuta un proceso de mejora continua en las instituciones de la Administración Pública. El EGSI no reemplaza a las normas técnicas ecuatorianas INEN ISO/IEC 27000.

La implementación del EGSI procura incrementar la seguridad de la información en las instituciones públicas, así como alcanzar la confianza de los ciudadanos en la Administración Pública.

"El Esquema Gubernamental de Seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos de seguridad de la información y la selección de controles para el tratamiento de los riesgos identificados".

GUÍA PARA LA IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

(NTE INEN ISO/IEC 27001:2017)

INTRODUCCIÓN

Esta guía se ha preparado para proporcionar los requisitos para establecer, implementar y mantener el mejoramiento continuo del Esquema Gubernamental de Seguridad de la Información, que pretende ser el Sistema de Gestión de Seguridad en las instituciones Públicas de la APCID.

El establecimiento y la implementación del Esquema Gubernamental de Seguridad de la Información, están influenciados por las necesidades y objetivos de la institución, los requisitos de seguridad, los procesos utilizados, el tamaño y estructura de la institución.

El Esquema Gubernamental de Seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos de seguridad de la información y la selección de controles para el tratamiento de los riesgos identificados.

OBJETIVO

Brindar los primeros lineamientos para que las instituciones de la APCID inicien con la implementación del Esquema Gubernamental de Seguridad de la Información.

ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN EN LAS INSTITUCIONES DE LA APCID

La asignación de responsabilidades se definió en los artículos 5, 6, 7 y 8 del acuerdo ministerial, sin embargo, en esta guía se esclarece la estructura organizacional en materia seguridad de la información en las instituciones públicas de la APCID. A continuación, se presenta las 2 figuras o roles que son base para el trabajo en seguridad de la información, estableciendo las responsabilidades que cada uno debería tener.

Queda abierto el realizar ampliaciones en cada institución, a las responsabilidades definidas, de manera que se adapte a cada realidad particular y se cumpla con la implementación del EGSI.

Oficial de Seguridad de la Información (OSI)

El Comité de Seguridad de la Información (CSI) designará al interior de su Institución a un funcionario como Oficial de Seguridad de la Información (OSI).

El Oficial de Seguridad debe tener conocimiento en Seguridad de la Información y Gestión de Proyectos, podrá ser si existiere el responsable de la Unidad de Seguridad de la Información, se recomienda que no pertenezca al área de Tecnologías de la Información.

El Oficial de Segundad de la Información, será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento del Esquema Gubernamental de Seguridad de la Información. Es

recomendable que el oficial de Seguridad de la Información sea un miembro independiente de las áreas de tecnología o sistemas, puesto que deberá mantener su independencia para observar las necesidades de seguridad entre la estrategia de la institución y tecnología.

Es importante que este funcionario cuente con la aceptación y apoyo de todas las áreas de la institución, es por esto que a la hora de elegir al funcionario que lleve adelante este rol es necesario que sea elegido en consenso.

Cualidades como: liderazgo, capacidad para lograr acuerdos, aceptación de sus pares, poder de gestión; son fundamentales para llevar con éxito la tarea de Oficial de Seguridad de la Información -OSI-.

Dentro de sus principales responsabilidades se encuentra:

a) Identificar todas las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI:

- *Identificar convenientemente las partes interesadas relacionadas con el negocio y en especial con la seguridad de la información.*
- *Identificar los requisitos / necesidades de las partes interesadas.*
- *Identificar los canales de comunicación con las partes interesadas especialmente con las autoridades y grupos de interés especiales.*
- *Ejercer una labor de coordinación con las tareas y medios de protección de datos personales.*

b) Generar propuestas para la elaboración de la documentación esencial del Esquema Gubernamental de Seguridad de la Información (EGSI):

- *Política de Seguridad de la información*
- *Política de control de la Documentación*
- *Política de control de accesos*
- *Uso aceptable de los activos*
- *Evaluación de riesgos*
- *Metodología de tratamiento de riesgos*
- *Declaración de aplicabilidad*
- *Plan de tratamiento de riesgos*
- *Política de revisión y actualización de la documentación*

c) Asesorar a los funcionarios en la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas:

- *Formación interna a los funcionarios propietarios de los activos de información, para que colaboren en la realización de la evaluación de riesgos*
- *Coordinar el proceso de evaluación del riesgo.*
- *Proponer la selección de controles para el tratamiento del riesgo.*
- *Proponer plazos de aplicación para los controles.*

d) Elaborar el Plan de concienciación en Seguridad de la Información basado en el Esquema Gubernamental de Seguridad de la Información (EGSI):

- *Preparar el plan de formación y concienciación para la seguridad de la información y el cumplimiento del EGSI.*
- *Realizar actividades continuas relacionadas con la concienciación.*
- *Planificar charlas de Seguridad de Información para nuevos funcionarios.*
- *Plan de medidas disciplinarias para violaciones a la seguridad de la Información.*

e) Elaborar un plan de seguimiento y control de la implementación de las medidas de mejora o acciones correctivas:

- *Plan de control de implementación de las medidas de mejora o acciones correctivas.*
- *Control de la efectividad de las medidas adoptadas*

f) Coordinar la elaboración del Plan de Continuidad de Seguridad de la Información:

- *Coordinar la elaboración de un plan de continuidad de seguridad de la información.*
- *Coordinar la revisión del plan con ejercicios y pruebas.*
- *Verificar los planes de recuperación después de incidentes.*

g) Orientar y generar un procedimiento adecuado para el manejo de los incidentes de seguridad de la información detectados o reportados.

h) Coordinar la gestión de incidentes de seguridad con nivel de criticidad alto a través de otras instituciones gubernamentales.

i) Mantener la documentación de la implementación del EGSI debidamente organizada.

j) Verificar el cumplimiento de las normas, procedimientos y controles de seguridad institucionales establecidos.

k) Informar al Comité de Seguridad de la Información, el avance de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), así como las alertas que impidan su implementación:

- *Plan de comunicación de los beneficios de la Seguridad de la Información*
- *Proponer objetivos de Seguridad de la Información*
- *Informe de resultados sobre indicadores medibles*
- *Propuestas de mejoras en la Seguridad de la Información*
- *Evaluación de recursos necesarios para la Seguridad de la Información*

l) Previa la terminación de sus funciones el Oficial de Seguridad realizará la transferencia de la documentación e información de la que fue responsable al nuevo Oficial de Seguridad, en caso de ausencia, al Comité de Seguridad de la Información.

Comité de Seguridad de la Información (CSI)

El Comité de Seguridad de la Información (CSI), estará integrado por los responsables de las siguientes áreas o quienes haga sus veces: Talento Humano, Administrativa, Planificación y Gestión Estratégica, Comunicación Social, Tecnologías de la Información, Unidades Agregadores de Valor y el Área Jurídica participará como asesor.

Este comité tendrá reuniones bimensualmente, de manera recomendada durante el transcurso del primer año de implementación, desde la emisión del acuerdo ministerial.

Es imprescindible que desde las primeras reuniones del comité, puedan estar presentes todos los líderes/responsables de las áreas, con el fin de estimular la aprobación de políticas y normativas en relación a la Seguridad de la Información en cada institución; en las siguientes reuniones el enfoque puede orientarse a la planificación estratégica y gestión de aspectos vinculados a la seguridad de la información, por lo que se podría delegar la participación a los representantes de las respectivas áreas involucradas.

El Comité tendrá como principales responsabilidades:

a) Gestionar la aprobación de la política y normas institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la Institución.

b) Realizar el seguimiento de los cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

c) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto.

d) Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI.

e) Promover la difusión de la seguridad de la información dentro de la institución.

f) Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.

g) El comité deberá convocarse trimestralmente o cuando las circunstancias lo ameriten, se deberá llevar registros y actas de las reuniones.

h) Informar a la máxima autoridad los avances de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

i) Reportar a la máxima autoridad las alertas que impidan la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

j) Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

Para lograr el objetivo planteado con la Implementación del Esquema Gubernamental de Seguridad de la Información – EGSI -, es decir que la implementación sea orientada como un Sistema de Gestión de Seguridad de la Información (SGSI), es primordial conocer los principios, beneficios, modelo, entre otros aspectos de un SGSI.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

El Sistema de Gestión de Seguridad de la Información es el elemento más importante de la norma ISO 27001, que unifica los criterios para la evaluación de los riesgos asociados al manejo de la información institucional.

PRINCIPIOS

El Sistema de Gestión de Seguridad de la Información tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de la información:

Figura No.1 PRINCIPIOS DE LA S.I., Fuente: https://infosegur.wordpress.com/tag/disponibilidad/

- **Confidencialidad**: La información solo tiene que ser accesible o divulgada a aquellos que están autorizados.
- **Integridad**: La información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros.
- **Disponibilidad**: La información debe estar siempre accesible para aquellos que estén autorizados.

BENEFICIOS

Entre los beneficios relevantes de un SGSI podemos citar los siguientes:

- Establece una metodología de Gestión de la Seguridad estructurada y clara.
- Reduce el riesgo de pérdida, robo o integridad de la información sensible.
- Los riesgos y los controles son continuamente revisados.
- Se garantiza la confianza de los usuarios en los servicios institucionales.
- Facilita la integración con otros sistemas de gestión.
- Se garantiza la continuidad de negocio tras un incidente grave.
- Cumple con la legislación vigente sobre información personal, propiedad intelectual y otras.

- La imagen de la institución mejora.
- Aumenta la confianza y las reglas claras para los miembros de la institución.
- Reduce los costes y la mejora de los procesos y el servicio.
- Se incrementa la motivación y la satisfacción del personal.
- Aumenta la seguridad en base la gestión de procesos en lugar de una compra sistemática de productos y tecnologías.

CICLO DE VIDA (modelo PDCA)

Es recomendable que los sistemas de gestión sean desarrollados bajo la metodología de la "mejora continua" o ciclo de Deming, conocido como círculo PDCA, del inglés Plan-Do-Check-Act.

Figura No.2 MODELO PDCA, Fuente: https://www.jacquelinebetancourt.com/single-post/2019/03/04/Mejora-Continua-Excelencia-a-nuestro-alcance

La relación que existe entre el modelo PDCA Y La ISO 27001:2013 se presenta a continuación:

Figura No.3, ESTRUCTURA PDCA-ISO27001, Fuente: elaboración propia.

PROCESO PDCA ASOCIADO AL ESTANDAR INTERNACIONAL ISO 27001

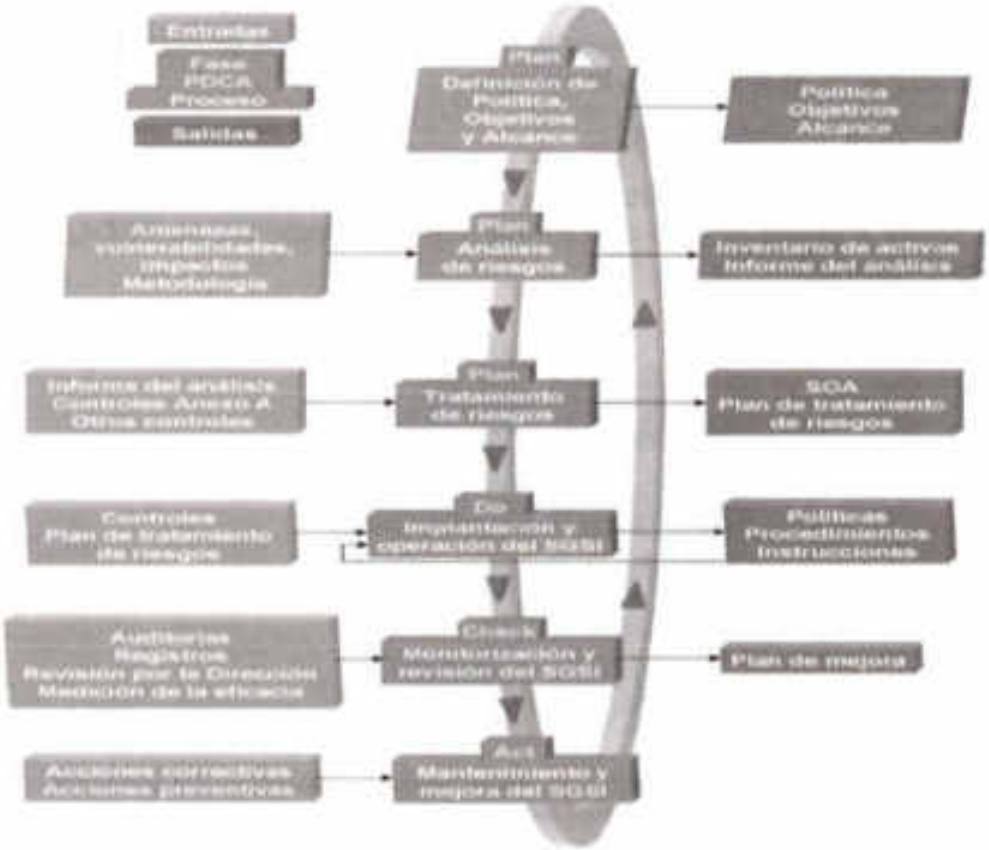

Figura No.4, PROCESO PDCA-ISO27001, Fuente: http://www.iso27000.es/sgsi.html

"La adecuada Gestión de los Riesgos en Seguridad de la Información, conllevará a una efectiva implantación de un Sistema de Gestión de Seguridad de la Información. Sólo una vez identificado los riesgos existentes, permitirá aplicar los controles necesarios para su tratamiento".

GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

(NTE-INEN ISO/EC 27005:2008 & MAGERIT)

INTRODUCCIÓN

La revolución digital ha generado que las organizaciones a nivel mundial tomen mayor atención a la información, actor principal de este proceso de cambio. Este proceso ha permitido establecer nuevas alianzas y acortar distancias entre naciones, donde el internet cumple un papel fundamental en la comunicación.

En términos de gestión de riesgos de seguridad de la información, el activo a proteger es la información, tanto de información digital, contenida en los sistemas de información como aquella contenida en cualquier otro medio como por ejemplo el papel. Debemos tener presente que la gestión debe ocuparse de todo el ciclo de vida de la información.

Es necesario un enfoque sistemático para la gestión del riesgo en la seguridad de la información para identificar las necesidades de la organización con respecto a los requisitos de seguridad de la información y para crear un eficaz sistema de gestión de la seguridad de la información – SGSI -.

Este enfoque debe ser adecuado para el entorno de la institución y, en particular, debería cumplir los lineamientos de toda la gestión del riesgo de la institución.

Los esfuerzos de seguridad deben abordar los riesgos de una manera eficaz y oportuna donde y cuando sean necesarios. La gestión del riesgo de la seguridad de la información debe ser una parte integral de todas las actividades de la gestión de la seguridad de la información y se deben aplicar tanto a la implementación como al funcionamiento continuo de un SGSI.

La gestión del riesgo de la seguridad de la información debe ser un proceso continuo. Tal proceso debe establecer el contexto, evaluar los riesgos, tratar los riesgos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones.

"La gestión del riesgo analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debe hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable".

CONCEPTOS BÁSICOS

La información es el activo principal pero también debemos considerar: infraestructura informática, equipos auxiliares, redes de comunicaciones, instalaciones y personas.

Cuando hablamos de seguridad de la información hablamos de protegerla de riesgos que puedan afectar a una o varias de sus tres principales propiedades:

- **Confidencialidad**: La información solo tiene que ser accesible o divulgada a aquellos que están autorizados.
- **Integridad**: La información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros.

- **Disponibilidad**: La información debe estar siempre accesible para aquellos que estén autorizados.

Figura No.1 PRINCIPIOS DE LA S.I., Fuente: https://infosegur.wordpress.com/tag/disponibilidad/

Para facilitar el proceso de análisis y valoración de los riesgos es importante entender algunos conceptos básicos:

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Amenaza: causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Impacto: es la consecuencia de la materialización de una amenaza sobre un activo. El costo para la institución de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros (ejem.: pérdida de reputación, implicaciones legales, entre otros).

Riesgo inherente: Es el riesgo existente y propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo.

PROCESO PARA LA GESTIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

El proceso de gestión del riesgo de la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o de tratamiento del riesgo. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración. El enfoque iterativo suministra un buen equilibrio entre la reducción del tiempo y el esfuerzo requerido para identificar los controles, incluso garantizando que los riesgos de impacto alto se valoren de manera correcta.

Actividades para la gestión del riesgo de la seguridad de la información:

- Establecimiento del contexto
- Valoración del riesgo

- Tratamiento del riesgo
- Aceptación del riesgo
- Comunicación del riesgo
- Monitoreo y revisión del riesgo

Pasos de las actividades del proceso de gestión del riesgo:

PROCESO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN	
ACTIVIDADES	**PASO**
Establecimiento del contexto	*1. Consideraciones Generales - Levantamiento de información inicial* *2. Establecer criterios básicos para la Gestión del Riesgo* *3. Definir alcance y límites de la Gestión del Riesgo* *4. Establecer una organización para la operación del SGRSI*
Valoración del Riesgo	*5. Identificar Activos de Información* *6. Identificar las amenazas y las vulnerabilidades* *7. Identificar los controles existentes* *8. Identificar consecuencias* *9. Valorar las consecuencias* *10. Valorar los incidentes* *11. Determinar el nivel de estimación del riesgo* *12. Evaluar el riesgo*
Tratamiento del Riesgo	*13. Seleccionar controles*
Aceptación del Riesgo	*14. Aceptar el riesgo*
Comunicación del Riesgo	*15. Comunicar el riesgo*
Monitoreo y Revisión del Riesgo	*16. Monitorear y revisar los riesgos*

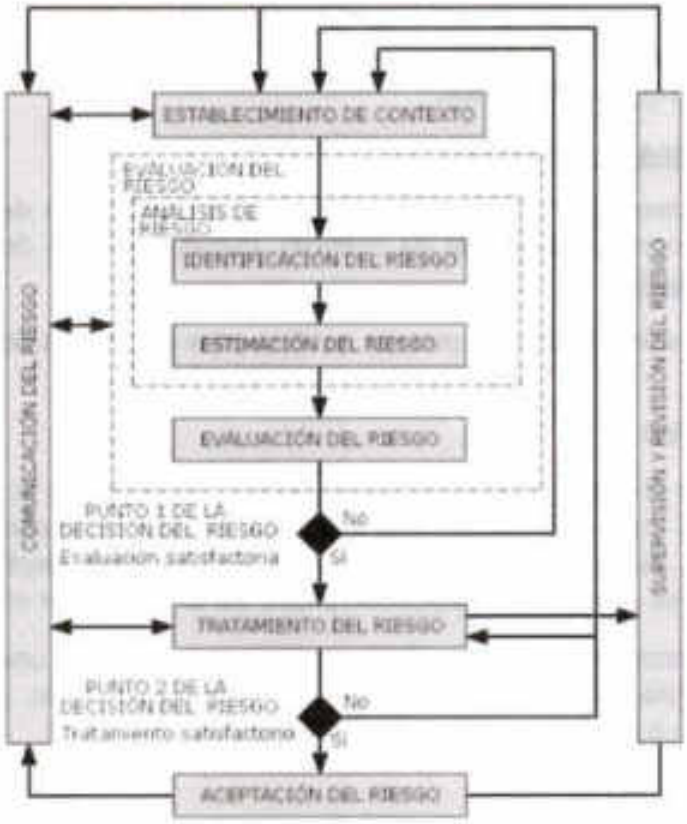

Figura No. 2 PROCESO DE GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN, Fuente: ISO27005

ESTABLECIMIENTO DEL CONTEXTO

CONSIDERACIONES GENERALES

"Se debe establecer el contexto para la gestión del riesgo de la seguridad de la información, lo cual implica establecer los criterios básicos que son necesarios para la gestión del riesgo de la seguridad de la información: definir el alcance y los límites, establecer una organización adecuada que opere la gestión del riesgo de la seguridad de la información".

CRITERIOS BÁSICOS

Dependiendo del alcance y los objetivos de la gestión del riesgo, se pueden aplicar diferentes enfoques. El enfoque también podría ser diferente para cada iteración.

Es aconsejable seleccionar o desarrollar un enfoque adecuado para la gestión del riesgo que aborde los criterios básicos tales como: criterios de evaluación del riesgo, criterios de impacto, criterios de aceptación del riesgo, entre otros.

Criterios de identificación del riesgo

Es recomendable considerar los activos de información con el valor de impacto alto para el proceso de evaluación del riesgo.

Criterios de evaluación del riesgo

Es recomendable desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo de la seguridad de la información de la institución.

Criterios de impacto

Es recomendable desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la organización, causados por un evento de seguridad de la información.

Criterios de la aceptación del riesgo

Es recomendable desarrollar y especificar criterios de aceptación del riesgo. Estos criterios dependen con frecuencia de las políticas, metas, objetivos de la institución y de las partes interesadas.

Las instituciones pueden definir sus propias escalas para los niveles de aceptación del riesgo.

ALCANCE Y LÍMITES

Es necesario definir el alcance del proceso de gestión del riesgo de la seguridad de la información, con el fin de garantizar que todos los activos relevantes se toman en consideración en la valoración del riesgo. Además, es necesario identificar los límites para abordar aquellos riesgos que se pueden presentar al establecer estos límites.

Los ejemplos del alcance de la gestión del riesgo pueden ser una aplicación de tecnología de la información, infraestructura de tecnología de la información, un proceso del negocio o una parte definida de la institución

"El alcance y los límites de la gestión del riesgo de la seguridad de la información se relacionan con el alcance y los límites del Esquema Gubernamental de Seguridad de la información – EGSI -"

ORGANIZACIÓN PARA LA GESTIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

Se recomienda establecer y mantener la organización y las responsabilidades en el proceso de gestión del riesgo y la seguridad de la información definidas en el acuerdo ministerial.

Esta organización para la gestión del riesgo, debería ser aprobada por la máxima autoridad de cada institución.

VALORACIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

"Los riesgos se deberían identificar, describir cuantitativa o cualitativamente y priorizar frente a los criterios de evaluación del riesgo y los objetivos relevantes para la institución"

Un riesgo es una combinación de las consecuencias que se presentarían después de la ocurrencia de un evento indeseado y de su probabilidad de ocurrencia. La valoración del riesgo cuantifica o describe cualitativamente el riesgo y permite a los propietarios de los activos priorizar los riesgos de acuerdo con su gravedad percibida u otros criterios establecidos.

"En este proceso se obtiene toda la información necesaria para conocer, valorar y priorizar los riesgos"

La valoración del riesgo consta de las siguientes actividades:

- Análisis del riesgo
  - Identificación del riesgo
  - Estimación del riesgo
- Evaluación del riesgo

ANÁLISIS DEL RIESGO

Identificación del riesgo

Consiste en determinar qué puede provocar pérdidas a la institución. La identificación del riesgo consta de las siguientes actividades:

- Identificación de los activos
- Identificación de las amenazas
- Identificación de vulnerabilidades
- Identificación de la existencia de controles.

Identificación de los activos

Un activo es todo aquello que tiene valor para la organización y que, por lo tanto, requiere de protección. Para la identificación de los activos se recomienda tener en cuenta que el sistema de información consta de más elementos que sólo hardware y software.

Se debería identificar al propietario de cada activo, para asignarle la responsabilidad y rendición de cuentas sobre éste. El propietario del activo puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la organización

"La identificación de los activos es un punto clave para la identificación de las amenazas, vulnerabilidades, y determinar el nivel de riesgo o exposición de los activos y la selección de controles para mitigarlos"

De este proceso se genera una lista de los activos que van a estar sometidos a gestión del riesgo, y una lista de los procesos del negocio relacionados con los activos y su importancia.

Para realizar la valoración de los activos, es necesario que la institución identifique primero sus activos (con un grado adecuado de detalles). De manera general se pueden diferenciar dos clases de activos:

Los activos primarios:
- Actividades y procesos del negocio.
- Información.

Los activos de soporte (de los cuales dependen los elementos primarios del alcance) de todos los tipos:
- Hardware.
- Software.
- Redes.
- Personal.
- Ubicación.
- Estructura de la organización.

Ejemplo de identificación de activos:

IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN						
Nro. Activo	**Proceso Macro**	**Subproceso**	**Tipo de Activo**	**Nombre de Activo**	**Descripción del activo**	**Ubicación**
A1	Apoyo de Tecnologías de la Información y Comunicaciones	Infraestructura	Hardware	Controladora Wireless, puntos de acceso	puntos de acceso inalámbrico en toda la institución	Data Center
A2			Hardware	Firewall Fortigate	Control de acceso y permisos de seguridad perimetral para la red institucional	Data Center
A3		Redes y comunicaciones	Redes	Switch Core Cisco 4700	Procesamiento de trafico de red para distribución en la red interna e Internet	Data Center
A4			Redes	Switchs de Acceso Cisco 2960	Procesamiento de trafico de red de acceso en cada piso del edificio	Data Center
A5		Aplicaciones informáticas	Software	Antivirus Institucional	Software de seguridad end point	Data Center
A6			Software	Servicio de correo Exchange	Información de buzones de correo electrónico institucional	Data Center
A7		Instalaciones	Localidad	Datacenter	Centro de Datos Institucional	Edificio Matriz
A8		Talento Humano	Personal	Personal de soporte	Funcionarios de Soporte Técnico Nivel 1 - Institucional	Edificio Matriz
A9			Personal	Personal de desarrollo de sistemas	Personal técnico que desarrolla aplicaciones o automatiza procesos	Edificio Matriz

Valoración de los activos / Ponderación de la criticidad de activos

La ponderación de activos es una etapa en la que participan las unidades del negocio involucradas con el fin de determinar en términos cualitativos la criticidad de los distintos activos.

Esta ponderación fue realizada en términos de "alto, medio o bajo" donde se asigna un valor cuantitativo a cada valor cualitativo

A continuación, se presentan las referencias para la valoración del impacto en los activos de la información.

Valoración del impacto en términos de la perdida de la confidencialidad:

CONFIDENCIALIDAD	Criterio
Alto (3)	La divulgación no autorizada de la información tiene un efecto crítico para la institución Ej. Divulgación de información confidencial o sensible.
Medio (2)	La divulgación no autorizada de la información tiene un efecto limitado para la institución Ej. Divulgación de información de uso interno
Bajo (1)	La divulgación de la información no tiene ningún efecto para la institución Ej. Divulgación de información pública.

Valoración del impacto en términos de la perdida de la integridad:

INTEGRIDAD	Criterio
Alto (3)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución
Medio (2)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución
Bajo (1)	La destrucción o modificación de la información tiene un efecto leve para la institución

Valoración del impacto en términos de la perdida de la disponibilidad:

DISPONIBILIDAD	Criterio
Alto (3)	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución
Medio (2)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución
Bajo (1)	interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución

Con referencia a las tablas mencionadas, la valoración se la realiza respecto a la confidencialidad, integridad y disponibilidad ya que estas son las dimensiones en que se basa la seguridad de la información.

VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN							
Nro. Activo	Nombre de Activo	Tipo de soporte	Ubicación	Valoración de Impacto (pérdida) C: Confidencialidad I: Integridad D: Disponibilidad			
				C	I	D	VA
A1	Controladora Wireless, puntos de acceso	Físico y Lógico	Centro de Datos	1	1	2	1,33
A2	Red de datos	Físico	Edificio Institucional	1	1	3	1,67
A3	Firewall Fortigate	Físico y Lógico	Centro de Datos	2	2	2	2,00
A4	Biométricos	Físico y Lógico	Sala de recepción Institucional	1	1	1	1,00
A5	Cámaras de seguridad	Físico y Digital	Edificio Institucional	1	1	1	1,00
A6	Switch Core Cisco 4700	Físico y Lógico	Centro de Datos	1	1	3	1,67
A7	Switchs de Acceso Cisco 2960	Físico y Lógico	Centro de Datos	1	1	1	1,00
A8	Enlaces de internet	Físico y Lógico	Centro de Datos	1	1	1	1,00
A9	Antivirus Institucional	Lógico	Centro de Datos	1	1	2	1,33
A10	Sistema Talento Humano SIRHA	Lógico	Centro de Datos	1	1	1	1,00

* La valoración del impacto de un activo (VA), es el promedio de los valores de las tres dimensiones de la Gestión de la Seguridad de la Información:

$$VA = \frac{C + I + D}{3}$$

Identificación de Amenazas

Se deben identificar las amenazas y sus orígenes. Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas, por lo tanto, a las organizaciones.

Algunas amenazas pueden afectar a más de un activo. En tales casos pueden causar diferentes impactos dependiendo los activos que se vean afectados.

