ANEXO

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION (EGSI)

Versión 3.0

"Sistema de Gestión de Seguridad de la Información para las Instituciones del Sector Público"

INTRODUCCIÓN

La masificación de los servicios con la ayuda de las tecnologías de la información, ha transformado a la información, y lo ha convertido en uno de los activos más valiosos para las instituciones del sector público, la pérdida, la exposición no autorizada o la corrupción de la información pueden tener consecuencias importantes, como pérdida de confianza de la ciudadanía, procesos legales y en general daño a la reputación de las instituciones.

La seguridad de la información garantiza la confidencialidad, disponibilidad e integridad de la información; involucra la aplicación y gestión de controles apropiados considerando las amenazas existentes, con el objetivo de minimizar el impacto ocasionado por los incidentes de seguridad de la información y garantizar la continuidad del negocio.

La seguridad de la información se consigue mediante la implementación de un conjunto de controles aplicables, seleccionados a través de un adecuado proceso de gestión de riesgos y gestionados mediante un Sistema de Gestión de Seguridad de la Información.

El Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, como ente rector de la seguridad de la información y cumpliendo su potestad en el establecimiento de políticas, directrices y planes aplicables en tal área para el desarrollo de la sociedad de la información; ha desarrollado el Esquema Gubernamental de Seguridad de la Información - EGSI v3, como un Sistema de Gestión de Seguridad de la Información para las Instituciones del Sector Público, que establece un conjunto de recomendaciones para la gestión de la seguridad de la información y ejecuta un proceso de mejora continua.

Esta actualización responde a las necesidades estratégicas que actualmente tienen las instituciones del sector público, con la interrelación entre la ciberseguridad, seguridad de la información y protección de la privacidad; proporcionando una comprensión más profunda de cómo implementar y mantener un sistema de gestión de seguridad de la información efectivo, lo que ayudará a la institución a proteger su información y mantener la confianza de la ciudadanía en los servicios públicos.

En consecuencia el Esquema Gubernamental de Seguridad de la Información (EGSI) es una norma técnica con un enfoque ordenado y estructurado diseñado para proteger la confidencialidad, integridad y disponibilidad de la información sensible y crítica de las instituciones del sector público del Ecuador; proporcionando un marco adecuado que permita gestionar eficazmente los riesgos de seguridad de la información, establecer políticas y procedimientos claros además de fomentar una cultura de seguridad.

El EGSI v3 está estructurado por tres guías, cada una hace referencia a los estándares más importantes para la gestión de la seguridad de la información:

- Guía para la implementación del EGSI: en esta guía se proporciona los lineamientos y requisitos para establecer, implementar y mantener el mejoramiento continuo del Esquema (basado en la NTE INEN ISO/IEC 27001).
- Guía para la gestión de riesgos de seguridad de la información: en esta guía se proporciona una metodología para la gestión de los riesgos de seguridad de la información (basado en la NTE INEN ISO/IEC 27005 y la metodología MAGERIT).
- Guía para la implementación de controles de seguridad de la información: esta guía está diseñada para que las instituciones la usen como referencia a la hora de seleccionar controles dentro del proceso de implementación del Esquema (basado en la NTE INEN ISO/IEC 27002).

El EGSI es un recurso invaluable para proteger la información y salvaguardar los intereses de la institución, en una sociedad digitalmente interconectada; este esquema tiene como objetivo, preservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos de seguridad de la información y la selección de controles para el tratamiento de los riesgos identificados.

ANEXO A

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

INTRODUCCIÓN

Esta guía le proporciona los requisitos para establecer, implementar y mantener el mejoramiento continuo del Esquema Gubernamental de Seguridad de la Información, que es el Sistema de Gestión de Seguridad de la información para las instituciones del Sector Público.

El establecimiento y la implementación del Esquema Gubernamental de Seguridad de la Información son determinados por las necesidades y objetivos de la institución, la criticidad de la información, los requisitos de seguridad, los procesos utilizados, y la estructura de la institución.

El Esquema Gubernamental de Seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de una adecuada evaluación de riesgos de seguridad de la información, que permite la selección e implementación de controles para modificar los riesgos identificados y proveer de servicios seguros a la ciudadanía.

OBJETIVO

Proveer las directrices a las instituciones del Sector Público, para que comiencen y mantengan la implementación del Esquema Gubernamental de Seguridad de la Información mediante un proceso constante de mejora continua.

RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS INSTITUCIONES DEL SECTOR PUBLICO.

La asignación de responsabilidades se definió en los artículos 5, 6, 7, 8 y 9 del acuerdo ministerial, sin embargo, en esta guía se esclarece la los roles y responsabilidades de los actores claves en la implementación y mejora continua del EGSI.
Queda a criterio institucional el realizar ampliaciones, a las responsabilidades definidas, de acuerdo a su necesidad, para cumplir con la implementación del EGSI.

Máxima autoridad (Alta dirección)

Es responsabilidad de la máxima autoridad de cada institución, conformar la **Estructura de Seguridad de la Información Institucional**, con personal formado y experiencia en gestión de seguridad de la información, así como asignar los recursos necesarios.
Además, deberá designar al interior de la Institución:

1. Al Comité de Seguridad de la Información (CSI) y;
2. Al Oficial de Seguridad de la Información (OSI).

Oficial de Seguridad de la Información (OSI)

La máxima autoridad designará al interior de su Institución a un funcionario como Oficial de Seguridad de la Información (OSI), será:

El responsable de la implementación y mejora continua del EGSI, así como el de coordinar las acciones del Comité de Seguridad de la Información en relación a la implementación y cumplimiento del Esquema Gubernamental de Seguridad de la Información.

El Oficial de Seguridad de la Información debe tener formación o especializado y con experiencia de al menos 2 años en áreas de seguridad de la información, ciberseguridad, de preferencia del nivel jerárquico superior, podrá ser el responsable del área de Seguridad de la Información (en el caso de existir) y no debe pertenecer a las áreas de procesos, riesgos, administrativo, financiero y tecnologías de la información.

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

Dentro de sus principales responsabilidades se encuentra:

a) Identificar y conocer la estructura organizacional a través del estatuto por procesos de la institución.
b) Identificar las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI:

    - *Identificar convenientemente las partes interesadas relacionadas con el negocio y en especial con la seguridad de la información.*
    - *Identificar los requisitos / necesidades de las partes interesadas.*
    - *Identificar los canales de comunicación con las partes interesadas especialmente con las autoridades y grupos de interés especiales.*

c) Implementar y actualizar del Esquema Gubernamental de Seguridad de la Información EGSI.
d) Elaborar y coordinar con las áreas respectivas las propuestas para la elaboración de la documentación esencial del Esquema Gubernamental de Seguridad de la Información (EGSI).

Para la elaboración del OSI

- *Alcance de Implementación*
- *Política de Seguridad de la información*
- *Proceso de gestión de riesgos*
- *Declaración de aplicabilidad*
- *Plan de gestión de riesgos*
- *Objetivos de Seguridad de la Información*
- *Informes de evaluación y de gestión de riesgos*
- *Procedimiento de respuesta a incidentes*
- *Registros de capacitaciones, habilidades, experiencia y cualificaciones*
- *Reportes, seguimiento y mediciones*
- *Programa o plan de auditoría interna*
- *Resultados de la Auditoría Internas*

- *Resultado de las revisiones por parte de la dirección o de las autoridades*
- *Registros de las actividades de usuarios*

Para coordinar con las áreas respectivas

- *Inventario de activos*
- *Uso aceptable de los activos*
- *Requisitos reglamentarios y contractuales*
- *Procedimientos Operativos de Seguridad para la Gestión de TI*
- *Definición de roles y responsabilidades de seguridad de la información*
- *Política de control de accesos*
- *Definición de configuraciones de seguridad*
- *Principios de ingeniería de sistemas seguros*

NOTAS:

- La documentación listada anteriormente es la esencial no siendo la única
- Proceso de gestión de riesgos en la versión anterior se conocía como Metodología de gestión de riesgos,
- Plan de gestión de riesgos en la versión anterior se le conocía como Plan de tratamiento de riesgos

e) Elaborar, asesorar y coordinar con los funcionarios, la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas:

- *Formación interna a los funcionarios propietarios de los activos de información, para que colaboren en la realización de la evaluación de riesgos*
- *Coordinar el proceso de evaluación del riesgo.*
- *Proponer la selección de controles para el tratamiento del riesgo.*
- *Proponer plazos de aplicación para los controles.*
- *Es deber del OSI identificar los procedimientos de seguridad de la información específicos, que fortalezcan la política de seguridad de la información institucional.*

f) Elaborar y coordinar el Plan de concienciación en Seguridad de la Información basado en el Esquema Gubernamental de Seguridad de la Información (EGSI), con las áreas involucradas que intervienen y en coordinación con el área de comunicación institucional.

