Estado Plurinacional de Bolivia

SEG – 001

Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público

ctic CONSEJO PARA LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público

Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público

SEG – 001

Este documento ha sido elaborado por los miembros del Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB) y el Centro de Gestión de Incidentes Informáticos (CGII).

Coordinación Secretaria Técnica del CTIC-EPB: Cristina Loma y Carolina Ovale

Grupo de Trabajo de Seguridad: Adhemar Paz Mancilla, Aldo Tórrez García, Alejandro Monasterio, Boris Cusicanqui, Carlos Ramírez García, César Chávez Martínez, Crispín Quizo Melendrez, Daniel Rojas, Daniel Torrico Álvarez, Daniela Lenz Ardaya, Diego Brayan Alcon Tarqui, Edwin Salcedo Aliaga, Esteban Lima, Fabián Espinoza Valencia, Fernando Choque Alarcon, Fidel Rolando Morales Quisbert, Franco Camargo, Franklin Tórrez Álvarez, Franz Rojas Castillo, Gabriela Murguía Tórrez, Gladys Alanoca, Gonzalo Vargas Ramos, Harold Franz Chávez Bellido, Henrry Cenzano Loza, Henry Lin Zambrana, Herlan Cameo Ugarte, Hernan Enríquez, Hilder Vladimir Flores Leon, Horacio Lopez Justiniano, Hugo Gutiérrez Espada, Humberto Martín Bellido, Jarmila Lejsek Halas, Javier Wilson Condori Machicado, Jhoseeline Camacho López, Jorge Fabricio Bailey Torres, Jose Antonio Jiménez Mancilla, José Dante Córtez Guachalla, José Luis Suárez Mollinedo, Juan Carlos Canaza, Juan Carlos Choque, Juan Carlos Mendoza Calderón, Juan Carlos Patón Mamani, Juan Yañez Bernal, Juan Pablo Conde Mendoza, Karina Medinaceli, Khantuta Muruchi, Krissia Ferreira, Leonardo Pacheco, Lorena Quinteros Pinto, Luis Ariel Huancario Tupa, Luis Calle Blanco, Luis Catacora Vásquez, Luis Fernando Zegarra Castro, Luis Freddy Velasco Poma, Luz Maribel Garay Quisbert, Marcelo Romero, Marco Mercado Bustillos, Miguel Fernando Chambi Cari, Miguel Medina Berdeja, Erick Palenque Ríos, Nataniel Saavedra, Patricia López Avendaño, Patricia Mónica Urquiola Torres, Ramiro Lazarte, Ramiro Oña, Roberto Escalante Mendoza, Ronald Moscoso Pinto, Rosmery Ana Zegarra, Rosse Mary Gonzales, Stael Candy Álvarez Guzmán, Stephanie Ferreira, Valeria Méndez Salinas, Verónica Donaire, Víctor Aramayo, Víctor Hugo Vega Gareca, Vladimir Terán, Wilma Choque Salas, Alberto Guillermo Arnez Flores.

Edición, diseño y diagramación: Natalia Antezana, Mariela Padilla y Orestes Sotomayor

Depósito Legal: 4-1-273-17 P.O.

La Paz, Bolivia

2017


ctic
CONSEJO PARA LAS
TECNOLOGÍAS DE INFORMACIÓN
Y COMUNICACIÓN

Contenido

1 Antecedentes

El Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB) se constituye en una instancia de coordinación técnica para la implementación de Gobierno Electrónico y para el uso y desarrollo de Tecnologías de Información y Comunicación en el país.

Entre las principales tareas asignadas al CTIC-EPB se encuentran:

- Formular propuestas de políticas y normativa relacionada con Gobierno Electrónico, a ser presentadas a la AGETIC;
- Presentar proyectos y programas de Gobierno Electrónico y Tecnologías de Información y Comunicación en el ámbito gubernamental a la AGETIC para su gestión;
- Generar mecanismos de participación para instituciones y organizaciones de la sociedad civil en la proposición y formulación de políticas y acciones relacionadas con Gobierno Electrónico y Tecnologías de Información y Comunicación en el ámbito gubernamental;
- Establecer espacios de coordinación entre las entidades del sector público para el desarrollo conjunto de programas, proyectos o acciones de Gobierno Electrónico y Tecnologías de Información y Comunicación en el ámbito gubernamental;
- Desarrollar y proponer estándares abiertos oficiales del Estado Plurinacional de Bolivia en materia de Gobierno Electrónico y Tecnologías de Información y Comunicación aplicables a las entidades del sector público;
- Establecer espacios de coordinación de comunidades de desarrollo informático, dentro del Estado, con la ciudadanía y a nivel internacional.

El 5 de mayo de 2016 se llevó a cabo la inauguración y la primera Reunión del Pleno del CTIC-EPB, en la que se conformaron seis grupos temáticos de trabajo: Interoperabilidad, Software Libre, Seguridad, Infraestructura, Desarrollo de Software y Datos Abiertos.

Cada Grupo de Trabajo estuvo integrado por servidores públicos de las entidades del nivel central del Estado: Órgano Ejecutivo, Legislativo, Judicial y Electoral, incluyen-

do sus instituciones descentralizadas, autárquicas, empresas públicas y autoridades de regulación sectorial; Ministerio Público y Procuraduría General del Estado.

Adicionalmente, se invitó a participar, en calidad de miembros adjuntos, a representantes de entidades territoriales autónomas, universidades públicas e indígenas y sociedad civil, a fin de trabajar y elaborar propuestas a ser presentadas al Consejo para su posible implementación a nivel estatal.

Cabe mencionar que el desarrollo de los Grupos de Trabajo y del Consejo se enmarca en el Reglamento de Funcionamiento del CTIC-EPB, aprobado mediante la Resolución Administrativa N° 024/2016 de la AGETIC, de fecha 31 de mayo de 2016.

El Grupo de Trabajo de Seguridad se planteó como objetivo la formulación de los lineamientos para que las entidades o instituciones públicas del Estado Plurinacional de Bolivia, puedan elaborar e implementar sus Planes Institucionales de Seguridad de la Información.

El Grupo estuvo conformado por los representantes de las siguientes entidades:

- Administradora Boliviana de Carreteras (ABC).
- Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC).
- Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB).
- Autoridad de Fiscalización y Control Social de Electricidad (AE).
- Autoridad de Impugnación Tributaria (AIT).
- Autoridad de Supervisión del Sistema Financiero (ASFI).
- Aduana Nacional de Bolivia (ANB).
- Banco Central de Bolivia (BCB).
- Banco de Desarrollo Productivo (BDP-SAM) .
- Banco Unión S.A (BUSA).

- Programa Bono Juana Azurduy (BJA).
- Dirección Estratégica de Reivindicación Marítima (DIREMAR).
- Empresa de Apoyo a la Producción de Alimentos (EMAPA).
- Instituto Nacional de Estadística (INE).
- Empresa Estatal de Transporte por cable "Mi Teleférico".
- Escuela de Gestión Pública Plurinacional (EGPP).
- Gobierno Autónomo Departamental de Potosí.
- Ministerio de Defensa (MIN-DEF).
- Ministerio de Economía y Finanzas Públicas (MEFP).
- Ministerio de Salud (MIN-SAL).
- Empresa Pública QUIPUS.
- Registro Único para la Administración Tributaria Municipal (RUAT).
- Senado Nacional (Cámara de Senadores de la Asamblea Legislativa Plurinacional).
- Servicio de Impuestos Nacionales (SIN).
- Servicio General de Identificación Personal (SEGIP).
- Servicio Geológico Minero (SERGEOMIN).
- Servicio Nacional del Sistema de Reparto (SENASIR).
- Sistema Nacional de Información en Salud y Vigilancia Epidemiológica (SNISyVE).
- Universidad Mayor de San Andrés (UMSA).
- Yacimientos Petrolíferos Fiscales Bolivianos (YPFB).
- Sociedad Civil.

Asimismo, es importante resaltar que otras entidades u órganos del Estado participaron a través de sugerencias y acotaciones al documento inicial elaborado por el Grupo. Entre estas entidades se encuentran:

- Administración de Aeropuertos y Servicios Auxiliares a la Navegación Aérea (AASANA).
- Agencia Nacional de Hidrocarburos (ANH).
- Contraloría General del Estado (CGE).
- Dirección General de Migración (DIGEMIG).
- Escuela Militar de Ingeniería (EMI).
- Fondo de Desarrollo del Sistema Financiero y de Apoyo al Sector Productivo (FONDESIF).
- Instituto Boliviano de Metrología (IBMETRO).
- Ministerio de Obras Públicas Servicios y Vivienda (MOPSV).
- Ministerio de Gobierno (MIN-GOB).
- Observatorio Plurinacional de la Calidad Educativa (OPCE).
- Órgano Plurinacional Electoral (OPE).
- Procuraduría General del Estado (PGE).
- Servicio de Desarrollo de las Empresas Públicas Productivas (SEDEM).
- Servicio Nacional de Registro y Control de la Comercialización de Minerales y Metales (SENARECOM).
- Servicio Nacional de Sanidad Agropecuaria e Inocuidad Alimentaria (SENASAG).
- Tribunal Agroambiental.
- Unidad de Análisis de Políticas Sociales y Económicas (UDAPE).

En el caso de la AGETIC, los participantes de la mesa son miembros del Centro de Gestión de Incidentes Informáticos (CGII), que tiene, entre una de sus funciones (véase el Decreto Supremo N° 2514 de 9 de septiembre de 2015) el establecimiento de los lineamientos para la elaboración de Planes de Seguridad de Información de las entidades del sector público. Sin embargo, con el fin de hacer de ese proceso un ejercicio más abierto y participativo, su trabajo se enmarcó dentro de la dinámica del Grupo de Seguridad, del que formaron parte todas las entidades a las que se hizo mención, además de miembros de la sociedad civil, dando como resultado el presente documento de "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público", que recoge las deliberaciones, análisis y sugerencias del Grupo de Seguridad del CTIC-EPB.

2 Marco normativo referencial

La elaboración del presente documento se enmarca en el mandato institucional respaldado por:

- El inciso t) del Artículo 22 del Decreto Supremo No 29894, de 7 de febrero de 2009, de Organización del Órgano Ejecutivo, que establece que: "El Ministerio de la Presidencia es el ente rector de Gobierno Electrónico y de Tecnologías de Información y Comunicación para el sector público del Estado Plurinacional de Bolivia, siendo el encargado de establecer las políticas, lineamientos y normativa específica para su implementación, seguimiento y control".

- El Artículo 2 del Decreto Supremo N° 2514, sobre la creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación - AGETIC, como "una institución pública descentralizada de derecho público, con personalidad jurídica, autonomía de gestión administrativa, financiera, legal y técnica y patrimonio propio, bajo tuición del Ministerio de la Presidencia".

- Lo señalado en los artículos 9, 10 y 11 del Decreto Supremo N° 2514 acerca de la creación del Consejo para las Tecnologías de Información y Comunicación para formular y presentar propuestas de políticas, normativa, programas y proyectos de Gobierno Electrónico y Tecnologías de Información y Comunicación por parte de las entidades del ámbito gubernamental.

El marco normativo concerniente a la seguridad de la información incluye:

- El Parágrafo I del Artículo 72 de la Ley N° 164 de 28 de julio de 2011, Ley General de Telecomunicaciones, que establece que: "El Estado en todos sus niveles, fomentará el acceso, uso y apropiación social de las tecnologías de información y comunicación, el despliegue y uso de infraestructura, el desarrollo de contenidos y aplicaciones, la protección de las usuarias y usuarios, la seguridad informática y de redes, como mecanismos de democratización de oportunidades para todos los sectores de la sociedad y especialmente para aquellos con menores ingresos y con necesidades especiales".

- El inciso d) del Artículo 4 (Principios), parágrafo II, del Decreto Supremo N° 1793 de 13 de noviembre de 2013, que señala que: "Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento".

- El Artículo 8 (Plan de contingencia) del Decreto Supremo N° 1793, de 13 de noviembre de 2013, que menciona que: "Las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad".

- El Decreto Supremo N° 2514 de 9 de septiembre de 2015, en los siguientes artículos, incisos o disposiciones transitorias:

    ◊ Inciso f) del Artículo 7, que sostiene que la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) establecerá "los lineamientos técnicos en seguridad de información para las entidades del sector público".

    ◊ Inciso i) del Artículo 7, que establece entre las funciones de la AGETIC, "Elaborar, proponer, promover, gestionar, articular y actualizar el Plan de Implementación de Gobierno Electrónico y el Plan de Implementación de Software Libre y Estándares Abiertos para las entidades del sector público; y otros planes relacionados con el ámbito de gobierno electrónico y seguridad informática".

    ◊ Parágrafo I del Artículo 8, de creación del "Centro de Gestión de Incidentes Informáticos – CGII como parte de la estructura técnico operativa de la AGETIC".

    ◊ Inciso c) del Parágrafo II del Artículo 8, que menciona como una de las funciones del Centro de Gestión de Incidentes Informáticos – CGII, "Establecer los lineamientos para la elaboración de Planes de Seguridad de Información de las entidades del sector público".

- ◊ Parágrafo III del Artículo 17, que establece que "Las entidades del sector público deberán desarrollar el Plan Institucional de Seguridad de la Información acorde a los lineamientos establecidos por el CGII".

- ◊ Parágrafo II del Artículo 18, que señala que "Las entidades del sector público, en el marco de la Soberanía Tecnológica, deben designar un Responsable de Gobierno Electrónico y Tecnologías de Información y Comunicación y un Responsable de Seguridad Informática, encargados de coordinar con la AGETIC".

- ◊ Disposición transitoria segunda, que sostiene que "Las entidades del nivel central del Estado deberán presentar a la AGETIC, en un plazo no mayor a un (1) año, desde la aprobación de las políticas de seguridad de la información por la AGETIC[1], su Plan Institucional de Seguridad de la Información".

- El Decreto Supremo N° 3251 del 12 de Julio de 2017 de aprobación del Plan de Implementación de Gobierno Electrónico, que establece como una de las líneas estratégicas la seguridad informática y de la información.

■

[1] Dado que las políticas de seguridad de la información están incorporadas dentro del Plan Institucional de Seguridad de la Información, el presente documento equivale a la aprobación de los lineamientos para las políticas de seguridad de información por parte de la AGETIC.

3 Objetivo

El presente documento tiene como objetivo establecer los lineamientos para que las entidades del sector público del Estado Plurinacional de Bolivia puedan elaborar e implementar sus Planes Institucionales de Seguridad de la Información, en concordancia con la normativa vigente.

4 Alcance y ámbito de aplicación

En este documento se formulan los lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información y las directrices técnicas para la aplicación de controles de seguridad de la información en las entidades del sector público.

La presentación del Plan Institucional de Seguridad de la Información es de cumplimiento obligatorio para las entidades públicas del nivel central de acuerdo a normativa vigente.

Además, los lineamientos contenidos en este documento deberán ser asumidos por todas las entidades del sector público, sin perjuicio del trabajo desarrollado por aquellas que hayan asumido como parámetros rectores, normas y estándares nacionales e internacionales vigentes, o de otra naturaleza, en materia de seguridad de la información, siempre y cuando no sean contrapuestas a los lineamientos establecidos en el presente documento.

Las entidades o instituciones públicas que ya tengan implementado un Sistema de Gestión de Seguridad de la Información bajo normas nacionales o internacionales, podrán realizar un mapeo o cuadro de equivalencia para la verificación de concordancia con los presentes lineamientos.

5 Términos y definiciones

Activo. En general, activo es todo aquello que tiene valor para la entidad o institución pública.

Activo de información. Conocimientos o datos que tienen valor para la organización.[2]

Acuerdo de confidencialidad. Documento en el cual el servidor público y/o terceros se comprometen a respetar la confidencialidad de la información y a usarla solo para el fin que se estipule.

Apetito del riesgo. Nivel máximo de riesgo que una entidad o institución está dispuesta a aceptar o soportar.

Comité de Seguridad de la Información (CSI). Equipo de trabajo conformado para gestionar, promover e impulsar iniciativas en seguridad de la información.

Confidencialidad. Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.[3]

Custodio del activo de información. Servidor público encargado de administrar y hacer efectivo los controles de seguridad definidos por el responsable del activo de información.

Disponibilidad. Propiedad de acceso y uso de información a entidades autorizadas cuando estas lo requieran.

Integridad. Propiedad que salvaguarda la exactitud y completitud de la información.

Política de Seguridad de la Información (PSI). Acciones o directrices que establecen la postura institucional en relación a la seguridad de la información, incluidas dentro del Plan Institucional de Seguridad de la Información.

Plan Institucional de Seguridad de la Información (PISI). Documento que establece las actividades relativas a la organización y gestión de la seguridad de la información en la entidad o institución pública.

■

[2] Términos y Definiciones NB/ISO/IEC 27000:2010.
[3] Términos y Definiciones NB/ISO/IEC 27000:2010.

Responsable del activo de información. Servidor público de nivel jerárquico que tiene la responsabilidad y atribución de establecer los requisitos de seguridad y la clasificación de la información vinculada al activo enmarcado al proceso del cual es responsable.

Responsable de procesos. Servidor público de nivel jerárquico que tiene la responsabilidad y atribución de establecer las actividades, roles y responsabilidades de los procesos.

Responsable de Seguridad de la Información (RSI). Servidor público responsable de gestionar, planificar, desarrollar e implementar el Plan Institucional de Seguridad de la Información.