Ejemplo de análisis de riesgos:

ANÁLISIS DE RIESGOS			
Subprocesos	Nro. Activo	Nombre Activo	Amenaza
Infraestructura	A1	Controladora Wireless, puntos de acceso	Intrusos en la red
			Indisponibilidad de servicios
	A2	Red de datos	Indisponibilidad de servicios
	A3	Firewall Fortigate	Acceso no deseado a activos críticos

			Indisponibilidad de servicios
	A4	Biométricos	Desarrollo de nuevas funcionalidades para la gestión de TH
	A5	Cámaras de seguridad	Acceso de personas no deseables y/o pérdidas de activos.
			Acceso de personas no deseables y/o pérdidas de activos.

Identificación de Vulnerabilidades

Se debe identificar las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos o a la institución.

La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios. Conviene anotar que un control implementado de manera incorrecta o que funciona mal, o un control que se utiliza de modo incorrecto podrían por sí solo constituir una vulnerabilidad.

Ejemplo del análisis de riesgos:

ANÁLISIS DE RIESGOS				
Subprocesos	**Nro. Activo**	**Nombre Activo**	**Amenaza**	**Vulnerabilidad**
Infraestructura	A1	Controladora Wireless, puntos de acceso	Intrusos en la red	Actualización de firmware equipo antiguo
			Indisponibilidad de servicios	No existe equipo de redundancia
	A2	Red de datos	Indisponibilidad de servicios	Red de datos mixta (cat. 5e, 6a)
	A3	Firewall Fortigate	Acceso no deseado a activos críticos	imposibilidad de actualizar firmware por falta de recursos del equipo
			Indisponibilidad de servicios	Inexistencia de equipo de redundancia
	A4	Biométricos	Desarrollo de nuevas funcionalidades para la gestión de TH	Incompatibilidad del software base con plataforma de desarrollo actual (pdqt)
	A5	Cámaras de seguridad	Acceso de personas no deseables y/o pérdidas de activos.	Existencia de áreas sin vigilancia
			Acceso de personas no deseables y/o pérdidas de activos.	Vigencia Tecnología, equipos continuamente dañados

Identificación de Existencia de Controles

"Se debe identificar los controles existentes y los planificados".

Se debe realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo, en la duplicación de los controles. Además, mientras se identifican los controles existentes es recomendable hacer una verificación para garantizar que los controles funcionan correctamente - una referencia a los reportes de auditoría del SGSI ya existente debería limitar el tiempo que tarda esta labor. Si el control no funciona como se espera, puede causar vulnerabilidades.

Ejemplo de los controles existentes (implementados):

Análisis de Riesgos					Evaluación de Riesgos				
					Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo
Subprocesos	Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad		
Infraestructura	A4	Controladora Wireless, puntos de acceso	Indisponibilidad de servicios	Red de datos mixta (cat. 5e, 6a)	1,67	1	1	Mantenimiento local	1,67
Infraestructura	A5	Red de datos	Acceso no deseado a activos críticos	Imposibilidad de actualizar firware por falta de recursos del equipo	2,00	2	2	Soporte contratado	8,00
			Indisponibilidad de servicios	Inexistencia de equipo de redundancia	2,00	2	2	Soporte contratado	8,00
Infraestructura	A6	Firewall Fortigate	Desarrollo de nuevas funcionalidades para la gestión de TH	Incompatibilidad del software base con plataforma de desarrollo actual (php)	1,00	1	1	Mantenimiento local	1,00
Infraestructura	A7	Biometricos	No cumplimiento de actividades del usuario con daño en su equipo	Ausencia de equipos de reemplazo temporal	1,33	1	2	Mantenimiento local	2,67
			Disminución de la gestión del proceso	Hardware con recursos limitados	1,33	1	2	Mantenimiento local	2,67
Infraestructura	A9	Cámaras de Seguridad	Acceso de personas no deseables y/o pérdidas de activos.	Existencia de áreas sin vigilancia	1,00	1	2	Mantenimiento local	2,00
			Acceso de personas no deseables y/o pérdidas de activos.	Vigencia Tecnología, equipos continuamente dañados	1,00	1	1	Mantenimiento local	1,00

Estimación o Análisis del riesgo

"Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo"

Consiste en utilizar métodos cuantitativos o cualitativos para obtener una cuantificación de los riesgos identificados, tomando en cuenta los activos, las amenazas y las políticas.

Luego de identificar los riesgos, el marco de trabajo debe considerar una metodología de análisis de riesgo. El análisis de riesgo cualitativo usa una escala de calificación de atributos para describir la magnitud de las consecuencias potenciales (por ejemplo, baja, media y alta) y la probabilidad de esas consecuencias.

EVALUACIÓN DEL RIESGO

Consiste en comparar los riesgos estimados con los criterios de evaluación y de aceptación de riesgos definidos en el establecimiento del contexto.

Proceso de comparación del riesgo estimado contra un criterio de riesgo calculado dado para determinar la importancia del riesgo. El grado del riesgo es expresado numéricamente basado en las medidas del valor de los activos de información, el impacto de la amenaza y el alcance de la vulnerabilidad.

Criterios de probabilidad de ocurrencia de amenazas:

En la tabla se detallan los criterios calificativos y los valores numéricos a ser utilizados para la valoración de la probabilidad de amenazas que podrían explotar alguna vulnerabilidad existente.

Nivel de amenaza	Criterio por probabilidad	Criterio por condición de ocurrencia	Criterio por atractivo	Ejemplo
Alto (3)	La ocurrencia es muy probable (probabilidad > 50%)	Bajo circunstancias normales	El atacante se beneficia en gran medida por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Código malicioso
Medio (2)	La ocurrencia es probable (probabilidad <50%)	Por errores descuidos	El atacante se beneficia de alguna manera por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Falla de hardware
Bajo (1)	La ocurrencia es menos probable (probabilidad >0 y <50%)	en rara ocasión	El atacante no se beneficia del ataque	desastres naturales

Criterio de probabilidad de ocurrencia de vulnerabilidades

Nivel de vulnerabilidad	Criterio	Ejemplo
Alto (3)	No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza	No se utilizan contraseñas para que los usuarios ingresen a los sistemas
Medio (2)	Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable	Existen normas para la utilización de contraseñas, pero no se implementa
Bajo (1)	La medida de seguridad es adecuada	Existen normas para la utilización de contraseñas y es aplicada

Criterio de la Evaluación de Riesgos

El producto de la probabilidad de ocurrencia de una amenaza, la probabilidad de ocurrencia de vulnerabilidades y el valor del impacto del activo de la información (CID), tenemos como resultado el nivel de riesgo de cada activo

$$\textbf{\textit{Nivel de riesgo}} = \textbf{VA(CID)} * \textbf{Nivel de amenaza} * \textbf{Nivel de vulnerabilidad}$$

Nivel de Riesgo	
1 - 3	El riesgo es BAJO
4 - 8	El riesgo es MEDIO
9 - 27	El riesgo es ALTO

Ejemplo del cálculo de la evaluación de riesgos:

				Evaluación de Riesgos					
				Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad			
A1	Controladora Wireless, puntos de acceso	Intrusos en la red	Actualización de firware equipo antiguo	1,33	1	1	Soporte contratado	1,33	BAJO
		Indisponibilidad de servicios	No existe equipo de redundancia	1,33	1	1	Soporte contratado	1,33	BAJO
A2	Red de datos	Indisponibilidad de servicios	Red de datos mixta (cat. 5e, 6a)	1,67	1	1	Mantenimiento local	1,67	BAJO
A3	Firewall Fortigate	Acceso no deseado a activos críticos	imposibilidad de actualizar firware por falta de recursos del equipo	2,00	2	2	Soporte contratado	8,00	MEDIO
		Indisponibilidad de servicios	Inexistencia de equipo de redundancia	2,00	2	2	Soporte contratado	8,00	MEDIO
A4	Biometricos	Desarrollo de nuevas funcionalidades para la gestión de TH	Incompatibilidad del software base con plataforma de desarrollo actual (php)	1,00	1	1	Mantenimiento local	1,00	BAJO
A5	Cámaras de seguridad	Acceso de personas no deseables y/o pérdidas de activos.	Existencia de áreas sin vigilancia	1,00	1	2	Mantenimiento local	2,00	BAJO
		Acceso de personas no deseables y/o pérdidas de activos.	Vigencia Tecnología, equipos continuamente dañados	1,00	1	1	Mantenimiento local	1,00	BAJO

TRATAMIENTO DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

El tratamiento de los riesgos es tomar decisiones frente a los diferentes riesgos existentes de acuerdo a la estrategia de la institución.

Se deben seleccionar controles para reducir, aceptar/retener, evitar o transferir los riesgos y se debe definir un plan para el tratamiento del riesgo.

Existen cuatro opciones disponibles para el tratamiento del riesgo:

- Reducción del riesgo
- Aceptación del riesgo
- Evitación del riesgo
- Transferencia del riesgo

La Figura ilustra la actividad del tratamiento del riesgo dentro de los procesos de gestión del riesgo de la seguridad de la información:

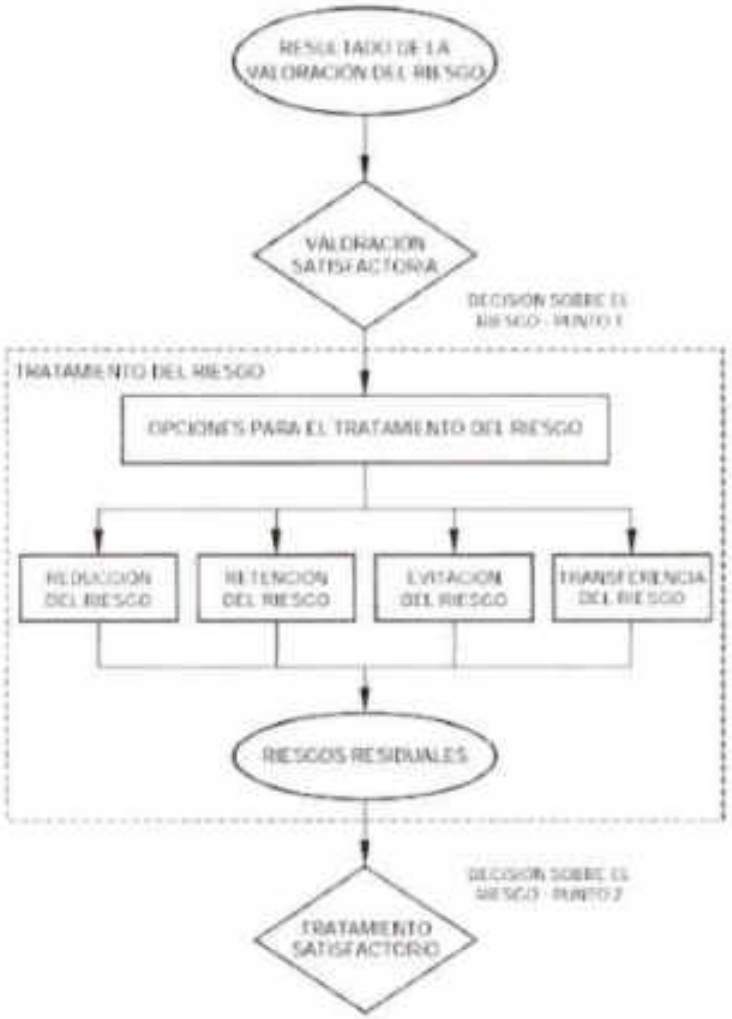

Figura No. 3 ACTIVIDADES PARA EL TRATAMIENTO DE LOS RIESGOS, Fuente: ISO27005

Las opciones para el tratamiento del riesgo se deberían seleccionar con base en el resultado de la valoración del riesgo, el costo esperado para implementar estas opciones y los beneficios esperados como resultado de tales opciones.

Cuando se pueden obtener reducciones grandes en los riesgos con un costo relativamente bajo, se deberían implementar esas opciones. Las opciones adicionales para las mejoras pueden no ser económicas y es necesario estudiarlas para determinar si se justifican o no.

En general, las consecuencias adversas de los riesgos deberían ser tan bajas como sea razonablemente viable e independientemente de cualquier criterio absoluto. En tales casos, puede ser necesario implementar controles que no son justificables en términos estrictamente económicos (por ejemplo, los controles para la continuidad del negocio considerados para cumplir riesgos altos específicos).

REDUCCIÓN DEL RIESGO

Se debe reducir mediante la selección de controles, de manera tal que el riesgo residual se pueda reevaluar como aceptable.

Se debe seleccionar controles adecuados y justificados que satisfagan los requisitos identificados en la valoración y el tratamiento del riesgo. En esta selección se deberían tener en cuenta los criterios de aceptación del riesgo, así como requisitos legales, reglamentarios y contractuales. En esta selección también se deberían considerar los costos y el tiempo para la implementación de los controles, o los aspectos técnicos, ambientales y culturales. Con frecuencia es posible disminuir el costo total de la propiedad de un sistema con controles de seguridad de la información adecuadamente seleccionados.

> *"...tiene por objetivo reducir el nivel del riesgo para a su vez reducir el impacto y la probabilidad de ocurrencia de daños sobre los activos de información de la organización..."*

EVITACIÓN DEL RIESGO

Se debe evitar la actividad o la acción que da origen al riesgo particular.

Cuando los riesgos identificados se consideran muy altos, o si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios, se puede tomar una decisión para evitar por completo el riesgo, mediante el retiro de una actividad o un conjunto de actividades planificadas o existentes, o mediante el cambio en las condiciones bajo las cuales se efectúa tal actividad.

Por ejemplo, para los riesgos causados por la naturaleza, puede ser una alternativa más eficaz en términos de costo, transferir físicamente las instalaciones de procesamiento de la información a un lugar donde no exista el riesgo o esté bajo control

TRANSFERENCIA DEL RIESGO

El riesgo se debe transferir a otra parte que pueda gestionar de manera más eficaz el riesgo particular dependiendo de la evaluación del riesgo.

RETENCIÓN/ACEPTACIÓN DEL RIESGO

La decisión sobre la retención del riesgo sin acción posterior se debería tomar dependiendo de la evaluación del riesgo.

Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la institución para la aceptación de los riesgos.

Ejemplo del tratamiento de los riesgos:

Evaluación de Riesgos						Tratamiento de Riesgos								
Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Método de tratamiento de Riesgos	Tipo de control	Controles a implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control implementado	Riesgo residual
CID	Nivel de amenaza	Nivel de vulnerabilidad											
167	2	2	Soporte contratado	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	Migración a Cloud	1	1	1,67	BAJO	ACEPTABLE
167	2	2	Plan aplicado de pruebas y backup	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	Migración a Cloud	1	1	1,67	BAJO	ACEPTABLE
167	2	2	Plan aplicado de pruebas y backup	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	Migración a Cloud	1	1	1,67	BAJO	ACEPTABLE
167	1	2	Soporte contratado	3,33	BAJO	ACEPTAR	CONTROL PREVENTIVO	Migración a Cloud	1	1	1,67	BAJO	ACEPTABLE
167	2	2	Soporte contratado	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	Migración a Cloud	1	1	1,67	BAJO	ACEPTABLE
167	1	2	Soporte contratado	3,33	BAJO	ACEPTAR	CONTROL PREVENTIVO	Migración a Cloud	1	1	1,67	BAJO	ACEPTABLE

ACEPTACIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

Se deber tomar la decisión de aceptar los riesgos y las responsabilidades de la decisión, y registrarla de manera formal.

Esta opción se toma cuando los costos de implementación de un control de seguridad sobrepasan el valor del activo de información que se desea proteger o cuando el nivel del riesgo es muy bajo, en ambos casos la organización asume los daños provocados por la materialización del riesgo.

En algunos casos, es posible que el nivel del riesgo residual no satisfaga los criterios de aceptación del riesgo porque los criterios que se aplican no toman en consideración las circunstancias prevalentes. Por ejemplo, se puede argumentar que es necesario aceptar los riesgos porque los beneficios que los acompañan son muy atractivos o porque el costo de la reducción del riesgo es demasiado alto.

La organización debería definir sus propias escalas para los niveles de aceptación del riesgo.

Durante el desarrollo, se deberían considerar los siguientes aspectos:

- *Los criterios de aceptación del riesgo pueden incluir umbrales múltiples*, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas.
- Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado (u otros beneficios del negocio) y el riesgo estimado.
- Los diferentes criterios de aceptación del riesgo se pueden aplicar a diferentes clases de riesgos, por ejemplo, los riesgos que podrían resultar en incumplimiento con reglamentos o leyes, podrían no ser aceptados, aunque se puede permitir la aceptación de riesgos altos, si esto se especifica como un requisito contractual.
- Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo, se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

COMUNICACIÓN DE LOS RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN

"La información acerca de los riesgos se debe intercambiar y/o compartir entre quienes toman las decisiones y las partes involucradas."

La comunicación del riesgo es una actividad para lograr un acuerdo sobre la manera de gestionar los riesgos al intercambiar y/o compartir la información acerca de los riesgos. La información incluye, pero no se limita a la existencia, naturaleza, forma, probabilidad, gravedad, tratamiento y aceptabilidad de los riesgos.

La comunicación eficaz entre las partes involucradas es importante dado que puede tener un impacto significativo en las decisiones que se deben tomar. La comunicación garantizará que aquellos responsables de la implementación de la gestión del riesgo y aquellos con intereses establecidos comprendan las bases sobre las cuales toman las decisiones y por qué se requieren acciones particulares. La comunicación es bidireccional.

La comunicación del riesgo se debería realizar con el fin de lograr lo siguiente:

- Proporcionar seguridad del resultado de la gestión del riesgo de la institución.
- Recolectar información del riesgo.
- Compartir los resultados de la valoración del riesgo y presentar el plan para el tratamiento del riesgo.
- Evitar o reducir tanto la ocurrencia como la consecuencia de las brechas de seguridad de la información debido a la falta de entendimiento entre quienes toman las decisiones y las partes involucradas.
- Brindar soporte para la toma de decisiones.
- Obtener conocimientos nuevos sobre la seguridad de la información.
- Coordinar con otras partes y planificar las respuestas para reducir las consecuencias de cualquier incidente.
- Dar a quienes toman las decisiones y a las partes involucradas un sentido de responsabilidad acerca de los riesgos.
- Mejorar la toma de conciencia.

La coordinación entre las personas principales que toman las decisiones y las partes involucradas se puede lograr en el Comité de Seguridad de la Información (CSI) en el cual pueda tener lugar el debate acerca de los riesgos, su prioridad, el tratamiento adecuado y la aceptación.

MONITOREO Y REVISIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

MONITOREO Y REVISIÓN DE LOS FACTORES DE RIESGO

Los riesgos no son estáticos. Las amenazas, las vulnerabilidades, la probabilidad o las consecuencias pueden cambiar abruptamente sin ninguna indicación. Por ende, es necesario el monitoreo constante para detectar estos cambios.

Esta actividad puede estar soportada por servicios externos que brinden información con respecto a nuevas amenazas o vulnerabilidades.

Las organizaciones deberían garantizar el monitoreo continuo de los siguientes aspectos:

- Activos nuevos que se han incluido en el alcance de la gestión del riesgo.
- Modificaciones necesarias de los valores de los activos, por ejemplo, debido a cambios en los requisitos del negocio.
- Nuevas amenazas que podrían estar activas tanto fuera como dentro de la organización y que no se han valorado.
- Probabilidad de que nuevas vulnerabilidades o el incremento en las vulnerabilidades existentes permitan que las amenazas las exploten.
- Vulnerabilidades identificadas para determinar aquellas que se exponen a nuevas amenazas o que vuelven a surgir.
- El incremento en el impacto o las consecuencias de las amenazas evaluadas, las vulnerabilidades y los riesgos en conjunto que dan como resultado un nivel inaceptable de riesgo.
- Incidentes de la seguridad de la información.

Los factores que afectan a la probabilidad y a las consecuencias de las amenazas que se presentan podrían cambiar, como lo harían los factores que afectan a la idoneidad o el costo de las diversas opciones de tratamiento. Los cambios importantes que afectan a la organización deberían ser la razón para una revisión más específica. Por lo tanto, las actividades de monitoreo del riesgo se deberían repetir con regularidad y las opciones seleccionadas para el tratamiento del riesgo se deberían revisar periódicamente.

MONITOREO, REVISIÓN Y MEJORA DE LA GESTIÓN DEL RIESGO

"El proceso de gestión del riesgo en la seguridad de la información se debe monitorear, revisar y mejorar continuamente, según sea necesario y adecuado".

El monitoreo y la revisión continuos son necesarios para garantizar que el contexto, el resultado de la valoración del riesgo y el tratamiento del riesgo, así como los planes de gestión siguen siendo pertinentes y adecuados para las circunstancias actuales.

La organización debe garantizar que el proceso de gestión del riesgo de la seguridad de la información y las actividades relacionadas aún son adecuadas en las circunstancias actuales y se cumplen. Todas las mejoras acordadas para el proceso o las acciones necesarias para mejorar la conformidad con el proceso se deberían notificar al Comité de Seguridad de la Información, para tener seguridad de que no se omite ni subestima ningún riesgo o elemento del riesgo, y que se toman las acciones necesarias y las decisiones para brindar una comprensión realista del riesgo y la capacidad para responder.

GUÍA PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

(NTE-INEN ISO/IEC 27002:2017)

ANTECEDENTES Y CONTEXTO

Esta guía está diseñada para que las instituciones públicas de la APCID la usen como referencia a la hora de seleccionar controles dentro del proceso de implementación del Esquema Gubernamental de Seguridad de la Información como un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001 o bien como documento referencial para instituciones que implementen controles de seguridad de la información comúnmente aceptados.

Las instituciones públicas de todo tipo y tamaño recogen, procesan, almacenan y transmiten información de muchas formas que incluyen medios electrónicos, físicos y verbales. El valor de la información va más allá de las palabras escritas, números e imágenes: conocimientos, conceptos, ideas y marcas son ejemplos de formas intangibles de la información.

En un mundo interconectado, información y procesos relacionados, sistemas, redes y personal que participan en su operación, manejo y protección de los activos, al igual que otros activos comerciales importantes, son valiosos para el desarrollo de una institución, por lo que requieren protección contra diversos riesgos.

Los activos están sujetos tanto a amenazas deliberadas como accidentales, mientras que los procesos relacionados, los sistemas, las redes y las personas tienen vulnerabilidades inherentes. Los cambios en los procesos y sistemas de negocio u otros cambios externos (por ejemplo, nuevas leyes y reglamentos) pueden crear nuevos riesgos de seguridad de la información. Por lo tanto, dada la multitud de formas en que las amenazas podrían aprovecharse de las vulnerabilidades para dañar a la institución, los riesgos de seguridad de la información están siempre presentes. Una seguridad de la información eficaz reduce estos riesgos protegiendo a la organización frente a las amenazas y vulnerabilidades, y en consecuencia reduce el impacto en sus activos.

La seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, incluidas las políticas, procesos, procedimientos, estructuras institucionales, de software y funciones del hardware. Estos controles se deben establecer, implementar, supervisar, revisar y mejorar, cuando sea necesario, para asegurar que se cumplen los objetivos de seguridad y de los objetivos estratégicos de cada institución.

"La seguridad que se puede lograr a través de medios técnicos es limitada y debe ser apoyada por la administración y los procedimientos apropiados".

"Un Sistema de Gestión de Seguridad de la Información exitoso requiere el apoyo de todos los miembros de la institución, se requiere la participación de la máxima autoridad, los líderes de áreas, proveedores u otras partes externas. El asesoramiento especializado de las partes externas puede ser necesario".

REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN

Es fundamental que las instituciones identifiquen sus requisitos de seguridad, para lo cual existen tres fuentes principales de requisitos de seguridad:

- La evaluación de los riesgos de la institución.
- El conjunto de requisitos legales.
- El conjunto de principios, objetivos y requisitos de negocio que la institución ha desarrollado para el manejo, procesamiento, almacenamiento, comunicación y archivo de la información que da soporte a sus operaciones.

"Los recursos utilizados en la implementación de los controles han de estar equilibrados con el nivel de daños probables que resultarían de problemas de seguridad en ausencia de dichos controles".

SELECCIÓN DE CONTROLES

La selección de los controles depende de las decisiones de carácter organizativo basadas en los criterios de aceptación del riesgo, las opciones de procesamiento del riesgo y de los enfoques generales de gestión del riesgo aplicados en la institución, y debería depender también de toda la legislación y reglamentación nacional e internacional aplicable.

La selección de los controles también depende del modo en que los controles interactúan para proporcionar una protección en profundidad.

Algunos de los controles en esta guía, pueden considerarse como principios que guían la gestión de la seguridad de la información, siendo aplicables a la mayoría de las instituciones.

"Se pueden agregar nuevos controles para cubrir adecuadamente las necesidades específicas de cada institución".

ESTRUCTURA DE ESTA GUÍA

Esta guía contiene 14 capítulos (dominios) de controles de seguridad que en conjunto contienen un total de 35 categorías (objetivos de control) principales de seguridad y 114 controles.

Cada capítulo que define controles de seguridad, contiene una o más categorías principales de controles de seguridad.

"El orden de los capítulos de esta guía no implica un orden de importancia. En función de las circunstancias, los controles de seguridad de uno o todos los capítulos pueden ser importantes, por lo tanto, cada institución que aplique esta guía debe identificar qué controles son aplicables, qué tan importantes son y su aplicación a cada proceso de negocio. De la misma manera, el orden de la lista de controles de esta norma no implica orden de prioridad".

CONTENIDO

1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

1.1 Dirección de gestión de seguridad de la información

1.1.1 Políticas de seguridad de la información

Control

Elaborar, implementar y socializar las políticas de seguridad de la información, definidas para la institución, debidamente aprobada por la Máxima Autoridad o su delegado.

Recomendaciones para la implementación:

1.1.1.1 La máxima autoridad dispondrá la implementación de este Esquema Gubernamental de Seguridad de la Información (EGSI) en su institución.

1.1.1.2 Difundir la siguiente política de seguridad de la información como referencia:

Las instituciones de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera".

1.1.1.3 Las instituciones públicas podrán especificar y difundir una política de seguridad más amplia o específica en armonía con la Constitución, leyes y demás normativa legal propia o relacionada, así como su misión y competencias.

1.1.2 Revisión de las políticas para la seguridad de la información

Control

Para garantizar la vigencia de la política de seguridad de la información en la institución, esta debe ser revisada anualmente o cuando se produzcan cambios significativos a nivel operativo, legal, tecnológica, económico, entre otros; los cuales deben ser documentados y versionados.

2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

2.1 Organización interna

2.1.1 Compromiso de la máxima autoridad de la institución con la seguridad de la información.

Control

La institución debe definir y asignar claramente todas las responsabilidades para la seguridad de la información

Recomendaciones para la implementación:
Aquellas áreas hacia las cuales los individuos tienen asignadas responsabilidades deberían quedar establecidas, en particular con relación a los siguientes aspectos:

2.1.1.1 Realizar el seguimiento de la puesta en marcha de las normas de este documento.
2.1.1.2 Disponer la difusión, capacitación y sensibilización del contenido de este documento.
2.1.1.3 Información y reportará a la máxima autoridad de la institución.
2.1.1.4 Definir y hacer cumplir lo definido para la coordinación y supervisión de seguridad de la información con los proveedores
2.1.1.5 Identificar y definir los activos institucionales y los procesos de seguridad de la información
2.1.1.6 Designar funcionarios competentes, para completar las responsabilidades en el área de seguridad de la información.
2.1.1.7 Definirse las responsabilidades para las actividades de gestión de riesgos de seguridad de la información y, en particular, para la aceptación del riesgo residual.

2.1.1.12 Asignación de responsabilidades para la seguridad de la información.

2.1.2 Separación de funciones

Control

La institución debe separar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la institución.

Recomendaciones para la implementación:

2.1.1.1 Se debería cuidar el hecho de que una persona por sí sola no pueda acceder, modificar o utilizar los activos sin autorización o sin que se detecte.

2.1.3 Contacto con las autoridades

Control

La institución debe establecer el procedimiento respectivo para mantener los contactos apropiados con las autoridades pertinentes.

Recomendaciones para la implementación:

2.1.3.1 Establecer un procedimiento que especifique el contacto con autoridades a las cuales se reportarán incidentes derivados del incumplimiento de la política de seguridad o por acciones de seguridad de cualquier origen (ej. fiscalía, policía, bomberos, 911, salud, otros). Todo incidente de seguridad de la información que sea considerado crítico deberá ser reportado al oficial de seguridad y este a su vez al comité de seguridad y la máxima autoridad según los casos.

2.1.3.2 Identificar y mantener actualizados los datos de contacto de proveedores de bienes o servicios de telecomunicaciones o de acceso a Internet para gestionar potenciales incidentes.

2.1.3.3 Establecer acuerdos para compartir información con el objeto de mejorar la cooperación y la coordinación de los temas de la seguridad. Tales acuerdos deberían identificar los requisitos para la protección de la información sensible.