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

g) Fomentar la cultura de seguridad de la información en la institución, en coordinación con las áreas respectivas.

h) Elaborar el plan de seguimiento y control de la implementación de las medidas de mejora o acciones correctivas, y coordinar su ejecución con las áreas responsables.

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

i) Coordinar la elaboración de un Plan de Recuperación de Desastres (DRP), con el área de TI y las áreas clave involucradas, para garantizar la continuidad de las operaciones institucionales ante una interrupción:

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

j) Elaborar el procedimiento o plan de respuesta para el manejo de los incidentes de seguridad de la información presentados al interior de la institución.

k) Coordinar la gestión de incidentes de seguridad de la información con nivel de impacto alto y que no pudieran ser resueltos en la institución, a través del Centro de Respuestas a Incidentes Informáticos (CSIRT) sectorial y/o nacional.

l) Coordinar la realización periódica de revisiones internas al Esquema Gubernamental de Seguridad de la Información – (EGSI), así como, dar seguimiento en corto plazo a las recomendaciones que hayan resultado de cada revisión.

m) Mantener toda la documentación generada durante la implementación, seguimiento y mejora continua del EGSI, debidamente organizada y consolidada, tanto políticas, controles, registros y otros.

n) Coordinar con las diferentes áreas que forman parte de la implementación del Esquema Gubernamental de Seguridad de la Información, la verificación, monitoreo y el control del cumplimiento de las normas, procedimientos políticas y controles de seguridad institucionales establecidos de acuerdo a las responsabilidades de cada área.

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

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

p) Previa la terminación de sus funciones el Oficial de Seguridad de la información realizará la entrega recepción de la documentación generada al nuevo Oficial de Seguridad de la información, y de la transferencia de conocimientos propios de la institución adquiridos durante su gestión, en caso de ausencia, al Comité de Seguridad

de la Información; procedimiento que será constatado por la unidad de talento humano, previo el cambio y/o salida del oficial de seguridad de la información.

q) Administrar y mantener el EGSI mediante la definición de estrategias políticas normas y controles de seguridad, siendo responsable del cumplimiento el propietario de la información del proceso.

r) Actuar como punto de contacto del Ministerio de Telecomunicaciones y de la Sociedad de la Información.

Comité de Seguridad de la Información (CSI)

La máxima autoridad designará al interior de la Institución, un Comité de Seguridad de la Información (CSI), que estará integrado por los responsables de las siguientes áreas o quienes haga sus veces: Planificación quien lo presidirá, Talento Humano, Administrativa, Comunicación Social, Tecnologías de la Información, Jurídica y el Delegado de protección de datos.

El Oficial de Seguridad de la Información asistirá a las reuniones del comité de seguridad de la información con voz, pero sin voto.

Los representantes de los procesos Agregadores de Valor asistirán a las reuniones del comité, cuando se trate información propia de su gestión.

Las instituciones del sector público que no cumplan con estas características, deberán identificar el modelo que corresponda a la institución en la conformación del comité de seguridad de la información, con al menos tres integrantes garantizando su funcionalidad.

El CSI es responsable de garantizar y facilitar la implementación de las iniciativas de seguridad de la información en la institución; y ser el responsable del control y seguimiento en su aplicación.

El Comité en la primera convocatoria designará un presidente, definirá su agenda y su reglamento interno.

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

El Comité tendrá como principales responsabilidades:

a) Establecer los objetivos de la seguridad de la información, alineados a los objetivos institucionales.

b) Gestionar la implementación, control y seguimiento de las iniciativas relacionadas a seguridad de la información.

- Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).
- Realizar el seguimiento a los indicadores de gestión definidos, para el buen funcionamiento del EGSI.

c) Gestionar la aprobación de la política de seguridad de la información institucional, por parte de la máxima autoridad de la Institución.

d) Aprobar las políticas específicas internas de seguridad de la información, que deberán ser puestas en conocimiento de la máxima autoridad.

e) Realizar el seguimiento del comportamiento de los riesgos que afectan a los activos y recursos de información frente a las amenazas identificadas.

f) Conocer y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto de acuerdo a la categorización interna de incidentes.

g) Coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios, con base al EGSI.

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

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

j) El comité deberá reunirse ordinariamente de forma bimestralmente y extraordinariamente en cualquier momento previa convocatoria

k) Informar semestralmente a la máxima autoridad los avances de la implementación y mejora continua del Esquema Gubernamental de Seguridad de la Información (EGSI).