Seguridad de la información. La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.[4]

Seguridad informática. Es el conjunto de normas, procedimientos y herramientas, las que se enfocan en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.[5]

Servidor público. Persona individual, que independientemente de su jerarquía y calidad, presta servicios en relación de dependencia a una entidad, u otras personas que presten servicios en relación de dependencia, cualquiera sea la fuente de su remuneración.[6]

Usuario de la información. Persona autorizada que accede y utiliza la información en medios físicos o digitales para propósitos propios de su labor.

[4] Artículo 3 (Definiciones), Parágrafo VI, inciso b) del D.S. 1793.
[5] Artículo 3 (Definiciones), Parágrafo VI, inciso a) del D.S. 1793.
[6] Artículo 4, Ley 2027 del Estatuto del Funcionario Público.

6 Lineamientos para la elaboración del PISI

Las entidades o instituciones públicas deberán elaborar su Plan Institucional de Seguridad de la Información conforme a los lineamientos establecidos en el presente documento.

El siguiente cuadro describe el proceso de elaboración del PISI en sus dos etapas.

Cuadro 1: Proceso de Elaboración de PISI por Etapas

PROCESO DE ELABORACIÓN DEL PISI			
Etapa	Objetivo	Actividades	Responsables
Inicial	Organización Interna	Designación del Responsable de Seguridad de la Información Conformación del Comité de Seguridad de la Información	Máxima Autoridad Ejecutiva
Desarrollo	Estructura y contenido del Plan Institucional de Seguridad de la Información - PISI	Introducción, objetivos, alcances Metodología de gestión de riesgos Política de Seguridad de la Información Cronograma de implementación	Responsable de Seguridad de la Información
	Aprobación del PISI	Revisión y aprobación del PISI	Comité de Seguridad de la Información Máxima Autoridad Ejecutiva

A continuación, la descripción de las actividades involucradas en cada etapa.

6.1 Etapa inicial

La etapa inicial tiene como objetivo la organización interna en la entidad o institución pública para la elaboración de su PISI y comienza por la designación del Responsable de Seguridad de la Información y la conformación del Comité de Seguridad de la Información en la entidad o institución pública por parte de la Máxima Autoridad Ejecutiva (MAE).

En esta etapa, el Responsable de Seguridad de la Información debe identificar las siguientes fuentes principales de insumo para elaborar el PISI:

- Requisitos legales, estatutarios, normativos y contractuales que la institución y sus dependencias hayan establecido con los proveedores de servicio o terceros asociados a la entidad.
- Conjunto de principios y objetivos, Planes Estratégicos Institucionales, Planes Operativos Anuales, manuales de funciones y cualquier otra fuente documental que sirva para el manejo, procesamiento, almacenamiento, comunicación o resguardo de la información, que apoye a las operaciones de la institución.
- Evaluación de riesgos previos que la institución haya realizado: informes, reportes de incidentes y/o cualquier documento relacionado a amenazas o vulnerabilidades a las que la institución haya sido expuesta.
- Cualquier otra documentación interna o externa que la institución determine como apropiada y necesaria para la elaboración del PISI.

6.1.1 Responsabilidades de la Máxima Autoridad Ejecutiva (MAE) respecto a la seguridad de la información

La Máxima Autoridad Ejecutiva deberá:

a) Estar informada sobre el estado de seguridad de la información de la entidad o institución pública bajo su tutela.

b) Tomar conocimiento de la normativa vigente respecto a seguridad de la información (Decreto Supremo N° 2514 de 9 de septiembre de 2015 y Decreto Supremo N° 1793, de 13 de noviembre de 2013, de reglamentación a la Ley 164).

c) Designar al Responsable de Seguridad de la Información (RSI).

d) Conformar el Comité de Seguridad de la Información (CSI).

e) Asegurar que los objetivos y alcances del Plan Institucional de Seguridad de la Información sean compatibles con los objetivos del Plan Estratégico Institucional.

f) En lo posible, destinar los recursos administrativos, económicos y humanos para la elaboración e implementación del Plan Institucional de Seguridad de la Información.

g) Aprobar el Plan Institucional de Seguridad de la Información de su entidad o institución.

h) Cumplir y hacer cumplir el Plan Institucional de Seguridad de la Información de su entidad o institución.

i) Asumir otras acciones a favor de la seguridad de la información.

6.1.2 Designación y funciones del Responsable de Seguridad de la Información (RSI)

El Responsable de Seguridad de la Información (RSI) será el o la profesional, con perfil y experiencia en gestión de seguridad de la información, designado por la MAE, que tendrá como función principal la elaboración e implementación del PISI.

Independientemente del tamaño de la entidad, el RSI corresponderá a un cargo de nivel jerárquico y deberá contar con un equipo de apoyo bajo su supervisión y coordinación, que coadyuve en el proceso de elaboración e implementación del PISI.

El RSI tendrá las siguientes funciones:

a) Gestionar, elaborar e implementar el Plan Institucional de Seguridad de la Información (PISI).

b) Realizar la evaluación de riesgos de seguridad de la información en coordinación con los responsables de activos de información.

c) Proponer la Política de Seguridad de la Información (PSI), que estará incorporada dentro del PISI.

d) Gestionar el cumplimiento del PISI.

e) Elaborar manuales de procesos y/o procedimientos de seguridad específicos que se desprendan de los lineamientos del Plan Institucional de Seguridad de la Información y promover su difusión en la entidad o institución pública.

f) Sugerir prácticas de desarrollo de software seguro para generar procesos formales que tengan presentes los controles de seguridad necesarios para la entidad o institución.

g) Coordinar la inducción, capacitación y comunicación del personal, en el marco del PISI.

h) Gestionar y coordinar la atención y respuesta a incidentes de seguridad de la información en su entidad o institución.

i) Coadyuvar en la gestión de contingencias tecnológicas.

j) Proponer estrategias y acciones en mejora de la seguridad de la información.

k) Promover la realización de auditorías al Plan Institucional de Seguridad de la Información.

l) Gestionar la mejora continua de la seguridad de la información.

m) Sugerir medidas de protección ante posibles ataques informáticos que puedan poner en riesgo las operaciones normales de la Institución.

n) Realizar acciones de informática forense, en caso de ser necesario, para identificar, preservar, analizar y validar datos que puedan ser relevantes.

o) Monitorear la implementación y uso de mecanismos de seguridad, que coadyuven a la reducción de los riesgos identificados.

p) Otras funciones que resulten necesarias para preservar la seguridad de la información.

6.1.3 Conformación y funciones del Comité de Seguridad de la Información (CSI)

Mediante resolución administrativa, la Máxima Autoridad Ejecutiva designará al personal que conformará el Comité de Seguridad de la Información (CSI), de acuerdo al tamaño de la estructura organizativa de su entidad, volumen y complejidad de sus operaciones.

El CSI estará conformado por:

a) La Máxima Autoridad Ejecutiva en calidad de presidente del CSI, con la posibilidad de delegar sus funciones.

b) Personal de nivel jerárquico, de acuerdo a la estructura organizativa de la entidad o institución pública.

c) El Responsable de Seguridad de la Información (RSI).

En caso de la existencia de Comités similares, se considerará la posibilidad de que estos asuman las funciones del CSI.

El CSI establecerá su organización interna y asumirá como mínimo las siguientes funciones:

a) Revisar el Plan Institucional de Seguridad de la Información (PISI).

b) Promover la aprobación del PISI a través de la MAE.

c) Revisar los manuales de procesos y/o procedimientos de seguridad que se desprendan de la Política de Seguridad de la Información incorporada en el PISI.

d) Proponer estrategias necesarias para la implementación y/o fortalecimiento de controles de seguridad en el marco de la mejora continua.

e) Realizar el seguimiento y control de los indicadores y métricas establecidos y definir las acciones que correspondan al respecto.

f) Promover la concientización y capacitación en seguridad de la información al interior de la entidad o institución pública.

g) Proponer y promover las acciones necesarias en función a la gravedad de los incidentes de seguridad de la información, con el fin de prevenir incidentes futuros.

h) Otras funciones que resulten necesarias para la seguridad de la información.

6.2 Etapa de desarrollo del PISI

Tiene como objetivo establecer las actividades para la elaboración y aprobación del PISI.

6.2.1 Definición de los alcances del PISI

La entidad o institución pública definirá, dentro de su PISI, los alcances relacionados a proyectos, procesos y operaciones considerados prioritarios para cumplir con la misión, visión y objetivos estratégicos de la entidad.[7]

6.2.2 Adopción de una metodología de gestión de riesgos

El PISI contempla la gestión de riesgos en el ámbito de la seguridad de la información. Para esto, la entidad o institución pública deberá adoptar un estándar y/o metodología de gestión de riesgos dentro de los alcances del PISI, con el objetivo de implementar controles de seguridad o mejorar la eficacia de los controles ya existentes.

La adopción de dicha metodología deberá incorporar los siguientes aspectos:

a) Identificación, clasificación y valoración de activos de información

El RSI, de forma conjunta con los responsables de los procesos identificados dentro de los alcances del Plan Institucional de Seguridad de la Información, coordinará el proceso de identificación, clasificación y valoración de activos de información. Para esta parte, se recomienda usar la guía incluida en el Anexo B.

b) Evaluación del riesgo

El RSI, en coordinación con los responsables de los procesos identificados, realizará la identificación, análisis y valoración de los riesgos asociados a los ac-

[7] Existen controles mínimos que deberán ser considerados dentro de los alcances del Plan, que están descritos en el punto 6.2.3.2.

tivos de información previamente identificados, clasificados y valorados. Esto le permitirá a la entidad o institución pública identificar las vulnerabilidades de sus activos de información y amenazas a las cuales están expuestas. Las tareas necesarias para la evaluación de riesgos son las siguientes:

Cuadro 2: Evaluación de Riesgos

Tarea	Descripción
Identificación del riesgo	Para la identificación del riesgo se tomarán en cuenta las vulnerabilidades y amenazas que inciden en la confidencialidad, integridad y disponibilidad de la información.
Análisis y valoración del riesgo	Para el análisis y valoración del riesgo se evaluarán las posibles consecuencias de la materialización de una amenaza producto de las vulnerabilidades presentes en los activos de información. El RSI presentará los resultados de la evaluación de riesgos al CSI para analizar su priorización y tratamiento posterior. Esta priorización puede ser establecida a partir del nivel de riesgo máximo definido previamente por la entidad o institución pública a través del CSI.

c) Tratamiento del riesgo

Los resposables de los activos de información, en coordinación con el RSI, deberán tomar decisiones acerca de las medidas más apropiadas para el tratamiento del riesgo identificado.

Los controles a implementar deberán ser clasificados por el orden de prioridad establecido en la valoración de riesgos y analizados por el CSI para su aplicación. Este proceso de implementación contemplará plazos de cumplimiento, capacitación, métodos de evaluación, responsables, recursos y otros.

d) Controles implementados y por implementar

La entidad o institución pública elaborará un listado de los controles implementados y por implementar, en el que se enumerarán y, mínimamente, se tomarán en cuenta los controles del punto 6.2.3.2. (Controles mínimos de seguridad de la información) y otros que resulten necesarios fruto de la evaluación de riesgos.

Los controles que no sean implementados deberán contar con un respaldo justificado, documentado y aprobado por el Comité de Seguridad de la Información.

Para los puntos b), c) y d) se recomienda el uso de la guía del Anexo B.

6.2.3 Contenido de la Política de Seguridad de la Información (PSI)

La Política de Seguridad de la Información (PSI) deberá incluir mínimamente y de forma no limitativa principios y posturas institucionales respecto a:

a) Protección de la información institucional ante amenazas que se originan del recurso humano.

b) Uso y protección de activos de información.

c) Control de accesos a recursos de red, información, sistemas y aplicaciones.

d) Protección de información transmitida a través de redes de comunicaciones.

e) Protección de áreas e instalaciones donde se genere, procese, transmita o almacene información considerada sensible y crítica.

f) Seguridad en el ciclo de vida de los sistemas y/o software que se desarrolle y/o adquiera.

g) Continuidad de las operaciones y procesos mediante la gestión de incidentes en seguridad de la información.

h) Protección de información física documental.

i) Otras acciones fruto de la evaluación de riesgos.

La redacción de la Política de Seguridad de la Información de la entidad o institución pública deberá ser coherente con las normas y leyes del Estado Plurinacional de Bolivia, dando cumplimiento a Normas Básicas Gubernamentales que definen la

jerarquía documental, las características y formato de cada documento referente a políticas.

6.2.3.1 Estructura de la Política de Seguridad de la Información

La estructura de la Política de Seguridad de la Información deberá contener mínimamente los siguientes puntos:

- **Introducción**

  La introducción deberá describir los antecedentes del documento, el asunto o la materia que se desarrollará en relación a seguridad de la información.

- **Términos y definiciones**

  Se debe desglosar y aclarar la terminología, acrónimos y palabras propias utilizadas para el desarrollo de la Política de Seguridad de la Información.

- **Objetivo general**

  El objetivo general se debe enfocar en el resguardo de los activos de información de la institución respecto a la confidencialidad, integridad y disponibilidad de la información asociada.

- **Objetivos específicos**

  Tienen como base al objetivo general y deben establecer la orientación para su consecución. Dentro de los objetivos se pueden identificar temas relacionados a la gestión de activos de información, gestión de riesgos, gestión de incidentes, capacitación y sensibilización de los documentos que regulan la seguridad.

- **Alcance**

  El alcance define la trascendencia y el ámbito de aplicación de la PSI al interior de la entidad o institución.

  Idealmente, debe estar circunscrito a toda la institución y se recomienda que se defina en conjunto con el Comité de Seguridad de la Información.

- **Roles y responsabilidades**

  En este punto se deben establecer los roles del CSI, del RSI, de los responsables de activos de información y del conjunto de servidores públicos, sobre los cuales se definirán las responsabilidades relacionadas con la organización y gestión de la seguridad de la información.

- **Desarrollo**

  Dentro del desarrollo se debe explicar la postura institucional respecto al Plan Institucional de Seguridad de la Información, los controles mínimos de seguridad contemplados, y otros requerimientos de seguridad de la información de acuerdo a los resultados del análisis de riesgo realizado.

  El contenido deberá incorporar el título del ámbito de seguridad, una breve descripción del mismo y la postura institucional respecto a los lineamientos y reglas generales para desarrollar los controles de seguridad.

  Ejemplo.

  Ámbito de seguridad: Seguridad en recursos humanos

  Descripción: Se implementarán controles para la protección de la información institucional ante amenazas que se originan del recurso humano.

- **Difusión**

  La PSI debe contener y describir la posición institucional en cuanto a la difusión de toda la documentación generada a partir de ella, así como los medios y mecanismos de su difusión.

- **Cumplimiento**

  Este punto debe establecer de forma clara la obligatoriedad del cumplimiento de la PSI y de toda la documentación asociada que genere y regule su operatividad.

- **Sanciones**

  Se debe establecer de forma clara que el incumplimiento a la PSI y todo

lo relacionado a la misma conlleva sanciones, que no deben ser descritas puntualmente, sino simplemente hacer referencia a normativa(s) legal(es) existente(s) para ejercer sanciones.

- **Histórico de cambios**

  Se recomienda que la documentación generada a partir de la PSI cuente con el respectivo control de cambios, que identifique a los responsables de la elaboración, aprobación y modificación de la documentación con fechas específicas por cada operación.

6.2.3.2 Controles mínimos de seguridad de la información

La entidad o institución pública deberá implementar mínimamente los siguientes controles de seguridad de la información, conforme a los principios establecidos en la Política de Seguridad de la Información:

a) Seguridad en recursos humanos (Véase el punto 1 del Anexo A).

b) Gestión de activos de información (Véase el punto 2 del Anexo A).

c) Control de accesos (Véase el punto 3 del Anexo A).

d) Criptografía (Véase el punto 4 del Anexo A).

e) Seguridad física y ambiental (Véase el punto 5 del Anexo A).

f) Seguridad de las operaciones (Véase el punto 6 del Anexo A).

g) Seguridad de las comunicaciones (Véase el punto 7 del Anexo A).

h) Desarrollo, mantenimiento y adquisición de sistemas (Véase el punto 8 del Anexo A).

i) Gestión de incidentes de seguridad de la información (Véase el punto 9 del Anexo A).

j) Plan de contingencias tecnológicas (Véase el punto 10 del Anexo A).

k) Cumplimiento (Véase el punto 11 del Anexo A).

6.2.3.3 Indicadores y métricas

El RSI establecerá indicadores y métricas de cumplimiento al momento de elaborar y desarrollar un determinado control de seguridad, con la finalidad de evaluar la eficacia de dichos controles una vez que se implementen.

En general, un indicador y métrica deberá ser:

a) Específico.

b) Medible cualitativa o cuantitativamente y/o con indicadores y atributos.

c) Alcanzable.

d) Relevante.

e) Repetible en periodos de tiempo.

6.3 Cronograma de implementación

En el marco del Plan Institucional de Seguridad de la Información, la entidad o institución pública deberá elaborar un cronograma de implementación de los controles definidos. Para esto, todos los procesos y/o procedimientos que se desprendan de la Política de Seguridad de la Información deberán estar previamente elaborados para su aplicación. El cronograma de implementación deberá contemplar mínimamente:

a) Fechas.

b) Controles a implementarse.

c) Roles y responsabilidades.

d) Actividades relacionadas a capacitación, seguimiento, revisión y aplicación de controles.

La implementación del Plan Institucional de Seguridad de la Información estará sujeta al cronograma y no debería exceder el plazo de un año desde su aprobación por parte de la entidad o institución pública. De acuerdo al contexto de cada institución y sus recursos, este plazo podrá ser ampliado previa justificación escrita por

la MAE y la documentación de respaldo elaborada por el RSI indicando las causales del retraso.