2.1.4 Contacto con los grupos de interés especial

Control

Mantener contacto apropiados con organizaciones públicas y privadas, asociaciones profesionales y grupos de interés especializados en seguridad de la información para mejorar el conocimiento

Recomendaciones para la implementación:

La participación como miembro en grupos de interés especial o foros debería ser considerado como medio para:

2.1.4.1 Mejorar el conocimiento sobre las mejores prácticas y mantenerse actualizado sobre información relevante de seguridad de la información;
2.1.4.2 Asegurar un entendimiento, del entorno de seguridad de la información, actual y completo interactuando los responsables de la implementación del EGSI (CSI);
2.1.4.3 Recibir avisos tempranos de alertas, asesoramiento y parches relacionados con ataques a las vulnerabilidades de la institución, por parte de instituciones públicas, privadas y académicas reconocidas por su aporte en la gestión de la seguridad de la información;
2.1.4.4 Obtener acceso a asesoramiento especializado en seguridad de la información con instituciones públicas o privadas especializadas en seguridad de la información;
2.1.4.5 Compartir e intercambiar información sobre nuevas tecnologías, productos, amenazas o vulnerabilidades entre las instituciones públicas que implementan el EGSI;
2.1.4.6 Proporcionar adecuados puntos de contacto cuando ocurran incidentes de seguridad de la información; definidos en el dominio de Gestión de incidentes de seguridad de la información y mejoras.

2.1.5 Seguridad de la Información en la gestión de proyectos

Control

Contemplar la seguridad de la información en la gestión de proyectos, independientemente del tipo de proyecto a desarrollar por la institución.

Recomendaciones para la implementación:

Los métodos de gestión de proyectos en uso deberían exigir que:

2.1.5.1 Los objetivos de seguridad de la información estén incluidos en los objetivos del proyecto, de ser pertinente;
2.1.5.2 Determinar los riesgos de seguridad de la información para identificar e implementar los controles necesarios;
2.1.5.3 La seguridad de la información es parte de todas las fases de la metodología aplicada en el proyecto.

2.1.6 Consideraciones de la seguridad cuando se trata con ciudadanos o clientes

Recomendaciones para la implementación:

2.1.6.1 Identificar requisitos de seguridad antes de facilitar servicios a ciudadanos o clientes de instituciones gubernamentales que utilicen o procesen información de los mismos o de la institución. Se podrá utilizar los siguientes criterios:
a. Protección de activos de información;
b. Descripción del producto o servicio;
c. Las diversas razones, requisitos y beneficios del acceso del cliente;
d. Política de control del acceso;

e. Convenios para gestión de inexactitudes de la información, incidentes de la Seguridad de la información y violaciones de la seguridad;
f. Descripción de cada servicio que va a estar disponible;
g. Nivel de servicio comprometido y los niveles inaceptables de servicio;
h. El derecho a monitorear y revocar cualquier actividad relacionada con los Activos de la institución;
i. Las respectivas responsabilidades civiles de la institución y del cliente;
j. Las responsabilidades relacionadas con asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales
k. Derechos de propiedad intelectual y asignación de derechos de copia y la protección de cualquier trabajo colaborativos
l. Protección de datos en base la Constitución y leyes nacionales, particularmente datos personales o financieros de los ciudadanos

2.2 Dispositivos móviles y teletrabajo

2.2.1 Política de dispositivos móviles

Control

Elaborar implementar y socializar una política formal, adoptar medidas de seguridad adecuadas para la protección y gestión de los riesgos generados por el uso de dispositivos móviles.

Recomendaciones para la implementación:

La política de dispositivos móviles debería considerar:

2.2.1.1 Registro de dispositivos móviles, debidamente autorizados;
2.2.1.2 Requisitos para la protección física;
2.2.1.3 Restricciones de instalación de software;
2.2.1.4 Requisitos para las versiones de software de dispositivos móviles y para la aplicación de parches;
2.2.1.5 Restricciones de conexión a sistemas de gestión de la información;
2.2.1.6 Controles de acceso;
2.2.1.7 Técnicas criptográficas;
2.2.1.8 Protección contra virus;
2.2.1.9 Inhabilitación, borrado y bloqueos remotos;
2.2.1.10 Copias de respaldo;
2.2.1.11 Control sobre la utilización de servicios y aplicaciones web.

Cuando la política de dispositivos móviles permita el uso de dispositivos móviles personales o privados, la política y las medidas de seguridad relacionadas deberían considerar también:

2.2.1.12 La separación del uso de los dispositivos con fines privados respecto a los de la institución, incluyendo el uso de software de soporte para permitir dicha separación y proteger los datos de la institución en un dispositivo privado;
2.2.1.13 Determinar los protocolos de seguridad inalámbrica su madurez y debilidades;
2.2.1.14 Considerar que no se haga una copia de respaldo, de la información

almacenada en los equipos móviles, por ancho de banda o conexión a la red el momento de ejecutar el respaldo.

2.2.2 Teletrabajo

Control

Implementar la política y medidas de seguridad de apoyo, para proteger la información a la que se accede, procesa o almacena en ubicaciones destinadas a esta modalidad de trabajo.

Recomendaciones para la implementación:

2.2.2.1 Considerar las condiciones necesarias para la institución sobre la seguridad física del personal en el lugar de teletrabajo, teniendo en cuenta la seguridad física del edificio y del entorno local;
2.2.2.2 Considerar las condiciones necesarias para la institución en el entorno físico de teletrabajo propuesto;
2.2.2.3 Considerar las condiciones necesarias de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la institución, la sensibilidad de la información a la que se va a acceder y transmitir a través del enlace de comunicación, así como la sensibilidad del sistema interno;
2.2.2.4 Considerar la provisión de un acceso a escritorio virtual que prevenga el procesamiento y almacenamiento de información en equipos de uso personal o privado, de ser necesario;
2.2.2.5 Implementar control para minimizar la amenaza de un intento de acceso no autorizado a la información o a los recursos por parte de otras personas de la misma ubicación, por ejemplo, familia y amigos etc.;
2.2.2.6 Considerar el uso de redes domésticas y los requisitos o restricciones en la configuración de los servicios de la red inalámbrica;
2.2.2.7 Implementar las políticas y procedimientos para prevenir las disputas relativas a los derechos de propiedad intelectual de lo desarrollado por el propietario del equipo de manera privada;
2.2.2.8 Implementar un convenio de acceso a la parte privada del equipo del propietario (para comprobar la seguridad de la máquina o durante una investigación), de acuerdo a la norma legal vigente;
2.2.2.9 Acuerdos de licencia de software que puede hacer la institución para ser responsables de licenciar software de cliente en los puestos de trabajo propiedad privada de empleados, contratistas o usuarios de terceras partes;
2.2.2.10 Implementar los requisitos de protección contra un malware y firewalls.

Las directrices y disposiciones a ser consideradas deberían incluir:

2.2.2.11 Considerar la provisión del equipo adecuado y del mobiliario de almacenamiento para las actividades de teletrabajo, donde no se permita el uso de equipos privados que no estén bajo el control de la institución;
2.2.2.12 Considerar la definición del trabajo permitido, las horas de trabajo, la clasificación de la información que puede manejarse y los sistemas y servicios internos a los que el teletrabajador está autorizado a acceder;
2.2.2.13 Considerar la provisión de los equipos de comunicación adecuados, que incluyen los métodos para asegurar el acceso remoto, de acuerdo a las necesidades institucionales;

2.2.2.14 Considerar la seguridad física del sitio del teletrabajo.
2.2.2.15 Implementar reglas y directrices para el acceso de la familia y los accesos de los visitantes al equipo y a la información;
2.2.2.16 Políticas de provisión de soporte y mantenimiento de hardware y software;
2.2.2.17 La provisión de seguros de ser necesario;
2.2.2.18 Definir los procedimientos para las copias de respaldo y para la continuidad del negocio;
2.2.2.19 Establecer los requisitos necesarios para la auditoría y monitoreo de seguridad;
2.2.2.20 Política de revocación de la autorización y de los derechos de acceso, y la devolución del equipo cuando se terminan las actividades de teletrabajo.

3 SEGURIDAD DE LOS RECURSOS HUMANOS

3.1 Antes del empleo

3.1.1 Investigación de antecedentes

Control

Verificar antecedentes de candidatos a ser empleados, contratistas o usuarios de terceras partes, designaciones y promociones de funcionarios de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a la naturaleza y actividades de la institución pública, a la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos. No debe entenderse este control como discriminatorio en ningún aspecto.

Recomendaciones para la implementación:

3.1.1.1 Definir los criterios y las limitaciones para las revisiones de verificación de personal actual (por motivos de designación o promoción), potenciales empleados y de terceras partes.
3.1.1.2 Informar del procedimiento de revisión y solicitar el consentimiento al personal actual (por motivos de designación o promoción), potenciales empleados y de terceras partes.
3.1.1.3 Referencias satisfactorias tanto personal como profesional de considerarlo necesario, por la criticidad de la información institucional.
3.1.1.4 Verificación (completa y precisa) de la hoja de vida del candidato;
3.1.1.5 Confirmación de las calificaciones académicas y profesionales declaradas, de ser necesario de acuerdo a la norma legal vigente.

3.1.1.6 Verificación de documentos de identidad debidamente legalizados de acuerdo a la norma legal vigente (Cédula, pasaporte, etc);
3.1.1.7 Verificaciones más detalladas, tales como comprobaciones crediticias y certificado de antecedentes, de ser necesario de acuerdo a la norma legal vigente.

Cuando un funcionario es reclutado para un perfil especifico de seguridad de la información, las instituciones deberían asegurar que el candidato:

3.1.1.6 Si es reclutado con un perfil especifico de seguridad de la información, verificar que tiene la competencia necesaria para desarrollar su rol en seguridad de la información;

3.1.1.7 Verificar si es confiable para asumir dicho perfil, especialmente si su desempeño es crítico para la institución.

3.1.2 Términos y condiciones laborales

Control

Los funcionarios, contratistas y terceros deben aceptar y firmar los términos y condiciones del contrato de trabajo, el cual establece sus responsabilidades y obligaciones de acuerdo a la norma legal vigente.

Recomendaciones para la implementación:

3.1.2.1 Realizar la firma del acuerdo de confidencialidad o no-divulgación, antes de que los empleados, contratistas y usuarios de terceras partes, tengan acceso a la información. Dicho acuerdo debe establecer los parámetros tanto de vigencia del acuerdo, información confidencial referida, formas de acceso, responsabilidades y funciones.;

3.1.2.2 Socializar los derechos y responsabilidades legales de los empleados, los contratistas y cualquier otro usuario sobre la protección de datos y derechos de propiedad intelectual; dejando constancia de lo actuado a través de hojas de registro, informes o similares, que evidencie la realización de la misma.

3.1.2.3 Responsabilizar al personal o contratistas por la clasificación de la información y la gestión de la información de la institución y de otros activos relacionados con la información, instalaciones de procesamiento de la información y a los servicios de información.

3.1.2.4 Responsabilizar al personal sobre el manejo y creación de la información tanto interna como externa, resultante durante la ejecución de la relación laboral establecida con la institución;

3.1.2.5 Comunicar al personal o contratista las acciones legales que se tomaran si hace caso omiso de cumplir con las normas legales vigentes en la institución.

3.2 Durante el empleo

3.2.1 Responsabilidades de la Máxima Autoridad o su delegado

Control

Exigir a los funcionarios, contratistas que se aplique la seguridad de la información, de acuerdo con las políticas y procedimientos definidos por la institución.

Recomendaciones para la implementación:

3.2.1.1 Explicar y definir las funciones y las responsabilidades respecto a la seguridad de la información, antes de otorgar el acceso a la información, contraseñas o sistemas de información sensibles.

3.2.1.2 Conseguir la concienciación sobre la seguridad de la información correspondiente a sus funciones y responsabilidades dentro de la

institución.

3.2.1.3 Motivar al personal y contratistas para cumplir con las políticas del Esquema Gubernamental de Seguridad de la Información en la institución.

3.2.1.4 Acordar los términos y las condiciones laborales, las cuales incluyen la política de la seguridad de la información de la institución y los métodos apropiados de trabajo;

3.2.1.5 Verificar el cumplimiento de las funciones y responsabilidades respecto a la seguridad de la información mediante la utilización de reportes e informes;

3.2.1.6 Disponer de un canal reservado para reportar posibles violaciones de las políticas, norma legal vigente o procedimientos de seguridad de la información ("voz de alerta").

3.2.2 Concienciación, educación y formación en seguridad de la información

Control

Los funcionarios de la institución y cuando sea necesario los contratistas y usuarios de terceros; deben recibir capacitación adecuada sobre las políticas y procedimientos de la institución, de acuerdo a su puesto de trabajo.

Recomendaciones para la implementación:

La educación y formación en seguridad de la información debería cubrir aspectos generales tales como:

3.2.2.1 Capacitar de forma periódica al menos una vez al año sobre las normas y los procedimientos para la seguridad de la información, las responsabilidades legales y los controles de la institución sobre la información institucional y de terceras, así como en la capacitación del uso correcto de los servicios de información;

3.2.2.2 Que tengan conocimiento sobre los procedimientos básicos de seguridad de la información (tales como la notificación de incidentes de seguridad de la información) y los controles básicos (tales como la seguridad de las contraseñas, los controles de un *malware* y mesas despejadas) etc.;

3.2.2.3 Conocimiento los puntos de contacto y los recursos de información y consejos adicionales sobre cuestiones de seguridad de la información, que incluyan materiales adicionales para profundizar en la educación y formación en seguridad de la información (Ejm. Intranet).

3.2.3 Proceso disciplinario

Control

Socializar y garantizar el tratamiento imparcial y correcto para los empleados que han cometido violaciones comprobadas a la seguridad de la información, considerando sanciones de acuerdo a la norma legal vigente.

3.3 Finalización o cambio de empleo

3.3.1 Responsabilidades ante la finalización o cambio de empleo

Control

Las responsabilidades y obligaciones en seguridad de la información que siguen vigentes después del cambio o terminación del empleo se deberian definir, comunicar al empleado o contratista y se deberian cumplir.

Recomendaciones para la implementación:

3.3.1.1 Comunicar oficialmente al personal las responsabilidades para la terminación de su relación laboral, lo cual debe incluir los requisitos permanentes para la seguridad de la información y las responsabilidades legales o contenidas en cualquier acuerdo de confidencialidad

3.3.1.2 Los cambios en la responsabilidad o en el contrato laboral deberán ser gestionados como la terminación de la responsabilidad o el contrato laboral respectivo, y la nueva responsabilidad o contrato laboral se deberá instaurar en el contrato de confidencialidad respectivo.

3.3.1.3 Previa la terminación de un contrato se deberá realizar la transferencia de la documentación e información de la que fue responsable al nuevo funcionario a cargo, en caso de ausencia, al jefe inmediato y al Oficial de Seguridad de la Información.

3.3.1.4 Los contratos del empleado, el contratista o el usuario de terceras partes, deben incluir las responsabilidades válidas aún después de la terminación del contrato laboral.

4 GESTIÓN DE ACTIVOS

4.1 Responsabilidad de los activos

4.1.1 Inventario de activos

Control

Inventariar, identificar y actualizar todos los activos asociados con la información, y las instalaciones para el procesamiento de la información.

Recomendaciones para la implementación:

4.1.1.1 Inventariar los activos primarios, en formatos físicos y/o electrónicos:

4.1.1.1.1 Los procesos estratégicos, claves y de apoyo de la institución, activos de información.

4.1.1.1.2 Las normas y reglamentos que son la razón de ser de la institución.

4.1.1.1.3 Planes estratégicos y operativos de la institución y áreas específicas.

4.1.1.1.4 Los archivos generados por los servidores públicos, tanto de manera física como electrónica, razón de ser de la función que desempeñan en la institución.

4.1.1.1.5 Los manuales e instructivos de sistemas informáticos: instalación, guía de usuario, operación, administración, mantenimiento, entre otros.

4.1.1.1.6 De la operación de los aplicativos informáticos de los servicios informáticos: datos y meta-datos asociados, archivos de configuración, código fuente, respaldos, versiones, etc.

4.1.1.1.7 Del desarrollo de aplicativos de los servicios informáticos: actas de levantamiento de requerimientos, documento de análisis de requerimientos, modelos entidad - relación, diseño de componentes, casos de uso, diagramas de flujo y estado, casos de prueba, etc.

4.1.1.1.8 Del soporte de aplicativos de los servicios informáticos: tickets de soporte, reportes físicos y electrónicos, evaluaciones y encuestas, libros de trabajo para capacitación, etc.

4.1.1.1.9 De la imagen corporativa de la institución: manual corporativo (que incluye manual de marca y fuentes en formato electrónico de logos), archivos multimedia, tarjetas de presentación, volantes, banners, trípticos, etc.

4.1.1.2 Inventariar los activos de soporte de Hardware:

4.1.1.2.1 Equipos móviles: teléfono inteligente (smartphone), teléfono celular, tableta, computador portátil, asistente digital personal (PDA), etc.

4.1.1.2.2 Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, computadoras portátiles, etc.

4.1.1.2.3 Periféricos de entrada: teclado, ratón, micrófono, escáner plano, escáner de mano, cámara digital, cámara web, lápiz óptico, pantalla de toque, etc.

4.1.1.2.4 Periféricos de salida: monitor, proyector, audífonos, parlantes, impresora láser, impresora de inyección de tinta, impresora matricial, impresora térmica, plóter, máquina de fax, etc.

4.1.1.2.5 Periféricos y dispositivos de almacenamiento: sistema de almacenamiento (NAS, SAN), librería de cintas, cintas magnéticas, disco duro portátil, disco flexible, grabador de discos (CD, DVD, Blu-ray), CD, DVD, Blu-ray, memoria USB, etc.

4.1.1.2.6 Periféricos de comunicaciones: tarjeta USB para redes inalámbricas (Wi-Fi, Bluetooth, GPRS,

4.1.1.2.7 HSDPA), tarjeta PCMCIA para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta USB para redes alámbricas/inalámbricas de datos y de telefonía, etc.

4.1.1.2.8 Tableros: de transferencia (bypass) de la unidad ininterrumpible de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc.

4.1.1.2.9 Sistemas: de control de accesos, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión, etc.

4.1.1.3 Inventariar los activos de soporte de Software:

4.1.1.3.1 Sistemas operativos.

4.1.1.3.2 Software de servicio, mantenimiento o administración de: gabinetes de servidores de cuchilla, servidores (estantería/rack, torre, virtuales), sistema de redes de datos, sistemas de almacenamiento

4.1.1.3.3 (NAS, SAN), telefonía, sistemas (de UPS, grupo electrógeno, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión), etc.

4.1.1.3.4 Paquetes de software o software base de: suite de ofimática, navegador de Internet, cliente de correo electrónico, mensajería instantánea, edición de imágenes, vídeo conferencia, servidor (proxy, de archivos, de correo electrónico, de impresiones, de mensajería instantánea, de aplicaciones, de base de datos), etc.

4.1.1.3.5 Aplicativos informáticos del negocio.

4.1.1.3.6 Inventariar los activos de soporte de redes:

4.1.1.3.7 Cables de comunicaciones (interfaces: RJ-45 o RJ-11, SC, ST o MT-RJ, interfaz V35, RS232,

4.1.1.3.8 USB, SCSI, LPT), panel de conexión (patch panel), tomas o puntos de red, racks (cerrado o abierto, de piso o pared), etc.

4.1.1.3.9 Switchs (de centros de datos, de acceso, de borde, de gabinete de servidores, access-point, transceiver, equipo terminal de datos, etc.).

4.1.1.3.10 Ruteador (router), cortafuego (firewall), controlador de red inalámbrica, etc.

4.1.1.3.11 Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, balanceador de carga, switch de contenido, etc.

4.1.1.3.12 Inventariar los activos referentes a la estructura organizacional:

4.1.1.3.13 Estructura organizacional de la institución, que incluya todas las unidades administrativas con los cargos y nombres de las autoridades: área de la máxima autoridad, área administrativa, área de recursos humanos, área financiera, etc.

4.1.1.3.14 Estructura organizacional del área de las TIC, con los cargos y nombres del personal: administrador (de servidores, de redes de datos, de respaldos de la información, de sistemas de almacenamiento, de bases de datos, de seguridades, de aplicaciones del negocio, de recursos informáticos, etc.), líder de proyecto, personal de capacitación, personal de mesa de ayuda, personal de aseguramiento de calidad, programadores (PHP, Java, etc.).

4.1.1.3.15 Inventario referente a los sitios y edificaciones de la institución: planos arquitectónicos, estructurales, eléctricos, sanitarios, de datos, etc.

4.1.1.3.16 Dirección física, dirección de correo electrónico, teléfonos y contactos de todo el personal de la institución.

4.1.1.3.17 De los servicios esenciales: número de líneas telefónicas fijas y celulares, proveedor de servicios de Internet y transmisión de datos, proveedor del suministro de energía eléctrica, proveedor del suministro de agua potable, etc.

4.1.1.3.18 Los activos deberán ser actualizados ante cualquier modificación de la información registrada y revisados con una periodicidad no mayor a seis meses.

4.1.2 Propiedad de los activos

Control

Asignar los activos asociados (o grupos de activos) a un individuo que actuará como responsable del Activo. Por ejemplo, debe haber un responsable de los computadores de escritorio, otro de los celulares, otro de los servidores del centro de datos, etc. El término "responsable" no implica que la persona tenga realmente los derechos de propiedad de los activos.

Recomendaciones para la implementación:

El propietario del activo debería:

4.1.2.1 Asegurar que los activos sean inventariados;
4.1.2.2 Asegurar que los activos se clasifican y protegen debidamente;
4.1.2.3 Definir y revisar periódicamente restricciones de acceso y clasificación de activos importantes, teniendo en cuenta las políticas aplicables de control de acceso;
4.1.2.4 Asegurar el manejo adecuado para el borrado o destrucción del activo.

4.1.3 Uso aceptable de los activos

Control

Identificar, documentar e implementar las reglas sobre el uso aceptable de los activos asociados con los servicios de procesamiento de la información y las instalaciones.

Recomendaciones para la implementación:

4.1.3.1 Para la elaboración de las reglas, el responsable del Activo deberá tomar en cuenta las actividades definidas en los controles correspondientes a los ámbitos de "Intercambio de Información" y "Control de Acceso", donde sea aplicable
4.1.3.2 El Oficial de Seguridad de la Información es el encargado de asegurar que los lineamientos para la utilización de los recursos de las Tecnologías de la Información contemplen los requerimientos de seguridad establecidos, según la criticidad de la información que procesan.
4.1.3.3 La información y documentos generados en la institución y enviados por cualquier medio o herramienta electrónica son propiedad de la misma institución.
4.1.3.4 Reglamentar el uso de correo electrónico institucional:
- 4.1.3.4.1 Este servicio debe utilizarse exclusivamente para las tareas propias de las funciones que se desarrollan en la institución y no debe utilizarse para ningún otro fin.
- 4.1.3.4.2 Cada persona es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte.
- 4.1.3.4.3 Todos los mensajes deben poder ser monitoreados y conservados permanentemente por parte de las instituciones.
- 4.1.3.4.4 Toda cuenta de correo electrónico debe estar asociada a una única cuenta de usuario.
- 4.1.3.4.5 La conservación de los mensajes se efectuará en carpetas personales, para archivar la información de acceso exclusivo del usuario y que no debe compartirse con otros usuarios. Debe definirse un límite de espacio máximo.
- 4.1.3.4.6 Toda la información debe ser gestionado de forma centralizados y no en las estaciones de trabajo de los usuarios.
- 4.1.3.4.7 Todo sistema debe contar con las facilidades automáticas que notifiquen al usuario cuando un mensaje enviado por él no es recibido correctamente por el destinatario, describiendo detalladamente el motivo del error.
- 4.1.3.4.8 Deben utilizarse programas que monitoreen el accionar de virus informáticos tanto en mensajes como en archivos adjuntos, antes de su ejecución.

4.1.3.4.9 Todo usuario es responsable por la destrucción de los mensajes con origen desconocido, y asume la responsabilidad por las consecuencias que pueda ocasionar la ejecución de los archivos adjuntos.

4.1.3.4.10 En estos casos, no deben contestar dichos mensajes y deben enviar una copia al Oficial de

4.1.3.4.11 Seguridad de la Información para que efectúe el seguimiento y la investigación necesaria.

4.1.3.4.12 Para el envío y la conservación de la información, debe implementarse el cifrado (criptografía) de datos.

4.1.3.4.13 Todo usuario es responsable de la cantidad y tamaño de mensajes que envíe. Debe controlarse el envío no autorizado de correos masivos.

4.1.3.5 Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios:

4.1.3.5.1 Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la institución, y no debe utilizarse para ningún otro fin.

4.1.3.5.2 Cada usuario es responsable de la información y contenidos a los que accede y de aquella que copia para conservación en los equipos de la institución.

4.1.3.5.3 Debe limitarse a los usuarios el acceso a portales, aplicaciones o servicios de la Internet y la Web que pudieren perjudicar los intereses y la reputación de la institución. Específicamente, se debe bloquear el acceso por medio de dispositivos fijos y/o móviles a aquellos portales, aplicaciones o servicios de la Internet y la Web sobre pornografía, racismo, violencia, delincuencia o de contenidos ofensivos y contrarios a los intereses, entre otros, y valores de la institución o que impacten negativamente en la productividad y trabajo de la institución (ej., mensajería instantánea-chats, redes sociales, video, otros) y particularmente a los que atenten a la ética y moral.

4.1.3.5.4 El Oficial de Seguridad de la Información debe elaborar, poner en marcha y controlar la aplicación de un procedimiento institucional para acceso y uso de la Internet y la Web por parte de todo funcionario sin excepción, y en el cual se acepten las condiciones aquí especificadas y otras que la institución considere apropiadas.

4.1.3.5.5 Todos los accesos deben poder ser sujetos de monitoreo y conservación permanente por parte de la institución.

4.1.3.5.6 El Oficial de Seguridad de la Información, puede acceder a los contenidos monitoreados, con el fin de asegurar el cumplimiento de las medidas de seguridad.

4.1.3.5.7 La institución podrá en cualquier momento bloquear o limitar el acceso y uso de la Internet a los funcionarios o a terceros que accedan tanto por medio alámbrico como inalámbrico.

4.1.3.5.8 Se debe bloquear y prohibir el acceso y uso de servicios de correo electrónico de libre uso tales como: Gmail, Hotmail, Yahoo, Facebook, entre otros.

4.1.3.5.9 Se prohíbe expresamente a las instituciones de la Administración Pública la contratación, acceso y uso de servicios de correo electrónico en la Internet (Nube), para uso institucional o de servidores públicos, con empresas privadas o públicas cuyos centros de datos, redes (salvo la Internet), equipos, software base y de gestión de correo electrónico y cualquier elemento tecnológico necesario, se encuentren fuera del territorio nacional; y adicionalmente, si las condiciones de los servicios que tales empresas prestaren no se someten a la Constitución y Leyes Ecuatorianas.

4.1.3.5.10 Reglamentar el uso de los sistemas de video-conferencia.
4.1.3.5.11 Definir un responsable para administrar la video-conferencia.
4.1.3.5.12 Definir y documentar el procedimiento de acceso a los ambientes de pruebas y producción.
4.1.3.5.13 Elaborar un documento tipo "lista de chequeo" (check-list) que contenga los parámetros de seguridad para el acceso a la red interministerial que soporta el servicio de video-conferencia.
4.1.3.5.14 Crear contraseñas para el ingreso a la configuración de los equipos y para las salas virtuales de
4.1.3.5.15 video-conferencia.
4.1.3.5.16 Deshabilitar la respuesta automática de los equipos de video-conferencia y todo procedimiento que sea necesario para mantener la seguridad del tráfico.

4.1.4 Devolución de activos

Control

Realizar el procedimiento respectivo para la entrega de los activos a cargo del funcionario saliente antes de salir de la institución, asegurándose por parte del Nivel jerárquico Superior el cumplimiento en la entrega, tanto en activos físicos como de gestión de la información.

Recomendaciones para la implementación:

4.1.4.1 Formalizar el proceso de terminación de la relación laboral, para incluir la devolución de software, documentos corporativos y los equipos. También es necesaria la devolución de otros activos de la institución tales como los dispositivos de cómputo móviles, tarjetas de crédito, las tarjetas de acceso, tokens USB con certificados de electrónicos, certificados electrónicos en archivo, memorias flash, teléfonos celulares, cámaras, manuales, información almacenada en medios electrónicos y otros estipulados en las políticas internas de cada institución.
4.1.4.2 Aplicar los debidos procesos para garantizar que toda la información generada por el empleado, contratista o usuario de terceras partes dentro de la institución, sea transferida, archivada o eliminada con seguridad.
4.1.4.3 Realizar el proceso de traspaso de conocimientos por parte del empleado, contratistas o terceras partes, luego de la terminación de su contrato laboral, para la continuación de las operaciones importantes dentro de la institución.