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

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)[1]

El Sistema de Gestión de Seguridad de la Información unifica los criterios para la evaluación de los riesgos asociados al manejo de la información institucional.

[1] Basado en la norma NTE-INEN-ISO-IEC-27001

PRINCIPIOS

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

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

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

BENEFICIOS

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

- Establece una metodología de Gestión de la Seguridad estructurada y clara.
- Reduce el riesgo de pérdida, robo o integridad de la información sensible.
- Los riesgos y los controles son continuamente revisados.
- Facilita la identificación y gestión de riesgos de seguridad de la información, lo que reduce la probabilidad de incidentes de seguridad.
- Se garantiza la confianza de los usuarios en los servicios institucionales.
- Facilita la integración con otros sistemas de gestión.
- Se garantiza la continuidad de negocio tras un incidente grave.
- Fortalece la capacidad de la institución para resistir y recuperarse de incidentes de seguridad, mejora la resiliencia.
- Cumple con la legislación vigente sobre transformación digital, protección de datos, propiedad intelectual y otras.
- La imagen de la institución mejora, por lo tanto, su competitividad.
- Aumenta la confianza y las reglas claras para los miembros de la institución, socios comerciales y en general para las partes interesadas.
- Ayuda a crear una cultura de seguridad en toda la institución.
- Reduce los costes y la mejora de los procesos y el servicio.
- Se incrementa la motivación y la satisfacción del personal.
- Aumenta la seguridad en base la gestión de procesos en lugar de una compra sistemática de productos y tecnologías.

- Fomenta la mejora continua al establecer un ciclo de revisión y actualización constante de políticas y procedimientos de seguridad.
- Prepara a la institución para adaptarse a nuevas amenazas y desafíos en el entorno de ciberseguridad en constante evolución.

CICLO DE VIDA (modelo PDCA)

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

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

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

ISO 27001:2022 & EL CICLO PDCA (Estructura General)						
PLAN/PLANEAR				DO/HACER	CHECK/VERIFICAR	ACT/ACTUAR
4. Contexto de la Organización	5. Liderazgo	6. Planificación	7. Soporte	8. Operación	9. Evaluación del desempeño	10. Mejora
Entendiendo la organización y su contexto	Liderazgo y Compromiso	Acciones para abordar riesgos y oportunidades	Recursos	Control y Planificación Operacional	Monitoreo, medición, análisis y evaluación.	Acciones correctivas y no conformidades
Expectativa de las partes interesadas	Política		Competencias			
Alcance del SGSI		Objetivos de S.I. y planes para alcanzarlos.	Concienciación	Evaluación de riesgos de seguridad de la Información	Auditoría interna	Mejora continua
SGSI	Organización, roles, responsabilidades y autoridades		Comunicación		Revisión de gestión	
				Tratamiento de riesgos de seguridad de la Información		
			Información Documentada			