La disposición transitoria segunda del Decreto Supremo 2514 de 9 de septiembre de 2015, establece que: "las entidades del nivel central del Estado deberán presentar a la AGETIC, en un plazo no mayor a un (1) año desde la aprobación de las políticas de seguridad de la información por la AGETIC, su Plan Institucional de Seguridad de la Información".

6.4 Aprobación del PISI

El PISI deberá ser revisado por el CSI que impulsará su aprobación ante la Máxima Autoridad Ejecutiva de la entidad o institución pública.

El PISI deberá ser flexible a actualizaciones periódicas en función de la mejora continua de la seguridad de la información.

7 Lineamientos para la implementación del PISI

Tiene el objetivo de establecer las actividades para la implementación del PISI. El siguiente cuadro describe el proceso antes mencionado.

Cuadro 3: Proceso de implementación de PISI

PROCESO DE IMPLEMENTACIÓN DEL PISI			
Etapa	Objetivo	Actividades	Responsables
Implementación	Implementar el PISI	Aplicación de controles Capacitación e inducción Evaluación y mejora continua Gestión de incidentes	Responsable de Seguridad de la Información Comité de Seguridad de la Información

7.1 Aplicación de controles

La entidad o institución pública deberá aplicar los controles mínimos contemplados en la etapa de elaboración de acuerdo al cronograma de implementación y aprobación establecido dentro del PISI.

7.2 Capacitación e inducción

La capacitación e inducción al personal es parte integral en la implementación del Plan Institucional de Seguridad de la Información. El Área de Recursos Humanos, en coordinación con el RSI, planificará actividades de capacitación aplicables a la totalidad de los servidores públicos (fijos, eventuales y de reciente incorporación) en relación al Plan Institucional de Seguridad de la Información y manuales de procesos y/o procedimientos de seguridad, generados a partir de la Política de Seguridad de la Información.

Para este fin, se deberán establecer mecanismos de formación continua en relación al PISI.

7.3 Gestión de incidentes de seguridad de la información

La entidad o institución pública elaborará procedimientos para la gestión de incidentes, que establecerán con claridad procesos de planificación y preparación, detección y reporte, valoración y decisión, respuesta y erradicación para la mejora continua ante la ocurrencia de incidentes relacionados a la seguridad de la información.

El RSI será la persona de contacto al interior y exterior de la entidad o institución pública para la gestión de incidentes y tendrá la responsabilidad de reportar la ocurrencia de los mismos al CGII de acuerdo a normativa vigente.

Las entidades o instituciones públicas que tengan conformados equipos de respuesta ante incidentes informáticos (CSIRT, CERT o similares) deberán reportar sus incidentes y vulnerabilidades identificadas, así como el tratamiento realizado, al Centro de Gestión de Incidentes Informáticos (CGII), de acuerdo al artículo 17 del Decreto Supremo 2514.

El Anexo C contiene una guía para la gestión de incidentes de seguridad de la información.

7.4 Revisión y mejora continua

El RSI deberá promover la realización de revisiones periódicas a los controles implementados dentro del Plan Institucional de Seguridad de la Información, en relación al cumplimiento y eficacia de procesos y/o procedimientos de la Política de Seguridad de la Información.

Los resultados de la revisión permitirán medir la efectividad y cumplimiento de los controles implementados para que, en función de los mismos, se realice la mejora continua de la seguridad de la información.

8 Auditoría al PISI

La unidad de auditoría interna de la entidad o institución deberá evaluar, controlar y dar seguimiento al Plan Institucional de Seguridad de la Información y los controles de seguridad de la información contemplados en la Política de Seguridad de la Información.

La unidad de auditoría interna será la encargada de la revisión de cumplimiento del Plan Institucional de seguridad de la información referida a documentos operativos, métricas o normas de auditoría de la Contraloría General del Estado.

El auditor podrá definir el enfoque de la auditoría interna de forma no limitativa: enfoque a las seguridades, enfoque a la información, enfoque a la infraestructura tecnológica, enfoque al software de aplicación, enfoque a las comunicaciones y redes.

Como resultado de la auditoría, podrá expresar una opinión independiente respecto a: la confidencialidad, integridad, disponibilidad y confiabilidad de la información; el uso eficaz de los recursos tecnológicos; la efectividad del PISI de control interno asociado a las tecnologías de la información y la comunicación.

9 Presentación del PISI

La entidad o institución pública presentará a la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación su Plan Institucional de Seguridad de la Información de acuerdo a normativa vigente en el Estado Plurinacional de Bolivia.

Opcionalmente, la entidad o institución pública podrá presentar los avances en la elaboración de su PISI.

10 Revisión de los lineamientos

En cumplimiento al Decreto Supremo 2514 Artículo 7, inciso i), se realizarán actualizaciones periódicas a los lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público.

ANEXO A

Controles de seguridad de la información

1. Seguridad en recursos humanos

Es necesario establecer mecanismos de relación, en materia de seguridad de la información, entre el recurso humano y la entidad o institución pública con el objetivo de preservar la información a la que tienen acceso durante y después de la vinculación laboral.

1.1. Términos y condiciones de la relación laboral

Establecer las responsabilidades en el marco de seguridad de la información del servidor público o cualquiera que tenga un vínculo laboral con la entidad o institución pública, debe formar parte integrante de la documentación de los archivos personales de cada servidor público o cualquiera que tenga un vínculo laboral con la entidad o institución pública.

1.1.1 Acuerdo de confidencialidad

A. Objetivo

Prevenir posibles fugas, divulgación no autorizada, mal uso o resguardo de la información.

B. Aplicabilidad

Servidores públicos o cualquier persona jurídica o natural que tenga un vínculo laboral con la entidad o institución pública.

C. Directrices

i. Elaborar el acuerdo de confidencialidad.

ii. Definir las restricciones y alcances del uso de la información, así como roles y responsabilidades.

iii. Coordinar con el área jurídica o legal la legalidad del acuerdo de confidencialidad.

iv. Garantizar la anuencia del servidor público o cualquier persona natural o jurídica que tenga un vínculo laboral con la entidad o institución pública con el acuerdo de confidencialidad.

v. Revisar y actualizar el acuerdo de confidencialidad en caso de cambios sustanciales en la clasificación de la información o a requerimiento interno.

vi. Respetar los datos de carácter personal, garantizar la privacidad y protección de la información personal identificable.

1.2 Concientización, educación y formación en seguridad de la información

Se debe generar una cultura de seguridad de la información institucional que involucre a todos los servidores públicos y a cualquier persona natural o jurídica que tenga un vínculo laboral con la entidad o institución pública.

1.2.1 Capacitación y formación

A. Objetivo

Capacitar en temas relacionados a seguridad de la información.

B. Aplicabilidad

Servidores públicos o cualquier persona jurídica o natural que tenga un vínculo laboral con la entidad o institución pública.

C. Directrices

i. Realizar eventos de concientización sobre la seguridad de la información, donde además se muestren roles y responsabilidades de los funcionarios para procedimientos de seguridad.

ii. Realizar capacitaciones acerca del Plan Institucional de Seguridad de la Información y las Políticas de Seguridad de la Información incluidas, con énfasis en las áreas de desempeño de los servidores públicos a ser capacitados.

iii. Informar sobre las responsabilidades adquiridas por acción u omisión e incumplimiento al Plan Institucional de Seguridad de la Información.

iv. Informar sobre los medios y puntos de contacto en temas relacionados a seguridad de la información.

v. Evaluar el grado de conocimiento de los servidores públicos respecto al Plan institucional de Seguridad de la Información.

1.3 Sanciones o amonestaciones a consecuencia del incumplimiento del PISI institucional

Implementar mecanismos disuasivos y preventivos para los casos de incumplimiento, por acción u omisión, de los documentos normativos relacionados a seguridad de la información.

A. Objetivo

Sancionar el incumplimiento de la normativa de seguridad de la información institucional vigente.

B. Aplicabilidad

Servidores públicos y cualquier persona jurídica o natural que tenga un vínculo laboral con la entidad o institución pública.

C. Directrices

i. Establecer las sanciones al incumplimiento de la normativa de seguridad de la información institucional vigente.

ii. Verificar la concordancia de la aplicación de las sanciones a los procesos o procedimientos internos de cada entidad o institución pública.

iii. Informar sobre los alcances y consecuencias de las sanciones fruto de infracciones al PISI.

1.4 Desvinculación de personal o cambio de cargo

Es necesario velar por el resguardo de la información e intereses de la entidad o institución pública al momento de la desvinculación o cambio del cargo de algún servidor público o cualquier persona natural o jurídica que tenga un vínculo laboral.

A. Objetivo

Preservar la disponibilidad, confidencialidad e integridad de la información al momento de la desvinculación o cambio de cargo de algún servidor público.

B. Aplicabilidad

Servidores públicos y cualquier persona natural o jurídica, al término o cambio de cargo de la relación laboral.

C. Directrices

i. Elaborar un proceso y procedimiento de desvinculación del personal que considere mínimamente: la devolución de los activos de información bajo custodia, el retiro de credenciales y cuentas de acceso a servicios y sistemas que permitan precautelar la seguridad de la información.

ii. Documentar el proceso de desvinculación y cambio de cargo.

iii. Controlar las copias no autorizadas de información durante la desvinculación.

iv. Responsabilidades y deberes que serán vigentes aun después de la finalización de la relación contractual.

2. Gestión de activos de información

Con el fin de preservar la integridad, disponibilidad y confidencialidad de los activos de información, se debe administrar, controlar y asignar responsabilidades en el uso y protección de los mismos.

2.1. Identificación y responsables de los activos de información

Identificar los activos de información de la entidad o institución pública y definir las responsabilidades para una protección apropiada.

2.1.1. Inventario de activos de información

A. Objetivo

Inventariar todos los activos de información dentro de los alcances del Plan Institucional de Seguridad de la Información.

B. Aplicabilidad

Activos de información de la entidad o institución pública.

C. Directrices

i. Identificar los activos de información considerando mínimamente: el tipo de activo, el formato, la ubicación, la información de soporte, la información sobre licencias y el valor para la entidad o institución pública.

ii. Clasificar los activos de información.

iii. Asignar un valor cuantitativo y/o cualitativo a cada uno de los activos.

iv. Revisar y actualizar el inventario de activos de información mínimamente una vez al año y/o cuando se requiera.

v. Restringir el acceso al inventario solo al personal autorizado de la entidad o institución pública.

vi. El inventario podrá incluir, en caso de no ser tangible el ciclo de vida de la información donde se considere la creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción.

2.1.2. Responsabilidad y custodia de los activos de información

A. Objetivo

Asignar para cada activo de información un responsable y/o custodio de acuerdo a sus funciones y competencias.

B. Aplicabilidad

Responsables/custodios de los activos de información.

C. Directrices

i. Identificar a los responsables y/o custodios de activos de información.

ii. Documentar el proceso de asignación y devolución de los activos de información a propietarios y/o custodios.

iii. El responsable identificado en caso de no ser una persona, puede ser una entidad que cuente con las responsabilidades de la dirección aprobada para controlar todo o parte del ciclo de vida de la información, también el propietario puede no tener los derechos de propiedad del activo, pero sí de custodia.

2.1.3. Uso aceptable de los activos de información

A. Objetivo

Establecer las restricciones y condiciones de uso adecuado de activos de información.

B. Aplicabilidad

Responsables y/o custodios de activos de información.

C. Directrices

i. Definir los requisitos de seguridad en relación a los activos de información.

ii. Establecer reglas para el uso correcto de los activos de información dentro y fuera de las instalaciones.

iii. Elaborar e implementar un reglamento de uso aceptable de activos de información, considerando mínimamente los puntos anteriores.

iv. Garantizar la aceptación de las restricciones y condiciones de uso de los activos de información a todos los servidores públicos y cualquier persona natural o jurídica que tenga un vínculo contractual con la entidad o institución pública, a los cuales se les haya asignado uno de ellos.

2.1.4. Devolución de los activos de información

A. Objetivo

Precautelar la disponibilidad, integridad y confidencialidad de los activos de información al momento de la desvinculación o cambio de cargo.

B. Aplicabilidad

En casos de desvinculación o cambio de cargos.

C. Directrices

i. Desarrollar e implementar un procedimiento de devolución de activos de información.

ii. En los casos donde el empleado o el usuario externo cuente con conocimiento importante para las operaciones de continuidad de la institución, dicha información se debería documentar y transferir.

2.2. Clasificación de la información

Identificar y clasificar la información según el grado de sensibilidad y criticidad para su uso y tratamiento adecuado.

2.2.1. Clasificación

A. Objetivo

Identificar y clasificar la información en relación a su valor, requisitos legales, sensibilidad, criticidad para su uso y tratamiento adecuado en la entidad o institución pública.

B. Aplicabilidad

Información, en cualquier medio en el que se encuentre.

C. Directrices

i. Elaborar un procedimiento de clasificación de la información institucional, que contenga los requisitos, nivel de clasificación, los responsables, las restricciones y la gestión de la información en general.

ii. Establecer requisitos de protección para cada nivel de clasificación definido que deberán considerar las necesidades de la entidad o institución

pública respecto a la apertura o restricción de la información.

iii. Reclasificación de la información de acuerdo a requerimiento y/o normativa vigente.

2.2.2. Etiquetado y manejo

A. Objetivo

Manejar adecuadamente la información, acorde a los requisitos y nivel de clasificación establecidos.

B. Aplicabilidad

Información, en cualquier medio en el que se encuentre.

C. Directrices

i. Definir dentro del procedimiento de clasificación institucional el proceso de etiquetado de la información en formatos físicos y digitales.

ii. Adecuación del proceso de etiquetado a los niveles de sensibilidad y criticidad establecidos.

iii. Definir los procedimientos de manejo, procesamiento, almacenamiento, transmisión, desclasificación y destrucción segura de la información, para cada nivel de clasificación.

2.2.3. Protección del archivo

A. Objetivo

Gestionar la seguridad del archivo de documentos.

B. Aplicabilidad

Documentación archivada.

C. Directrices

i. Definir un proceso y/o procedimiento para el archivo de documentación institucional.

ii. Elaborar controles para evitar la modificación y el acceso no autorizado a la información archivada.

iii. Elaborar controles para el acceso al archivo.

iv. Elaborar procedimientos de solicitud de documentación archivada.

v. Elaborar controles para la trazabilidad de la documentación archivada, que permita revisar las modificaciones realizadas.

2.3. Gestión de medios de almacenamiento removibles

La gestión de medios de almacenamiento removibles es necesaria para evitar la divulgación, modificación, manipulación o destrucción de información no autorizada en los medios de almacenamiento.

2.3.1. Gestión de medios removibles

A. Objetivo

Gestionar los medios informáticos removibles de acuerdo a los niveles de clasificación de información de la entidad o institución pública.

B. Aplicabilidad

Información en medios removibles.

C. Directrices

i. Elaborar procedimientos de uso de medios removibles donde mínimamente se establezcan quién, cómo, cuándo y para qué se accede a esos medios.

ii. Elaborar e implementar procesos y/o procedimientos para la autorización, uso y retiro de medios removibles al interior y exterior de la entidad o institución pública.

iii. Mantener un registro de auditoría del uso de medios removibles.

iv. Considerar el uso de cifrado de información en medios removibles, de acuerdo a la clasificación de información.

v. El contenido de los medios removibles que ya no se requieran deben ser destruidos e irrecuperables.

2.3.2. Eliminación segura de información

A. Objetivo

Eliminar la información de manera segura independientemente del medio en el que se encuentre, de acuerdo a los niveles de clasificación definidos por la entidad o institución pública.

B. Aplicabilidad

Información, en cualquier medio en el que se encuentre.

C. Directrices

i. Establecer y elaborar procesos/procedimientos para la eliminación de información, independientemente del medio en el que se encuentre, de acuerdo a los niveles de clasificación definidos por la entidad o institución pública y normativa legal vigente en el Estado Plurinacional de Bolivia.

ii. Para la eliminación de información, considerar la normativa legal vigente relacionada a la retención y resguardo de información.

2.3.3. Traslado físico de los medios de almacenamiento

A. Objetivo

Proteger los medios de almacenamiento que contienen información contra el acceso, uso y manipulación no autorizada al interior y fuera de las instalaciones de la entidad o institución pública.

B. Aplicación

Medios de almacenamiento.

C. Directrices

i. Elaborar procesos/procedimientos para el traslado de medios de almacenamiento.

ii. Establecer controles de protección física en medios de almacenamiento que eviten la intercepción, copia, modificación y destrucción.

iii. Mantener un registro de los medios de almacenamiento que permita identificar el contenido y custodio.

iv. En caso de considerar como no necesaria la información almacenada en cualquier medio removible, la misma será retirada de la entidad o institución pública sin posibilidad de recuperación.

3. Control de accesos

Gestionar los accesos a servicios y aplicaciones que permitan controlar, autorizar y asignar privilegios a cuentas de usuario.

3.1. Documentos normativos y operativos para el control de accesos

Establecer e implementar el reglamento para el control de accesos.

3.1.1. Normativa de control de acceso

A. Objetivo

Prevenir el acceso no autorizado a servicios, sistemas y aplicaciones.

B. Aplicabilidad

Aplica a sistemas, servicios y aplicativos de los que hace uso la entidad o institución pública para el cumplimiento de sus funciones.