4.2 Clasificación de la información

4.2.1 Directrices de Clasificación de la información

Control

Clasificación de la información en relación a su valor, normativa legal vigente, sensibilidad y criticidad para la institución y/o el estado, ante revelación o modificación no autorizada.

Recomendaciones para la implementación:

4.2.1.1 Clasificar la información como pública o confidencial.
4.2.1.2 Elaborar y aprobar un catálogo de clasificación de la información. Se la deberá clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la institución.
4.2.1.3 El nivel de protección se debe evaluar considerando la confidencialidad, integridad y disponibilidad de la información.
4.2.1.4 Los propietarios de los activos de información deben ser responsables de su clasificación con el asesoramiento del área legal de la institución

4.2.2 Etiquetado de la información

Control

Implementar los procedimientos necesarios para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la institución.

Recomendaciones para la implementación:

4.2.2.1 Incluir datos mediante abreviaturas, acerca del tipo de activo y su funcionalidad para la generación de etiquetas.
4.2.2.2 En caso de repetirse la etiqueta del activo, deberá añadirse un número secuencial único al final.
4.2.2.3 En caso de documentos en formato electrónico, la etiqueta deberá asociarse a un metadato único, pudiendo ser éste un código MD5.
4.2.2.4 Las etiquetas generadas deberán estar incluidas en el inventario, asociadas a su respectivo activo.
4.2.2.5 Los responsables de los activos supervisarán el cumplimiento del proceso de generación de etiquetas y rotulación de los activos.
4.2.2.6 Para el caso de etiquetas físicas, los responsables de los activos verificarán con una periodicidad no mayor a 6 meses, que los activos se encuentren rotulados y con etiquetas legibles.
4.2.2.7 En caso de destrucción de un activo, la etiqueta asociada a éste debe mantenerse en el inventario respectivo con los registros de las acciones realizadas.

4.2.3 Manejo de los activos

Control

Implementar procedimientos para la manipulación de los activos de acuerdo con el esquema de clasificación de la información definido por la institución.

Recomendaciones para la implementación:

4.2.3.1 Restringir el acceso a la información de acuerdo a su clasificación, definiendo usuarios autorizados a los activos.
4.2.3.2 Realizar el mantenimiento del registro formal de receptores autorizados de los activos;
4.2.3.3 Definir los controles necesarios para proteger las copias sean temporales o permanentes, a un nivel consistente con la protección de la información original, marcando claramente el contenido.
4.2.3.4 Realizar el almacenamiento de activos de TI conforme a las

especificaciones de sus fabricantes;

4.2.3.5 Realizar el marcado claro en todas las copias de los medios para la debida atención del receptor autorizado.

4.3 Manejo de los Soportes de almacenamiento - medios

4.3.1 Gestión de medios extraibles

Control

Implementar procedimientos para la gestión de los medios extraibles, de acuerdo con el esquema de clasificación implementado por la institución, se debe documentar los procedimientos y los niveles de autorización.

Recomendaciones para la implementación:

4.3.1.1 En caso de que ya no sean necesarios, deberían borrarse definitivamente los contenidos de cualquier medio reutilizable que vaya a ser retirado;

4.3.1.2 Cuando sea necesario por la norma legal vigente de la institución, solicitar la autorización para extraer medios de la institución, debiendo mantener el registro respectivo para mantener la trazabilidad por efectos de auditoría.

4.3.1.3 Todos los medios deberían almacenarse en un entorno seguro y protegido, conforme a las especificaciones de sus fabricantes;

4.3.1.4 Deben emplearse técnicas criptográficas para proteger datos en medios extraibles en caso de que apliquen requisitos importantes de confidencialidad o integridad;

4.3.1.5 Los datos deberían transferirse a medios de fabricación reciente antes de que se conviertan en ilegibles, a fin de modificar el riesgo de degradación del medio durante el tiempo en que los datos almacenados aún son necesarios;

4.3.1.6 Deben almacenarse copias múltiples de datos valiosos en medios separados para reducir aún más el riesgo de daño o pérdida simultánea de los datos;

4.3.1.7 El registro de medios extraibles debería considerarse para limitar las posibilidades de pérdida de datos;

4.3.1.8 Solo deberían permitirse reproductores de medios extraibles cuando haya una necesidad institucional para ello;

4.3.1.9 La transferencia de información a medios extraibles debería ser monitorizada, cuando haya necesidad de usar dichos medios.

4.3.2 Eliminación de los medios

Control

Los medios deberían eliminarse de forma segura cuando ya no sean necesarios, mediante procedimientos formales, para evitar acumulación de información no sensible, catalogando medios dañados con información sensible que deban ser destruidos en lugar de ser recuperados, después del análisis de riesgos respectivo.

Recomendaciones para la implementación:

4.3.2.1 Aquellos medios que contengan información confidencial deberían almacenarse y desecharse con seguridad, por ejemplo, por incineración o triturado, o mediante el borrado de datos para la reutilización de los soportes por la institución;
4.3.2.2 Deberían implementarse procedimientos para identificar los elementos que requieran una eliminación segura;
4.3.2.3 Puede ser más simple organizar la recolección y eliminación segura de todos los medios en lugar de tratar de segregar elementos sensibles;
4.3.2.4 Muchas organizaciones ofrecen servicios de recolección y eliminación de medios, deberían tomarse cautelas en la selección de terceras partes apropiados, con la adecuada experiencia y controles;
4.3.2.5 La eliminación de elementos sensibles debería quedar registrado a fin de mantener trazabilidad para su auditoría.

4.3.3 Transferencia de medios físicos

Control

Durante el transporte fuera de los límites físicos de la institución, los medios que contengan información deberían estar protegidos contra accesos no autorizados, usos indebidos o deterioro, considerando la criticidad de la información.

Recomendaciones para la implementación:

4.3.3.1 Debería emplearse un servicio fiable de transporte o mensajería;
4.3.3.2 Establecer una lista de mensajeros autorizados y aprobados por el área responsable.
4.3.3.3 Desarrollar procedimientos para verificar la identidad e integridad de los mensajeros;
4.3.3.4 Embalar de forma segura medios o información enviada a través de servicios de mensajería, siguiendo las especificaciones del proveedor o del fabricante.
4.3.3.5 Debería mantenerse registros, e identificar el contenido de los medios, la protección aplicada, así como reflejando los momentos de transferencia a los custodios y la recepción en el destino.

5 CONTROL DE ACCESO

5.1 Requisitos institucionales para el control de acceso

5.1.1 Política de control de acceso

Control

Elaborar, implementar y socializar la política de control de acceso a los sistemas de información, de acuerdo a la necesidad institucional y considerando la seguridad de la información.

Recomendaciones para la implementación:

5.1.1.1 Gestionar los accesos de los usuarios a los sistemas de información, asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados.
5.1.1.2 Definir responsabilidades para identificar, gestionar y mantener perfiles de los custodios de información.
5.1.1.3 Definir los requisitos para la autorización formal de los pedidos de acceso.
5.1.1.4 Revisión periódica de los usuarios y los permisos otorgados, retirando aquellos permisos que hayan cambiado su situación.
5.1.1.5 Definir claramente los autorizadores de los permisos de acceso a la información.
5.1.1.6 Relación directa entre los derechos de acceso y las políticas de clasificación de la información de sistemas y redes.
5.1.1.7 Definir la política para el acceso a la información, considerando quien tiene la necesidad de conocer y los niveles de seguridad, considerando la clasificación de la información.
5.1.1.8 Considerar la norma legal vigente sobre el acceso a datos o servicios.
5.1.1.9 Definir formalmente la gestión de derechos de acceso en un ambiente de distribución e interconexión, que reconozca los tipos de conexión disponibles.
5.1.1.10 Registro de los eventos realizados por el usuario, considerando también a los derechos de acceso privilegiado.
5.1.1.11 Establecer la regla "Todo está prohibido a no ser que se permita expresamente" en vez de la regla más débil "Todo está permitido a no ser que se prohíba expresamente". Se aplica el principio de menor privilegio.

5.1.2 Acceso a redes y servicios de red

Control

Elaborar, implementar y socializar la política para proveer a los usuarios acceso a las redes y a los servicios de red, para los que han sido especificamente autorizados.

Recomendaciones para la implementación:

5.1.2.1 Identificar y documentar los equipos que se encuentran en las redes debidamente autorizados.
5.1.2.2 Procedimientos de autorización que determinen quién tiene permitido el acceso a qué redes y a que servicios de red.
5.1.2.3 Implementar los controles necesarios para el ingreso a la red y los procedimientos respectivos para proteger el acceso a las conexiones de red y a los servicios de la red.
5.1.2.4 Políticas para identificar usuarios debidamente autorizados para acceder a las redes y servicios de red a través de VPN, redes virtuales y redes inalámbricas entre otras.
5.1.2.5 Utilizar métodos para que la identificación del equipo esté en relación a la autenticación del usuario.
5.1.2.6 Monitorear continuamente el uso de los servicios de la red, con alertas sobre aquellos recursos que se considere críticos.

5.2 Gestión de acceso de los usuarios

5.2.1 Registro y retiro de usuarios

Control

Implementar un procedimiento formal de registro, retiro y modificación de usuarios, con el objetivo de habilitar la asignación de derechos de acceso

Recomendaciones para la implementación:

5.2.1.1 Establecer un procedimiento formal, documentado y difundido, en el cual se evidencie detalladamente los derechos de acceso.
5.2.1.2 Definir el administrador de accesos que debe controlar los perfiles y roles;
5.2.1.3 Gestionar el documento de requerimiento de accesos de los usuarios tanto internos como externos, que contemple: el solicitante del requerimiento o iniciador del proceso, validación del requerimiento, autorizador del requerimiento, ejecutor del requerimiento, forma y medio de entrega del acceso al usuario (manteniendo confidencialidad);
5.2.1.4 Crear los accesos para los usuarios, para lo cual la institución debe generar convenios de confidencialidad y responsabilidad con el usuario solicitante; además, validar que el usuario tenga los documentos de ingreso con Recursos Humanos (o quien haga estas funciones) en orden y completos.
5.2.1.5 Modificar los accesos de los usuarios;
5.2.1.6 Eliminar los accesos de los usuarios;
5.2.1.7 Suspender temporalmente los accesos de los usuarios en caso de vacaciones, comisiones, licencias, es decir, permisos temporales;
5.2.1.8 Proporcionar accesos temporales a usuarios externos o terceros de acuerdo al tiempo de su permanencia y limitados según las actividades para las que fueron contratados y firmar un convenio de confidencialidad;
5.2.1.9 Mantener un registro de la gestión de accesos a aplicaciones, redes, que evidencie, fecha de creación, eliminación, suspensión, activación o eliminación del acceso; al igual que de cada usuario, disponer de los permisos de acceso que han sido asignados.

5.2.2 Provisión de accesos a usuarios

Control

Implementar un procedimiento formal para asignar o revocar las credenciales de acceso para todos los tipos de usuarios de todos los sistemas y servicios.

Recomendaciones para la implementación:

5.2.2.1 Evidenciar documentadamente que cada activo de información tecnológico tenga definido los niveles de acceso basados en perfiles y permisos, a fin de determinar que privilegios se deben asignar según las actividades de los usuarios y la necesidad de la institución y su función;
5.2.2.2 Verificar que los privilegios asociados con cada servicio o sistema estén de acuerdo con las políticas de acceso y coherente con los requisitos definidos en las funciones que se desempeñan los funcionarios.
5.2.2.3 Asegurar que las credenciales de acceso no se activen con terceros (proveedores etc.) hasta completar con los procedimientos de autorización;
5.2.2.4 Mantener un registro documentado de permisos de acceso a sistemas

de información y servicios concedidos a un funcionario;

5.2.2.5 Actualizar las credenciales de acceso de usuarios que han cambiado de rol o de tareas y la eliminación o bloqueo inmediato de los derechos de acceso de los usuarios que han dejado la institución;

5.2.2.6 Revisar periódicamente las credenciales de acceso a los sistemas de información o de los servicios con los propietarios de los sistemas de información.

5.2.3 Gestión de los derechos de acceso con privilegios especiales

Control

Establecer un proceso formal para funcionarios que tengan la asignación de credenciales de acceso con privilegios especiales; estos deben ser controlados y restringidos.

Recomendaciones para la implementación:

5.2.3.1 Mantener un cuadro de identificación de los usuarios y sus privilegios especiales asociados con cada servicio o sistema operativo, sistema de gestión de base de datos y aplicaciones;

5.2.3.2 Las credenciales de acceso con privilegio especial deben asignarse a los usuarios con base en la necesidad de usar y caso a caso de acuerdo con la política de control de acceso, es decir, basados en los requisitos mínimos para el desempeño de sus funciones;

5.2.3.3 Un proceso de autorización y registro de todos los privilegios especiales asignados. Los niveles de acceso privilegiados no deberían concederse hasta que se complete el proceso de autorización;

5.2.3.4 Definir las causas para el vencimiento de las credenciales de acceso con privilegio especial.

5.2.3.5 Las credenciales de acceso con privilegio especial, deben asignarse a un identificador de usuario diferente al usado en las actividades normales de la institución. Las actividades cotidianas de la institución no deberían ser ejecutadas por credenciales con privilegios.

5.2.3.6 Evaluar continuamente las competencias de los usuarios con credenciales de acceso con privilegios especiales verificando que se correspondan con sus actividades;

5.2.3.7 Establecer procedimientos específicos para evitar el uso no autorizado de credenciales de usuario administrador genérico en relación con las capacidades de configuración de los sistemas;

5.2.3.8 Para credenciales de usuario administrador genérico, debería mantenerse la confidencialidad de la información secreta de autenticación cuando esta sea compartida (por ejemplo, cambiando las contraseñas con frecuencia y tan pronto como sea posible cuando un usuario privilegiado deje la institución o cambie de trabajo, comunicándolas a los usuarios privilegiados a través de los mecanismos apropiados).

5.2.4 Gestión de la información confidencial de autenticación de los usuarios

Control

Establecer un proceso formal de gestión para la entrega de información confidencial de las credenciales de acceso al sistema y/o servicios.

Recomendaciones para la implementación:

5.2.4.1 Se debería requerir de los usuarios la firma de un compromiso de mantener la confidencialidad de la información secreta para la autenticación personal y mantener la información de autenticación secreta del grupo (es decir, la compartida) entre los miembros del mismo; este compromiso firmado podría incluirse en los términos y condiciones del acuerdo de confidencialidad del empleo de ser necesario de acuerdo a la gestión institucional.

5.2.4.2 Cuando la institución requiera que los usuarios mantengan su información de autenticación confidencial, debería proporcionárseles inicialmente una autenticación temporal a ser cambiada obligatoriamente en el primer uso;

5.2.4.3 Establecer los procedimientos necesarios para verificar la identidad de un usuario antes de proporcionarle la información de autenticación confidencial ya sea nueva, de sustitución o provisional;

5.2.4.4 La información de autenticación confidencial debería proporcionarse a los usuarios de manera segura; evitando el uso de terceras partes o de correos electrónicos no protegidos (texto sin cifrar);

5.2.4.5 La información de autenticación secreta temporal debería ser única para el individuo y no debería poder predecirse;

5.2.4.6 Utilizar el procedimiento adecuado para que los usuarios confirmen la recepción de la información de autenticación confidencial;

5.2.4.7 La información de autenticación confidencial entregada por el proveedor, debería cambiarse tras la instalación de los sistemas o del software.

5.2.5 Revisión de los derechos de acceso de usuario

Control

Los propietarios de los activos deberán revisar o coordinar la revisión de los derechos de acceso, a intervalos regulares definidos por la institución.

Recomendaciones para la implementación:

5.2.5.1 Las credenciales de acceso del usuario deben revisarse al menos cada 90 días o de acuerdo a las necesidades de la institución y tras cualquier cambio institucional o de funciones de los usuarios.

5.2.5.2 La asignación de privilegios debe verificarse al menos cada 30 días o de acuerdo a las necesidades de la institución, para asegurar que no se han obtenido privilegios no autorizados;

5.2.5.3 Los cambios en cuentas de usuarios deben registrarse en los logs de los sistemas de gestión de información para su revisión periódica.

5.2.6 Retiro o adaptación de los derechos de acceso

Control

Retirar los privilegios de acceso a los empleados y usuarios de terceras partes a la información y a las instalaciones de procesamiento de información (ej., sistema de directorio, correo electrónico, accesos físicos,

aplicaciones de software, etc.,) inmediatamente luego de que se comunique la terminación de la relación laboral por parte del área correspondiente.

Recomendaciones para la implementación:

Retirar los derechos de acceso a la información y los activos asociados a las instalaciones de procesamiento de la información deberían restringirse o eliminarse antes de que el empleado finalice o cambie de puesto de trabajo, dependiendo de la evaluación de factores de riesgo como:

5.2.6.1 Si el funcionario presenta su renuncia o solicita su cambio de área, así como la razón para la finalización.
5.2.6.2 Las responsabilidades del funcionario, y de cualquier usuario el momento de la renuncia o cambio.
5.2.6.3 El valor de los activos a los que han tenido acceso el momento de renuncia o cambio.

5.3 Responsabilidades del usuario

5.3.1 Uso de la información confidencial para la autenticación

Control

Elaborar la política, implementarla y socializar a los usuarios las responsabilidades del uso de las credenciales de acceso a la información y a los equipos puestos a su disposición.

Recomendaciones para la implementación:

5.3.1.1 Mantener la confidencialidad de la información de autenticación, asegurando su no divulgación, incluyendo a personas con autoridad;
5.3.1.2 Evitar guardar (por ejemplo, en papel, en un fichero software o en un dispositivo portátil) las credenciales de acceso, a no ser que esta pueda ser almacenada de forma segura y que el método de almacenamiento haya sido aprobado (por ejemplo, en repositorios seguros para contraseñas);
5.3.1.3 Cambiar las contraseñas de autenticación siempre que haya indicios de su posible divulgación;
5.3.1.4 Cuando se usen contraseñas como información secreta de autenticación, seleccionar contraseñas de calidad con una longitud mínima de 8 caracteres que:
  5.3.1.4.1 Sean fáciles de recordar,
  5.3.1.4.2 Que no estén basadas en algo que alguien más pueda adivinar con facilidad u obtener usando información asociada a la persona, por ejemplo, nombres, números de teléfono, fechas de nacimiento, etc.,
  5.3.1.4.3 Que no sea vulnerable a ataques de diccionario (es decir, que no consista en palabras incluidas en diccionarios),
  5.3.1.4.4 Que estén libres de caracteres consecutivos bien sean todos numéricos o todos alfabéticos,
  5.3.1.4.5 Si es temporal, que sea cambiada en el primer inicio de sesión,
5.3.1.5 Asegurar una protección adecuada de las contraseñas cuando estas sean usadas como información secreta de autenticación y almacenadas en procesos automáticos de inicio de sesión;

5.3.1.6 No usar las mismas contraseñas de autenticación para propósitos laborales y privados.

5.3.1.7 El Oficial de Seguridad de la Información deberá gestionar actividades periódicas (una vez cada mes como mínimo) para la revisión al contenido de las pantallas de los equipos, con el fin de que no se encuentren iconos y accesos innecesarios, y carpetas y archivos que deben ubicarse en la carpeta de documentos del usuario.

5.4 Control de acceso a sistemas y aplicaciones

5.4.1 Restricción del acceso a la información

Control

Restringir el acceso de los usuarios a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.

Recomendaciones para la implementación:

5.4.1.1 Control del acceso a las funciones del sistema de aplicaciones;

5.4.1.2 Monitorear cuales son los datos a los que acceda un usuario determinado, de acuerdo al perfil definido;

5.4.1.3 Implementar controles sobre los perfiles de acceso de los usuarios, por ejemplo, de lectura, de escritura, de borrado y de ejecución de la información, etc.;

5.4.1.4 Implementar controles para el ingreso a otras aplicaciones de acuerdo a los perfiles de usuario determinados.

5.4.1.5 Generar revisiones periódicas de las salidas de los sistemas de aplicación para garantizar el retiro de la información redundante.;

5.4.1.6 Implementar controles de acceso tanto físico o lógico para aislar las aplicaciones sensibles, los datos de aplicación o los sistemas. (DMZ).

5.4.2 Procedimientos seguros de inicio de sesión

Control

Implementar un procedimiento seguro de inicio de sesión cuando se requiera una autenticación robusta, para controlar el acceso a los sistemas y aplicaciones institucionales por ejemplo medios criptográficos, tarjetas inteligentes, dispositivos hardware o medios biométricos

Recomendaciones para la implementación:

5.4.2.1 Controlar que no se muestren identificadores del sistema o aplicación hasta que el proceso de inicio de sesión se haya completado con éxito;

5.4.2.2 Socializar un aviso general de que únicamente deben acceder al computador los usuarios autorizados;

5.4.2.3 Evitar que se desplieguen mensajes de ayuda durante el proceso de inicio de sesión que pudieran ayudar a un usuario no autorizado;

5.4.2.4 Validar la información de inicio de sesión solo cuando se hayan registrado todos los datos de entrada. Si ocurre alguna condición de error, el sistema no debería indicar qué parte del dato es correcto o incorrecto;

5.4.2.5 Limitar la cantidad de intentos permitidos de registro de inicio de sesión;

por ejemplo, tres intentos;

5.4.2.6 Llevar un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros de alarmas cuando se violan las políticas de seguridad del sistema, generando la alerta respectiva;

5.4.2.7 Mostrar la siguiente información tras completar con éxito el inicio de sesión:

9.4.2.8.1 Fecha y hora del anterior inicio de sesión con éxito,

9.4.2.8.2 Los detalles de cualquier intento de inicio de sesión sin éxito desde el anterior con éxito,

5.4.2.8 No exponer la contraseña que se está introduciendo;

5.4.2.9 No transmitir por la red contraseñas sin cifrar;

5.4.2.10 Terminar las sesiones inactivas tras un periodo definido de tiempo de inactividad, especialmente en lugares de alto riesgo, como áreas públicas o externas que queden fuera de la gestión de la seguridad de la institución o en dispositivos móviles;

5.4.2.11 Restringir los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo y reducir la ventana de oportunidad para accesos no autorizados.

5.4.3 Sistema de gestión de contraseñas

Control

Elaborar la política para la gestión de contraseñas, debe ser interactiva y asegurar la calidad de las mismas.

Recomendaciones para la implementación:

5.4.3.1 Evidenciar en la política de accesos, la responsabilidad del buen uso de la contraseña y que debe ser secreta e intransferible para mantener la responsabilidad;

5.4.3.2 Permitir a los usuarios escoger y cambiar sus propias contraseñas e incluir un procedimiento de confirmación que tenga en cuenta los errores de entrada;

5.4.3.3 Imponer la complejidad de contraseñas para asegurar el ingreso a los sistemas;

5.4.3.4 Forzar a los usuarios el cambio de contraseña en el primer inicio de sesión;

5.4.3.5 Forzar a los usuarios el cambio regular de contraseñas, del personal de tecnología, de los administradores de tecnología, en rangos de tiempo y complejidad y cuando sea necesario;

5.4.3.6 Mantener un registro de las contraseñas usadas anteriormente y evitar su reutilización, especialmente en activos críticos;

5.4.3.7 No mostrar las contraseñas en la pantalla cuando el usuario este ingresando;

5.4.3.8 Generar un procedimiento formal para la administración y custodia de las contraseñas de acceso de administración e información de la institución, de manera separada de los datos del sistema.

5.4.3.9 Almacenar y transmitir las contraseñas en formatos protegidos (encriptados o codificados).

5.4.3.10 Documentar el control de acceso para los usuarios temporales

5.4.3.11 Generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la Información.

5.4.4 Uso de herramientas de administración de sistemas

Control

El uso de programas utilitarios o software que puedan ser capaces de anular o evitar los controles del sistema y aplicaciones, deben ser restringidos y fuertemente controlados.

Recomendaciones para la implementación:

5.4.4.1 Uso de procedimientos de identificación, autenticación y autorización para los programas utilitarios;
5.4.4.2 Separación de los programas utilitarios del software de aplicaciones;
5.4.4.3 Limitación del uso de programas utilitarios a la cantidad mínima viable de usuarios de confianza autorizados;
5.4.4.4 Autorización del uso de programas utilitarios, no estandarizados en la institución;
5.4.4.5 Limitar la disponibilidad de los programas utilitarios, por ejemplo, a la duración de un cambio autorizado;
5.4.4.6 Registrar todo uso de programas utilitarios;
5.4.4.7 Definir y documentar los niveles de autorización para los programas utilitarios de administración;
5.4.4.8 Retirar, eliminar o inhabilitar todos los programas utilitarios que sean innecesarios;

5.4.5 Control de acceso al código fuente del programa

Control

Restringir el acceso al código fuente de las aplicaciones software, programas, de acuerdo a las políticas establecidas por la institución.

Recomendaciones para la implementación:

5.4.5.1 Asignar a un administrador del código fuente de programas, software, quien tendrá en custodia los mismos y deberá:
- 5.4.5.1.1 Utilizar un manejador de versiones para el código fuente, proporcionar permisos de acceso a los desarrolladores bajo autorizaciones.
- 5.4.5.1.2 Proveer al área de Desarrollo los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente/ejecutable.
- 5.4.5.1.3 Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, autorizador, versión, fecha de última modificación y fecha/hora de compilación y estado (en modificación o en producción).
- 5.4.5.1.4 Verificar que el autorizador de la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario.
- 5.4.5.1.5 Registrar cada solicitud aprobada.
- 5.4.5.1.6 Administrar las distintas versiones de una aplicación.

5.4.5.1.7 Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador, sin un manejador de versiones.

5.4.5.1.8 Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos como respaldos de información

5.4.5.2 Cuando sea posible, las librerías de programas fuente no deben guardarse en los sistemas en producción o en explotación;

5.4.5.3 El código fuente de programas y las librerías fuente de programas se deberán gestionar de acuerdo con los procedimientos establecidos;

5.4.5.4 El personal de soporte no debe tener acceso sin restricciones al código de programas fuente.

5.4.5.5 La actualización del código fuente de programas y de los elementos asociados, así como la emisión de fuentes de programa a los programadores, solamente se deberá efectuar después de recibir la autorización respectiva;

5.4.5.6 Los listados del código de programa deben guardarse en un entorno seguro;

5.4.5.7 Conservar un registro para auditoría de todos los accesos al código fuente de programas;

5.4.5.8 El mantenimiento y el copiado del código fuente de programas deberán estar sujetos a un procedimiento estricto de control de cambios

6 CRIPTOGRAFÍA

6.1 Controles criptográficos

6.1.1 Política de uso de los controles criptográficos

Control

Elaborar, implementar y socializar una política que regule el uso de controles criptográficos para la protección de la información, de acuerdo al nivel de protección requerida.

Recomendaciones para la implementación:

6.1.1.1 Definir la política institucional con respecto al uso de los algoritmos de cifrado, que se utilizarán en toda la institución, dependiendo del tipo de control a aplicar, el propósito y el proceso del negocio. Esta política debe ser periódicamente revisada y actualizada;

6.1.1.2 Considerando la evaluación de los riesgos, identificarse el nivel de protección requerido, considerando el tipo, la fortaleza y la calidad del algoritmo de cifrado necesario;

6.1.1.3 Utilizar controles de cifrado para la protección de la información sensible transportada a través de medios extraíbles, móviles, removibles, por dispositivos especiales, o a través de las líneas de comunicación;

6.1.1.4 Desarrollar procedimientos de administración de claves, de recuperación de información cifrada en caso de pérdida, vulneración, de compromiso o daño de las claves.

6.1.1.5 Los responsables del área de Tecnologías de la Información, Oficial de Seguridad propondrán la siguiente asignación de funciones:

6.1.1.5.1 Implementación de la Política de Controles,

6.1.1.5.2 Administración de claves: gestión de claves, incluyendo su generación,

6.1.1.6 Definir las normas de controles de cifrado (criptográficos) que se adoptarán, para la implementación eficaz en toda la institución; establecer la solución a usar para cada proceso del negocio;

6.1.1.7 Determinar el impacto del uso de información cifrada en los controles que se basan en la inspección del contenido (por ejemplo, la detección de un malware).

Los controles criptográficos pueden utilizarse para alcanzar distintos objetivos de seguridad de la información, por ejemplo:

6.1.1.8 Garantizar la confidencialidad: uso de cifrado (encriptación) de la información para proteger información sensible o crítica, bien sea almacenada o transmitida;

6.1.1.9 Garantizar la integridad / autenticidad: uso de firmas electrónicas o códigos de autenticación de mensajes para verificar la autenticidad e integridad de la información sensible o crítica transmitida o almacenada;

6.1.1.10 Garantizar el No-repudio: uso de técnicas de criptográficas para obtener pruebas de la existencia o no existencia de un evento o acción;

6.1.1.11 Garantizar la integridad / autenticación: uso de técnicas criptográficas para autenticar credenciales de acceso y transacciones en el sistema.