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

PROCESO PDCA ASOCIADO AL ESTANDAR INTERNACIONAL ISO 27001

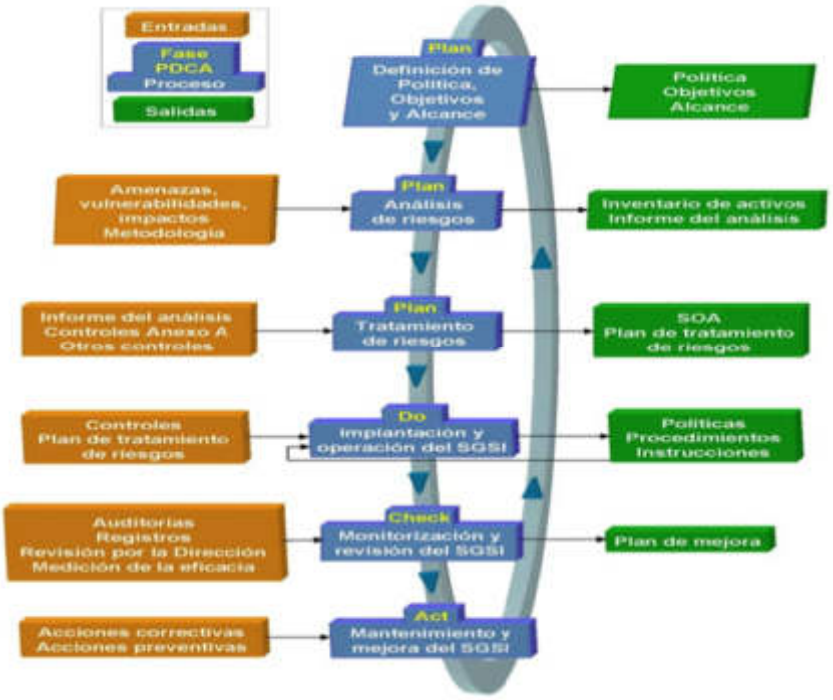

Figura No.4, PROCESO PDCA-ISO27001, Fuente: http://www.iso27000.es/sgsi.html

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

MEJORA CONTINUA

Una vez que las instituciones realizaron el proceso de implementación inician el ciclo de mejora continua.

La mejora continua implica realizar una revisión general de lo que se ha implementado, es decir: revisión de la política de seguridad si sigue siendo eficaz, cumple con los objetivos de seguridad, si los riesgos cambiaron son aceptables, cambios en el contexto organizacional, resultado de las evaluaciones, no conformidades, acciones correctivas, entre otros.

La mejora continua en el Esquema Gubernamental de Seguridad de la Información (EGSI) es un proceso esencial para garantizar que los datos y la información estén protegidos de manera efectiva, para lo cual es recomendable observar entre otras las siguientes consideraciones:

- Compromiso de la máxima autoridad con la mejora continua.
- Políticas y procedimientos actualizados.
- Formación y concienciación a los funcionarios de la institución.
- Monitorización y detección de amenazas.

- Proceso sólido de gestión de incidentes.
- Auditorías internas y externas.

La mejora continua en el EGSI es un proceso cíclico y constante. A medida que evolucionan las amenazas, los riesgos cambian en la institución, por lo cual es fundamental adaptarse y mejorar constantemente para proteger los activos de información de manera efectiva.

ANEXO B

GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN[2]

INTRODUCCIÓN

La revolución digital ha provocado que las organizaciones a nivel global pongan mayor atención en la información que se genera, actor principal de este proceso de cambio; el cual ha permitido establecer nuevas alianzas y acortar distancias entre naciones, donde el internet cumple un papel fundamental en la comunicación.

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

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

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

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

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

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

CONCEPTOS BÁSICOS

La información es el activo principal pero también debemos considerar: infraestructura informática, equipos auxiliares, redes de comunicaciones, instalaciones y personas.
Cuando hablamos de seguridad de la información hablamos de protegerla de riesgos que puedan afectar a una o varias de sus tres principales propiedades:

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

[2] Basado en la norma ISO-IEC-27005:2022

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

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

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

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

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

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

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

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

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

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

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

Si la evaluación de riesgos proporciona información suficiente para determinar eficazmente las acciones necesarias para modificar los riesgos a un nivel aceptable, entonces la tarea está completa y sigue el tratamiento del riesgo. Si la información es insuficiente, se debe realizar otra iteración de la evaluación de riesgos.

El tratamiento de riesgos implica también un proceso iterativo, es posible que dicho tratamiento no conduzca inmediatamente a un nivel aceptable de riesgos residuales, en este caso se puede realizar otro intento de encontrar un tratamiento de riesgo adicional o ejecutar otra iteración de la evaluación de riesgos en su totalidad o en partes.

El conocimiento sobre las amenazas o vulnerabilidades relevantes puede conducir a mejores decisiones sobre las actividades adecuadas de tratamiento de riesgos en la siguiente iteración de la evaluación de riesgos.

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

- Establecimiento del contexto
- Evaluación del riesgo
- Tratamiento del riesgo
- Comunicación y consulta de los riesgos
- Seguimiento y revisión del riesgo
- Información documentada

Pasos de las actividades del proceso de gestión del riesgo:

PROCESO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN	
ACTIVIDADES	**PASO**
Establecimiento del contexto	*1. Consideraciones Generales organizativas - Levantamiento de información inicial, definición del alcance* *2. Establecer criterios básicos de las partes interesadas* *3. Aplicación de la evaluación de riesgos* *4. Establecer y mantener criterios de riesgos de seguridad de la información*
Evaluación del Riesgo	*Identificación del riesgo* *5. Identificar Activos de Información* *6. Identificar las amenazas y las vulnerabilidades* *7. Identificar los controles existentes* *Análisis de riesgos* *8. Identificar consecuencias* *9. Evaluación de las consecuencias* *10. Evaluación de la probabilidad de incidentes* *11. Determinar el nivel de riesgo* *Valorar el riesgo*
Tratamiento del Riesgo	*12. Seleccionar controles*
Comunicación y consulta del Riesgo	*13. Comunicar y consultar el riesgo con las partes interesadas externas e internas en todas las etapas del proceso de gestión del riesgo*
Seguimiento y Revisión del Riesgo	*14. Monitorear y revisión de los riesgos*
Información Documentada	*15. Mantener Información documentada sobre el proceso de evaluación de riesgos*