C. Directrices

i. Elaborar un reglamento de control de accesos.

ii. El reglamento deberá establecer el objetivo, alcance, roles, frecuencias y responsabilidades para el control de accesos.

iii. El reglamento deberá ser revisado y actualizado cada cierto periodo de tiempo según normativa interna de la entidad o a la ocurrencia de un cambio significativo.

iv. Establecer sanciones al incumplimiento e infracciones en el control de accesos.

v. Implementar registros de acceso acorde a las necesidades de la entidad o institución pública.

vi. Se deberá establecer la periodicidad de cambios de información de autenticación.

vii. Establecer en las reglas la premisa "Generalmente todo está prohibido a menos que se permita de forma expresa".

3.2. Administración de accesos

Administrar la creación, registro y cancelación de cuentas de acceso para usuarios y las responsabilidades de uso adecuado de la información de autenticación, de parte de los usuarios.

3.2.1. Administración de accesos, cancelación y privilegios de usuarios

A. Objetivo

Gestionar la creación y cancelación de cuentas de usuario para los distintos servicios, sistemas y aplicaciones que dispone la entidad o institución pública.

B. Aplicabilidad

Accesos a servicios, sistemas y aplicaciones.

C. Directrices

i. Se deberán establecer los requisitos de autorización para la creación y asignación de roles y privilegios de una cuenta.

ii. Se deberán establecer procesos/procedimientos que reflejen el flujo de actividades a seguir, responsables, tiempos, quién autoriza, quién es consultado, quién es informado, quién es responsable de la cuenta de acceso y la forma y medio de entrega de las credenciales. Se deberá tomar en cuenta el criterio de menor privilegio.

iii. Se deberá establecer el flujo de actividades a seguir para la revisión y cancelación de accesos al momento de la desvinculación laboral.

iv. Identificar de forma única el acceso de los usuarios. Para esto se recomienda utilizar servicios de autenticación centralizada.

v. Elaborar procesos/procedimientos especiales para el acceso a servicios privilegiados como bases de datos, sistemas operativos y aplicaciones de administración.

vi. Para accesos privilegiados se deberán implementar medidas de seguridad adicionales que permitan monitorear y verificar las actividades acorde a las funciones establecidas.

vii. Las cuentas de acceso temporal o de invitados deberán contar con la autorización correspondiente.

viii. Habilitar las cuentas de acceso basado en roles de usuario para el procesamiento, administración, consulta o uso de la información.

ix. Establecer el periodo de tiempo de inactividad máximo que deshabilite las cuentas de acceso.

x. Establecer procesos/procedimientos para gestionar credenciales de cuentas perdidas, robadas o comprometidas.

xi. Implementar técnicas seguras para fortalecer la información de autenticación.

3.2.2. Responsabilidades de los usuarios para la autenticación

A. Objetivo

Asegurar que la información de autenticación tenga un uso responsable acorde al reglamento de acceso.

B. Aplicabilidad

Usuarios que cuenten con credenciales de acceso a sistemas, servicios y aplicaciones.

C. Directrices

i. Capacitar y concientizar sobre las responsabilidades del uso de credenciales de acceso.

ii. Se deberá dejar constancia sobre la aceptación del servidor público para el uso responsable de la información de accesos.

iii. Los servidores públicos deben evitar mantener la información de autenticación en lugares visibles o de acceso fácil para los demás.

iv. Los usuarios deberán cumplir el cambio de contraseñas de acuerdo a la periodicidad y requisitos de seguridad que se establezcan en la normativa de control de accesos.

v. La información de autenticación no deberá compartirse sin previa autorización justificada.

vi. La información de autenticación no deberá utilizarse para otros fines ajenos a las funciones asignadas de la entidad o institución pública.

vii. El usuario propietario de la cuenta de acceso es responsable del uso de la contraseña.

3.2.3. Revisión, eliminación o ajuste de los derechos de acceso

A. Objetivo

Revisar, eliminar o ajustar los derechos de acceso a servicios, sistemas y aplicaciones.

B. Aplicabilidad

Cuentas de acceso.

C. Directrices

i. Revisar periódicamente los derechos de acceso para identificar accesos no autorizados.

ii. Se deberán revisar los accesos privilegiados con más frecuencia y renovar los mismos en intervalos de tiempo razonables.

iii. Mantener un registro de las modificaciones de privilegios.

3.3. Control de acceso a redes y servicios de red

Gestionar el acceso a las redes de datos de la entidad o institución pública para prevenir accesos no autorizados y riesgos. La entidad debe establecer parámetros mínimos de cifrado para proteger la confidencialidad e integridad de la información.

3.3.1. Acceso remoto

A. Objetivo

Establecer un proceso/procedimiento para la gestión de acceso remoto a servicios, sistemas y aplicaciones.

B. Aplicabilidad

Solicitudes de acceso remoto.

C. Directrices

i. Establecer requisitos técnicos mínimos para la identificación y autenticación de usuarios para una conexión remota.

ii. Se deberá exigir la autorización por parte del propietario de la información.

iii. La entidad deberá definir la información que puede ser accedida y administrada mediante esta conexión, tomando en cuenta la clasificación de la información.

iv. Monitorear los accesos remotos a servicios, sistemas y aplicaciones.

v. Implementar controles de acceso a los servicios de red o aplicaciones de acuerdo a requisitos de autorización y privilegios de uso.

vi. Previsión de procedimientos de respaldo de continuidad del negocio en caso de fallas en los accesos remotos.

3.3.2. Acceso por redes inalámbricas

A. Objetivo

Gestionar la solicitud de accesos a redes inalámbricas de la Institución.

B. Aplicabilidad

Solicitudes de acceso a redes inalámbricas.

C. Directrices

i. Elaborar y establecer un proceso/procedimiento para la gestión de acceso a redes inalámbricas.

ii. Establecer requisitos técnicos mínimos para la identificación y autenticación de usuarios.

iii. La entidad deberá definir la información a la que se puede acceder mediante esta conexión.

iv. Monitorear los accesos de la red inalámbrica.

v. Implementar protección de las redes inalámbricas para evitar accesos no autorizados, en lo posible utilizando técnicas criptográficas.

3.3.3. Acceso de dispositivos móviles

A. Objetivo

Definir restricciones técnicas y uso de la información accedida a través de teléfonos inteligentes o dispositivos móviles para proteger la integridad y confidencialidad de la información.

B. Aplicabilidad

Acceso mediante teléfonos inteligentes, dispositivos móviles.

C. Directrices

i. Establecer requisitos técnicos mínimos para la identificación y autenticación de usuarios de acceso desde teléfonos inteligentes y dispositivos móviles.

ii. La entidad o institución debe definir la información que puede ser accedida mediante estos dispositivos.

iii. Se debe monitorear los accesos.

4. Criptografía

El uso de técnicas criptográficas aporta mayores niveles de seguridad para proteger la confidencialidad, autenticidad e integridad de la información, además del no repudio y autenticación.

4.1. Controles criptográficos

Utilizar técnicas criptográficas para proteger la confidencialidad, autenticidad e integridad de la información.

4.1.1. Uso de criptografía

A. Objetivo

Preservar la confidencialidad, autenticidad e integridad de la información, además del no repudio y autenticación.

B. Aplicabilidad

Información de acuerdo a los niveles de clasificación establecida e información transmitida a través de redes de comunicación.

C. Directrices

i. Elaborar e implementar un reglamento sobre el uso de criptografía para la protección de la información.

ii. Definir la fortaleza y la calidad del algoritmo de cifrado de acuerdo al tipo y criticidad de la información.

iii. Utilizar cifrado para proteger la información en medios de almacenamiento, transferencia de archivos, información transmitida por redes de comunicación y otros que se considere necesario.

iv. Utilizar firma digital para asegurar la autenticidad e integridad de la información.

v. Elaborar un proceso/procedimiento para la administración de claves, que considere: la generación, distribución, almacenamiento, cambio o actualización, recuperación, respaldo, destrucción y otras que se considere necesario.

vi. Utilizar técnicas criptográficas de claves bajo custodia.

5. Seguridad física y ambiental

Asegurar áreas e instalaciones donde se genere, procese, transmita o almacene información considerada sensible y crítica para la entidad o institución pública, con el objetivo de prevenir accesos no autorizados que comprometan la seguridad de la información.

5.1. Áreas e instalaciones seguras

Establecer medidas de seguridad física en áreas e instalaciones denominadas seguras o críticas de la entidad o institución pública.

5.1.1. Seguridad física en áreas e instalaciones

A. Objetivo

Prevenir y controlar el acceso físico no autorizado a instalaciones seguras o críticas de la entidad o institución pública.

B. Aplicabilidad

Áreas e instalaciones denominadas seguras donde se genere, procese, almacene o transmita información considerada sensible y crítica.

C. Directrices

i. Elaborar un reglamento de control de acceso físico.

ii. El reglamento debe considerar la identificación de áreas e instalaciones seguras o críticas, requisitos de seguridad para el ingreso de personal autorizado, condiciones de trabajo y operación.

iii. Identificar las áreas e instalaciones consideradas seguras o críticas.

iv. Elaborar procesos/procedimientos de acceso a las diferentes áreas e instalaciones según las características de seguridad de la información.

v. El acceso a áreas e instalaciones deberá ser autorizado.

vi. Señalizar las áreas e instalaciones denominadas seguras.

vii. Contar con áreas de recepción para el control y autorización de ingreso a las instalaciones de la entidad o institución pública.

viii. Instalar sistemas de monitoreo y vigilancia enmarcados a la normativa legal vigente.

ix. Contar con procesos/procedimientos para la entrega de grabaciones de sistemas de monitoreo y vigilancia de la entidad o institución pública.

x. Se deberá contar con equipamiento para mitigar posibles incendios, los cuales deben ser normados, revisados y probados periódicamente.

xi. Los ingresos y salidas de visitas deberán ser registradas, autorizadas y controladas. Asimismo deberán portar la identificación de visitante en lugar visible.

xii. Los servidores públicos deberán portar la identificación correspondiente en un lugar visible.

xiii. La seguridad física perimetral de la entidad o institución pública deberá inspeccionar y verificar el ingreso de elementos que comprometa la seguridad.

xiv. Implementar mecanismos de alerta al interior y exterior de las instalaciones ante la ocurrencia de eventos de seguridad.

xv. Se deberán realizar simulacros de evacuación y respuesta ante amenazas internas, externas, ambientales y/o revueltas sociales.

xvi. Impedir el acceso a las instalaciones a personas no autorizadas que no tienen relación directa o indirecta con las funciones de la entidad o institución pública.

xvii.Contar con señalética visible, para evacuaciones o contingencias de la institución.

5.1.2. Trabajo en áreas e instalaciones seguras

A. Objetivo

Gestionar las actividades de trabajo y operación dentro de las áreas e instalaciones acorde a los requisitos de seguridad.

B. Aplicabilidad

Aplicable a áreas e instalaciones seguras.

C. Directrices

i. Se deberán definir las acciones permitidas y no permitidas en las áreas o instalaciones consideradas seguras.

ii. En instalaciones con información sensible se deberá evitar el trabajo no supervisado a servidores públicos y terceras personas para evitar posibles incidentes de seguridad.

iii. El uso de cámaras de seguridad y otros controles deberán estar sujetos a normativa legal, que autorice el uso de las mismas en instalaciones donde se trabaje.

iv. El personal que trabaje en estas áreas deberá estar al tanto de las acciones permitidas y no permitidas y firmar un documento de aceptación de las mismas.

5.2. Equipamiento

Proteger el equipamiento interno y externo de la entidad o institución pública para prevenir el robo, daño, pérdida o compromiso de los mismos.

5.2.1. Seguridad del equipamiento

A. Objetivo

Prevenir y/o minimizar el impacto sobre el equipamiento ante amenazas, peligros ambientales y accesos no autorizados.

B. Aplicabilidad

Equipamiento interno y externo de la entidad o institución pública.

C. Directrices

i. Los servidores públicos deberán conocer los cuidados de seguridad en el uso del equipamiento.

ii. Las instalaciones con información y equipamiento crítico para las operaciones de la entidad deberán ser controladas para evitar el acceso no autorizado y su compromiso.

iii. Implementar controles para minimizar el impacto ocasionado por condiciones ambientales, incendios, inundaciones, polvo, vibraciones, interferencias eléctricas y otros.

iv. Establecer criterios para restringir el consumo de alimentos en proximidades de áreas e instalaciones seguras.

v. Realizar mantenimientos periódicos y pruebas de funcionalidad por personal calificado al equipamiento de acuerdo a las especificaciones del fabricante.

vi. Mantener y documentar los registros de fallas de operación del equipamiento, mantenimientos preventivos y correctivos.

vii. Se deberá llevar un inventario de las especificaciones técnicas de los equipos adquiridos.

viii. Los equipos, la información y el software no se deberán retirar de las instalaciones sin previa autorización, para ello se debe establecer responsables y responsabilidades.

ix. Se deberá respaldar la información que contiene el equipo previo a la destrucción de la misma.

5.2.2. Escritorio y pantalla limpia

A. Objetivo

Minimizar el riesgo de acceso no autorizado para prevenir la divulgación, uso indebido, robo de información o modificación.

B. Aplicabilidad

Información considerada sensible y crítica.

C. Directrices

i. La información sensible y crítica en medios de almacenamiento físico deben ser resguardados bajo llave u otro mecanismo de control.

ii. Bloquear la pantalla cuando se encuentre sin supervisión.

iii. Finalizar sesiones activas en aplicaciones o servicios de redes cuando no sean utilizadas

iv. Se deberán controlar los medios de almacenamiento conectados al equipo.

v. En instalaciones de atención al público se deberá mantener el escritorio despejado.

vi. Se deberá mantener un monitoreo continuo para el cumplimento de escritorio y pantalla limpia.

5.3. Seguridad física y ambiental en el centro de procesamiento de datos

Establecer controles de seguridad físico ambiental para la operación del Centro de Procesamiento de Datos – CPD.

5.3.1. Condiciones operativas

A. Objetivo

Garantizar las condiciones operativas del centro de procesamiento de datos.

B. Aplicabilidad

Centro de procesamiento de datos.

C. Directrices

i. Establecer procesos/procedimientos formales para la administración del CPD, en cuanto a accesos, mantenimiento de equipos, supervisión de trabajos externos y otros no limitativos a la presente directriz.

ii. La instalación física del CPD deberá contar con medidas de seguridad que eviten el acceso no autorizado, la debida separación de otros ambientes que comprometan la operación normal del CPD.

iii. Implementar medidas de seguridad ambiental para minimizar riesgos de incendio, inundación, polvo, humedad, vibraciones, interferencia de suministro de energía, interferencia de las comunicaciones y radiación electromagnética.

iv. En función de los requisitos de seguridad que se establezcan, se deberán implementar controles de autenticación robustos para el acceso al CPD.

v. El acceso físico a terceros deberá contar con autorización formal y escrita para trabajos al interior del CPD bajo supervisión.

vi. La disposición del equipamiento al interior del CPD debe estar organizado y distribuido.

vii. Se debe elaborar un mapa de la disposición del equipamiento del CPD.

viii. Las condiciones de operación del equipamiento deberán estar bajo especificaciones del fabricante.

ix. Se debe controlar la temperatura de operación del CPD.

x. Se deberá implementar dispositivos de enfriamiento y extracción de aire.

xi. El CPD deberá estar debidamente señalizado e iluminado.

xii. Se deberá instalar alarmas de detección de fallas en el suministro eléctrico y condiciones ambientales.

xiii. Se deberá organizar el cableado al interior del CPD, en lo posible cumplir con un cableado estructurado.

xiv. El suministro eléctrico al equipamiento del CPD deberá estar regulado y cumplir con las especificaciones técnicas.

xv. De acuerdo a requerimientos de disponibilidad, se deberá implementar suministro alterno de energía eléctrica y/o banco de baterías.

xvi. Se deberán programar mantenimientos periódicos del equipamiento del CPD.

6. Seguridad de las operaciones

Garantizar y asegurar que las actividades operacionales en instalaciones de procesamiento de información se realicen de forma correcta.

6.1. Responsabilidad de las operaciones

Establecer responsables y responsabilidades para la ejecución de operaciones.

6.1.1. Documentación de procedimientos operacionales

A. Objetivo

Documentar y esquematizar procedimientos de operación.

B. Aplicabilidad

Actividades operativas en instalaciones de procesamiento de información.

C. Directrices

i. Identificar los procesos operacionales relacionados a seguridad de la información que requieran ser formalizados y documentados.

ii. Elaborar procesos/procedimientos que describan los procesos operacionales mediante esquemas (flujogramas) explicados en un lenguaje de fácil entendimiento.

iii. Los procedimientos deberán ser comunicados y estar a disposición de los servidores públicos que así lo requieran.

iv. Se deberá documentar la instalación, configuración, recuperación, reinicio y mantenimiento de Infraestructura Tecnológica.

6.1.2. Gestión de cambios

A. Objetivo

Controlar y documentar cambios significativos en las operaciones.

B. Aplicabilidad

Procesos estratégicos e instalaciones y tecnologías de la información.

C. Directrices

i. Designar responsables para la aprobación de cambios.

ii. Identificar y registrar cambios significativos en procesos operativos.

iii. Los cambios de configuración deberán considerar el impacto asociado y realizarse en un ambiente controlado.

iv. Elaborar procesos/procedimientos para realizar un retroceso y/o abortar los cambios ante errores o eventos inesperados y para la recuperación ante cambios fallidos o imprevistos

v. Comunicar de forma previa y posterior a los interesados sobre los cambios autorizados a realizarse.