6.1.1.12 Uso de firma electrónica:

6.1.1.13.1 Utilizar certificados electrónicos de Entidades de Certificación de Información reconocidas por el Estado Ecuatoriano para la firma de cualquier tipo de documento, mensaje de dato, transacción que se procese electrónicamente o para comunicaciones entre sistemas, aplicaciones y medios físicos.

6.1.1.13.2 Utilizar los certificados electrónicos emitidos bajo estándares por las Entidades de Certificación de Información, las cuales deben ser instituciones u organizaciones reconocidas, con controles y procedimientos idóneos establecidos para proporcionar el grado requerido de confianza.

6.1.1.13.3 Uso de los certificados electrónicos según el ámbito para la cual fue generado.

6.1.1.13 Utilizar controles de cifrado (criptográficos) para la transmisión de información clasificada, fuera del ámbito de la institución

6.1.1.14 Utilizar controles criptográficos para la protección de claves de acceso a: sistemas, datos y servicios. Las claves deberán ser almacenadas de manera codificada, cifrada (encriptada) en la base de datos y/o en archivos de parámetros.

6.1.2 Gestión de Claves

Control

Elaborar e Implementar una política para la administración de claves cifradas (criptográficas) para respaldar la utilización por parte de la institución.

Recomendaciones para la implementación:

6.1.2.1 Utilizar de los tipos de técnicas criptográficas: técnicas de clave secreta (criptografía simétrica), técnicas de clave pública (criptografía asimétrica) y técnicas de la clave secreta y pública (criptografía hibrida); a través de

su ciclo de vida, entre otros.

6.1.2.2 Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones incluyendo fechas de inicio y caducidad de las claves.;

6.1.2.3 Generar y obtener certificados de claves públicas;

6.1.2.4 Distribuir la primera clave a los usuarios, incluyendo la forma de activar y confirmar la recepción de la clave. Luego, a través de un correo electrónico recibirá un acceso al sistema, el cual validará la entrega de la clave y la obligatoriedad de cambiar dicha clave;

6.1.2.5 Implementar normas y procedimientos para almacenar claves, incluyendo la forma de acceso a las mismas, por parte de los usuarios autorizados;

6.1.2.6 Incorporar funcionalidad para cambiar o actualizar las claves, incluyendo reglas sobre cuándo cambiarlas, cómo hacerlo y la forma en que los usuarios autorizados tendrán acceso a ellas;

6.1.2.7 Incorporar funcionalidad para recuperar claves pérdidas o corruptas como parte de la gestión de continuidad de los servicios informáticos;

6.1.2.8 Permitir revocar las claves, incluyendo la forma de retirarlas o desactivarlas cuando las claves se han puesto en peligro o cuando un usuario se retira de la institución (en cuyo caso, las claves también deberían archivarse);

6.1.2.9 Incorporar funcionalidad para tratar las claves pérdidas o corruptas. Bajo pedido del usuario que pierde una clave se generará una nueva, la entrega será a través del procedimiento definido para la entrega de la primera clave;

6.1.2.10 Proporcionar una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico.

6.1.2.11 Permitir la destrucción de claves que se dejen de utilizar;

6.1.2.12 Registrar y auditar las actividades relacionadas con la gestión de claves.

6.1.2.13 Proteger todas las claves contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.

6.1.2.14 Habilitar en los sistemas, la generación de claves en la creación de usuarios. Se generará la primera clave la cual deberá obligatoriamente cambiar el propio usuario la primera vez que ingresa al sistema

7 SEGURIDAD FÍSICA Y DEL ENTORNO

7.1 Áreas seguras

7.1.1 Perímetro de seguridad física

Control

Se deberían definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica.

Recomendaciones para la implementación:

7.1.1.1 Definir y documentar claramente los perímetros de seguridad (barreras, paredes, puertas de acceso controladas con tarjeta, etc.), con una ubicación y fortaleza adecuadas de acuerdo a los resultados de la evaluación del riesgo;

112

7.1.1.2 Definir un área de recepción, con personal y otros medios para controlar el acceso físico al lugar o edificio, se deberían restringir los accesos a las instalaciones y edificios únicamente al personal autorizado.;
7.1.1.3 Extender las barreras físicas necesarias desde el piso hasta el techo a fin de impedir el ingreso inapropiado y la contaminación del medio ambiente;
7.1.1.4 Disponer de alarmas de incendio y puertas de evacuación debidamente monitoreadas que cumplan normas nacionales e internacionales;
7.1.1.5 Disponer de un sistema de vigilancia mediante el uso de circuitos cerrados de televisión
7.1.1.6 Las instalaciones de procesamiento de información gestionadas por la institución, deberían estar físicamente separadas de aquellas gestionadas por terceras partes.
7.1.1.7 Todas las puertas del perímetro de seguridad que actúen como *firewalls* deberían estar dotadas de un sistema de alarma, monitorizadas y probadas conjuntamente con las paredes, para establecer el nivel requerido de resistencia de acuerdo con las normas regionales, nacionales e internacionales; se debería operar de acuerdo a los códigos locales de protección contra incendios en modo de fallo seguro;
7.1.1.8 Se deberían instalar sistemas de detección de intrusión adecuados conforme a las normas regionales, nacionales e internacionales, y ser probados periódicamente para dar cobertura a todas las puertas externas y ventanas accesibles; las áreas no ocupadas deberían estar dotadas de un sistema de alarma en todo momento; se deberían también cubrir otras áreas, por ejemplo, la sala de computadoras o las salas de comunicaciones;

7.1.2 Controles físicos de entrada

Control

Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso.

Recomendaciones para la implementación:

7.1.2.1 Supervisar la permanencia de los visitantes en las áreas restringidas y registrar la hora y fecha de su ingreso y salida;
7.1.2.2 Controlar y limitar el acceso, exclusivamente a personal autorizado, a la información clasificada y a las instalaciones de procesamiento de información. Se debe utilizar controles de autenticación como tarjetas de control de acceso más el número de identificación personal;
7.1.2.3 Mantener y monitorear de manera segura un libro físico de registro o una pista de auditoría electrónica de todos los accesos;
7.1.2.4 Implementar el uso de una identificación visible para todo el personal y visitantes, quienes deberán ser escoltados por una persona autorizada para el tránsito en las áreas restringidas;
7.1.2.5 Para el personal proveniente de terceras partes que prestan servicios de soporte, proporcionar acceso restringido a las áreas seguras o a las instalaciones de procesamiento de la información confidencial únicamente cuando sea requerido; este acceso debería estar autorizado y controlado;
7.1.2.6 Revisar, actualizar periódicamente los derechos de accesos a las áreas restringidas y revocar cuando sea pertinente, mismos que serán

documentados y firmados por el responsable.

7.1.2.7 El acceso a las áreas donde se procesa o se almacena información confidencial debería estar controlado y restringido únicamente a personal autorizado; se deberían utilizar controles de autenticación para autorizar y validar todos los accesos, por ejemplo, implementando un mecanismo de doble factor de autenticación como tarjetas de control de acceso con número de identificación personal secreto (PIN);

7.1.3 Seguridad de oficinas, despachos e instalaciones

Control

Diseñar e implementar seguridad física para las oficinas, despachos e instalaciones de la institución.

Recomendaciones para la implementación:

7.1.3.1 Proteger las instalaciones claves de tal manera que se evite el acceso al público.;

7.1.3.2 Establecer que los edificios o sitios de procesamiento sean discretos y tengan un señalamiento mínimo apropiado;

7.1.3.3 Las instalaciones deben adecuarse para evitar que las actividades o la información de tipo confidencial sean visibles o audibles desde el exterior. Considerar los campos electromagnéticos de ser necesario;

7.1.3.4 Los directorios y las guías telefónicas internas que identifiquen las ubicaciones de las instalaciones de procesamiento de la información confidencial, no deberían ser de fácil acceso a la lectura por personas no autorizadas.

7.1.3.5 Ubicar los equipos de reproducción de documentos sensibles como impresoras, copiadoras, etc., en un área protegida.

7.1.4 Protección contra las amenazas externas y ambientales

Control

Diseñar y aplicar la protección física contra desastres naturales, ataques maliciosos o accidentes.

Recomendaciones para la implementación:

7.1.4.1 Almacenar los materiales combustibles o peligrosos a una distancia prudente de las áreas protegidas.

7.1.4.2 Ubicar los equipos de repuesto y soporte a una distancia prudente para evitar daños en caso de desastre que afecte las instalaciones principales.

7.1.4.3 Suministrar el equipo apropiado contra incendios y ubicarlo adecuadamente.

7.1.4.4 Realizar mantenimientos de las instalaciones eléctricas y UPS.

7.1.4.5 Realizar mantenimientos en los sistemas de climatización y ductos de ventilación.

7.1.4.6 Adoptar controles para minimizar el riesgo de amenazas físicas potenciales como robo, incendio, explosión, humo, agua, polvo, vibración, efectos químicos, interferencia del suministro eléctrico e interferencia a las comunicaciones.

7.1.5 Trabajo en áreas seguras

Control

Elaborar, Implementar y socializar procedimientos para el desarrollo de trabajos y actividades en áreas seguras.

Recomendaciones para la implementación:

7.1.5.1 Dar a conocer al personal, la existencia de un área segura o de sus actividades, únicamente en el caso de que sea necesario para su trabajo;
7.1.5.2 Evitar el trabajo no supervisado para evitar actividades maliciosas;
7.1.5.3 Revisar periódicamente y disponer de un bloqueo físico de las áreas seguras vacías;
7.1.5.4 No permitir equipos de grabación, cámaras, equipos de video y audio, dispositivos móviles, etc., a menos de que estén autorizados.

7.1.6 Áreas de carga y entrega

Control

Controlar puntos de acceso a la institución como las áreas de entrega y carga/descarga (entre otros) para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de procesamiento de información.

Recomendaciones para la implementación:

7.1.6.1 Permitir el acceso al área de despacho y carga, únicamente a personal identificado y autorizado;
7.1.6.2 Descargar y despachar los suministros, únicamente en el área de descarga y despacho sin que el personal de entrega tenga que acceder a otras zonas del edificio;
7.1.6.3 Las puertas externas de un área de carga y entrega deben estar cerradas cuando las puertas internas estén abiertas;
7.1.6.4 El material entrante debería ser inspeccionado para evitar amenazas potenciales como explosivos, productos químicos y otros materiales de riesgo antes de trasladarlo desde el área de carga y entrega hasta su lugar de utilización;
7.1.6.5 Cuando sea posible, separar físicamente la entrada y la salida de envíos;
7.1.6.6 Inspeccionar el material entrante en busca de indicios de manipulación durante su traslado. Si se descubre tal manipulación informar de inmediato al personal de seguridad.

7.2 Seguridad de los Equipos

7.2.1 Ubicación y protección de equipos

Control

Los equipos se deberían ubicar y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado.

Recomendaciones para la implementación:

7.2.1.1 Ubicar los equipos de modo que se elimine el acceso innecesario a las áreas de trabajo restringidas;
7.2.1.2 Aislar los servicios de procesamiento de información con datos sensibles y elementos que requieran protección especial, para reducir el riesgo de visualización de la información de personas no autorizadas;
7.2.1.3 Asegurar las instalaciones de almacenamiento para evitar los accesos no autorizados;
7.2.1.4 Aislar los elementos que requieran protección especial para reducir el nivel de protección general requerido;
7.2.1.5 Adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales como, por ejemplo, robo, fuego, explosivos, humo, agua (o fallo de suministro de agua), polvo, vibración, agentes químicos, interferencias en el suministro eléctrico, interferencias en las comunicaciones, radiaciones electromagnéticas y vandalismo;
7.2.1.6 Establecer directrices para no comer, beber y fumar en las cercanías de las áreas de procesamiento de información;
7.2.1.7 Monitorear las condiciones ambientales de temperatura y humedad;

7.2.1.8 Tener protección contra descargas eléctricas en todas las edificaciones de la institución y disponer de filtros protectores en el suministro de energía y en las líneas de comunicación;
7.2.1.9 Disponer de métodos especiales de protección para equipos en ambientes industriales;
7.2.1.10 Proteger los equipos que procesan la información sensible para minimizar el riesgo de fugas de información debidas a una emanación electromagnética.

7.2.2 Instalaciones de suministro

Control

Los equipos deberían estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo.

Recomendaciones para la implementación:

7.2.2.1 Tener un sistema de suministro de energía sin interrupción (UPS) o al menos permitir el cierre/apagado ordenado de los servicios y equipos que soportan las operaciones críticas de los servicios informáticos de la institución.
7.2.2.2 Estar conformes a las especificaciones del fabricante de los equipos y a los requisitos legales locales;
7.2.2.3 Inspeccionar regularmente todos los sistemas de suministro mediante pruebas apropiadas;
7.2.2.4 Disponer de los interruptores de emergencia cerca de las salidas, para suspender el paso de energía eléctrica, en caso de un incidente o problema;
7.2.2.5 Tener al alcance el suministro de combustible para que el grupo electrógeno pueda funcionar mientras dure la suspensión del suministro eléctrico público.
7.2.2.6 Implementar y documentar los servicios de electricidad, agua, calefacción, ventilación y aire acondicionado, suministrados a la institución

7.2.3 Seguridad del cableado

Control

Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños.

Recomendaciones para la implementación:

7.2..3.1 Disponer de líneas de fuerza (energía) y de telecomunicaciones subterráneas protegidas, en cuanto sea posible;
7.2..3.2 Separar los cables de energía de los cables de comunicaciones;
7.2..3.3 Proteger el cableado de la red contra la interceptación o daño
7.2..3.4 Identificar y rotular los cables de acuerdo a normas locales o internacionales para evitar errores en el manejo
7.2..3.5 Disponer de documentación, diseños/planos y la distribución de conexiones de: datos en redes alámbricas/inalámbricas (locales y remotas), voz, eléctricas polarizadas, etc.

7.2..3.6 Controlar el acceso a los módulos de cableado de conexión (patch panel) y cuartos de cableado
7.2..3.7 Considerar medidas adicionales para sistemas sensibles o críticos, como:
7.2.3.3.1 Instalación de conductos blindados y cajas o salas cerradas en los puntos de inspección y terminación,
7.2.3.3.2 Uso de apantallamiento electromagnético para proteger los cables,
7.2.3.3.3 Implementación de barreras técnicas e inspecciones físicas para detectar la conexión al cableado de dispositivos no autorizados,

7.2.4 Mantenimiento de los equipos

Control

Elaborar, socializar, implementar y evaluar el plan de mantenimiento que garantice la disponibilidad e integridad continua de los equipos.

Recomendaciones para la implementación:

7.2.4.1 Brindar mantenimientos periódicos a los equipos y dispositivos, de acuerdo a las especificaciones y recomendaciones del proveedor.;
7.2.4.2 Realizar el mantenimiento de los equipos únicamente con personal calificado y autorizado.
7.2.4.3 Conservar los registros de los mantenimientos preventivos, correctivos y fallas relevantes o sospechosas.
7.2.4.4 Establecer controles apropiados para realizar mantenimientos programados y emergentes, considerando el tratamiento de la información sensible; si el mantenimiento se realiza en la institución o fuera de ella.
7.2.4.5 Cumplir con todos los requisitos de mantenimiento que exijan las pólizas de seguros, de ser el caso;
7.2.4.6 Antes de poner el equipo en funcionamiento después del mantenimiento, validar que el equipo no ha sido manipulado y que funciona correctamente.
7.2.4.7 Gestionar mantenimientos planificados con hora de inicio, fin, impacto y responsables y poner previamente en conocimiento de administradores y usuarios finales.

7.2.5 Salida de los activos fuera de las instalaciones de la institución

Control

Sin la autorización legal, los activos no deben sacarse de las instalaciones de la institución

Recomendaciones para la implementación:

7.2.5.1 Autorizar, registrar e identificar claramente a los usuarios y empleados de terceras partes con permiso para sacar los activos fuera de la institución.
7.2.5.2 Establecer técnicamente el tiempo que el equipo puede estar fuera de las instalaciones de la institución.
7.2.5.3 Controlar el registro de salida e ingreso de equipos de las instalaciones de la institución.
7.2.5.4 Registrar y confirmar la identidad, las funciones y de que institución es el funcionario que maneja o usa los activos, tanto a la salida como al ingreso juntamente con el equipo, información o software.

7.2.6 Seguridad de los equipos y activos fuera de las instalaciones

Control

Aplicar medidas de seguridad a los equipos ubicados afuera de las instalaciones de la institución, considerando los riesgos que surgen el trabajar fuera de las mismas.

Recomendaciones para la implementación:

7.2.6.1 Los equipos y medios sacados de las instalaciones no se deberían dejar desatendidos en lugares públicos.
7.2.6.2 Custodiar los equipos y medios que se encuentren fuera de las instalaciones de la institución;
7.2.6.3 Tomar en cuenta las instrucciones del fabricante para la protección de los equipos que se encuentran fuera de las instalaciones, sobre la protección contra exposiciones a campos electromagnéticos intensos;
7.2.6.4 Disponer de controles para el trabajo que se realiza en equipos fuera de las instalaciones (domicilio personal, teletrabajo y lugares de trabajo temporales), mediante una evaluación de riesgos.
7.2.6.5 Cuando el equipo afuera de la institución se transfiere entre diferentes individuos o instituciones externas, se debe mantener un registro que defina la cadena de custodia de los equipos incluyendo, al menos, los nombres y las organizaciones de aquellos responsables de los equipos.
7.2.6.6 Establecer una cobertura adecuada del seguro, para proteger los equipos que se encuentran fuera de las instalaciones

7.2.7 Seguridad en la reutilización o eliminación segura de dispositivos de almacenamiento

Control

Todos los medios de almacenamiento deberían ser comprobados para

confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos o reutilizarlos.

Recomendaciones para la implementación:

7.2.7.1 Destruir, borrar o sobrescribir los dispositivos que contienen información sensible utilizando técnicas que permitan la no recuperación de la información original, antes de su retirada o reutilización.
7.2.7.2 Evaluar los dispositivos deteriorados que contengan información sensible antes de enviar a reparación, borrar la información o determinar si se debería eliminar físicamente el dispositivo.

Adicionalmente al borrado seguro de los discos, un cifrado completo de los mismos reduce el riesgo de divulgación de la información confidencial cuando el equipo es retirado o, en el caso de ser redistribuido, siempre que:

7.2.7.3 El proceso de cifrado sea suficientemente fuerte y cubra el disco completamente (incluyendo el espacio libre, archivos temporales de intercambio de memoria, etc.);

7.2.7.4 Las llaves de cifrado son suficientemente largas para resistir ataques de fuerza bruta;
7.2.7.5 Las llaves de cifrado se mantienen confidenciales (por ejemplo, nunca se almacenan en el mismo disco).

7.2.8 Equipo informático de usuario desatendido

Control

Los usuarios deberían asegurarse de que el equipo desatendido tiene la protección adecuada.
Recomendaciones para la implementación:

7.2.8.1 Implementar medidas para que, en un determinado tiempo (ej., no mayor a 10 minutos), si el usuario no está realizando ningún trabajo en el equipo, este se bloquee, y se desbloquee únicamente si el usuario ingresa nuevamente su clave.
7.2.8.2 Salir de las aplicaciones o servicios de red cuando ya no se necesiten;
7.2.8.3 Asegurar las computadoras personales o los terminales frente a accesos no autorizados a través de un bloqueo con clave o un control equivalente, por ejemplo, contraseñas de acceso cuando no están en uso.

7.2.9 Política de puesto de trabajo despejado y pantalla limpia

Control

Deberia adoptarse una política de puesto de trabajo despejado de papeles, medios de almacenamiento extraíbles y una política de monitores sin información.

Recomendaciones para la implementación:

7.2.9.1 El Oficial de Seguridad de la Información deberá gestionar actividades

periódicas (una vez cada mes como mínimo) para la revisión al contenido de las pantallas de los equipos, con el fin de que no se encuentren iconos y accesos innecesarios, y carpetas y archivos que deben ubicarse en la carpeta de documentos del usuario.

7.2.9.2 Mantener bajo llave la información sensible (cajas fuertes o gabinetes), en especial cuando no estén en uso y no se encuentre personal en la oficina.

7.2.9.3 Desconectar de la red, servicio o sistema, las computadoras personales, terminales, impresoras asignadas a funciones críticas, cuando se encuentren desatendidas. Por ejemplo, haciendo uso de protectores de pantalla con clave.

7.2.9.4 Proteger los puntos de recepción de correo y fax cuando se encuentren desatendidas.

7.2.9.5 Retirar información sensible una vez que ha sido impresa.

7.2.9.6 Bloquear las copiadoras y disponer de un control de acceso debidamente autorizado y a otros equipos de reproducción como escáneres y cámaras digitales.

7.2.9.7 Cifrar los discos duros de los computadores personales (escritorio, portátiles, etc.) y otros dispositivos que se considere críticos, de las máximas autoridades de la institución de ser necesario.

7.2.9.8 Retirar información sensible, como las claves, de sus escritorios y pantallas.

7.2.9.9 Retirar los dispositivos removibles una vez que se hayan dejado de utilizar.

8 SEGURIDAD DE LAS OPERACIONES

8.1 Procedimientos y responsabilidades operacionales

8.1.1 Documentación de procedimientos de operación

Control

Elaborar, implementar y socializar los procedimientos de operación y poner a disposición de los usuarios del área respectiva.

Recomendaciones para la implementación:

8.1.1.1 Documentar el procedimiento en la instalación y configuración de sistemas;

8.1.1.2 Documentar el procesamiento y manejo de la información tanto automatizada como manual;

8.1.1.3 Documentar el proceso de respaldo y restauración de la información.

8.1.1.4 Documentar todos los procesos de los servicios de procesamiento de

datos, incluyendo la interrelación con otros sistemas;

8.1.1.5 Documentar las instrucciones para el manejo de errores y otras condiciones excepcionales que pueden surgir durante la ejecución de las tareas incluyendo restricciones en las funcionalidades del sistema.

8.1.1.6 Documentar los contactos de soporte y escalada, necesarios en caso de incidentes.

8.1.1.7 Documentar las instrucciones para el manejo de los medios de resultados especiales, como el uso de papel especial o la gestión de resultados confidenciales, incluyendo procedimientos de eliminación segura de resultados producidos como consecuencia de tareas fallidas.

8.1.1.8 Documentar los procedimientos para reinicio y recuperación del sistema en caso de fallas;

8.1.1.9 Documentar los registros de pistas de auditoría y de la información de registro de sistemas;

8.1.1.10 Documentar los procedimientos de monitoreo de los sistemas.

8.1.2 Gestión de cambios

Control

Controlar los cambios que afectan a la seguridad de la información en el giro del negocio de la institución, en las instalaciones y sistemas de procesamiento de información.

Recomendaciones para la implementación:

8.1.2.1 Identificar y registrar los cambios significativos.

8.1.2.2 Realizar pruebas del cambio antes de liberar al usuario final.

8.1.2.3 Evaluar el impacto de dichos cambios;

8.1.2.4 Aprobar de manera formal los cambios propuestos;

8.1.2.5 Planificar el proceso de cambio considerando el registro de auditoría que contenga toda la información importante.

8.1.2.6 La verificación de que los requisitos de seguridad de la información se cumplen;

8.1.2.7 Comunicar el detalle de cambios a todas las personas y áreas involucradas.

8.1.2.8 Identificar responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos;

8.1.2.9 Disponer de un proceso de cambio de emergencia que habilite la implementación rápida y controlada de los cambios necesarios para resolver un incidente.

8.1.2.10 Establecer responsables y procedimientos formales del control de cambios en los equipos y software. Los cambios deben efectuarse únicamente cuando haya razón válida para el negocio, como: cambio de versión, corrección de vulnerabilidades, costos, licenciamiento, nuevo hardware, etc.

8.1.3 Gestión de capacidades

Control

Monitoreo y ajuste en la utilización de los recursos, para proyectar adecuadamente las capacidades futuras de acuerdo a la gestión institucional, asegurando el desempeño óptimo del sistema.

Recomendaciones para la implementación:

8.1.3.1 Realizar proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos.

8.1.3.2 Borrar datos obsoletos para optimizar el espacio de disco;

8.1.3.3 Desmantelamiento de aplicaciones, sistemas, bases de datos o entornos que ya no sean necesarios observando la normativa legal vigente.

8.1.3.4 Optimizar los procesos en lotes y su calendarización;

8.1.3.5 Optimizar la lógica de la aplicación o las consultas de base de datos, para mejorar la respuesta.

8.1.3.6 Utilizar la información del monitoreo para la adquisición, asignación de recursos y evitar cuellos de botella.

8.1.3.7 Análisis para limitar el consumo del ancho de banda para servicios consumidores de muchos recursos, si estos no son críticos para la institución.

8.1.4 Separación de ambientes de desarrollo, pruebas y producción

Control

Separar los ambientes de desarrollo, pruebas y producción, para reducir los riesgos de acceso no autorizado a los cambios del sistema en producción.

Recomendaciones para la implementación:

8.1.4.1 Definir y documentar las reglas para la transferencia de software desde el estado de desarrollo hasta el estado de producción;

8.1.4.2 Definir y documentar diferentes entornos para desarrollo, pruebas, capacitación y producción. Para el caso que no se pueda definir diferentes entornos con recursos físicos independientes, se debe implementar

ambientes virtuales con las credenciales de acceso respectivas.

8.1.4.3 Aislar los ambientes de desarrollo, pruebas, capacitación y producción.

8.1.4.4 Los cambios en las aplicaciones y sistemas en producción deben probarse en un ambiente de pruebas previo a ser aplicados en sistemas en producción;

8.1.4.5 Aislar los datos sensibles de los ambientes de desarrollo, pruebas y capacitación

8.1.4.6 Utilizar sistemas de autenticación y autorización independientes para las diversas instancias o ambientes.

8.1.4.7 Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deberían ser accesibles desde los sistemas de operación cuando no sea necesario;

8.1.4.8 Definir perfiles de usuario para las diferentes instancias o ambientes.

8.1.4.9 Controlar la instalación y uso de herramientas de desarrollo de software y/o acceso a bases de datos y redes en los equipos informáticos, salvo que sean parte de las herramientas de uso estándar o su instalación sea autorizada de acuerdo a un procedimiento expresamente definido.

8.1.4.10 Los datos críticos no deben ser copiados en un ambiente de prueba, a menos que existan controles similares al ambiente de producción.

8.2 Protección contra un malware

8.2.1 Controles contra malware

Control

Implementar controles para detectar, prevenir y recuperarse de afectaciones de malware, en combinación con la concientización adecuada a los usuarios.

Recomendaciones para la implementación:

8.2.1.1 Elaborar, implementar y socializar una política formal para prohibir el uso de software no autorizado por la institución. Elaborar un listado del software autorizado.

8.2.1.2 Mantener los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas versiones de seguridad disponibles.

8.2.1.3 Implementar controles para detectar el uso de software no autorizado (por ejemplo, una lista de aplicaciones autorizadas);

8.2.1.4 Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la institución.

8.2.1.5 Socializar a los funcionarios institucionales información puntual sobre malware y recomendaciones a ejecutar.

8.2.1.6 Implementar controles para evitar la navegación en sitios web maliciosos (por ejemplo, listas negras);

8.2.1.7 Establecer procedimientos para evitar riesgos en la obtención/descarga de archivos y software desde o a través de redes externas o por cualquier otro medio.

8.2.1.8 Revisar regularmente los servidores con activos de información críticos de la institución, para evitar la presencia de archivos extraños o modificación del contenido con accesos no autorizados.

8.2.1.9 Instalar y actualizar periódicamente software de antivirus y contra código malicioso.

8.2.1.10 Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos o en archivos recibidos a través de redes no confiables, correos electrónicos y/o archivos descargados.

8.2.1.11 Establecer procedimientos y responsabilidades para asegurar la gestión de los sistemas ante la presencia de un malware, informes y recuperación de posibles ataques.

8.2.1.12 Desarrollar implementar y socializar planes de continuidad del negocio, para la recuperación ante ataques de malware.