6.1.3. Gestión de la capacidad

A. Objetivo

Adaptar, supervisar el uso de recursos críticos y proyectar futuros requisitos para asegurar el desempeño, disponibilidad y un uso eficiente de los mismos.

B. Aplicabilidad

Aplicable a tecnologías de la información y cualquier otro recurso denominado crítico.

C. Directrices

i. Identificar los recursos críticos e indispensables para las operaciones.

ii. Se deberán revisar y eliminar los datos obsoletos almacenados.

iii. Se deberá sacar de servicio a las aplicaciones, sistemas, bases de datos o entornos en desuso y/o obsoletos.

6.2. Respaldos

Brindar protección contra la pérdida de datos y generar respaldos de la información.

6.2.1. Respaldos de información

A. Objetivo

Preservar la disponibilidad de la información.

B. Aplicabilidad

Información sensible y/o crítica.

C. Directrices

i. Identificar la información estratégica y clave para el cumplimiento de los objetivos institucionales.

ii. Se deberán establecer procesos y/o procedimientos de respaldo, donde se brinden los requisitos institucionales para realizar copias de respaldo, la periodicidad, pruebas de restauración, tiempos de retención de los respaldos en función a los requisitos institucionales y la normativa nacional.

iii. Se deberán respaldar y restaurar la información y configuración de redes, bases de datos, servicios, servidores, servidores virtuales, entre otros.

iv. Se deberán establecer frecuencias de respaldos de acuerdo a los requisitos de seguridad y/o criticidad de la información de la entidad o institución pública.

v. Se deberá extraer sumas de comprobación a copias de respaldo para

preservar la integridad de la información y en caso de ser necesario se deberá cifrar la información para mantener la integridad de la misma.

vi. Se deberán realizar regularmente pruebas de restauración a los respaldos para verificar su operatividad.

vii. El ambiente para el almacenamiento de copias de respaldo deberán contar con las condiciones ambientales adecuadas.

viii. En caso de tratarse de información crítica y/o estratégica se deberán almacenar los respaldos en múltiples medios de acuerdo a requerimiento.

ix. En situaciones donde el respaldo contenga información confidencial, estas deben estar protegidas con el uso de técnicas criptográficas.

7. Seguridad de las comunicaciones

Establecer controles que permitan proteger la información transmitida a través de las redes de telecomunicaciones reflejada en documentos.

7.1. Gestión de la seguridad en redes

Garantizar la protección y la disponibilidad de la Información en las redes de datos.

7.1.1. Gestión de la red

A. Objetivo

Gestionar y administrar las redes de datos y la información en tránsito por este medio.

B. Aplicabilidad

Redes de datos.

C. Directrices

i. Establecer un reglamento para la gestión de la red.

ii. El reglamento debe considerar roles y responsabilidades, procedimientos, requisitos de seguridad, tipos, métodos de autenticación,

monitoreo, autorización para acceso acorde al control de accesos y administración de la infraestructura de red.

iii. Considerar la implementación de dispositivos de red redundantes para puntos de fallo único donde la disponibilidad sea un factor crítico.

iv. Elaborar procesos/procedimientos para la gestión de la infraestructura de red.

v. Implementar controles para el resguardo de la integridad, confidencialidad, disponibilidad, no repudio y trazabilidad de la información transmitida al interior y exterior de la entidad o institución pública.

vi. El cableado de red a nivel de núcleo, distribución y acceso deberá estar identificado, etiquetado y ser operativo.

vii. Se deberán elaborar y actualizar periódicamente los diagramas de red y documentar la arquitectura de la red.

viii. Establecer las condiciones de uso aceptable de internet, considerando restricciones para la conexión a internet, siguiendo el principio del mínimo privilegio que garantice la calidad de servicio.

ix. Restringir el ancho de banda para recursos de alto consumo acorde al puesto laboral.

7.1.2. Seguridad en servicios de red

A. Objetivo

B. Aplicabilidad

Servicios de red internos y externos.

C. Directrices

i. Implementar controles de conexión, autenticación y cifrado para los servicios de red.

ii. En función de las necesidades de protección de confidencialidad de la

información, considerar la implementación de controles para la comunicación segura en servicios de red.

iii. Se recomienda que servicios de red externos se encuentren en una o varias zonas desmilitarizadas.

7.1.3. Seguridad en la red perimetral

A. Objetivo

Proteger la infraestructura de red interna ante amenazas que se originan de redes ajenas y/o públicas.

B. Aplicabilidad

Infraestructura de red.

C. Directrices

i. Implementar controles de seguridad perimetral que protejan la red ante posibles intrusiones.

ii. De acuerdo a los requisitos de seguridad se deberán implementar y documentar reglas de acceso y salida en los dispositivos de seguridad.

iii. Establecer una o varias zonas desmilitarizadas (DMZ).

iv. Se deberán implementar reglas de control de salida y registro según corresponda.

v. Se deberá monitorear regularmente la actividad en las redes de datos.

vi. Se deberán implementar protocolos de conexión segura.

vii. Se deberán implementar, cuando se vea necesario, parámetros técnicos de encriptación para conexiones seguras y reglas de seguridad.

7.1.4. Segmentación de la red

A. Objetivo

Separar la red en subredes de acuerdo a requerimiento institucional.

B. Aplicabilidad

Red institucional, sistemas, servicios, bases de datos, servidores y grupos de usuarios entre otros.

C. Directrices

i. Segmentar la red para los sistemas, servicios informáticos, bases de datos, servidores y grupos de usuarios entre otros.

ii. Para un uso más eficiente de las redes de datos se recomienda utilizar redes locales virtuales (VLAN).

iii. Las regionales deberán tener un subdominio de red específico.

iv. Segmentar las salidas de internet relacionadas con el consumo interno de servicios.

v. Se deberán segmentar el dominio institucional interno (DNS interno) del dominio institucional externo (DNS externo).

vi. Se deberá establecer una o varias zonas desmilitarizadas (DMZ) de acuerdo a requerimiento.

7.1.5. Seguridad en redes WiFi

A. Objetivos

Gestionar la seguridad de redes WiFi.

B. Aplicabilidad

Redes WiFi.

C. Directrices

i. Comunicar e informar las redes WiFi oficiales y autorizadas para uso.

ii. Concientizar sobre el uso seguro de las redes WiFi, que informe sobre los riesgos de conexión a redes desconocidas y no autorizadas.

iii. Implementar una red virtual local dedicada para redes WiFi diferente a la red cableada.

iv. Filtrar el acceso a la red WiFi por dirección MAC, servidor proxy o cualquier otro método de acuerdo al reglamente de gestión de la red de comunicaciones.

v. Utilizar algoritmos de cifrado robustos en las redes WiFi.

7.2. Seguridad del servicio de mensajería electrónica

Gestionar de forma eficiente y segura el servicio de mensajería y/o correo electrónico.

7.2.1. Mensajería y correo electrónico

A. Objetivo

Asegurar la disponibilidad, integridad y confidencialidad de la información transmitida a través de estos servicios.

B. Aplicabilidad

Mensajería y correo electrónico institucional.

C. Directrices

i. Elaborar un reglamento de uso aceptable del correo electrónico institucional.

ii. El reglamento debe establecer reglas de uso del servicio de correo electrónico y mensajería.

iii. El servicio de correo electrónico deberá ser independiente y pertenecer a un dominio institucional, evitando el uso de correos comerciales.

iv. El servicio de correo electrónico deberá implementarse en un servidor independiente.

v. Utilizar técnicas de autenticación robustas, además de control a las redes de acceso público.

vi. Las cuentas de usuario deberán ser autenticadas para prevenir y controlar la suplantación de correo electrónico.

vii. Utilizar protocolos y puertos seguros para la configuración del servicio de correo electrónico.

viii. Gestionar regularmente el almacenamiento de correo electrónico basura.

ix. Se deberán establecer la restricción de uso para archivos adjuntos.

x. Se deberá instalar software anti-spam.

7.3. Control sobre información transferida

Asegurar la información transferida.

7.3.1. Transferencia de información

A. Objetivo

Preservar la integridad y confidencialidad de la información transferida.

B. Aplicabilidad

Información institucional transferida.

C. Directrices

i. Definir los requisitos de seguridad para la transferencia de información de acuerdo a la criticidad y sensibilidad de la misma.

ii. Elaborar procesos/procedimientos orientados a prevenir la interceptación, manipulación, duplicación, repetición, descubrimiento no autorizado y destrucción de la información transferida en cualquier medio.

iii. Utilizar técnicas de cifrado para transferencia de información sensible y crítica.

iv. Se deberá firmar un acuerdo de confidencialidad para la transferencia de la información entre partes, de acuerdo a la criticidad y sensibilidad de la misma.

8. Desarrollo, mantenimiento y adquisición de sistemas

Establecer requisitos de seguridad para el desarrollo, mantenimiento y adquisición de sistemas que consideren pruebas de seguridad, pruebas de calidad y aceptación para desarrollos internos y externos

8.1. Desarrollo y mantenimiento de sistemas

Establecer requisitos de seguridad para el diseño, desarrollo, pruebas y mantenimiento de sistemas nuevos o existentes.

8.1.1. Elaboración de la normativa de desarrollo

A. Objetivo

Normar el desarrollo y mantenimiento seguro de sistemas.

B. Aplicabilidad

Desarrollo y mantenimiento de sistemas nuevos y existentes.

C. Directrices

i. Elaborar un reglamento que considere los requisitos de seguridad, roles y responsabilidades para el desarrollo y mantenimiento de sistemas apoyado en procesos/procedimientos.

ii. El reglamento debe ser revisable, actualizable y comunicado a las partes interesadas.

iii. Elaborar procesos/procedimientos para el control de versiones, despliegues, pruebas de seguridad, evaluación de vulnerabilidades, codificación segura, nuevos parches, correcciones y otros no limitativos a la presente directriz.

iv. Realizar procesos de gestión de actualizaciones de sistemas en caso de ser necesario. Todos los cambios deben ser probados, validados, evaluados, documentados y comunicados previamente.

8.1.2. Identificación de requisitos de seguridad

A. Objetivo

Establecer requisitos de seguridad desde el inicio del desarrollo y durante el ciclo de vida del sistema.

B. Aplicabilidad

Desarrollo y mantenimiento de sistemas.

C. Directrices

i. Identificar requisitos de seguridad para el desarrollo y mantenimiento de sistemas. Una forma de identificar es consultando los registros de incidentes, el valor de la información que representa para la entidad o institución pública, las vulnerabilidades conocidas y/o requisitos de las partes interesadas.

ii. Evaluar la criticidad de la información en términos de confidencialidad, integridad y disponibilidad para dotar de mayores controles de seguridad.

iii. Los requisitos de seguridad deberán contemplar requerimientos de infraestructura tecnológica como disponibilidad y redundancia de almacenamiento.

iv. Considerar como requisito la identificación de tipos de usuarios, autorización, autenticación, ambientes de desarrollo, pruebas y despliegue a producción.

v. Identificar requisitos criptográficos y firma digital.

vi. Las partes interesadas deberían formar parte integral durante el proceso de desarrollo.

vii. Las partes interesadas deberán coordinar temas relacionados a seguridad, funcionalidad, usabilidad y otros.

viii. Considerar la protección y privacidad de los datos personales recolectados a través de las aplicaciones.

8.1.3. Seguridad en el desarrollo y mantenimiento de sistemas

A. Objetivo

Asegurar el desarrollo y mantenimiento de sistemas para evitar un impacto operacional adverso.

B. Aplicabilidad

Desarrollo y mantenimiento de sistemas.

C. Directrices

i. Establecer procesos/procedimientos para técnicas de programación segura.

ii. Se deberán separar los ambientes de desarrollo, pruebas y producción.

iii. El proceso de desarrollo deberá contar con la documentación necesaria.

iv. Establecer procedimientos para el control de cambios, uso de repositorios seguros, documentar cambios funcionales y de seguridad a producción.

v. Los cambios a producción deberán ser autorizados y documentados previa realización de pruebas.

vi. El uso de librerías de terceros deberían ser evaluadas en relación a la funcionalidad, seguridad, fuentes confiables y referenciados localmente.

vii. Elaborar procesos/procedimientos de actualización de seguridad para librerías, bases de datos y software dependiente.

viii. Establecer procesos/procedimientos para la realización de copias de seguridad, estos deben contemplar el medio de almacenamiento, el ambiente y la frecuencia de las copias.

ix. De acuerdo a los requerimientos institucionales, se deberá considerar implementar medidas de seguridad para el acceso físico/lógico a los recursos de los ambientes de desarrollo, pruebas y producción según corresponda.

x. Se deben validar datos de entrada y salida, porque este tema es parte de las vulnerabilidades conocidas de los sistemas.

xi. Los procedimientos de desarrollo de sistemas deben aplicar técnicas de ingeniería segura que brinden orientación sobre las técnicas de autentificación, control, validación de datos, sanitización y eliminación de código de depuración.

8.1.4. Interoperabilidad de sistemas

A. Objetivo

Asegurar la transacción e intercambio de información entre sistemas de información.

B. Aplicabilidad

Sistemas que consumen o proveen información a otros sistemas.

C. Directrices

i. Utilizar técnicas de cifrado para transacción e intercambio de información que preserve la confidencialidad e integridad de la información.

ii. La información de autenticación de usuarios deberá ser válida y verificable.

iii. Utilizar protocolos de comunicación cifrada.

iv. Se deberán establecer términos y condiciones de uso del servicio entre las partes.

v. La protección de la información de los sistemas puede involucrar la transferencia o el acceso de la información desde puntos externos o fronteras. En este caso la institución debe tener conocimiento de las responsabilidades legales y contractuales para seguridad de la información.

8.1.5. Pruebas de seguridad

A. Objetivo

Evaluar la seguridad de los sistemas.

B. Aplicabilidad

Desarrollo, mantenimiento y adquisición de sistemas.

C. Directrices

i. Las pruebas de seguridad deberán especificarse desde el diseño del sistema y realizarse durante el proceso de desarrollo del mismo.

ii. Para las pruebas se deberán tomar como referencias las vulnerabilidades conocidas.

iii. Documentar las pruebas de aceptación para desarrollos internos y externos, de acuerdo a los requisitos de seguridad establecidos.

iv. Las pruebas deberán permitir evaluar el cumplimiento de la normativa de desarrollo en cuanto a buenas prácticas de codificación e identificar código malicioso.

v. Las pruebas se deberán realizar utilizando herramientas como analizadores de código, escáneres de vulnerabilidades y otros.

vi. El ambiente de pruebas deberá estar configurado con las mismas características de seguridad que el ambiente de producción.

vii. Las pruebas deben considerar canales ocultos para prevenir accesos no autorizados, monitoreo, validación, denegación de servicios, suplantación.

8.1.6. Seguridad en bases de datos

A. Objetivo

Gestionar y documentar la seguridad en bases de datos.

B. Aplicabilidad

Bases de datos

C. Directrices

i. Aplicar recomendaciones de configuración en seguridad provistas por el desarrollador del gestor de base de datos.

ii. Considerar implementar redundancia y alta disponibilidad según requisitos de seguridad establecidos.

iii. Para la gestión de copias de respaldo, se deberán elaborar procesos / procedimientos que establezcan responsables, periodicidad y otros que se considere necesario.

iv. Gestionar usuarios y privilegios para acceso a bases de datos, tablas, funciones y otros.

v. Las cuentas de usuario deberán tener propietarios con responsabilidades de uso.

vi. Para el acceso de cuentas de usuarios a las bases de datos en ambientes de desarrollo, pruebas y producción, se deberán implementar controles de autenticación y autorización.

vii. La extracción de datos de producción para las pruebas de funcionalidad deberán considerar la confidencialidad de la misma y los controles necesarios para resguardarla.

viii. Se deberán optimizar las consultas lógicas a bases de datos.

ix. Restringir el uso de cuentas de usuario por defecto.

x. En caso de cambios y/o modificaciones a las bases de datos se deberán realizar pruebas de aceptación y funcionalidad bajo autorización documentada.

8.2. Seguridad para la adquisición de sistemas

Establecer requisitos de seguridad para la adquisición de sistemas, software y aplicaciones a terceros.

8.2.1. Requisitos de seguridad

A. Objetivo

Contemplar requisitos de seguridad para la adquisición de sistemas, software y aplicaciones.

B. Aplicabilidad

Adquisición de software, sistemas y aplicaciones.

C. Directrices

i. Se deberán establecer los requerimientos de seguridad y aceptación de acuerdo a la normativa de desarrollo institucional en los términos de referencia.

ii. Comunicar la normativa de desarrollo a las partes interesadas en el proceso de adquisición y/o desarrollo terciarizado.

iii. Se deberán establecer acuerdos de nivel servicio (SLA) con la parte interesada.

iv. Debe obtenerse en la medida de lo posible, información oportuna de las vulnerabilidades técnicas de los sistemas, software y aplicaciones a ser adquiridos de terceros, así como la información relevante con respecto a actualizaciones y parches.

9. Gestión de incidentes de seguridad de la información

Establecer mecanismos para la gestión de incidentes en seguridad de la información dentro de la institución o entidad pública para dar continuidad a las operaciones y mejorar los controles de seguridad implementados.

9.1. Gestión de incidentes de seguridad de la información

Reducir la afectación negativa a la seguridad de la información y/o continuidad de las operaciones de la entidad o institución pública.

9.1.1. Gestión de incidentes

A. Objetivo

Establecer lineamientos, roles, responsabilidades y procedimientos en la gestión de incidentes, para una respuesta eficaz ante la ocurrencia de eventos adversos relacionados a la seguridad de la información.

B. Aplicabilidad

Incidentes en seguridad de la información.

C. Directrices

i. Se deberá elaborar procesos y/o procedimientos de gestión de incidentes de seguridad de la información, los mismos deben establecer roles, responsabilidades informar, evaluar y responder sobre eventos de seguridad.

ii. El RSI deberá identificar el incidente para registrar el mismo, el tratamiento que se le dío y/o escalamiento.

iii. El RSI deberá evaluar cada evento de seguridad clasificarlo para su reporte.

iv. Los incidentes que no puedan ser solucionados deberán ser escalados al Centro de Gestión de Incidentes Informáticos por el RSI.

v. El documento de reporte de incidentes y vulnerabilidades deberá ser socializado a los servidores públicos para que los mismos conozcan los medios de reporte.

vi. Ante la ocurrencia de incidentes se deberá recuperar y restablecer la operatividad normal de activos de información.

vii. El RSI deberá ser el punto de contacto al interior de la institución y con Responsables de Seguridad de la Información de entidades públicas.

viii. Una vez que haya pasado el incidente, se deberán documentar las actividades de respuesta.

ix. Se deberá llevar una bitácora de eventos para el análisis posterior sobre los costos asociados al incidente y sobre los cuales se deben implementar soluciones a corto, mediano y largo plazo para reducir la probabilidad de ocurrencia futura.

x. El RSI deberá nominar al personal de respuesta ante incidentes, con la responsabilidad, la autoridad y la competencia necesaria para administrar un incidente y mantener la seguridad de la información.

xi. El RSI deberá establecer, documentar, implementar y mantener los procesos, procedimientos y controles para dar respuesta a incidentes de Seguridad de la Información.

xii. En caso de ser necesario la institución debe realizar, acorde al incidente, un proceso para administrar y gestionar la evidencia forense.

xiii. En un proceso de atención a incidentes, el RSI en caso de requerir evidencia forense, podrá involucrar a un abogado o la Policía Nacional para el comienzo de acciones legales o asesoría sobre la evidencia.

10. Plan de contingencias tecnológicas

Implementar un Plan de Contingencias Tecnológicas que permita controlar un incidente de seguridad de la información o una situación de emergencia, minimizando sus consecuencias negativas. Asimismo deberá determinar sus requisitos para la seguridad de la información ante situaciones adversas.

10.1. Implementación del plan de contingencias tecnológicas

La entidad o institución pública debe contar con un Plan de Contingencias Tecnológicas formalizado, actualizado e implementado; aprobado por el Comité de Seguridad de la Información, asignando responsabilidades para su ejecución a los propietarios de los activos de información.

10.1.1. Elaboración del plan de contingencias tecnológicas

A. Objetivo

Definir las estrategias, acciones, procedimientos y responsabilidades para minimizar el impacto de una interrupción imprevista de las funciones críticas y conseguir la restauración de las mismas, dentro de los límites de tiempo establecidos.

B. Aplicabilidad

El plan de contingencias está circunscrito a los eventos tecnológicos.

C. Directrices

i. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en seguridad de la información; la mejora continua a partir de la Gestión de Incidentes de Seguridad de la Información; la determinación de los eventos que afecten la operación de los sistemas de información; la determinación de los procesos, operaciones críticos y los recursos tecnológicos asociados a estos.

ii. Implementar procesos y/o procedimientos de recuperación y restauración de operaciones críticas para cada evento identificado.

iii. Cada documento operativo debe incluir responsabilidades, procedimientos, funciones e identificación del personal que ejecutará el plan.

iv. Los responsables de activos de información en coordinación con el Comité de Seguridad de la Información definen los tiempos máximos de restauración.

v. La entidad o institución pública deberá identificar los requisitos institucionales para la disponibilidad de los sistemas de información.

vi. Cada Plan de Contingencias Tecnológicas deberá describir el enfoque para la continuidad, así como las condiciones necesarias para activar un plan de escalamiento si fuese necesario.

10.1.2. Pruebas y mantenimiento del plan de contingencias tecnológicas

A. Objetivo

El Plan de Contingencias Tecnológicas debe ser sujeto a revisiones periódicas y ejercicios de entrenamiento para asegurar su actualización.

B. Aplicabilidad

Aplica al Plan de Contingencias Tecnológicas y a los servidores públicos involucrados en el plan.

C. Directrices

i. El RSI coordinará de manera periódica la ejecución de las pruebas al Plan de Contingencias Tecnológicas para verificar, revisar y evaluar el mismo.

ii. Producto de las pruebas, el RSI podrá incorporar situaciones no cubiertas al plan.

iii. En caso de que las pruebas no sean exitosas, el RSI deberá gestionar la implementación de acciones correctivas o preventivas y ejecutar nuevamente las pruebas hasta cumplir con el objetivo planteado.

iv. Se debe documentar la realización de las pruebas y la implementación de los planes de acción correctivos o preventivos según correspondan.

v. El RSI, en coordinación con los involucrados, debe realizar revisiones periódicas al Plan de Contingencias Tecnológicas en función a la gestión de incidentes de seguridad de la información y al tratamiento de riesgos tecnológicos.

11. Cumplimiento

Asegurar el cumplimiento operativo del Plan Institucional de Seguridad de la Información que conlleva la Política de Seguridad y la documentación resultante de la misma.

11.1. Revisión de controles

Evaluar periódicamente el cumplimiento de la normativa documental del Plan Institucional de Seguridad de la Información, verificando que los mismos se encuentran en operación.

11.1.1. Revisión

A. Objetivo

Validar el cumplimiento de los controles de seguridad implementados.

B. Aplicabilidad

Plan Institucional de Seguridad de la Información.

C. Directrices

i. El Responsable de Seguridad de la Información, en coordinación con el Comité de Seguridad de la Información, será el encargado de verificar la correcta implementación, aplicación y cumplimiento, debiendo realizar revisiones y evaluaciones periódicas al Plan Institucional de Seguridad de la Información, en las que tomará en cuenta los siguientes criterios.

ii. Identificar causas del incumpliendo.

iii. Acciones para lograr el cumplimiento.

iv. Implementar acciones correctivas y preventivas para lograr un proceso continuo, iterativo y de mejora continua del PISI.

v. Revisar el cumplimiento de las acciones correctivas o preventivas.

vi. Los propietarios de procesos, activos de información e información serán los responsables del cumplimiento de las acciones correctivas.

vii. El RSI informará al CSI el estado de cumplimiento de los controles de seguridad implementados.

11.1.2. Verificación del cumplimiento técnico

A. Objetivo

Detectar vulnerabilidades técnicas en la infraestructura tecnológica.

B. Aplicabilidad

Tecnologías de la Información.

C. Directrices

i. Realizar evaluaciones de vulnerabilidades técnicas y hacking ético.

ii. Los resultados de la evaluación deben permitir identificar debilidades de seguridad para mitigar los mismos en el corto, mediano y largo plazo.

iii. Solicitar a la AGETIC u otras entidades la realización de evaluaciones de seguridad de la información, infraestructura, sistemas informáticos entre otros, en coordinación con el personal de la entidad pública que lo requiera.

iv. Realizar revisiones de cumplimiento técnico, que también involucra una revisión de los sistemas operacionales críticos y sensibles para ver que estos se hayan implementado de forma correcta.

11.2. Auditoría al Plan Institucional de Seguridad de la Información

Verificar el cumplimiento del Plan Institucional de Seguridad de la Información.

11.2.1. Evaluación de cumplimiento del plan Institucional de seguridad de la información

A. Objetivo

Evaluar el grado de cumplimiento del Plan Institucional de Seguridad y las métricas determinadas para cada control implementado por la entidad.

B. Aplicabilidad

Plan Institucional de Seguridad de la Información

C. Directrices

i. La unidad de auditoría interna será la encargada de la revisión del cumplimiento del Plan de Seguridad Institucional de la Información relacionado con los documentos normativos, operativos y métricas.

ii. En caso de ser necesario la unidad de auditoría interna podrá delegar a un especialista la revisión para identificar debilidades técnicas y operativas en los controles para la mejora continua de los mismos.

iii. La entidad o institución pública podrá presentar a la AGETIC los avances en el desarrollo e implementación del Plan Institucional de Seguridad de la Información.

iv. La entidad o institución pública presentará a la AGETIC el Plan Institucional de Seguridad de la Información, de acuerdo a normativa legal vigente en el Estado Plurinacional de Bolivia.

ANEXO B

Guía para la metodología de gestión de riesgos

1 . Introducción

Los lineamientos para la elaboración del Plan Institucional de Seguridad de la Información establecen que la entidad o institución pública deberá adoptar un estándar y/o metodología de gestión de riesgos dentro de los alcances del Plan, con el objetivo de implementar controles de seguridad o mejorar la eficacia de los controles ya existentes.

La presente guía brinda orientación para elaborar la metodología de gestión de riesgos acorde a las directrices establecidas en los lineamientos para la elaboración del Plan Institucional de Seguridad de la Información.

La entidad o institución pública es libre de elegir el método o metodología para la Gestión de riesgos.

2 . Objetivo

La presente guía tiene el objetivo de orientar en la metodología de gestión de riesgos a partir del cual se realizará:

a) Identificación, Clasificación y Valoración de Activos de Información.

b) La Evaluación del Riesgo.

c) Tratamiento del Riesgo.

d) Controles Implementados y por Implementar.

Esta guía toma como referencia la Metodología de Análisis y Gestión de Riesgos MAGERIT. Sin embargo, la entidad o institución pública es libre de elegir el método o metodología que considere adecuada para realizar la gestión de riesgos siempre y cuando esta se encuentre bajo algún estándar nacional o internacional.

3. Referencias

La presente guía toma como referencia el inventario de activos de información que sugiere la metodología de análisis y gestión de riesgos MAGERIT.

4. Documentos relacionados

La presente guía tiene relación con los siguientes documentos:

- Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público.
- MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Versión 3.
- Estándares de la Familia ISO 27000 de Tecnologías de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información.
- Si bien la presente guía hace referencia a buenas prácticas de gestión de riesgos del estándar NB/ISO/IEC 27005:2010, la misma no obliga su adopción. Existen normas, estándares y marcos de trabajo y metodologías como la NB/ISO 31000:2014, Objetivos de Control para Información y Tecnologías Relacionadas (COBIT), Biblioteca de Infraestructura de Tecnologías de Información (ITIL) entre otros y dependerá de la necesidad y experiencia de cada entidad o institución pública en gestión de riesgos.

5. Términos y definiciones

Activo.- En general, activo es todo aquello que tiene valor para la entidad o institución pública.

Activo de información.- Conocimientos o datos que tienen valor para la organización.[8]

Responsable del activo de información.- Servidor público de nivel jerárquico quien tiene la responsabilidad y las atribuciones de establecer los requisitos de seguridad y la clasificación de la información relacionada al activo, según el alcance definido del proceso al cual pertenece la misma.

■

[8] Términos y Definiciones NB/ISO/IEC 27000:2010

Custodio del activo de información.- El servidor público encargadodeadministraryhacerefectivo loscontrolesde seguridad, que el responsable del activo de información haya definido.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos autorizados.[9]

Integridad: Propiedad de salvaguardar la exactitud y completitud de los activos.[10]

Disponibilidad.- Propiedad de ser accesible y utilizable por solicitud de una entidad autorizada.[11]

Amenaza.- Causa potencial de un incidente no deseado, que puede dar lugar a daños en un sistema o en una organización.[12]

Riesgo.- Combinación de la probabilidad de un evento adverso y su consecuencia.[13]

Vulnerabilidad.- Debilidad de un activo o control, que puede ser explotada por una amenaza.[14]

Impacto.- Cambio adverso en la operación normal de un proceso de la institución pública.[15]

6. Identificación, clasificación y valoración de activos de información

La identificación del inventario de activos de información permite clasificar y valorar el activo entérminos cuantitativos o cualitativos, para brindar un mejor tratamiento y protección se debe identificar, especificar claramente sus características y la función al interior de los procesos alineados con los objetivos y alcances definidos.

Las directrices establecidas en el Anexo A sobre Gestión de Activos de Información mencionan la responsabilidad por los activos de información que contemple: el inventario, propiedad, custodia y el uso aceptable de los mismos.

■

[9] Términos y Definiciones NB/ISO/IEC 27000:2010
[10] Términos y Definiciones NB/ISO/IEC 27000:2010
[11] Términos y Definiciones NB/ISO/IEC 27000:2010
[12] Términos y Definiciones NB/ISO/IEC 27000:2010
[13] Términos y Definiciones NB/ISO/IEC 27000:2010
[14] Términos y Definiciones NB/ISO/IEC 27000:2010
[15] Términos y Definiciones NB/ISO/IEC 27000:2010

Las actividades para realizar y gestionar el inventario de activos de información son la identificación, valoración, revisión y actualización.

6.1 . Identificación

Consiste en determinar e identificar qué activos de información formarán parte del inventario. El Responsable de Seguridad de la Información debe orientar la correcta identificación de los mismos conjuntamente con los responsables o dueños de los procesos institucionales, dentro de los alcances definidos en el Plan Institucional de Seguridad de la Información.

Para la identificación de activos de información se sugiere la siguiente clasificación:

Información

En esta clasificación ingresan procesos relevantes para la institución e información en cualquier medio de soporte físico o digital. Los tipos de información que ingresarían son: información estratégica, información relacionada con el archivo personal, información relacionada a la documentación administrativa, legal, procesos de adjudicación y otros que tengan un coste económico y de cumplimiento con la normativa legal. También, en esta categoría está la información de archivos tales como respaldos, documentos, credenciales de acceso, entre otros.

Claves criptográficas

Algunos de los ejemplos de activos en esta categoría son: claves para cifrar, firmar, certificados x509, entre otros.

Servicios

En esta categoría ingresan: servicios de acceso remoto,transferencia de archivos, correo electrónico, servicios web, servicio de directorio, entre otros.

Software - aplicaciones informáticas

En esta categoría se encuentran: sistemas desarrollados y/o adquiridos, software de aplicación, sistemas operativos, software de virtualización, entre otros.

Equipamiento informático (Hardware)

En esta categoría están los medios físicos que soportan los procesos como ser: servidores, equipamiento de escritorio, periféricos, dispositivos de red perimetral, dispositivos de red, corta fuegos, entre otros.

Redes de comunicaciones

Están los servicios de comunicaciones como ser: la red telefónica, redes de datos, internet, entre otros.

Soportes de información

En esta categoría están: discos virtuales y físicos, memorias usb, discos y cintas, material impreso, entre otros.

Equipamiento auxiliar

En esta categoría están: fuentes de alimentación, generadores eléctricos, equipos de climatización, cableado eléctrico, mobiliario, entre otros.

Instalaciones

Edificio, vehículos, instalaciones de refuerzo, entre otros.

Personal

Incluye personal fijo, eventual, terceros, entre otros.

También se debe identificar a los responsables y custodios de la información asociada al activo; esto es importante porque a través de la identificación se realizará una mejor valoración para resguardar la información. Los custodios podrían ser los mismos servidores públicos o en otros casos una persona ajena a la entidad o institución pública.

6.2 . Valoración

La valoración de activos de información tiene como objetivo asegurar que la información asociada a los mismos reciba niveles de protección adecuados, ya que en base a su valor y otras características particulares se requerirá implementar o mejorar controles de seguridad.

Las características o atributos hacen que un activo sea valioso, estas se utilizan para valorar las consecuencias de la materialización de una amenaza, que a su vez produce perjuicio a los procesos relacionados y la afectación de activo en una o todas las propiedades de la información: disponibilidad, integridad y confidencialidad, además de otras como la autenticidad, trazabilidad y no repudio. Si se ve conveniente la entidad o institución pública tomará la decisión de valorar el activo en las dimensiones que requiera.

A continuación se conceptualizan las propiedades de la información asociadas a activos para la valoración:

Disponibilidad

Un activo tiene gran valor, desde el punto de vista de disponibilidad, si es que una amenaza afectase su disponibilidad con consecuencias graves para el normal desarrollo de las actividades. Por el contrario, un activo carece de un valor apreciable cuando puede no estar disponible por largos periodos de tiempo sin afectar o causar daño a las actividades de la entidad o institución pública.

Integridad

Una valoración alta de esta propiedad se da por el grado de afectación (daño grave) causado por la alteración voluntaria o no intencionada de los datos. Por el contrario, una valoración menor se da cuando su modificación no supone preocupación alguna.

Confidencialidad

La valoración de esta característica está en función del grado de afectación que ocasionaría la revelación o divulgación de información a personas no autorizadas.

En la presente guía se toma la valoración cualitativa, pero no limita a que la entidad realice la valoración cuantitativa y defina su propia escala de valoración, siempre y cuando esta se encuentre respaldada y aprobada.

La valoración la debe dar el reponsable del activo de información. Estas pueden ser en base a percepción, eventos anteriores relacionados a las propiedades de la información y otros.

La escala recomendada para la valoración cualitativa de las características del activo de información se presenta en la siguiente figura.

Figura 1. Escala de Valoración de Activos

Escala de Valoración	
1	Muy Bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

La entidad está en libertad de establecer sus propias escalas para valorar los activos de información.

También es conveniente realizarse las siguientes preguntas para clarificar la valoración asociada a cada característica del activo de información.

Tabla 1. Preguntas para Valoración de Activos

Disponibilidad	¿Qué importancia tendría que el activo no estuviera disponible?
Integridad	¿Qué importancia tendría que la información asociada al activo fuera modificada sin control?
Confidencialidad	¿Qué importancia tendría que la información asociada al activo fuera conocida por personas no autorizadas?