8.2.1.13 Implementar procedimientos para conocer información sobre nuevos malware y poner controles adecuados.

8.2.1.14 Implementar procedimientos para verificar la información relativa al *malware*, y asegurar que los boletines de alerta son precisos e informativos; el comité debería asegurarse de que se utilizan fuentes de confianza, tales como publicaciones acreditadas, sitios de internet o proveedores de software de protección contra un *malware* fiables, para diferenciar entre correos electrónicos engañosos (*hoaxes*) y el *malware* real; todos los usuarios deberían ser conscientes del problema de los correos electrónicos engañosos (*hoaxes*) y qué hacer cuando se reciban;

8.2.1.15 Aislar ambientes donde puedan producirse impactos catastróficos en activos críticos.

8.2.1.16 Concienciar al personal acerca del problema de los virus y cómo proceder frente a los mismos.

8.2.1.17 Contratar con el proveedor de Internet o del canal de datos los servicios de filtrado de: virus, spam, programas maliciosos (malware), en el perímetro externo, de ser necesario para la institución.

8.2.1.18 Redactar procedimientos para verificar toda la información relativa a software malicioso.

8.3 Copias de seguridad

8.3.1 Copias de seguridad de la información

Control

Elaborar, Implementar y socializar la política de respaldos de la información; verificar periódicamente su validez.

Recomendaciones para la implementación:

8.3.1.1 Los responsables del área de Tecnologías de la Información, Oficial de Seguridad de la Información junto con el propietario de la información, determinarán los procedimientos formales para el respaldo, resguardo y contención de la información.
8.3.1.2 Definir el procedimiento de etiquetado de las copias de respaldo, identificando su contenido, periodicidad y retención.
8.3.1.3 Establecer procedimientos regulares de verificación y restauración de los medios de respaldo para garantizar sean confiables para uso de emergencia.
8.3.1.4 Definir la extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo a los requisitos de la institución.
8.3.1.5 Guardar los respaldos en un sitio lejano, a una distancia suficiente para evitar cualquier daño debido a desastres en la sede principal de la institución.
8.3.1.6 Establecer procedimientos de los medios de respaldo, una vez concluida su vida útil recomendada por el proveedor y la destrucción de estos medios.
8.3.1.7 La información de los respaldos debe ubicarse en un ambiente adecuado tanto físico como ambiental.
8.3.1.8 Comprobar periódicamente los medios de las copias de seguridad para asegurar su respuesta y el funcionamiento del procedimiento de recuperación
8.3.1.9 Los respaldos de la información confidencial, deben ser protegidos mediante cifrado.
8.3.1.10 Considerar los respaldos a medios de almacenamiento y en el mismo sitio si se tiene suficientes recursos, ya que, en caso de mantenimientos de los sistemas de información, es más rápida su recuperación.

8.4 Registro y monitoreo

8.4.1 Registro de eventos

Control

Implementar el procedimiento para registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.

Recomendaciones para la implementación:

8.4.1.1 Identificadores (ID) de usuario;
8.4.1.2 Actividades del sistema;
8.4.1.3 Fechas, tiempos y detalles de eventos claves, por ejemplo, conexión y desconexión;
8.4.1.4 Identidad o localización del dispositivo, si es posible e identidad del sistema;
8.4.1.5 Registro de intentos de acceso a los sistemas exitosos y fallidos;
8.4.1.6 Registro de intentos de acceso a los recursos y a los datos exitosos y

fallidos;
8.4.1.7 Registrar cambios en la configuración del sistema;
8.4.1.8 Uso de privilegios;
8.4.1.9 Uso de utilidades y aplicaciones del sistema;
8.4.1.10 Archivos a los que se ha accedido y el tipo de acceso;
8.4.1.11 Direcciones y protocolos de red;
8.4.1.12 Alarmas generadas por el sistema de control de acceso;
8.4.1.13 Activación y desactivación de los sistemas de protección, tales como sistemas de antivirus y de detección de intrusión;
8.4.1.14 Registro de transacciones ejecutadas por usuarios en las aplicaciones.

8.4.2 Protección de los registros de información

Control

Establecer el procedimiento para proteger contra posibles alteraciones y accesos no autorizados la información de los registros

Recomendaciones para la implementación:

8.4.2.1 Proteger de alteraciones en todos los tipos de mensaje que se registren.

8.4.2.2 Proteger archivos de registro que no se editen o se eliminen.

8.4.2.3 Precautelar la capacidad de almacenamiento del medio donde están los archivos de registro, provocando bien un fallo del registro de eventos o bien sobrescribiendo los registros de eventos pasados.

8.4.2.4 Realizar respaldos periódicos de los registros de información.

8.4.3 Registros de administración y operación

Control

Registrar, proteger y revisar regularmente de acuerdo a las necesidades de la institución; las actividades del administrador y del operador del sistema.

Recomendaciones para la implementación:

8.4.3.1 Incluir al registro, la hora en la que ocurrió el evento.
8.4.3.2 Incluir al registro, información sobre el evento.
8.4.3.3 Incluir al registro, la cuenta de administrador y operador que estuvo involucrado.
8.4.3.4 Añadir al registro, los procesos que estuvieron implicados.

8.4.4 Sincronización de relojes

Control

Sincronizar los relojes de los sistemas de procesamiento de información

pertinentes con una fuente de tiempo exacta (ejemplo el tiempo coordinado universal o el tiempo estándar local). En lo posible, se debe sincronizar los relojes en base a un protocolo o servicio de tiempo de red para mantener todos los equipos sincronizados.

Recomendaciones para la implementación:

8.4.4.1 Verificar y corregir cualquier variación significativa de los relojes sobre todo en sistemas de procesamiento donde el tiempo es un factor clave.
8.4.4.2 Garantizar que la marca de tiempo refleja la fecha/hora real considerando especificaciones locales (por ejemplo, el horario de Galápagos o de países en donde existen representaciones diplomáticas del país, turistas extranjeros, entre otros).
8.4.4.3 Garantizar la configuración correcta de los relojes para la exactitud de los registros de auditoría o control de transacciones y evitar repudio de las mismas debido a aspectos del tiempo.

8.5 Control del software en producción

8.5.1 Instalación del software en sistemas en producción.

Control

Implementar procedimientos para controlar la instalación adecuada de software en los sistemas en producción.
Recomendaciones para la implementación:

8.5.1.1 Definir y aplicar procesos de control de cambios para la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas, a cargo de personal especializado con la debida autorización y credenciales de acceso.

8.5.1.2 Definir el proceso de paso a producción para cada sistema, después de concluir pruebas de usabilidad, seguridad, efectos en otros sistemas y facilidad de uso y deberían llevarse a cabo en sistemas independientes en sus ambientes respectivos;

8.5.1.3 Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.

8.5.1.4 Asignar un responsable de la implantación de cambios por sistema (no podrá ser personal que pertenezca al área de desarrollo o mantenimiento), quien tendrá como funciones principales:

8.5.1.4.1 Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
8.5.1.4.2 Asegurar que los aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
8.5.1.4.3 Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del área encargada del testeo y del usuario final.
8.5.1.4.4 Rechazar la implementación en caso de encontrar defectos

8.5.1.5 Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones para el paso a producción, el informe de pruebas previas y el informe de paso a producción.

8.5.1.6 Disponer del informe de paso a producción, el cual contendrá información de todos los cambios a realizar y el plan de contingencia.

8.5.1.7 Guardar o instalar únicamente los ejecutables y cualquier elemento necesario para la ejecución de un software en el ambiente de producción.

8.5.1.8 Implementar el ensayo en el ambiente de pruebas. Este ambiente debe ser similar al ambiente de producción. El ensayo será en base al informe de paso a producción. Se ejecutarán todas las acciones definidas y se realizarán pruebas sobre capacidad de uso, seguridad, efectos en otros sistemas y facilidad para el usuario.

8.5.1.9 Llevar un registro de auditoría de las actualizaciones realizadas.

8.5.1.10 Retener las versiones previas del sistema, como medida de contingencia.

8.5.1.11 Denegar permisos de modificación a los desarrolladores, sobre los programas fuentes bajo su custodia.

8.5.1.12 Usar un sistema de control de configuración para mantener el control del software instalado, así como de la documentación del sistema.

8.5.1.13 Entregar acceso físico o lógico al ambiente producción únicamente para propósitos de soporte, cuando sea necesario y con aprobación del responsable del área de Tecnologías de la Información o el que haga sus veces, esto se realizará tanto para usuarios internos de la dirección como para proveedores.

8.5.1.14 Monitorear las actividades de soporte realizadas sobre el ambiente de producción.

8.6 Gestión de la vulnerabilidad técnica

8.6.1 Gestión de las vulnerabilidades técnicas

Control

Elaborar e Implementar la política de monitoreo continuo sobre los sistemas en producción, detectar vulnerabilidades técnicas, adoptar las medidas necesarias para afrontar el riesgo asociado.

Recomendaciones para la implementación:

8.6.1.1 Definir e instaurar las funciones y responsabilidades asociadas con la gestión de la vulnerabilidad técnica, incluyendo el monitoreo de la vulnerabilidad, la evaluación de riesgos de la vulnerabilidad, el uso de parches, el rastreo de activos y todas las responsabilidades de coordinación requeridas.

8.6.1.2 Disponer de un inventario completo y actual de los activos de software. El inventario servirá para dar soporte a la gestión de la vulnerabilidad técnica e incluye los siguientes datos: vendedor del software, números de versión, estado actual de despliegue y las personas de la institución responsables del software.

8.6.1.3 Definir una línea de tiempo para reaccionar ante la notificación de vulnerabilidades técnicas potenciales pertinentes.

8.6.1.4 Identificar los recursos de información que se van a utilizar para

identificar las vulnerabilidades técnicas pertinentes y para mantener la concienciación sobre ellas para el software y otras tecnologías, con base en la lista de inventario de activos.

8.6.1.5 Identificar los riesgos asociados a una vulnerabilidad potencial y las acciones que se han de tomar; tales acciones podrían involucrar el uso de parches en los sistemas vulnerables y/o la aplicación de otros controles.

8.6.1.6 Actualizar los recursos de información en función de los cambios en el inventario o cuando se encuentren recursos nuevos o útiles.

8.6.1.7 Definir la urgencia y las acciones a tomar para tratar la vulnerabilidad técnica identificada, se realizará conforme a los controles relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta ante incidentes de seguridad de la información.

8.6.1.8 Evaluar los riesgos asociados con la instalación de un parche para cubrir vulnerabilidades. Los riesgos impuestos por la vulnerabilidad se deberán comparar con los riesgos de instalar el parche.

8.6.1.9 Probar y evaluar los parches antes de su instalación para garantizar que son eficaces y no producen efectos secundarios intolerables. Estas pruebas se realizarán en un ambiente similar al de producción considerando.

8.6.1.9.1 Apagar los servicios o capacidades relacionadas con la vulnerabilidad.

8.6.1.9.2 Adaptar o agregar controles de acceso; por ejemplo, cortafuegos (firewalls), en las fronteras de la red.

8.6.1.9.3 Aumentar el monitoreo para detectar o prevenir los ataques reales.

8.6.1.10 Crear conciencia en los desarrolladores y usuarios sobre la vulnerabilidad.

8.6.1.11 Conservar un registro para auditoría de todos los procedimientos efectuados.

8.6.1.12 Monitorear y evaluar a intervalos regulares las vulnerabilidades técnicas, para garantizar eficacia y eficiencia.

8.6.1.13 Tratar primero los sistemas con alto riesgo.

8.6.1.14 un proceso eficaz de gestión de las vulnerabilidades técnicas debería estar alineado con las actividades de gestión de incidentes, para comunicar datos sobre las vulnerabilidades relativas a la función de respuesta a incidentes y proporcionar procedimientos técnicos a desarrollar cuando ocurra un incidente;

8.6.1.15 definir un procedimiento para considerar la situación donde una vulnerabilidad ha sido identificada pero no es posible adoptar una contramedida. En esta situación, la institución debería evaluar los riesgos relativos a la vulnerabilidad conocida y definir acciones de detección y corrección adecuadas.

8.6.2 Restricciones en la instalación de software

Control

Elaborar implementar y socializar la política que rija la instalación de software por parte de los usuarios.

Recomendaciones para la implementación:

8.6.2.1 Disponer de la autorización del responsable del área de Tecnologías de la Información que apruebe la instalación.
8.6.2.2 Analizar los términos y condiciones de la licencia, si es del caso, a fin de determinar si las instalaciones se encuentran autorizadas.
8.6.2.3 Determinar la conveniencia de que la Instalación sea efectuada por la institución, por el proveedor o por un tercero, y evaluar el impacto.
8.6.2.4 Definir un proceso de gestión de las instalaciones del software para asegurarse en caso de actualizaciones, que los parches sean los más actualizados y aprobados.

8.7 Consideraciones sobre la auditoría de sistemas de información

8.7.1 Controles de auditoría de sistemas de información

Control

Planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas en producción con el objetivo de minimizar las interrupciones en los procesos relacionados con la institución.

Recomendaciones para la implementación:

8.7.1.1 Únicamente se deberá dar a los auditores acceso de lectura a la información.

8.7.1.2 Acordar los requisitos, así como el alcance de las auditorías con la dirección correspondiente.

8.7.1.3 Las comprobaciones deberían limitarse a accesos de solo lectura al software y a los datos;

8.7.1.4 Un acceso diferente al de solo lectura debería permitirse únicamente en copias aisladas de los archivos del sistema, que deberían borrarse cuando finalice la auditoría, o a las que debería protegerse adecuadamente si es obligatorio mantener dichos archivos de acuerdo con los requisitos de documentación de la auditoría;

8.7.1.5 Identificar y acordar los requisitos para el procesamiento especial o adicional.

8.7.1.6 Identificar explícitamente y poner en disposición los recursos correspondientes, para llevar a cabo las auditorías.

8.7.1.7 Las pruebas de auditoría que puedan afectar a la disponibilidad del

sistema deben realizarse fuera del horario laboral;

8.7.1.8 Monitorear y registrar todo acceso para crear un rastreo para referencia. El uso de rastreos de referencia de tiempo se debe considerar para datos o sistemas críticos.

8.7.1.9 Proteger la integridad y evitar el uso inadecuado de las herramientas de auditoría.

8.7.1.10 Salvaguardar los servicios de procesamiento de información y las herramientas de auditoría durante las auditorías de los sistemas de información.

8.7.1.11 Documentar todos los procedimientos, requisitos y responsabilidades de la auditoría.

8.7.1.12 Asegurar que la persona que realiza la auditoría sea independiente de las actividades auditadas.

9 SEGURIDAD EN LAS COMUNICACIONES

9.1 Gestión de la seguridad de redes

9.1.1 Controles de red

Control

Administrar y controlar las redes para proteger la información en sistemas y aplicaciones institucionales.

Recomendaciones para la implementación:

9.1.1.1 Establecer las responsabilidades y los procedimientos para la administración de los equipos en la infraestructura de la red;

9.1.1.2 Separar la responsabilidad del área de redes del área de la operación de los sistemas informáticos, cuando la capacidad de los recursos lo permitan.

9.1.1.3 Establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan por las redes públicas, redes locales e inalámbricas para proteger los sistemas y sus aplicaciones; así como para mantener la disponibilidad de las computadoras y los servicios de red conectados.

9.1.1.4 Registro y monitoreo de eventos que permita registrar y detectar acciones que podrían afectar, o ser relevantes para la seguridad de la información.

9.1.1.5 Garantizar la aplicación de los controles consistentemente, en la infraestructura de procesamiento de la información; mediante actividades de supervisión.

9.1.1.6 Autenticar el acceso a la red y a sus sistemas.

9.1.1.7 La conexión de los sistemas a la red debe ser restringido de acuerdo a la criticidad y la gestión institucional.

9.1.1.8 Designar procedimientos y responsabilidades para la gestión de equipos remotos como el caso de redireccionamiento de puertos y accesos por VPNs, incluyendo el área de operaciones y el área de usuarios finales.

9.1.1.9 Disponer de un esquema de red de los enlaces de datos, Internet y redes locales, así como la documentación respectiva.

9.1.2 Seguridad de los servicios de red

Control

Identificar e incluir en los acuerdos de servicio los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados. (SLA´s)

Recomendaciones para la implementación:

9.1.2.1 Incorporar tecnología aplicada para la seguridad de los servicios de red, como la autenticación, cifrada y controles de conexión de red.

9.1.2.2 Implementar soluciones que proporcionen valor agregado a las conexiones y servicios de red, como la implementación de firewalls, antivirus, etc.

9.1.2.3 Definir procedimientos para la utilización de los servicios de red para restringir el acceso a los mismos o a las aplicaciones, cuando sea necesario.

9.1.2.4 Definir e implementar los parámetros técnicos para conexiones seguras, de acuerdo a la necesidad institucional.

9.1.3 Separación en las redes

Control

Separar las redes en función de los grupos de servicios, usuarios y sistemas de información.

Recomendaciones para la implementación:

9.1.3.1 Realizar una evaluación de riesgos para identificar los segmentos de red donde se encuentren los activos críticos para la institución.

9.1.3.2 Dividir las redes en dominios lógicos de red, dominios de red interna, dominios de red externa e inalámbrica.

9.1.3.3 Documentar la segregación de red, identificando las direcciones IP que se encuentran en cada segmento de red.

9.1.3.4 Configurar la puerta de enlace (gateway) para filtrar el tráfico entre dominios y bloquear el acceso no autorizado.

9.1.3.5 Controlar los flujos de datos de red usando las capacidades de enrutamiento/conmutación (ej., listas de control de acceso).

9.1.3.6 La separación de las redes debe ejecutarse en base a la clasificación de la información almacenada o procesada en la red, considerando que el objetivo es dar mayor protección a los activos de información críticos en función del riesgo que éstos podrían presentar.

9.1.3.7 Separar redes inalámbricas procedentes de redes internas y privadas, para evitar el acceso a terceros y de usuarios externos a las redes privadas internas.

9.2 Transferencia de información

9.2.1 Políticas y procedimientos de transferencia de información

Control

Elaborar implementar políticas, procedimientos y controles formales que protejan la transferencia de información que viaja a través del uso de todo tipo de recursos de comunicación.

Recomendaciones para la implementación:

9.2.1.1 Establecer procedimientos para proteger la información intercambiada contra la intercepción, copiado, modificación, errores de enrutamiento y destrucción.

9.2.1.2 Definir procedimientos para detección y protección contra malware que puede ser transmitido a través de comunicaciones electrónicas.

9.2.1.3 Definir procedimientos para Proteger la información electrónica sensible que se encuentra en forma de adjunto, por ejemplo, mediante la difamación, el acoso, la suplantación, el reenvío de mensajes en cadena, las compras no autorizadas entre otras.

9.2.1.4 Establecer políticas o directrices para el uso de los servicios de comunicación.

9.2.1.5 Establecer responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer a la institución con un mal uso de la información.

9.2.1.6 Establecer controles por medio de técnicas criptográficas para proteger la confidencialidad, integridad y autenticidad de la información.

9.2.1.7 Definir directrices para la conservación y eliminación de correspondencia comercial, incluidos los mensajes, de acuerdo con la norma legal vigente.

9.2.1.8 Establecer los controles y reglas asociadas con el uso de los recursos de comunicación, por ejemplo, reenvío automático del correo electrónico a las direcciones de correo externas;

9.2.1.9 Instruir al personal para no revelar información sensible al momento de tener una conversación telefónica, mantener conversaciones etc. sin tomar los controles necesarios.

9.2.1.10 No dejar información sensible en copiadoras, impresoras, fax, contestadores, podría ser reproducido por personas no autorizadas etc.

9.2.1.11 Asesorar al personal en el uso adecuado de equipos institucionales o servicios de fax, definir una configuración segura con acceso a los perfiles autorizados.

9.2.1.12 Definir procedimientos para el uso de las redes inalámbricas en base a los riesgos involucrados.

9.2.1.13 No dejar datos demográficos al alcance de cualquier persona, como los correos electrónicos, ya que se puede hacer uso de ingeniería social para obtener más información.

9.2.2 Acuerdos de transferencia de información

Control

Elaborar e implementar acuerdos de transferencia de información y software segura, entre la institución y terceros.

Recomendaciones para la implementación:

9.2.2.1 Definir procedimientos y responsabilidades para el control y notificación de transmisiones, envíos y recepciones.
9.2.2.2 Definir las responsabilidades y obligaciones en caso de incidentes de seguridad de la información, como la pérdida de datos;
9.2.2.3 Establecer procedimientos para garantizar la trazabilidad y el no repudio.
9.2.2.4 Definir normas técnicas para el empaquetado y transmisión.

9.2.2.5 Establecer los procedimientos necesarios para identificar los mensajeros;

9.2.2.6 Conocer sobre la propiedad de la información y las condiciones de uso.

9.2.2.7 Establecer responsabilidades y obligaciones en caso de pérdida de datos.

9.2.2.8 Conocer los términos y condiciones de las licencias de software privativo o suscripciones de software de código abierto bajo las cuales se utiliza el software.

9.2.2.9 Utilizar un sistema para rotulado de la información clasificada, entendimiento inmediato y protección segura.

9.2.2.10 Definir procedimientos técnicos para la grabación y lectura de la información y del software en el intercambio de información.

9.2.2.11 Implementar los controles necesarios para proteger elementos sensibles como la criptografía.

9.2.2.12 Definir las políticas respectivas para el mantenimiento de una cadena

de custodia de la información mientras está en tránsito;
9.2.2.13 Definir niveles mínimos de control de acceso.

9.2.3 Mensajería electrónica

Control

Establecer las políticas y procedimientos necesarios, en la información de mensajería electrónica, debidamente reglamentada de acuerdo a la norma legal vigente.

Recomendaciones para la implementación:

9.2.3.1 Establecer lineamientos para proteger los mensajes contra los accesos no autorizados, modificación o denegación de los servicios.

9.2.3.2 Supervisar que la dirección y el transporte de mensajes sean correctos.

9.2.3.3 La fiabilidad y disponibilidad del servicio;

9.2.3.4 Tomar en cuenta consideraciones legales como la de firmas electrónicas.

9.2.3.5 Encriptar los contenidos y/o informaciones sensibles que puedan enviarse por mensajería electrónica; utilizando firmas electrónicas reconocidas por el Estado Ecuatoriano u otras tecnologías evaluadas y aprobadas por la institución o el Gobierno Nacional.

9.2.3.6 Considerar controles más estrictos cuando se den ingresos desde redes de acceso público.

9.2.3.7 Monitorear los mensajes de acuerdo al procedimiento que establezca la institución, sustentado en la norma legal vigente.

9.2.3.8 Establecer el procedimiento adecuado para autorizar/aprobar el uso de servicios públicos externos, como mensajería instantánea, redes sociales, sistemas de compartición de archivos entre otros.

9.2.4 Acuerdos de confidencialidad o no revelación

Control

Elaborar el acuerdo de confidencialidad observando los requisitos que deben ser parte del mismo, considerando la no divulgación de la información de acuerdo a la necesidad de la institución.

Recomendaciones para la implementación:

9.2.4.1 Determinar la duración prevista del acuerdo, incluyendo los casos en los que la confidencialidad necesite mantenerse indefinidamente;
9.2.4.2 Responsabilidades y acciones de los firmantes para evitar la revelación no autorizada de la información;
9.2.4.3 Propiedad intelectual de la información, considerar de acuerdo a las directrices de la clasificación de la información.
9.2.4.4 Implementar políticas para el uso de la información confidencial permitida.

9.2.4.5 Definir claramente el derecho de auditar y supervisar las actividades que involucren con la gestión de información en los equipos institucionales y que naveguen en la red de la institución.
9.2.4.6 Acciones que pueden ser tomadas en caso de incumplimiento del acuerdo, de acuerdo a la norma legal vigente.
9.2.4.7 Definir las acciones necesarias cuando se termine un acuerdo.
9.2.4.8 Definir procesos para notificación y aviso de la difusión no autorizada o fugas de información confidencial;
9.2.4.9 Elaborar y aprobar los acuerdos de confidencialidad y de no-divulgación de información conforme la Constitución, las leyes, las necesidades de protección de información de la institución y el EGSI.
9.2.4.10 Controlar que los acuerdos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción.

9.2.4.11 Gestionar la custodia de los acuerdos firmados, en los expedientes, físicos o electrónicos, de cada funcionario, por parte del área de gestión de recursos humanos.

9.2.4.12 Controlar que la firma de los acuerdos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionarios a la institución, sin excepción.
9.2.4.13 Gestionar la aceptación, entendimiento y firma de acuerdos de confidencialidad y de no divulgación de información por parte de terceros (ej., contratistas, proveedores, pasantes, entre otros) que deban realizar labores dentro de la institución sea por medios lógicos o físicos y que involucren el manejo de información.

10 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

10.1 Requisitos de seguridad de los sistemas de información

10.1.1 Análisis de requisitos y especificaciones de seguridad de la información

Control

Las directrices de seguridad de la información, deben incluirse entre los requisitos para los nuevos sistemas de gestión de información o mejoras a los sistemas existentes.

Recomendaciones para la implementación:

10.1.1.1 Definir los requerimientos de seguridad. Por ejemplo: criptografía, control de sesiones, etc.

10.1.1.2 Definir los controles apropiados, tanto automatizados como manuales. En esta definición deben participar personal del requerimiento funcional y personal técnico que trabajarán en el sistema.

10.1.1.3 Si se adquieren productos, los contratos con el proveedor deben contemplar los requisitos de la seguridad identificados.

10.1.1.4 Definir los procesos de aprobación y autorización de credenciales de

acceso, tanto para los usuarios de gestión como para los usuarios administradores y técnicos.

10.1.1.5 Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas por falla o falta de seguridad.

10.1.1.6 Emitir las directrices necesarias a los usuarios y operadores sobre las funciones y responsabilidades en el sistema y su información.

10.1.1.7 Definir los controles necesarios para la protección requerida en los activos involucrados, considerando la disponibilidad, la confidencialidad y la integridad de la información.

10.1.1.8 Directrices para considerar los requisitos derivados de los procesos de la institución, tales como el registro y monitorización de transacciones y requisitos de no repudio;

10.1.1.9 Los requisitos impuestos por otros controles de seguridad, por ejemplo, interfaces para el registro y la monitorización o sistemas de detección de fugas de datos.

10.1.2 Asegurar los servicios de aplicaciones en redes públicas

Control

Implementar los controles necesarios sobre las aplicaciones cuyo tráfico pasa a través de redes públicas, reglamentando de acuerdo a la norma legal vigente.

Recomendaciones para la implementación:

10.1.2.1 Credenciales de acceso a los sistemas institucionales, transversales etc.

10.1.2.2 Implementar procesos de autorización sobre el contenido, problemas o firmas de documentos transaccionales clave de la institución.

10.1.2.3 Políticas claras conociendo sus responsabilidades tanto para el que presta como para el que usa el servicio.

10.1.2.4 Establecer acuerdos de confidencialidad e integridad, prueba de envío y recepción de documentación importante y el no repudio de contratación pública.

10.1.2.5 Asegurar el nivel de confianza requerido para la integridad de los documentos clave;

10.1.2.6 Implementar los controles necesarios que permitan proteger la información confidencial.

10.1.2.7 Determinar la confidencialidad y la integridad de las transacciones

ejecutadas así como la confirmación de los recibos de entrega, información de pagos.

10.1.2.8 Seleccionar la forma más adecuada de pago para evitar el fraude en la institución cuando sea necesario.

10.1.2.9 Implementar el nivel de protección requerido para mantener la confidencialidad e integridad de la información de los pedidos, de acuerdo a la necesidad de la institución;

10.1.2.10 Determinar controles para evitar la pérdida o duplicación de información de la transacción;

10.1.2.11 Determinar la responsabilidad asociada con cualquier transacción ilegal;

10.1.2.12 Considerar los requisitos de los seguros contratados entre las partes.

10.1.3 Controles de transacciones en línea

Control

Implementar controles en las aplicaciones institucionales, para evitar transmisiones incompletas, errores de enrutamiento, alteración no autorizada, difusión, duplicación, o reproducción de mensajes no autorizados.

Recomendaciones para la implementación:

10.1.3.1 Definir procedimientos para el uso de certificados digitales (ejem.: firmas electrónicas) por las partes implicadas en la transacción.

10.1.3.2 Establecer procedimientos para garantizar todos los aspectos en la transacción como credenciales de usuario, confidencialidad de la transacción y privacidad de las partes.

10.1.3.3 Cifrar o encriptar el canal de comunicaciones entre las partes involucradas (por ejemplo, utilizando SSL/TLS).

10.1.3.4 Establecer protocolos seguros en la comunicación de las partes involucradas, por ejemplo, utilizando SSL/TLS).

10.1.3.5 Establecer procedimientos para que las transacciones se encuentren fuera del entorno de acceso público, por ejemplo, en una plataforma de almacenamiento existente en la intranet de la institución, y no se mantiene y está expuesta en un medio de almacenamiento accesible directamente desde internet;

10.1.3.6 Utilizar los servicios de una entidad certificadora confiable.

10.2 Seguridad en el desarrollo y en los procesos de soporte

10.2.1 Política de desarrollo seguro

Control

Definir la política y socializar al área respectiva, las reglas, modelo etc. para el desarrollo de aplicaciones y sistemas en la institución.