La valoración de cada una de las características estará en función a la escala y la posteriorvaloración final del activo, que será el promedio de las tres características.

6.2.1 . Ejemplo

Imaginemos que el responsable del activo de información es el Responsable de Tecnologías de Información de la entidad y este identifica un activo: "Servidor de Correo Institucional" que es el servicio por el cual se mantienen la comunicación y

envío de archivos al interior y exterior de la entidad. Se le pide que valore el servicio en términos de disponibilidad, confidencialidad e integridad de la información, asociada al servicio identificado y este es el resultado:

Tabla 2. Ejemplo de la Valoración de Activos

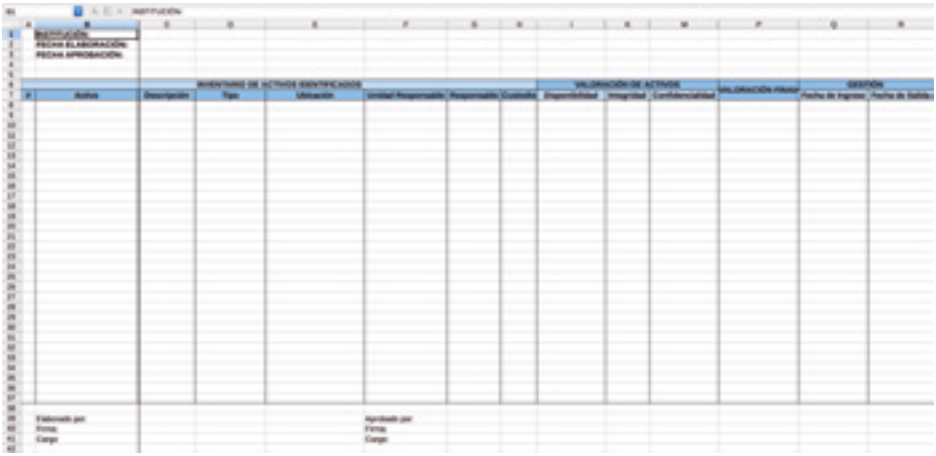
Disponibilidad	Alto
Integridad	Muy Alto
Confidencialidad	Medio

Además identifica que los custodios del activo son los usuarios que hacen uso del servicio. La valoración final del activo se da promediando las tres propiedades, por lo tanto su valoración llega a ser: Alto.

6.2.2 . Matriz de inventario y valoración

Para materializar la Identificación, Clasificación y Valoración de Activos de Información se sugiere el uso dela siguiente matriz:

Figura 2. Matriz de Inventario y Valoración



La información del encabezado consta del nombre de la institución, fecha de elaboración y fecha de aprobación.

El detalle de los campos del inventario se describen a continuación:

- Activo: Nombre del activo de información identificado.
- Descripción: Descripción del activo inventariado.
- Tipo: Clasificación del activo de acuerdo a MAGERIT u otro que se estime necesario.
- Ubicación: Detalle del lugar físico donde se encuentra el activo agregando condiciones de seguridad en las que se encuentra el activo.
- Unidad Responsable: La unidad organizacional responsable del activo.
- Responsable: Nombre y cargo de la persona responsable del activo; con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la institución. El responsable puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad según corresponda.
- Custodio: Nombre y cargo del encargado de resguardar la información.
- Valoración de Activos: De acuerdo a la confidencialidad, integridad y disponibilidad.
- Valoración Final: Valoración final promedio de la confidencialidad, disponibilidad e integridad.
- Fecha de Ingreso: Fecha de ingreso del activo de información en el inventario.
- Fecha de Salida: Fecha de exclusión del activo de información del inventario.

El inventario elaborado debe ser coordinado y aprobado por las partes interesadas (responsable del activo de información) de los procesos identificados.

6.3 . Revisión y actualización

La revisión es la verificación que se lleva a cabo para determinar si un activo continua siendo parte del inventario.

El inventario puede ser revisado o validado en cualquier momento a solicitud del responsable de seguridad de la información. Entre las razones por la que se debería realizar una revisión son:

- Actualizaciones al proceso al que pertenece el activo.
- Inclusión de nuevos procesos y procedimientos.
- Inclusión de un nuevo activo.
- Desaparición de una unidad organizacional, proceso o cargo en la entidad que tenía asignado el rol de responsable o custodio.
- Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.
- Cambios físicos de la ubicación de activos de información.

La actualización, fruto de la revisión, debe estar sujeta a control de cambios que permita identificar la fecha, el autor, los motivos por el cual se actualiza y otros que son necesarios para el control.

6.4 . Reserva

El inventario de activos de información debe ser un documento de carácter no público con medidas de restricción para evitar su modificación.

El Responsable de Seguridad de la Información debería tener acceso para modificar el inventario, además de ser el responsable de resguardarlo.

7 . Evaluación del riesgo

La evaluación del riesgo permitirá identificar las debilidades en cuanto a controles de seguridad inexistentes o ineficaces. Se sugiere que la evaluación se realice por tipo de activo agrupado por similares características.

La evaluación de riesgos es el proceso que permite determinar y categorizar las amenazas potenciales y vulnerabilidades asociadas a activos de información. El resultado de este proceso permitirá determinar la identificación de controles que reducirán los riesgos.

7.1 . Identificación

La identificación de amenazas y vulnerabilidades sobre activos de información es importante para determinar cuáles tienden a degradar las propiedades de Disponibilidad, Integridad y Confidencialidad de la información.

Las amenazas pueden generarse de diferentes fuentes: amenazas externas e internas, usualmente las internas son de más alto riesgo, más aún cuando no se cuentan con medidas ni controles apropiados para mitigar el riesgo.

Tabla 3. Catálogo de Amenazas (MARGERIT)

Amenaza	Degradación del activo		
	Disponibilidad	Integridad	Confidencialidad
Desastres Naturales			
Fuego (Incedios)	x		
Daños por agua (Inundaciones)	x		
Desastres Naturales	x		
De origen industrial			
Fuego (Incedios)	x		
Daños por agua (Inundaciones)	x		
Desastres industriales	x		
Contaminación mecánica	x		
Contaminación electromagnética	x		
Avería de origen físico o lógico	x		
Corte del suministro eléctrico	x		
Condiciones inadecuadas de temperatura o humedad	x		
Fallo de servicios de comunicaciones	x		
Interrupción de otros servicios y suministros esenciales	x		
Degradación de los soportes de almacenamiento de la información	x		
Emanaciones electromagnéticas			x
Errores y fallos no intencionados			
Errores de los usuarios	x	x	x
Errores del administrador	x	x	x
Errores de monitorización (log)		x	
Errores de configuración		x	
Deficiencias en la organización	x		
Difusión de software dañino	x	x	x
Errores de [re-]encaminamiento			x
Errores de secuencia		x	
Escapes de información		x	x
Alteración accidental de la información		x	

Amenaza	Degradación del activo		
	Disponibilidad	Integridad	Confidencialidad
Destrucción de información	x		
Fugas de información			x
Vulnerabilidades de los programas (software)	x	x	x
Errores de mantenimiento / actualización de programas (software)		x	x
Errores de mantenimiento / actualización de equipos (hardware)	x		
Caída del sistema por agotamiento de recursos	x		
Pérdida de equipos	x		x
Indisponibilidad del personal	x		
Ataques intencionados			
Manipulación de los registros de actividad (log)		x	
Manipulación de la configuración	x	x	x
Suplantación de la identidad del usuario	x	x	x
Abuso de privilegios de acceso	x	x	x
Uso no previsto	x	x	x
Difusión de software dañino	x	x	x
[Re-]encaminamiento de mensajes			x
Alteración de secuencia		x	
Acceso no autorizado		x	x
Análisis de tráfico			x
Repudio		x	
Interceptación de información (escucha)			x
Modificación deliberada de la información		x	
Destrucción de información	x		
Divulgación de información			x
Manipulación de programas	x	x	x
Manipulación de los equipos	x		x
Denegación de servicio	x		
Robo	x		x
Ataque destructivo	x		
Ocupación enemiga	x		x
Indisponibilidad del personal	x		
Extorsión	x	x	x
Ingeniería social (picaresca)	x	x	x

El responsable del activo de información debe determinar; en base a sucesos, y la importancia que tiene el activo sobre las posibles amenazas y vulnerabilidades a las que está expuesto y realizar una descripción del escenario en el cual se puede dar la materialización de la amenaza, asumiendo que el responsable conoce y entiende los riesgos sobre el activo.

Una vulnerabilidad es toda aquella debilidad que presenta el activo de información, dada comúnmente por la inexistencia o ineficacia de un control.

Una amenaza es todo elemento que haciendo uso o aprovechando una vulnerabilidad, atenta o puede atentar contra la seguridad de un activo de información. Las amenazas surgen a partir de la existencia de vulnerabilidades, independientemente de que se comprometa o no la seguridad de un sistema.

Tabla 4. Ejemplo de Vulnerabilidades (NB7ISO/IEC 27005: 2010)

Tipo Activo	Vulnerabilidad
Equipamiento informático	Susceptibilidad a la humedad, el polvo y la suciedad
	Sensibilidad a la radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Copia no controlada
	Otras ...
Software - Aplicaciones informáticas	Defectos bien conocidos de software
	Ausencia de terminación de la sesión cuando se abandona la estación de trabajo
	Ausencia de pistas de auditoría
	Asignación errada de los derechos de acceso
	Software ampliamente distribuido
	Interfaz de usuario compleja
	Ausencia de documentación
	Configuración incorrecta de parámetros
	Tablas de contraseñas sin protección
	Habilitación de servicios innecesarios
	Software nuevo o inmaduro
	Especificaciones incompletas o no claras para los desarrolladores
	Ausencia de control de cambios eficaz
	Ausencia de copias de respaldo
	Otros...
Redes de comunicaciones	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Tráfico sensible sin protección
	Conexión deficiente de los cables
	Punto único de falla
	Ausencia de identificación y autentificación de emisor y receptor
	Arquitectura insegura de la red
	Transferencia de contraseñas en claro
	Gestión inadecuada de la red (Tolerancia a fallos en el enrutamiento)
	Otros...

Tipo Activo	Vulnerabilidad
Personal	Ausencia del personal
	Procedimientos inadecuados de contratación
	Entrenamiento insuficiente en seguridad
	Uso incorrecto de software y hardware
	Falta de conciencia acerca de la seguridad
	Ausencia de mecanismos de monitoreo
	Trabajo no supervisado de personal externo o de limpieza
	Ausencia de políticas para el uso de los medios de telecomunicaciones y mensajería
	Otros...
Instalaciones	Uso inadecuado o descuidado del control de acceso físico a las edificaciones o recintos
	Ubicación en un área susceptible de inundación
	Red energética inestable
	Ausencia de protección física de la edificación, puertas y ventanas
	Otros...

Podrían existir más vulnerabilidades, pero eso dependerá de los análisis anteriores (que deberán ser documentados) que permitieron revelar falencias para evitar la materialización de amenazas. Es importante aclarar que una amenaza se aprovecha de una o más vulnerabilidades, de ahí la importancia de identificar las vulnerabilidades.

Para identificar las vulnerabilidades se pueden utilizar métodos proactivos, tales como evaluación de vulnerabilidades, pruebas de intrusión a sistemas de información, servicios como el protocolo de transferencia de archivos (FTP), correo electrónico y otros, en busca de vulnerabilidades potenciales que pueden ser explotadas. Entre los métodos para este fin están:

- Herramientas automáticas de explotación de vulnerabilidades.
- Prueba y evaluación de la seguridad.
- Pruebas de penetración.

- Revisión de código.
- Errores intencionados.

Una vez determinadas las amenazas,vulnerabilidades y el escenario posible, el siguiente paso es la medición del nivel de riesgo en términos de la probabilidad que suceda el incidente (materialización de la amenaza) y el impacto ocasionado sobre el activo de información en las propiedades de disponibilidad, integridad y confidencialidad.

7.2 . Análisis y valoración

El propósito de analizar y valorar el riesgo es establecer el nivel de riesgo que cada amenaza conlleva al activo de información. La determinación del riesgo para cada par activo/amenaza resulta de:

- La probabilidad de que ocurra el incidente, es decir, que la amenaza explote la vulnerabilidad.
- La magnitud del impacto que el evento produce sobre el activo.

El cómputo de la probabilidad de ocurrencia del evento adverso suele basarse en los valores históricos de frecuencia con la que ocurre (o podría ocurrir) un evento (en un periodo determinado de tiempo, por ejemplo: anual, semestral. En caso de no contar con referencias históricas, se debe tomar la percepción que da el responsable del activo.

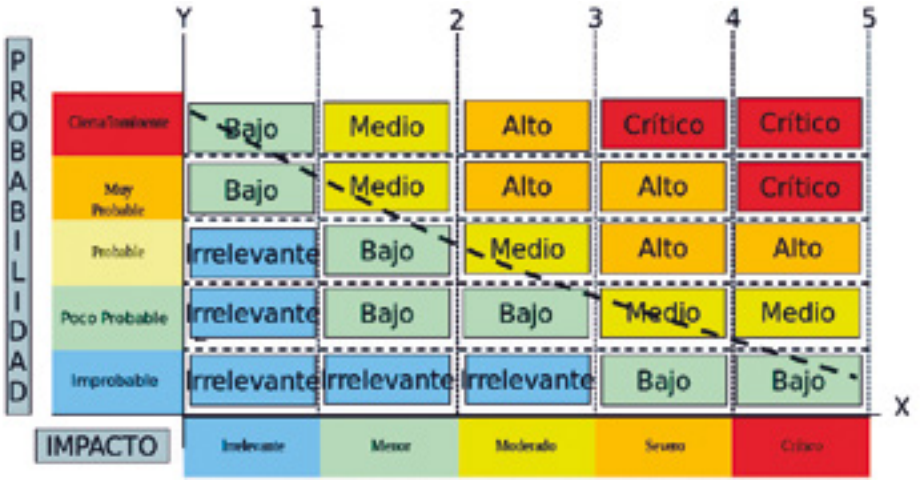
La valoración del riesgo se da en función de la probabilidad y el impacto ocasionado sobre el activo en escalas cualitativas.

Tabla 5. Valoración Cualitativa

ESCALAS	
Probabilidad	Impacto
Cierta/Inminente	Crítico
Muy Probable	Severo
Probable	Moderado
Poco Probable	Menor
Improbable	Irrelevante

La probabilidad y el impacto se combinan en una tabla para calcular y valorar el riesgo en una matriz de probabilidad versus impacto.

Figura 3. Matriz Para Valorar el Riesgo



La valoración cualitativa del riesgo no limita a la entidad o institución pública de utilizar valoraciones cuantitativas.

Los resultados de la valoración de riesgos con nivel "Crítico" deberían ser tratadas con prioridad, después los riesgos con nivel "Alto" y luego los riesgos con nivel "Medio", de acuerdo al enfoque de gestión de riesgos que se haya definido con antelación.

7.3 . Ejemplo de evaluación del riesgo

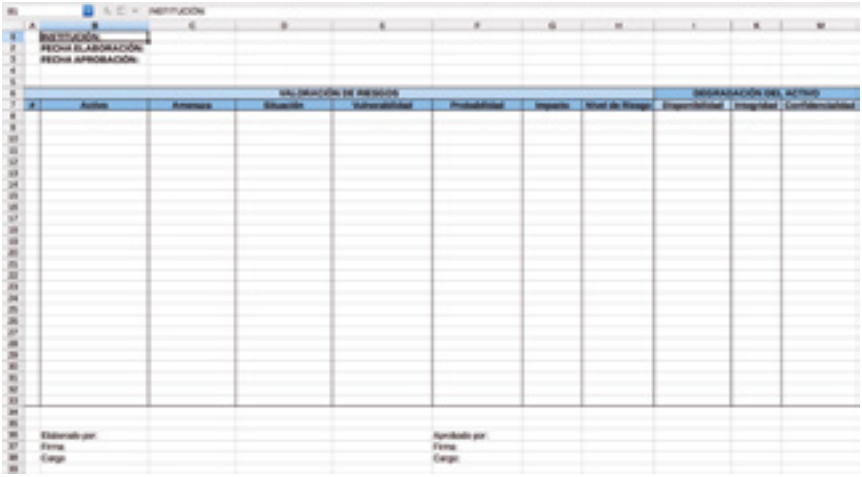
Suponiendo que el activo de información está en la categoría: Redes de comunicaciones.

Una amenaza identificada tiene relación a fallas eléctricas al menos una vez al mes. La frecuencia de dicha amenaza será Muy Probable y el impacto por causa del evento sobre el activo podría ser Severo. Si ocurre una inundación cada cuatro años, la frecuencia de dicha amenaza será Poco Probable y el impacto ocasionado si ocurriese el evento podría ser Crítico.

7.3.1 . Matriz de valoración del riesgo

Se sugiere una matriz para la valoración del riesgo en función de las amenazas y vulnerabilidades y el impacto por tipo de activo, según las características similares.

Figura 4. Matriz de Valoración del Riesgo



Por tipo de activo de información se debe identificar la(s) amenaza(s), vulnerabilidad(es), la situación en la que se produce la materialización de la amenaza, determinar la probabilidad y el impacto para establecer el nivel de riesgo del activo. Determinar la dimensión de afectación de las propiedades del activo (Disponibilidad, Integridad y Confidencialidad) marcando con una X.

El resultado de valorar el riesgo asociado a cada activo será la identificación de aquellos riesgos a ser tratados con prioridad mediante la aplicación de controles que mitiguen el riesgo. Esta determinación debe ir en el sentido de aplicabilidad y mitigación de los riesgos importantes, entendiendo de mayor importancia aquel riesgo “crítico” y menor el riesgo “irrelevante”.

8 . Tratamiento del riesgo

El tratamiento del riesgo implica tomar decisiones paraaceptar, reducir, retener, evitar o transferir los riesgos.

Aceptar el riesgo significa estar conscientes de la afectación que se produzca en caso de materializarse la amenaza o vulnerabilidad; para esto se deberían disponer de recursos ante una eventualidad. En el marco de la aceptación del riesgo, los que no sean considerados relevantes podrán ser excluidos de la selección de controles, pero se deberá incluir una justificación para no tratarlos.

Reducir el riesgo implica realizar un selección de Controles de Seguridad de la Información (ver Anexo A). O bien se pueden diseñar nuevos controles para cumplir con necesidades específicas que coadyuven a la reducción del riesgo.

Retener el riesgo implica establecer criterios para su aceptación, no es necesario implementar o seleccionar controles adicionales si el riesgo puede ser retenido.

El riesgo puede evitarse cuando estos se consideran muy altos, o si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios. Se puede tomar una decisión que logre evitar por completo el riesgo, mediante el retiro de una actividad, condiciones o conjunto de actividades ya sean planificadas o existentes. Esto deberá estar debidamente justificado y documentado.

Transferir el riesgo implica derivar de forma parcial o total a terceros que puedan gestionar de manera más eficaz el riesgo.

La decisión que se tome en cuanto al tratamiento de riesgos debe indicar la forma en que estos serán tratados; es decir, los controles que se aplicarán. Los lineamientos para la Elaboración del Plan Institucional de Seguridad de la Información indica ciertos controles mínimos que deben ser aplicados.

9 . Controles implementados y por implementar

Los listados de los controles implementados y por implementar vienen como consecuencia de la decisión de las opciones de tratamiento de riesgos y los controles de seguridad que se decidan implementar. Esta declaración no se limita a los controles mínimos requeridos, la cual puede incluir otros controles o medidas necesa-

rias para el tratamiento del riesgo (Ver punto 8).

Los controles implementados y por implementar deben indicar si un determinado control ya se ha implementado o no, junto con el medio de verificación que puede ser una referencia a documentación existente.

El listado permite ver de forma resumida aquellos controles mínimos requeridos y otros que se consideren necesarios. A continuación se muestra un cuadro que refleja los controles implementados y por implementar.

Tabla 6. Matriz de Controles Implementados y por Implementar

Control de Seguridad de la Información	Inclusión del Control	Control Existente	Justificación Inclusión	Justificación Exclusión	Documentación
Acuerdo de confidencialidad	Sí	No	Control mínimo requerido. Resultados de la evaluación de riesgos.		
Control de accesos	Sí	Sí	Control mínimo requerido. Resultados de la evaluación de riesgos.		Política de control de accesos. Procedimientos de altas y bajas de usuarios.
Uso de medios extraíbles	No	No		Aceptación del riesgo.	

ANEXO C

Guía para la gestión de incidentes de seguridad de la información

1. Introducción

Al implementar el Plan Institucional de Seguridad de la Información, la entidad debe planificar las acciones para responder ante incidentes que afecten a la seguridad de la información, fruto de errores intencionados o vulnerabilidades no contempladas en la evaluación de riesgos.

La gestión de incidentes llega a ser un control más para la seguridad de la información, porque entra en escena cuando los controles preventivos son ineficaces o están ausentes, sobre todo en aquellos riesgos, que luego de la valoración estos han sido asumidos, conscientes del riesgo que ello implica. Sobre los cuales se tienen que realizar monitoreos para mantener la seguridad en niveles aceptables.

Esta guía está basada en buenas prácticas de gestión de incidentes de la norma ISO/IEC 27035, pero la misma no obliga su adopción y la entidad o institución pública es libre de utilizar otro marco de trabajo.

2. Objetivo

Orientar sobre la planificación y organización del proceso de gestión de incidentes en seguridad de la información.

3. Referencias

La presente guía toma como referencia buenas prácticas en gestión de incidentes del estándar ISO/IEC 27035.

4. Documentos relacionados

La presente guía tiene relación con los siguientes documentos:

- Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público.
- Anexo A – Controles de Seguridad de la Información.

5. Términos y definiciones

Responsable de Seguridad de la Información.- Servidor público que tiene asignadas las funciones de desarrollar e implementar el Plan Institucional de Seguridad de la Información, que entre las responsabilidades está la de gestionar incidentes.

Evento de seguridad de la información.- Ocurrencia identificada de un estado de un sistema, servicio o red que indica que una posible violación de la política de seguridad de la información o la falla de controles o una situación previamente desconocida, que pueda ser relevante para la seguridad.[16]

Incidente de seguridad de la información.- Evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.[17]

6. Gestión de incidentes

La gestión de incidentes comprende la asignación de roles y responsabilidades para el desarrollo de actividades ante la ocurrencia de incidentes.

Una de las funciones del Responsable de Seguridad de la Información es la coordinación de acciones conjuntas con las partes interesadas para atención de incidentes.

El proceso de gestión de incidentes debe estar enmarcado en la mejora continua, que permita mejorar actividades para futuros incidentes. Los resultados de la gestión de incidentes deben ser documentados; esto permitirá analizar y realizar mejoras a controles existentes o implementar nuevos.

6.1. Planificación y preparación

Durante la planificación y preparación se debería considerar conformar un equipo de respuesta ante incidentes al interior de la entidad, liderado por el Responsable de Seguridad de la Información.

La planificación debe identificar y definir los elementos y recursos necesarios para

[16] Términos y Definiciones NB/ISO/IEC 27000:2010
[17] Términos y Definiciones NB/ISO/IEC 27000:201

cubrir actividades de gestión de incidentes. Una buena práctica es establecer procedimientos adecuados para el reporte por parte de los servidores públicos, seguido de programas de capacitación.

Contemplar actividades preventivas en la gestión de incidentes es una práctica que viene a minimizar la ocurrencia de los mismos, en la planificación se debería asegurar que los procedimientos para actividades críticas como respaldos, prevención de código malicioso, gestión de vulnerabilidades técnicas y otros se hagan efectivos, sobre todo la concientización y sensibilización al personal.

El RSI debe realizar el seguimiento de las actividades descritas anteriormente, para que cuando un evento ocurra, sea posible reanudar la continuidad de las operaciones en un tiempo oportuno.

Se deben definir canales de comunicación y puntos de contacto para reporte de incidentes y posterior atención, establecer procedimientos para el escalamiento de incidentes y su pronta resolución, además de elaborar directrices claras y entendibles para diferenciar entre un evento de seguridad y soporte técnico.

Una buena práctica en esta fase es clasificar los incidentes de acuerdo a las amenazas identificadas en el inventario de activos de información. La clasificación permite preparar acciones en caso de ocurrencia.

Algunos ejemplos de incidentes pueden relacionarse con:

- Accesos no autorizados
    - ◊ Acceso físico a instalaciones de procesamiento de información o áreas seguras.
    - ◊ Acceso lógico a información, servicios, sistemas, bases de datos y otros.
    - ◊ Inyección de contenido.
    - ◊ Puertas traseras.
    - ◊ Elevación de privilegios.
- Denegación de servicios

- ◊ Ataques de fuerza bruta.
- ◊ Ataques de denegación de servicio distribuido.
- ◊ Inundación SYN, ICMP, UDP, HTTP.

- Divulgación y pérdida de información
  - ◊ Ingeniería social.
  - ◊ Intencionada.
  - ◊ No intencionada.
  - ◊ Robo de documentación.
- Infección de malware
  - ◊ Virus.
  - ◊ Puertas traseras.
  - ◊ Ransomware.
  - ◊ Gusanos.
- Desfiguración de sitios
  - ◊ Cambio parcial o total del sitio web, sistemas y/o aplicaciones.
- Violación de la Política de Seguridad
  - ◊ Incumplimiento de la normativa.
  - ◊ Acciones premeditadas.
- Pérdida o robo de equipamiento
  - ◊ Dispositivos de red.
  - ◊ Periféricos.
  - ◊ Estaciones de trabajo.

- Correo electrónico
    - ◊ Suplantación de correo.
    - ◊ Spam.
- Otros Incidentes

6.2. Detección y reporte

En esta fase el Responsable de Seguridad de la Información, junto con los responsables de activos de información, deben establecer criterios que permitan detectar un posible evento de seguridad e implementar mecanismos de registro del suceso para posterior análisis.

El Responsable de Seguridad de la Información debe realizar el reporte formal de eventos de seguridad y los procesos de escalamiento que se puedan tener.

Los servidores públicos deberían conocer las responsabilidades que tienen con la seguridad de la información y la obligación de reportar la ocurrencia de incidentes producto de la violación de las políticas, omisión de procedimientos e identificación de vulnerabilidades. La entidad o institución debería establecer medios como el correo electrónico, números de teléfono, personas de contacto, implementación de sistemas de atención y seguimiento de incidentes.

Identificar distintas fuentes de detección como ser: software antivirus, reporte de usuarios, alertas por correo sobre caídas de servicio y otros convenientes. Esta información a corto plazo permitirá redefinir los procedimientos para minimizar el impacto, pero no solo basta detectar el incidente, también es importante implementar mecanismos que permitan la identificación y análisis en detalle, como pueden ser los registros de logs en el caso de servidores.

6.3. Valoración y decisión

Una vez detectado un incidente, el siguiente paso debe ser el análisis, valoración y decisión sobre las acciones a realizar. Los responsables de infraestructuras tecnológicas y responsables de procesos deben conocer la funcionalidad normal de los procesos para determinar la confirmación de un incidente.

Para la valoración se debería contar con la mayor cantidad de información posible para realizar el análisis, correlación de sucesos, patrones de comportamiento, consultar incidentes pasados y otros. La evaluación debe contar con escalas para medir el impacto y prioridad que se le dará al incidente; se recomienda que las escalas estén en función de valores establecidos en la evaluación de riesgos.

Ejemplo 1. Escala de Impacto

Escala	Definición
Bajo	La incidencia no afecta a un servicio crítico de la institución pública.
Medio	La incidencia tiene efectos mínimos sobre sistemas críticos. La institución pública puede proporcionar servicios críticos.
Alto	La incidencia tiene efecto significativo e inmediato sobre los sistemas críticos de la institución pública.
Crítico	Graves efectos en los sistemas críticos de la institución pública que impiden la continuidad de los servicios que esta proporciona.

Se deben establecer niveles de impacto ocasionado y actuar en consecuencia; el nivel puede ser el mismo que se ha definido para la evaluación de riesgos u otro. En este punto se debe haber definido previamente la clasificación de tipos de incidentes.

Se sugiere la siguiente clasificación:

Ejemplo 2. Clasificación de Incidentes

Tipo de incidente	Descripción
Acceso no autorizado	Acceso a información protegida implícita o explícita, provocando la degradación de información y otros.
Ataques por vulnerabilidades	En esta clasificación ingresarían los ataques por inyección sql, xss, redirecciones, envenenamiento de DNS, envenenamiento ARP, ataques de día cero y otros.
Código malicioso	En esta clasificación ingresan los virus, troyanos, puertas traseras, rootkits, keyloggers, ransomware y otros.
Denegación de servicio	Ingresan toda la gama de ataques de denegación de servicios como ser : DdoS, inundación SYN, ICMP, UDP y otros.
Desfiguración de sitio	Defacement total o parcial de sitios web y otros.
Divulgación de información	Ataques de ingeniería social, espionaje, phishing y otros.
Fallas de hardware o infraestructura tecnológica	Fallas de hardware, infraestructura tecnológica y otras.

Para la adecuada respuesta a incidentes se debe establecer el nivel de prioridad para los mismos, esto permitirá atender el incidente en función de criticidad y utilizar los recursos necesarios para contener y recuperar los servicios que se vean afectados. Se sugiere utilizar la siguiente escala:

Ejemplo 3. Escala de Prioridades

Prioridad	Descripción
Baja	Sistemas o servicios que tienen un impacto potencial de poca consideración.
Media	Sistemas o servicios que tienen relación con otros y esta provoca una afectación parcial en las mismas.
Alta	Sistemas o servicios relacionados al área de infraestructura tecnológica.
Crítico	Sistemas o servicios críticos para la entidad o institución pública.

También es buena práctica establecer tiempos de respuesta para la atención de incidentes, esto dependerá de la escala de prioridades y categorización; la pre-

sente guía no pretende establecer los mismos y deja a consideración de la entidad su definición.

En esta etapa se deben establecer procedimientos para escalar el incidente al Centro de Gestión de Incidentes Informáticos.

6.4. Respuesta y erradicación

La respuesta hace efectiva las actividades previamente descritas; para esto es necesario documentar las acciones que se vayan a realizar. Las actividades adicionales a la respuesta del incidente son: analizar posibles daños colaterales por la propagación del incidente que provoque afectación a la información o infraestructura tecnológica; para esto en la planificación se debería contar con procedimientos de acción para determinado incidente aunque no siempre se puede predecir el evento, pero tomar las previsiones ya es una ventaja.

Ejemplo 4. Posibles Acciones por Tipo de Incidente

Tipo de incidente	Causas comunes	Posibles acciones de respuesta
Acceso no autorizado	Acceso físico: Las causas comunes son la permisividad e inexistencia de control de instalaciones internas. Estas pueden ser por personas internas y externas. Acceso lógico: Configuraciones por defecto, errores de aplicación, vulnerabilidades o parches de seguridad no aplicados, entre otros.	Identificar a la persona que infringe la normativa interna, indagar motivos por los cuales se encuentra en instalaciones sin autorización, identificar causas que permitieron su ingreso. Para el acceso lógico es algo más complejo; las acciones a tomar dependerán del tipo y gravedad del incidente. Revisión de registros, recuperar el servicio afectado, correlación de accesos, permisos, horas, nombres de usuario, origen y otros.
Ataques por vulnerabilidades	Vulnerabilidades de día cero, versiones de aplicación desactualizadas o descontinuadas, entre otros.	Identificar el sistema y/o servicio afectado; contar con respaldos de información; dependiendo de la gravedad , detener el servicio; restaurar configuraciones e información anteriores.

Tipo de incidente	Causas comunes	Posibles acciones de respuesta
Código malicioso	Campañas de phising, uso descontrolado de dispositivos de almacenamiento, acceso a páginas sospechosas, vulnerabilidades a nivel de red que faciliten la propagación.	Identificar el tipo de código malicioso, aislar equipos comprometidos de la red, monitoreo del tráfico de red. Analizar el comportamiento del código malicioso, entre otras acciones.
Denegación de Servicio	Generalmente ocurren por motivos intencionados que buscan restringir el acceso y disponibilidad de servicios, aprovechando cambios incontrolados de configuración, mal funcionamiento de hardware, incidentes no intencionados, errores incontrolados en sistemas y otros.	Identificar el origen del ataque y bloquear el mismo; esto si no se trata de una denegación distribuida. Para su prevención se recomienda implementar reglas para identificar y bloquear automáticamente estos ataques.
Desfiguración de sitios web	Debido principalmente a vulnerabilidades en aplicación y servidor, como ser contraseñas débiles.	Acciones preventivas: copias de respaldo del sitio completo, archivo de la página principal en texto plano html. Acciones correctivas: extraer una o varias copias completas del sitio, reemplazar el archivo en texto plano. En estos casos el objetivo principal es restablecer la página original.
Divulgación de información	Accesos no autorizados a instalaciones con información sensible expuestas en lugares visibles sin seguridad.	Este tipo de incidentes debe tener tratamiento especial, porque la finalidad no es restablecer servicios. Las acciones deberían estar orientadas al análisis de las causas, origen y responsables, para prevenir futuros incidentes.

Todas las acciones deberían estar dirigidas a restablecer el servicio en los tiempos establecidos.

Después de que el incidente haya pasado y se hayan restablecido los servicios, se debería realizar la erradicación del problema adoptando estrategias de erradicación. Esto consiste en analizar las posibles consecuencias del incidente como ser: código malicioso que puede estar oculto, configuraciones del servidor y otras que, dependiendo del tipo de incidente, se pueden analizar otros servicios relacionados de forma directa o indirecta.

La respuesta al incidente debería finalizar con un informe que documente las actividades realizadas. La experiencia adquirida deberá permitir mejorar las acciones de respuesta para futuros incidentes con similar característica.

La gestión de incidentes es parte integral de la seguridad, ya que se pueden identificar debilidades en los controles y mejorar los mismos, con la modificación o la implementación de nuevos controles.

En caso de existir un incidente crítico que afecte la imagen institucional, se deberá designar un encargado de comunicar y otorgar información como portavoz autorizado.

6.5. Mejora continua

La experiencia adquirida en la atención al incidente, así como toda la información obtenida durante la atención, deberá permitir elaborar un plan de acción de mejora continua.

Un proceso de mejora continua debe ser aplicado para la respuesta al seguimiento, evaluación y en general a la gestión de incidentes de seguridad de la información, que permita que los responsables entiendan las prioridades de la institución para manejo de incidentes.

El objetivo de este plan de acción no deberá ser en ningún caso un objetivo de auditoría o de búsqueda de responsables, más al contrario el plan deberá fortalecer la seguridad de la entidad o institución pública para evitar la repetición de incidentes similares en el futuro.


AGETIC
agencia de gobierno electrónico y
tecnologías de información y comunicación