Recomendaciones para la implementación:

10.2.1.1 Implementar la respectiva seguridad en el área de desarrollo de software.

10.2.1.2 Implementar directrices de seguridad de acuerdo al modelo de desarrollo del software, en el ciclo de vida del desarrollo, considerando:

10.2.1.2.1 Seguridad en la metodología de desarrollo de software,

10.2.1.2.2 Manual de desarrollo seguro para cada lenguaje de programación utilizado,

10.2.1.3 Establecer los requisitos necesarios de seguridad en la fase de diseño;

10.2.1.4 Puntos de verificación de seguridad incorporados a los hitos del proyecto;

10.2.1.5 Repositorios seguros;

10.2.1.6 Seguridad en el control de versiones;

10.2.1.7 Elaborar implementar y socializar al área respectiva lo necesario sobre la seguridad de aplicaciones.

10.2.1.8 Capacidad de los desarrolladores de evitar, encontrar y reparar vulnerabilidades.

10.2.2 Procedimientos de control de cambios en sistemas

Control

Elaborar, implementar y socializar al área respectiva el procedimiento formal, para realizar los cambios a lo largo del ciclo de vida del desarrollo del software.

Recomendaciones para la implementación:

10.2.2.1 Mantener un registro de los niveles de autorización acordados.

10.2.2.2 Verificar que los cambios sean propuestos por usuarios autorizados y se respete los términos y condiciones que surjan de la licencia de uso, en caso de existir.

10.2.2.3 Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.

10.2.2.4 Mantener el catalogo actualizado e identificado de todo el software, la información, las entidades de base de datos y el hardware que requieren cambios;

10.2.2.5 Identificar y comprobar la seguridad del código crítico para evitar errores típicos.

10.2.2.6 Obtener aprobación formal por parte del responsable del área de Tecnologías de la Información o del área que hace sus veces, para las tareas detalladas, antes de comenzar las actividades.

10.2.2.7 Obtener la aprobación por parte del usuario autorizado y del área de pruebas, mediante pruebas en el ambiente correspondiente antes de la implementación.

10.2.2.8 Mantener un control de versiones para todas las actualizaciones de software.

10.2.2.9 Mantener el registro de auditoría de todas las solicitudes de cambio.

10.2.2.10 Implementar funcionalidades para que se pueda solicitar la autorización del propietario de la información (ej., información personal), cuando se hagan cambios a sistemas de procesamiento de la misma, cuando sea necesario.

10.2.2.11 Actualizar la documentación para cada cambio implementado, tanto en los manuales de usuario como en la documentación operativa, y la documentación obsoleta sea archivada o eliminada de acuerdo a la norma legal vigente en la institución.

10.2.2.12 Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.

10.2.2.13 Efectuar las actividades relativas al cambio en el ambiente de pruebas.

10.2.2.14 Definir si los cambios a realizar tienen impacto sobre la continuidad del servicio. Si un cambio implica mucha funcionalidad o impacto al software base o infraestructura, se deberá realizar un procedimiento más complejo de cambio, para que se apruebe con un plan de contingencia y se identifiquen los riesgos posibles.

10.2.2.15 Solicitar la revisión del Oficial de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.

10.2.2.16 Notificar a los usuarios del sistema sobre el cambio a realizar. Se enviará una notificación para informar sobre el tiempo que durará la ejecución del cambio y para informar cuando se haya terminado la ejecución del cambio.

10.2.2.17 Abrir ventanas de mantenimiento con una duración definida, en la cual se contemple las acciones del cambio, pruebas y configuraciones.

10.2.2.18 Elaborar el informe de paso de pruebas a producción, que deberá contener el detalle de los cambios y acciones a ejecutar, tanto de software, bases de datos y hardware:
- Archivos a modificar;
- Script de base de datos a ejecutar en la secuencia correcta de ejecución;
- Script de inicialización de datos;
- Creación de directorios;
- Script de creación de tareas periódicas, en caso de ser necesario;
- Plan de contingencia;
- Protocolo de pruebas de verificación el cambio;
- Definir el punto de no retorno;
- Definir las condiciones para determinar la restauración al estado anterior.

10.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

Control

Cuando se modifiquen los sistemas operativos de las aplicaciones criticas de la institución, deben ser revisadas y probadas, para asegurar que no existen efectos negativos en la gestión o seguridad institucional.

Recomendaciones para la implementación:

10.2.3.1 Revisar los procedimientos de control e integridad de las aplicaciones para garantizar que no hayan sido comprometidas por el cambio.

10.2.3.2 Garantizar que los cambios al sistema operativo tengan una planificación adecuada, para realizar pruebas y revisiones apropiadas antes de la implementación.

10.2.3.3 Probar que los cambios realizados retornen la funcionalidad esperada.

10.2.3.4 Realizar las pruebas inmediatamente después de realizar el cambio y durante la ventana de mantenimiento definida para el cambio.

10.2.3.5 Disponer de un protocolo de pruebas a realizar.

10.2.3.6 Entregar un informe de las pruebas realizadas.
10.2.3.7 Identificar si existen problemas con los cambios, para aplicar el plan de contingencia o realizar el retorno al estado anterior al cambio.

10.2.3.8 Garantizar que los cambios apropiados sean realizados en los planes de continuidad del negocio.

10.2.4 Restricciones a los cambios en los paquetes de software

Control

Evitar las modificaciones en el software suministrado o adquirido a terceros por la institución, limitarse a cambios realmente necesarios; considerar un control estricto sobre los cambios.

Recomendaciones para la implementación:

10.2.4.1 Disponer de la autorización del responsable del software y del área de Tecnologías de la Información que se apruebe el cambio.
10.2.4.2 Evitar que los controles y los procesos de integridad incorporados se vean complicados;

10.2.4.3 Analizar los términos y condiciones de la licencia, si es del caso, a fin de determinar si las modificaciones se encuentran autorizadas.

10.2.4.4 Determinar la posibilidad de obtener los cambios necesarios del proveedor como actualizaciones del programa estándar;

10.2.4.5 Considerar el impacto si la institución se convierte en responsable del mantenimiento futuro del software como resultado de los cambios;

10.2.4.6 Verificar la compatibilidad con otro software en uso.

10.2.4.7 Determinar la conveniencia de que la modificación sea efectuada por la institución, por el proveedor o por un tercero, y evaluar el impacto.

10.2.4.8 Conservar el software original que se va a cambiar y los cambios se deberán aplicar a una copia claramente identificada.

10.2.4.9 Definir un proceso de gestión de las actualizaciones del software para asegurarse de que los parches más actualizados aprobados y las actualizaciones de las aplicaciones están instalados en todo el software autorizado.

10.2.4.10 Probar y documentar en su totalidad todos los cambios, de manera que se puedan volver a aplicar, si es necesario, para mejoras futuras del software

10.2.5 Principios de ingeniería de sistemas seguros

Control

Establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.

Recomendaciones para la implementación:

10.2.5.1 Determinar al inicio los permisos mínimos, es mejor ir escalando privilegios por demanda de acuerdo a los perfiles establecidos en las etapas de diseño.
10.2.5.2 Si se utiliza un lenguaje que no sea compilado, asegurarse de limpiar el código que se pone en producción, para que no contenga rutinas de

pruebas, comentarios o cualquier tipo de mecanismo que pueda dar lugar a un acceso indebido.

10.2.5.3 Validar los datos que ingresan a la aplicación, todo debe ser verificado para garantizar que lo que está ingresando al sistema es lo que quiere ingresar y evitar inyecciones de código.

10.2.5.4 Analizar las tecnologías utilizadas para el desarrollo; Estas van evolucionando y cualquier mejora que se haga puede dejar obsoleta o inseguras versiones anteriores.

10.2.5.5 Todo tipo de acceso que se realice a los sistemas deben ser validados con las credenciales respectivas.

10.2.5.6 Al intercambiar información sensible utilizar protocolos para cifrar las comunicaciones, y en el caso de almacenamiento la información confidencial debería estar cifrada utilizando algoritmos fuertes y claves robustas.

10.2.5.7 Toda funcionalidad, campo, botón o menú nuevo debe agregarse de acuerdo a los requerimientos de diseño. De esta forma se evita tener porciones de código que resultan siendo innecesarias.

10.2.5.8 La información almacenada en dispositivos móviles debería ser la mínima, y más si se trata de contraseñas o datos de sesión. Este tipo de dispositivos son los más propensos a desaparecer y por lo tanto su información puede ser expuesta más fácilmente.

10.2.5.9 Documentar todo cambio que se realice, esto facilitará modificaciones futuras.

10.2.5.10 Poner más cuidado en los puntos más vulnerables, no hay que olvidar que el nivel máximo de seguridad viene dado por el punto más débil.

10.2.6 Ambiente de desarrollo seguro

Control

La institución debe establecer y proteger correctamente los ambientes de desarrollo seguro, para el desarrollo del sistema y los esfuerzos de integración, durante el ciclo de vida del desarrollo del sistema.

Recomendaciones para la implementación:

Un ambiente de desarrollo seguro incluya las personas, los procesos y la tecnología relacionados con el desarrollo e integración del sistema.

Las organizaciones deberían evaluar los riesgos asociados con los proyectos de desarrollo de sistemas individuales y establecer entornos de desarrollo seguros para los proyectos específicos de desarrollo del sistema, teniendo en cuenta:

10.2.6.1 Considerar la criticidad de los datos a ser procesados, almacenados y transmitidos por el sistema.

10.2.6.2 Aplicación de la norma legal vigente institucional y pública, por ejemplo leyes, reglamentos, política entre otros.

10.2.6.3 Cumplimiento controles de seguridad ya implementados por la institución que aseguren el desarrollo del sistema.

10.2.6.4 Honestidad de los funcionarios que trabajan en el área, debidamente validada por talento humano.

10.2.6.5 Nivel de participación externa relacionada con el desarrollo del sistema.

10.2.6.6 Separación de los diferentes ambientes de desarrollo, de ser necesario y procedente.
10.2.6.7 Control de accesos al ambiente de desarrollo;
10.2.6.8 Evaluar continuamente los cambios en el ambiente de desarrollo y el código almacenado en el mismo;
10.2.6.9 Respaldos adecuadamente almacenados, almacenamiento seguro de las copias de seguridad fuera de las instalaciones de la institución;
10.2.6.10 Control del movimiento de datos desde y hacia el ambiente.

10.2.7 Desarrollo externalizado

Control

La institución debe supervisar y monitorear las actividades del desarrollo del sistema que se esté contratando, validar que cumpla con los controles establecidos.

Recomendaciones para la implementación:

10.2.7.1 Definir acuerdos de licencias, acuerdos de uso, propiedad de código y derechos conferidos.

10.2.7.2 Definir los requerimientos contractuales para las prácticas de diseño seguro, calidad del código, codificación, la existencia de garantías y pruebas.

10.2.7.3 Entrega del modelo de amenazas aprobado al desarrollador externo;

10.2.7.4 Pruebas de aceptación de la calidad y la adecuación de las entregas;

10.2.7.5 Evaluar las evidencias de que los umbrales de seguridad se utilizan para establecer los niveles mínimos aceptables de seguridad y calidad de la privacidad;

10.2.7.6 Definir procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.

10.2.7.7 Presentación de evidencias de que se han realizado suficientes pruebas para proteger contra la presencia de vulnerabilidades conocidas;

10.2.7.8 Definir los requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.

10.2.7.9 Clausula en el contrato para auditar los procesos y controles de desarrollo implementados;

10.2.7.10 Verificar el cumplimiento de las condiciones de seguridad requeridas.

10.2.7.11 Definir el desarrollo del módulo que permita auditar al sistema.

10.2.7.12 Elaborar de acuerdo a la normativa legal vigente el respectivo contrato, determinando los objetivos y el alcance, así como cada una de las clausulas técnicas y administrativas.

10.2.7.13 Verificación por parte de la institución, de la eficacia de la aplicación del control.
10.2.7.14 Definir acuerdos de custodia de las fuentes del software o convenios de fideicomiso (y cualquier otra información requerida) en caso de quiebra de la tercera parte.
10.2.7.15 Realizar pruebas antes de la instalación para detectar códigos troyanos o código malicioso.

10.2.8 Pruebas de seguridad del sistema

Control

Realizar pruebas de funcionalidad, que considere necesarias la institución en aspectos de seguridad durante las etapas de desarrollo.

Recomendaciones para la implementación:

10.2.8.1 Los sistemas nuevos y los actualizados requieren pruebas y verificación exhaustivas en los procesos de desarrollo, incluyendo la preparación de un programa detallado de actividades y datos de prueba junto a los resultados esperados bajo las condiciones establecidas.
10.2.8.2 Para desarrollos propios, dichas pruebas inicialmente deberían ser realizadas por el equipo de desarrollo.
10.2.8.3 Se deberían realizar pruebas de aceptación independientes (tanto en los desarrollos internos como para los desarrollos externalizados) para asegurar que el sistema funciona como se esperaba.
10.2.8.4 La extensión de las pruebas debería ser proporcionales a la importancia y la naturaleza del sistema.

10.2.9 Pruebas de aceptación de sistemas

Control

Establecer programas de pruebas y criterios relacionados, para la aceptación de nuevos sistemas de información, actualización y/o nuevas versiones.

Recomendaciones para la implementación:

10.2.9.1 Verificar el desempeño y los requerimientos de cómputo necesarios para los nuevos sistemas.
10.2.9.2 Considerar procedimientos de recuperación y planes de contingencia.
10.2.9.3 Poner a prueba procedimientos operativos de rutina según normas definidas para el sistema.
10.2.9.4 Garantizar la implementación de un conjunto de controles de seguridad acordados.
10.2.9.5 Asegurar que la instalación del nuevo sistema no afecte negativamente los sistemas existentes, especialmente en períodos pico de procesamiento.
10.2.9.6 Considerar el efecto que tiene el nuevo sistema en la seguridad global de la institución.
10.2.9.7 Capacitar sobre el funcionamiento y utilización del nuevo sistema.
10.2.9.8 Para nuevos desarrollos, se debe involucrar a los usuarios y a todas las áreas relacionadas, en todas las fases del proceso, para garantizar la

eficacia operativa del sistema propuesto, cumplimiento del contrato de acuerdo a lo solicitado.

10.3 Datos de prueba

10.3.1 Protección de los datos de prueba

Control

Los datos de prueba deben ser seleccionados cuidadosamente y se deberían proteger y controlar.

Recomendaciones para la implementación:

10.3.1.1 Identificar por cada sistema, los datos que pueden ser copiados de un ambiente de producción a un ambiente de pruebas.

10.3.1.2 Efectuar pruebas de los sistemas en el ambiente de pruebas, sobre datos extraídos del ambiente de producción.

10.3.1.3 Personalizar los datos en el ambiente de pruebas, eliminando las contraseñas de producción y generando nuevas para pruebas.

10.3.1.4 Solicitar autorización formal para realizar una copia de la base de datos de producción como base de datos de prueba.

10.3.1.5 Aplicar los mismos procedimientos de control de acceso que existen en la base de producción.

10.3.1.6 Eliminar inmediatamente, una vez completadas las pruebas, la información de producción utilizada.

10.3.1.7 Registrar la copia y la utilización de la información para futuras auditorías.

11 RELACIONES CON PROVEEDORES

11.1 Seguridad de la información en relación con los proveedores

11.1.1 Política de seguridad de la información en las relaciones con los proveedores

Control

Elaborar implementar y socializar, la política relacionada con el acceso del proveedor y terceras personas, a los activos de la institución, debe documentarse formalmente los acuerdos con el proveedor, para mitigar los riesgos asociados.

Recomendaciones para la implementación:

11.1.1.1 Identificar, documentar los tipos de proveedores, a los cuales la institución permitirá acceder a su información. Ejm. servicios de TI, utilidades logísticas, servicios financieros, componentes de la infraestructura de TI etc.

11.1.1.2 Determinar en la documentación contractual respectiva, el ciclo de vida de la gestión de las relaciones con los proveedores.

11.1.1.3 Definir los tipos de acceso a la información que se permitirá a los

diferentes tipos de proveedores, con su supervisión y su control del acceso;

11.1.1.4 Implementar requisitos mínimos de seguridad de la información por cada tipo de acceso a la información, para servir de base en los acuerdos con cada uno de los proveedores de conformidad con las necesidades, requisitos institucionales y su perfil de riesgo;

11.1.1.5 Implementar procesos y procedimientos para supervisar el cumplimiento de los requisitos de seguridad de la información establecidos para cada tipo de proveedor y cada tipo de acceso, incluyendo la revisión por terceros y la validación de los productos;

11.1.1.6 Implementar controles efectivos, para garantizar la integridad de la información o del procesamiento de la misma, proporcionada por las partes.

11.1.1.7 Establecer el procedimiento necesario para el manejo de incidencias y contingencias asociadas al acceso de los proveedores, incluyendo responsabilidades, tanto de la institución, como de los proveedores;

11.1.1.8 Definir los acuerdos de resiliencia y, si fuesen necesarios, acuerdos de recuperación y de contingencia para asegurar la disponibilidad de la información o el procesamiento de la información proporcionada por cualquiera de las partes;

11.1.1.9 Concientizar a los funcionarios de la institución que se relaciona con los proveedores, sobre el cumplimiento legal, técnico y administrativo de las actuaciones según el tipo de proveedor y el nivel de acceso a los activos de gestión de información según su clasificación.

11.1.1.10 Documentación formal entre las partes, sobre los controles de seguridad de la información analizados e implementados.

11.1.1.11 Establecer el procedimiento para ejecutar migraciones necesarias de información, instalaciones de procesamiento de la información y todo aquello que necesite ser migrado, garantizando que la seguridad de la información se mantenga en todo el proceso.

11.1.2 Requisitos de seguridad en contratos con terceros

Control

La institución debe establecer y acordar todos los requisitos de seguridad de la información con cada proveedor antes que pueda ingresar, procesar, almacenar, comunicar o proporcionar componentes de TI que dan soporte a la información de la institución.

Recomendaciones para la implementación:

11.1.2.1 Identificar y evaluar los riesgos para la información y los servicios de procesamiento de información de la institución en los procesos que involucran terceras partes e implementar los controles apropiados antes de autorizar el acceso.

11.1.2.2 Bloquear el acceso al proveedor a la información de la institución

hasta haber implementado los controles apropiados y, cuando es viable, haber firmado un contrato que defina los términos y las condiciones del caso, así como acuerdos de confidencialidad respecto de la información a la que tendrán acceso.

11.1.2.3 Describir la información entregada o a la que acceden, así como los métodos para la entrega o acceso a la misma.

11.1.2.4 Utilizar el esquema de clasificación de la información definido por la institución, si es necesario aplicar el mismo esquema con el proveedor, en la relación contractual establecida.

11.1.2.5 Considerar la norma legal vigente, incluir la protección de datos personales, derechos de propiedad intelectual, derechos de autor y la descripción que garantice el cumplimiento.

11.1.2.6 Obligación contractual del proveedor y la institución en la implementación, de controles incluyendo el control de acceso, la evaluación de desempeño, monitoreo, informes y auditoria.

11.1.2.7 Solicitar al proveedor la lista del personal autorizado para ingresar o recibir información de la institución, procedimientos y las condiciones de la autorización.

11.1.2.8 Describir las políticas de seguridad de la información relevantes para la ejecución del contrato específico;

11.1.2.9 Garantizar que el proveedor es consciente de sus obligaciones y acepta las responsabilidades y deberes involucrados en el acceso, procesamiento, comunicación o gestión de la información y los servicios de procesamiento de información de la institución, nombrar una persona de contacto.

11.1.2.10 Mantener la potestad de auditar los procesos de los proveedores y los controles relacionados con el acuerdo.

11.1.2.11 Registrar y mantener las terceras partes vinculadas a la institución considerando los siguientes tipos:

- 11.1.2.11.1 proveedores de servicios (ej., Internet, proveedores de red, servicios telefónicos, servicios de mantenimiento, energía eléctrica, agua, entre otros);
- 11.1.2.11.2 servicios de seguridad;
- 11.1.2.11.3 contratación externa de proveedores de servicios y/u operaciones;
- 11.1.2.11.4 asesores y auditores externos;
- 11.1.2.11.5 limpieza, alimentación y otros servicios de soporte contratados externamente;
- 11.1.2.11.6 personal temporal (estudiantes, pasantes, funcionarios públicos externos);
- 11.1.2.11.7 ciudadanos/clientes;
- 11.1.2.11.8 Otros

11.1.3 Cadena de suministro de tecnologías de la información y de las comunicaciones

Control

Incluir en los acuerdos con los proveedores, los requisitos para enfrentar los riesgos de seguridad de la información que tienen relación con las TIC's, asociados con la cadena de suministros de los servicios y productos de TIC's.

Recomendaciones para la implementación:

11.1.3.1 Definir los requisitos de seguridad de la información para adquirir productos o servicios de TIC's, además los requisitos de seguridad de la información generales que tienen relación con los proveedores.

11.1.3.2 Requerir que los proveedores reproduzcan los requisitos de seguridad de la institución a lo largo de la cadena de suministro.

11.1.3.3 Implementar un proceso de monitoreo para validar que los productos y servicios de TIC entregados cumplan con las normas de seguridad establecidas.

11.1.3.4 Identificar los componentes críticos de productos o servicios para el mantenimiento de la funcionalidad y que, por tanto, requieren una mayor atención y control cuando se construyen fuera de la institución, especialmente si el proveedor principal subcontrata partes del producto o componentes del servicio a otros proveedores;

11.1.3.5 Obtener garantías que los componentes críticos se pueden monitorear a lo largo de la cadena de suministro.

11.1.3.6 Garantizar formalmente que los productos de TIC entregados funcionan correctamente y cumplen con el contrato respectivo.

11.1.3.7 Implementar procesos específicos para mitigar los riesgos asociados a la no entrega de los componentes de TIC. Esto incluye la gestión de los riesgos del fin de la disponibilidad de los componentes, debido al cese de negocio de los proveedores, o a que los proveedores no entreguen ya estos componentes por obsolescencia tecnológica.

11.2 Gestión de la provisión de servicios del proveedor

11.2.1 Monitoreo y revisión de los servicios de proveedores

Control

La institución tiene que monitorear, evaluar y auditar continuamente la provisión de servicios del proveedor.

Recomendaciones para la implementación:

11.2.1.1 Monitorear los niveles de rendimiento para validar el cumplimiento del nivel de servicio que la institución espera de su proveedor, conforme los acuerdos definidos en el proceso contractual.

11.2.1.2 Analizar los reportes emitidos por el proveedor del servicio y organizar

reuniones periódicas de progreso de acuerdo a lo establecido en el proceso contractual.

11.2.1.3 Ejecutar auditorías a los proveedores, junto con las auditorias independientes de existir, y dar seguimiento a problemas identificados y nuevos.

11.2.1.4 Proporcionar reportes de los incidentes de seguridad de la información, analizar la misma para verificar su cumplimiento conforme la relación contractual establecida en los procedimientos de soporte.

11.2.1.5 Analizar los registros de auditoria, los registros de incidentes de seguridad de la información, problemas operativos, incumplimiento del nivel de servicio, fallos, registro de errores e interrupciones relacionados con el servicio prestado.

11.2.1.6 Resolver gestionar cualquier problema detectado;

11.2.1.7 Revisar la seguridad de los proveedores del proveedor con quien se mantiene la relación contractual.

11.2.1.8 Justificar de acuerdo a la norma legal vigente, en el proceso de contratación la capacidad de servicio suficiente, junto con planes viables destinados a garantizar que los niveles de servicio planteados se mantengan en todo tipo de fallas.

11.2.2 Gestión de cambios en los servicios de proveedores

Control

Gestionar cambios en la provisión de servicios, mantenimiento, mejora de políticas, procedimientos y controles de seguridad de la información; considerando la criticidad de los procesos y sistemas de la institución afectados, así como la revisión y reapreciación de los riesgos, de acuerdo a la norma legal vigente.

Recomendaciones para la implementación:

11.2.2.1 Establecer un proceso de gestión de cambios; en los servicios ofrecidos por los proveedores, en el desarrollo de aplicaciones, mejoras en la provisión de servicios actuales, actualizaciones de las políticas y procedimientos institucionales, de hardware, software, redes, otros.

11.2.2.2 Coordinar el proceso de cambio cuando se realice cambio de proveedores, cambio de ubicación física en los servicios ofrecidos por proveedores.

11.2.2.3 Cambios realizados por la institución para implementar:

11.2.2.3.1 Mejoras en los servicios actuales ofrecidos

11.2.2.3.2 Desarrollo de nuevas aplicaciones y nuevos sistemas.

11.2.2.3.3 Modificaciones o actualizaciones de las políticas y procedimientos de la institución

11.2.2.3.4 Controles nuevos o modificados para resolver los incidentes de seguridad de la información y para mejorar la seguridad.

11.2.2.4 Cambios en los servicios de los proveedores para implementar:

11.2.2.4.1 Cambios y mejora de las redes,

11.2.2.4.2 Uso de nuevas tecnologías,

11.2.2.4.3 Instalación de nuevos productos o nuevas versiones,
11.2.2.4.4 Nuevas herramientas y entornos de desarrollo,
11.2.2.4.5 Cambio en la ubicación física de las instalaciones de servicios que presta la institución.
11.2.2.4.6 Cambio de proveedores,

12 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

12.1 Gestión de los incidentes de seguridad de la información y mejoras

12.1.1 Responsabilidades y procedimientos

Control

Establecer formalmente responsabilidades y procedimientos para asegurar una respuesta rápida, efectiva y acorde a los incidentes de seguridad de la información que pueden ocurrir en la institución.
Recomendaciones para la implementación:

12.1.1.1 Establecer responsabilidades formales en la gestión que nos aseguren, que los procedimientos se desarrollen y reporten correctamente en la institución considerando:

12.1.1.1.1 Establecer procedimientos para la planificación y preparación de la respuesta ante posibles incidentes,
12.1.1.1.2 Establecer procedimientos para monitorear, detectar, analizar y comunicar eventos e incidentes de seguridad de la información,
12.1.1.1.3 Definir procedimientos para identificar, clasificar, registrar las actividades de gestión de incidentes y preparar el reporte respectivo.
12.1.1.1.4 Recolectar y asegurar pistas de auditoría, manejo de evidencias forenses y toda la evidencia relacionada con el incidente.
12.1.1.1.5 Establecer procedimientos para evaluar y tomar decisiones sobre eventos de seguridad de la información y determinar puntos débiles de la seguridad de la información.
12.1.1.1.6 Ejecutar procedimientos de respuesta considerando los relativos al escalamiento, recuperación controlada a partir de un incidente, y comunicación a personas internas y externas o a terceras organizaciones,
12.1.1.1.7 Identificar y analizar las posibles causas de un incidente producido.

12.1.1.2 Establecer procedimientos que aseguren que:

12.1.1.2.1 El personal capacitado maneje los incidentes de seguridad de la información en la institución.
12.1.1.2.2 Monitoreo continuo para la detectar y comunicar incidentes de seguridad,
12.1.1.2.3 Mantener contactos efectivos con las autoridades, grupos de interés internos y externos, (EcuCert, Csirt); que tratan asuntos relacionados con los incidentes de seguridad de la información.
12.1.1.2.4 Planificar e implementar acciones correctivas para evitar la recurrencia del incidente

12.1.1.3 El Oficial de Seguridad de la Información, emitirá un reporte a los jefes

de las áreas afectadas por el incidente.

12.1.1.4 Incluir en los procedimientos de comunicación:

12.1.1.4.1 Preparar y remitir a los funcionarios, formularios de comunicación sobre eventos de seguridad de la información, para recordar el procedimiento que se debe ejecutar en caso de ocurrencia de un incidente de seguridad de la información,

12.1.1.4.2 El correcto comportamiento a tomarse en caso de una ocurrencia de un incidente de seguridad de la información, como registrar los detalles importantes, mensajes en la pantalla etc. e informar al Oficial de Seguridad, para coordinar las tareas pertinentes.

12.1.1.4.3 Referir el proceso disciplinario formal de acuerdo a la norma legal vigente, para tratar a los trabajadores, contratistas o terceras partes que hayan cometido el quebrantamiento de la seguridad.

12.1.1.4.4 Notificar a todos los funcionarios afectados por el incidente de la restauración del equipo, sistema o servicio afectado, una vez esté solucionado el incidente.

12.1.2 Reporte de los eventos de seguridad de la información

Control

Elaborar, implementar y socializar el procedimiento formal para reportar los eventos de seguridad de la información, a través de los canales respectivos.

Recomendaciones para la implementación:

12.1.2.1 Instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el evento, que establezca la acción que se ha de tomar al recibir el reporte sobre un evento que amenace la seguridad de la información.

12.1.2.2 Establecer un punto de contacto (Oficial de Seguridad de la Información) para el reporte de los eventos de seguridad de la información. Es conveniente garantizar que este punto de contacto sea conocido en toda la institución, siempre esté disponible y puede suministrar respuesta oportuna y adecuada. Todos los empleados, contratistas y usuarios contratados por los proveedores deberán tener conciencia de su responsabilidad para reportar todos los eventos de seguridad de la información lo más pronto posible.

Se considerarán como situaciones para comunicar incidentes de seguridad de la información las siguientes:

12.1.2.4 Control ineficaz de la seguridad de la información;

12.1.2.5 Violación de las expectativas de integridad, confidencialidad y disponibilidad de la información;

12.1.2.6 Errores humanos;

12.1.2.7 Incumplimientos en la aplicación de políticas o directrices;

12.1.2.8 Incumplimiento de las directrices de seguridad física;

12.1.2.9 Cambios incontrolados del sistema;

12.1.2.10 Fallas en el funcionamiento del software o hardware;

12.1.2.11 Accesos no permitidos.

12.1.3 Reporte de debilidades de seguridad de la información

Control

Los funcionarios de la institución, contratistas o terceras partes, deben obligatoriamente registrar y reportar, cualquier debilidad probable en la seguridad de la información, en los sistemas o servicios de información de la institución.

Recomendaciones para la implementación:

12.1.3.1 Todos los empleados, contratistas y usuarios de terceras partes deberán informar sobre estos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberán ser fáciles, accesibles y disponibles. Se les debe informar a ellos que, en ninguna circunstancia, deberán intentar probar una debilidad sospechada.

12.1.3.2 Cuando un empleado, contratista o usuario contratado por un proveedor detecte una vulnerabilidad o debilidad en un equipo, sistema o servicio deberá ejecutar las siguientes acciones:

12.1.3.2.1 Notificar a su jefe inmediato y este al Oficial de Seguridad de la Información de la debilidad o vulnerabilidad detectada.

12.1.3.2.2 Registrar la fecha, hora, apellidos y nombres del funcionario que detectó la debilidad o vulnerabilidad, descripción de la debilidad, descripción de posibles incidentes de seguridad que pudieran ocurrir producto de esta debilidad. El responsable de llevar este reporte denominado "Reporte de vulnerabilidades o debilidades de la seguridad de la información" es el Oficial de Seguridad de la Información.

12.1.3.2.3 Nunca, por razón alguna, deberá intentar probar la debilidad o vulnerabilidad detectada en la seguridad. El ensayo de las vulnerabilidades se podría interpretar como un posible uso inadecuado del sistema, equipo o servicio y también podría causar daño al sistema o servicio de información y eventualmente podría recaer en una responsabilidad legal.

12.1.3.2.4 El Oficial de Seguridad de la Información deberá tomar las medidas pertinentes para prevenir o eliminar la vulnerabilidad o debilidad detectada.

12.1.4 Apreciación y decisión sobre los eventos de seguridad de la información

Control

Evaluar los eventos de seguridad de la información y decidir si se clasifican como incidentes de seguridad de la información.

Recomendaciones para la implementación:

12.1.4.1 La información que se obtiene de la evaluación de los eventos de seguridad de la información se debe utilizar para identificar y determinar si el evento es un incidente de seguridad de la información.

12.1.4.2 La clasificación y priorización de los incidentes ayuda a identificar el impacto y el alcance.

12.1.4.3 En casos donde la institución tiene un equipo de respuesta a incidentes de seguridad de la información, la evaluación y decisión puede redirigirse al equipo para su confirmación o reevaluación.

12.1.5 Respuesta a incidentes de seguridad de la información

Control

Aplicación de procedimientos establecidos, para responder ante incidentes de seguridad de la información.
Recomendaciones para la implementación:

12.1.5.1 Cuando un incidente se produzca, el funcionario en turno responsable del equipo o sistema afectado, debe realizar las siguientes acciones en su orden:
- 12.1.5.1.1 Identificar el incidente: levantamiento de evidencias tan pronto como sea posible
- 12.1.5.1.2 Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del funcionario en turno, departamento o área afectada, equipo o sistema afectado y breve descripción del incidente.
- 12.1.5.1.3 Notificar al Oficial de Seguridad de la Información de la institución.
- 12.1.5.1.4 Clasificar el incidente de acuerdo al tipo de servicio afectado y al nivel de severidad.
- 12.1.5.1.5 Asignar una prioridad de atención al incidente en el caso de que se produjeran varios en forma simultánea.
- 12.1.5.1.6 Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas.
- 12.1.5.1.7 Escalar el incidente en el caso que el funcionario en turno no pueda solucionarlo, el escalamiento deberá ser registrado en la bitácora de escalamiento de incidentes. El funcionario en turno debe escalar el incidente a su jefe inmediato, en el caso en el que el funcionario no tuviere un jefe al cual escalarlo, este debe solicitar soporte al proveedor del equipo o sistema afectado.
- 12.1.5.1.8 Investigar y diagnosticar en forma definitiva las causas por las cuales se produjo el incidente.
- 12.1.5.1.9 Resolver y restaurar el servicio afectado por el incidente debido a la para de un equipo o un sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes.
- 12.1.5.1.10 Cerrar el incidente, actualizando el estado del registro del incidente en la bitácora de incidentes a "Resuelto". Confirmar con el funcionario en turno, responsable del equipo o del sistema de que el incidente ha sido resuelto.

12.1.5.2 Implementar controles para modificar el riesgo en las debilidades de seguridad de la información encontradas y que pudieran causar o contribuir al incidente;

12.1.6 Aprendizaje de los incidentes de seguridad de la información

Control

Utilizar el conocimiento obtenido para analizar y resolver incidentes de seguridad de la información, para reducir la probabilidad y/o impacto de incidentes en el futuro, aplicando los controles adecuados.

Recomendaciones para la implementación:

12.1.6.1 La información que se obtiene de la evaluación de los incidentes de seguridad de la información se debe utilizar para identificar los incidentes recurrentes o de alto impacto.
12.1.6.2 Determinar el número de incidentes por tipo, el número de incidentes graves, el tiempo medio de resolución de incidentes.
12.1.6.3 Determinar el costo promedio por incidente.
12.1.6.4 Determinar el número de incidentes recurrentes.
12.1.6.5 Determinar la frecuencia de un incidente recurrente.

12.1.7 Recopilación de evidencias

Control

Definir procedimientos para identificar, recolectar, adquirir y conservar la información, que pueden servir de evidencia, conservando la misma de acuerdo a la norma legal vigente.

Recomendaciones para la implementación:

12.1.7.1 Desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la institución.
12.1.7.2 Asegurar que los sistemas de información cumplan con las normas legales para la producción de evidencia, para lograr la admisibilidad, calidad y cabalidad de la misma.
12.1.7.3 Aplicar procedimientos adecuados para mantener la cadena de custodia, de acuerdo a lo que dispone la norma legal vigente.
12.1.7.4 Aplicar procedimientos adecuados para la protección de las personas;
12.1.7.5 Cambiar funciones o responsabilidades del personal implicado mientras se aclara el incidente;
12.1.7.6 Definir la competencia del personal en estas tareas y las ejecutadas en los sistemas de gestión de información.
12.1.7.7 Para lograr el peso de la evidencia, se debe demostrar la calidad y cabalidad de los controles empleados para proteger correcta y consistentemente la evidencia (es decir, evidencia del control del proceso) en todo el periodo en el cual la evidencia por recuperar se almacenó y procesó, mediante un rastreo sólido de la evidencia. En general, dicho rastreo sólido se puede establecer en las siguientes condiciones:

12.1.7.7.1 Se deberán tomar duplicados o copias de todos los medios removibles, la información en los discos duros o la memoria para garantizar la disponibilidad; es conveniente conservar el registro de todas las acciones durante el proceso de copiado y dicho proceso debería tener testigos; y, el medio y el registro originales se deberán conservar intactos y de forma segura;
12.1.7.7.2 Se debe proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debe estar supervisado por personal de confianza y se debe registrar la información sobre

cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron.

13 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

13.1 Continuidad de seguridad de la información

13.1.1 Planificación de la continuidad de seguridad de la información

Control

La institución debe determinar sus necesidades de seguridad de la información y la continuidad de su gestión de seguridad de la información, en situaciones adversas como una crisis o un desastre.

Recomendaciones para la implementación:

13.1.1.1 El responsable del área de Tecnologías de la Información o su similar será designado como coordinador de continuidad de los servicios informáticos, que se encargará de supervisar el proceso de elaboración e implantación del plan de continuidad de seguridad de la información, así como la Dirección Administrativa o su similar, de la seguridad del plan personal.

13.1.1.2 Identificar los activos involucrados en los procesos críticos de los servicios informáticos, así como de las actividades que se deben realizar.

13.1.1.3 Elaborar la política de continuidad de los servicios informáticos determinando los objetivos y el alcance del plan, así como las funciones y responsabilidades; un documento que establezca a alto nivel los objetivos, el alcance y las responsabilidades en la gestión de la continuidad. Por ejemplo, la plantilla del documento debería contener:

- INTRODUCCION: Detallando de forma resumida de que se trata, la estructura del documento y que se persigue.
- OBJETIVOS: que se satisfacen con la aplicación de la política, como se garantizará continuidad de las actividades y de los servicios, planes adicionales de contingencia.
- ALCANCE: Procesos y operaciones que son cubiertos y recursos que utilizan los procesos u Operaciones
- RESPONSABILIDADES: Diferentes responsables implicados en la gestión de la continuidad de los servicios informáticos

13.1.2 Implementación de la continuidad de seguridad de la información

Control

La institución debe establecer, documentar, implementar y mantener procesos, procedimientos, controles que aseguren el nivel necesario para la continuidad de seguridad de la información, durante una situación adversa.

Recomendaciones para la implementación:

13.1.2.1 El plan de continuidad de seguridad de la información debe detallar claramente la estructura de gestión adecuada y preparada para mitigar y responder a un evento disruptivo, usando el personal con la autoridad, experiencia y competencia necesarias.

13.1.2.2 Designar personal de respuesta al incidente y este cuenta con la responsabilidad, autoridad y competencia necesarias para gestionar el incidente y mantener la seguridad de la información;

13.1.2.3 La institución debe tener planes desarrollados, aprobados y procedimientos de respuesta y recuperación, que detallen como la institución tratara una interrupción brusca y mantendrá la seguridad de la información, basados en los objetivos de continuidad del de la seguridad de la información aprobados por la máxima autoridad.

De acuerdo con los requisitos de continuidad de seguridad de la información, la institución debería establecer, documentar, implementar y mantener:

13.1.2.4 Controles de seguridad de la información en los procesos, procedimientos y sistemas y herramientas de soporte de continuidad de la seguridad de la información o de recuperación de desastres;

13.1.2.5 Procesos, procedimientos de cambios para mantener los controles existentes de seguridad de la información durante una situación hostil.

13.1.2.6 Controles para mantener un nivel aceptable de seguridad de la información, para aquellos controles compensatorios que no pueden mantenerse durante una situación hostil.

13.1.3 Verificar, revisar y evaluar la continuidad de seguridad de la información

Control

La institución debe verificar permanentemente los controles de continuidad de la seguridad de la información establecidos e implementados para garantizar su efectividad ante eventos adversos.

Recomendaciones para la implementación:

13.1.3.1 Evaluar la capacidad de respuesta ante desastres verificando los tiempos de respuesta, validez de los procedimientos y capacidad de los responsables. Los resultados obtenidos permitirán actualizar y mantener los planes establecidos.

13.1.3.2 Ejecutar autoevaluaciones del plan de continuidad, estrategias y procesos generados.

13.1.3.3 Ejecutar y probar la funcionalidad de los procesos, procedimientos y controles para la continuidad de la seguridad de la información asegurando la consistencia con los objetivos planteados.

13.1.3.4 Realizar auditorías tanto internas como externas, identificando el tipo y alcance de la auditoría a realizar, se entregará un plan de medidas correctivas para llevar a cabo las recomendaciones acordadas.

13.1.3.5 Realizar pruebas de:

- Validez: revisar y discutir el plan;
- Simulación: escenario que permitirá verificar el plan de continuidad;
- Actividades críticas: pruebas en un entorno controlado sin poner en peligro la operación de los servicios informáticos;
- Completa: interrupción real y aplicación del plan de continuidad.

13.2 Redundancias

13.2.1 Disponibilidad de las instalaciones de procesamiento de la información

Control

La institución debe implementar la redundancia necesaria en las instalaciones de procesamiento de información, de acuerdo a los requisitos de disponibilidad de los sistemas.

Recomendaciones para la implementación:

13.2.1.1 La institución debe identificar los requisitos de disponibilidad para los sistemas de información.

13.2.1.2 Cuando la disponibilidad no pueda garantizarse usando la arquitectura de sistemas existentes, deberían considerarse componentes o arquitecturas redundantes

13.2.1.3 Cuando sea aplicable, los sistemas de información redundantes deberían probarse para asegurar que la conmutación de un componente a otro funciona como se espera.

14 CUMPLIMIENTO

14.1. Cumplimiento de los requisitos legales y contractuales

14.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

Control

Identificar de forma explícita los requisitos necesarios, legales, reglamentarios, contractuales y la visión de la institución para cumplir con estos requisitos, debe definirse claramente documentarse y mantenerse actualizados para cada sistema de información de la institución.

Recomendaciones para la implementación:

14.1.1.1 Inventariar todas las normas legales, estatutarias, reglamentarias y contractuales pertinentes para cada programa de software, servicio informático y en general todo activo de información que utiliza la institución.

14.1.1.2 Organizar para cada activo de información las normas legales, estatutarias, reglamentarias y contractuales pertinentes.

14.1.1.3 Considerar las normas y leyes más generales relacionadas a la gestión de los datos e información electrónica en el gobierno. A saber:

- Constitución de la República del Ecuador
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
- Ley Orgánica de Transparencia y Acceso a la Información Pública
- Ley del Sistema Nacional de Registro de Datos Públicos
- Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva

- Ley Orgánica y Normas de Control de la Contraloría General del Estado
- Leyes y normas de control del sistema financiero
- Leyes y normas de control de empresas públicas
- Ley del Sistema Nacional de Archivos
- Código orgánico de la economía social de los conocimientos, creatividad e innovación
- Otras normas cuya materia trate sobre la gestión de los activos de información en las instituciones de la Administración Pública

14.1.2 Derechos de propiedad intelectual

Control

Implementar procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, normativos y contractuales relacionados con los derechos de propiedad intelectual y sobre el uso de productos de software original.

Recomendaciones para la implementación:

14.1.2.1 Elaborar implementar y socializar una política para el cumplimiento de los derechos de propiedad intelectual, definiendo el uso legal de aplicativos y del software institucional.

14.1.2.2 Adquirir software únicamente a proveedores reconocidos para garantizar que no se violen derechos de propiedad intelectual. Si el Software es Libre Opensource se considerará los términos de las licencias públicas generales.

14.1.2.3 Implementar mecanismos para concienciar sobre las políticas para proteger derechos de propiedad intelectual y las acciones disciplinarias para el personal que las viole. Se aplica tanto al software libre como al privativo.

14.1.2.4 Mantener registros apropiados de los activos de información para proteger los derechos de propiedad intelectual. Se aplica tanto al software libre como al privativo.

14.1.2.5 Custodiar evidencia de la propiedad de licencias o suscripciones, contratos, discos maestros, manuales y toda la información relevante del software que se utiliza.

14.1.2.6 Controlar y asegurar que no se exceda el número máximo de usuarios permitidos para un programa de software. Se aplica tanto al software libre como al privativo, donde corresponda.

14.1.2.7 Verificar que se instale únicamente software autorizado y con las respectivas licencias en el caso de utilizar software privativo.

14.1.2.8 Cumplir los términos y condiciones de uso para el software y la información, obtenidos de la Internet o proveedores (programas freeware, shareware, demostraciones o programas para pruebas)

14.1.2.9 Disponer de una política para ceder o transferir el software de propiedad institucional a un tercero.

14.1.2.10 Controlar que no se copie total ni parcialmente software privativo, códigos fuente y la documentación de programas de software con derechos de propiedad intelectual. Se exceptúa los programas de software libre bajo los términos de sus licencias públicas

14.1.2.11 Controlar que no se duplique, convierta en otro formato, ni extraiga contenidos de grabaciones de audio y video, si no está expresamente permitido por su autor o la persona que tenga los derechos sobre el material

14.1.2.12 Definir y aplicar una licencia pública general al software desarrollado por la institución o contratado a terceros como desarrollo, para proteger la propiedad intelectual

14.1.2.13 Disponer a los funcionarios que utilicen solo software desarrollado, provisto o aprobado por la institución.

14.1.3 Protección de los registros

Control

Implementar el procedimiento adecuado para, proteger los registros contra pérdida, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con la norma legal vigente.

Recomendaciones para la implementación:

Para cumplir los objetivos de salvaguardar los registros, la institución debería seguir los siguientes pasos:

14.1.3.1 Clasificar los registros electrónicos y físicos por tipos, especificando los periodos de retención y los medios de almacenamiento, como discos, cintas, entre otros.

14.1.3.2 Mantener la documentación y especificaciones técnicas de los algoritmos y programas utilizados para el cifrado y descifrado de archivos y toda la información relevante relacionada con claves, archivos criptográficos o firmas electrónicas, para permitir el descifrado de los registros durante el periodo de tiempo para el cual se retienen.

14.1.3.3 Establecer un procedimiento para revisar el nivel de deterioro de los medios utilizados para almacenar los registros. Los procedimientos de almacenamiento y manipulación se deberán implementar según las recomendaciones del fabricante. Para almacenamiento a largo plazo, se recomienda considerar el uso de cintas y discos digitales utilizando formatos de archivos y datos abiertos.

14.1.3.4 Establecer un procedimiento para garantizar el acceso a los datos e información registrada, tanto el medio como el formato, durante todo el periodo de retención.

14.1.3.5 Establecer un procedimiento para cambiar o actualizar la tecnología del medio en el cual se almacenan los activos de información y registros de acuerdo a las innovaciones tecnológicas disponibles en el mercado.

14.1.3.6 Los sistemas de almacenamiento de datos se deberán seleccionar de manera que los datos requeridos se puedan recuperar en el periodo de

tiempo y en formatos legibles, dependiendo de los requisitos que se deben cumplir.

14.1.3.7 Garantizar la identificación de los registros y el periodo de retención de los mismos tal como se defina en normas legales ecuatorianas. Este sistema debe permitir la destrucción adecuada de los registros después de este periodo, si la institución no los necesita y las normas así lo especifican.

14.1.3.8 Establecer y difundir en la institución las directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información.

14.1.3.9 Inventariar las fuentes de información clave.

14.1.3.10 Implementar controles apropiados para proteger los registros contra pérdida, destrucción y falsificación de la información. Utilizar como referencia para la gestión de los registros de la institución la norma ISO 15489-1 o su homóloga ecuatoriana.

14.1.4 Protección y privacidad de la información de carácter personal

Control

La institución debe desarrollar, implementar y socializar la política de protección y privacidad de la información, según dispone la norma legal vigente.

Recomendaciones para la implementación:

14.1.4.1 El Oficial de Seguridad de la Información deberá controlar la aplicación de la política de protección de datos y privacidad de la información personal.

14.1.4.2 Implementar medidas técnicas y organizacionales apropiadas para gestionar de manera responsable la información personal de acuerdo con la legislación correspondiente.

14.1.4.3 Implementar mecanismos de carácter organizacional y tecnológico para autorización al acceso, uso e intercambio de datos personales de las personas o ciudadanos en custodia de las instituciones públicas. Prima el principio que los datos personales pertenecen a las personas y no a las instituciones, éstas los custodian al amparo de la normativa legal vigente.

14.1.5 Reglamentos de controles criptográficos

Control

La institución debe utilizar los controles de cifrado en cumplimiento con todos los acuerdos, leyes reglamentos de la legislación vigente.

Recomendaciones para la implementación:

14.1.5.1 Restringir importaciones y/o exportaciones de hardware y software de computadores para la ejecución de funciones criptográficas; o diseñados para adicionarles funciones criptográficas.

14.1.5.2 Restringir el uso de encriptación, y especificar y documentar los ámbitos en dónde se aplicarán tales procesos (ej., comunicaciones, firma de documentos, trasmisión de datos, entre otros).

14.1.5.3 Restringir métodos obligatorios o discrecionales de acceso por parte

de las autoridades del país a la información encriptada mediante hardware o software para brindar confidencialidad al contenido.

14.1.5.4 Garantizar el cumplimiento con las leyes y los reglamentos nacionales antes de desplazar información encriptada o controles criptográficos a otros países.

14.2 Revisiones de seguridad de la información

14.2.1 Revisión independiente de seguridad de la información

Control

La gestión de seguridad de la información debe ser revisada al menos 1 vez al año, o cuando se produzcan cambios significativos en la institución.

14.2.2 Cumplimiento de las políticas y normas de seguridad

Control

El Nivel Jerárquico Superior, debe revisar periódicamente de acuerdo a la criticidad de sus activos, el cumplimiento del procesamiento de la información y procedimientos en el área de su responsabilidad, que cumplan con las normas de seguridad de la información.

Recomendaciones para la implementación:

14.2.2.1 Revisar en intervalos regulares reportes e informes de seguridad de los sistemas de información.

14.2.2.2 Evaluar acciones necesarias para el cumplimiento de las políticas y normas de seguridad.

14.2.2.3 Auditar las plataformas técnicas y los sistemas de información para determinar el cumplimiento de las normas aplicables sobre implementación de la seguridad y sus controles.

14.2.2.4 Revisar con regularidad en su área de responsabilidad, el cumplimiento del procesamiento de información de acuerdo con la política de la seguridad, las normas y cualquier otro requisito de seguridad. Si se determina algún incumplimiento o no conformidad como resultado de la revisión, la dirección deberá:

- Determinar la causa del incumplimiento
- Evaluar la necesidad de acciones para garantizar que no se repitan estos incumplimientos
- Determinar e implementar la acción correctiva apropiada
- Revisar la acción correctiva que se ejecutó

14.2.2.5 Implementar acciones correctivas de ser necesario.

14.2.2.6 Revisar las acciones correctivas tomadas para verificar su efectividad e identificar cualquier deficiencia o debilidad.

14.2.2.7 Registrar y conservar los resultados de las revisiones y las acciones correctivas llevadas a cabo por la dirección. Los directores deberán informar de los resultados a las personas que realizan revisiones independientes, cuando la revisión independiente tiene lugar en el área de su responsabilidad.

14.2.3 Comprobación del cumplimiento técnico

Control

Implementar el procedimiento adecuado, para comprobar regularmente que los sistemas de información cumplen con las políticas y normas de seguridad de la información de la institución.

Recomendaciones para la implementación:

14.2.3.1 Verificar el cumplimiento técnico bien sea manualmente (con soporte de las herramientas de software apropiadas, si es necesario) por un ingeniero de sistemas con experiencia, y/o con la ayuda de herramientas automáticas que generen un informe técnico para la interpretación posterior por parte del especialista técnico.

14.2.3.2 Planificar evaluaciones de vulnerabilidad o pruebas de penetración considerando siempre el riesgo de que dichas actividades pueden poner en peligro la seguridad del sistema. Tales pruebas se deberán planificar, documentar y ser repetibles.

14.2.3.3 Controlar que la verificación del cumplimiento técnico sea realizado por personas autorizadas y competentes o bajo la supervisión de dichas personas.

14.2.3.4 Analizar los sistemas operativos para asegurar que los controles de hardware y software se han implementado correctamente. Este tipo de verificación del cumplimiento requiere experiencia técnica especializada.

14.2.3.5 Ejecutar o contratar pruebas de penetración y evaluaciones de la vulnerabilidad, las cuales pueden ser realizadas por expertos independientes especialmente contratados para este propósito. Ello puede ser útil para detectar vulnerabilidades en el sistema y verificar qué tan efectivos son los controles evitando el acceso no autorizado debido a estas vulnerabilidades. Las pruebas de penetración y las evaluaciones de vulnerabilidad no deben substituir las evaluaciones de riesgos.

GLOSARIO DE TÉRMINOS

Lista de términos relacionados en el contexto del Esquema Gubernamental de la Seguridad de la Información:

A.

Activo de información. - En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la institución.

Amenaza. - causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización.

Análisis de riesgos. - proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Aplicación. – solución de TI, incluyendo programas de aplicación, datos de aplicaciones y procedimientos diseñados para ayudar a los usuarios de las organizaciones a realizar tareas específicas o manejar tipos específicos de problemas de TI, automatizando un proceso o función del negocio

Ataque. - intento de destruir, exponer, alterar, deshabilitar, robar o lograr acceso no autorizado o hacer uso no autorizado de un activo.

Autenticación. - Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autenticidad. - Propiedad de que una entidad es lo que afirma ser.

C.

Comité de Seguridad de la información (CSI). – se encarga de gestionar la implementación y mejora continua del Esquema Gubernamental de Seguridad de la Información.

Confidencialidad. - Propiedad de que la información no esté disponible o no sea divulgada a personas, entidades o procesos no autorizados.

Contenidos maliciosos. - aplicaciones, documentos, archivos, datos u otros recursos que tienen características o capacidades maliciosas incrustadas, disfrazadas o escondidas en ellos.

Control. - Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Control contramedida. - los medios de gestión de riesgos, que incluyen las políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden ser de carácter administrativo, técnico, de gestión o de carácter legal.

D.

Directiva o directriz. - Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad. - Propiedad de estar disponible y utilizable en el momento que sea

requerido por una entidad autorizada.

E.

EGSI. - Esquema Gubernamental de Seguridad de la Información para las instituciones de la APCID para preservar la integridad, disponibilidad y confidencialidad de la información.

Evaluación de riesgos. - Proceso global de identificación, análisis y estimación de riesgos.

G.

Gestión de claves. - Controles referidos a la gestión de claves criptográficas.

Gestión de incidentes de seguridad de la información. - Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos. - Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

I.

Identificación de riesgos. - Proceso de encontrar, reconocer y describir riesgos.

Impacto. - El costo para la institución de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros (ejem.: pérdida de reputación, implicaciones legales, entre otros).

Incidente de seguridad de la información. - Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Es uno de los activos más importantes de las instituciones, en las formas que esta se manifieste: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, magnético, papel, electrónico, computadoras, audiovisual y otros.

Institución. - Grupo de personas e instalaciones con una disposición de responsabilidades, autoridades y relaciones.

Integridad. - Propiedad de proteger la precisión y completitud de los activos.

Internet (red interconectada), interconexión de redes. - una colección de redes interconectadas.

"La internet. - sistema global de redes interconectadas de dominio público"

Inventario de activos. - Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

N.

No repudio. - Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

M.

Malware, software malicioso. - Software diseñado con malas intenciones que contiene características o capacidades que potencialmente pueden causar daño directamente o indirectamente al usuario y/o al sistema informático del usuario.

O.

Objetivo. - Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

Oficial de Seguridad de la Información (OSI). - Es el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento del Esquema

P.

Parte interesada. - <gestión de riesgos> persona u organización que puede afectar, verse afectada por, o percibirse a sí misma como afectada por una decisión o actividad.

Phishing (engaño técnico). - proceso fraudulento o intento de adquirir información privada o confidencial de manera enmascarada haciéndose pasar por una entidad confiable en una comunicación electrónica.

Plan de continuidad del negocio. - Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos. - Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de escritorio despejado. - La política de la empresa que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.

Proceso. - Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Propietario del activo. - puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la institución.

Propietario de la Información. - es el responsable de clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

Propietario del riesgo. - persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Proveedor de servicios de Internet. - organización que presta servicios de Internet a un usuario y permite a sus clientes acceder a Internet.

R.

Resiliencia. - Capacidad de los activos institucionales, para regresar a su forma original.

Riesgo. - Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual. - El riesgo que permanece tras el tratamiento del riesgo.

S.

Seguridad de la información. - conjunto de medidas preventivas y reactivas de las instituciones y de los sistemas tecnológicos que permiten la preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de información. - Aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento

Software engañoso (spyware). - que recopila información privada o confidencial de un usuario de computador.

Software potencialmente no deseado. - software engañoso, incluyendo el malware y no malicioso, que exhibe las características de software engañoso.

Spam (correo basura). - abuso de los sistemas de mensajería electrónica para enviar indiscriminadamente mensajes masivos no solicitados.

T.

Tratamiento de riesgos. - Proceso de modificar el riesgo, mediante la implementación de controles.

Trazabilidad. - Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Troyano, caballo de Troya. - software malintencionado que aparece para realizar una función deseable.

V.

Vulnerabilidad. - Debilidad de un activo o control que puede ser explotada por una o más amenazas.