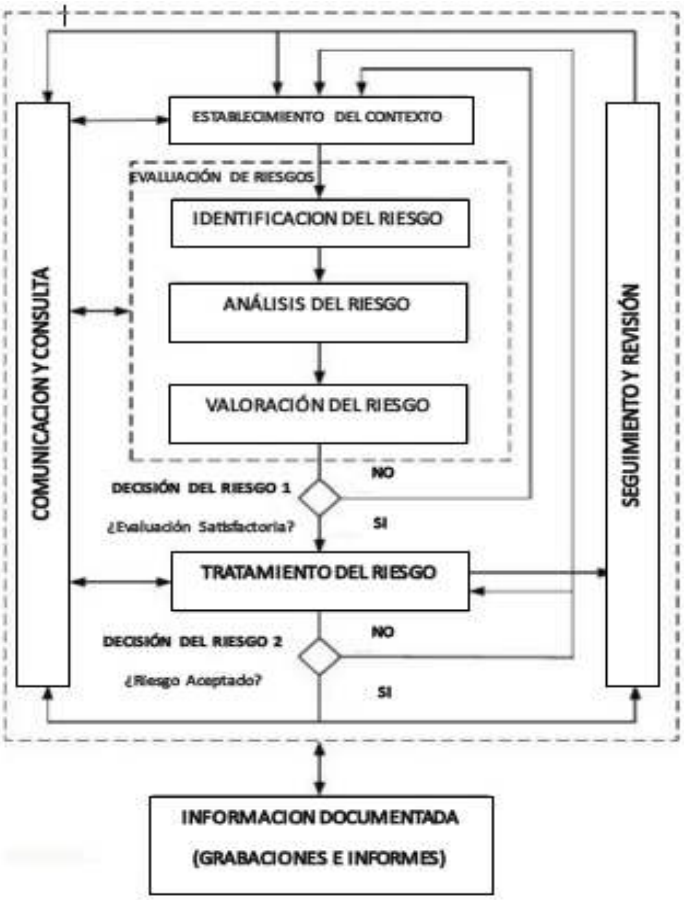

Figura No. 2 PROCESO DE GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN, Fuente: ISO27005

ESTABLECIMIENTO DEL CONTEXTO

CONSIDERACIONES GENERALES

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

CRITERIOS BÁSICOS

Dependiendo del alcance y los objetivos de la gestión del riesgo, se pueden aplicar diferentes enfoques. El enfoque también podría ser diferente para cada iteración.
Se debe seleccionar o desarrollar un enfoque apropiado de gestión del riesgo que aborde los criterios básicos tales como: criterios de valoración del riesgo, criterios de impacto, criterios de aceptación de riesgos, entre otros.

Criterios de identificación del riesgo

Es recomendable considerar los activos de información con el valor de impacto alto para el

proceso de evaluación del riesgo.

Criterios de valoración del riesgo

Es recomendable desarrollar criterios de valoración de riesgos para evaluar el riesgo de la seguridad de la información de la institución.

Criterios de impacto

Los criterios de impacto deben desarrollarse y especificarse en términos del grado de daño o costos para la institución, causados por un evento de seguridad de la información.

Criterios de la aceptación del riesgo

Se deben desarrollar y especificar criterios de aceptación de riesgos, a menudo dependen de las políticas, metas, objetivos y de las partes interesadas de la institución.

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

ALCANCE Y LÍMITES

Es necesario definir el alcance del proceso de gestión de riesgos de seguridad de la información con el fin de garantizar que todos los activos relevantes se tengan en cuenta en la evaluación de riesgos, además, se necesita identificar los límites para abordar aquellos riesgos que pueden surgir a través de estos límites.

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

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

ORGANIZACIÓN PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

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

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

EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

"Los riesgos se deben identificar, describir cuantitativa o cualitativamente y priorizarse frente a los criterios y objetivos de valoración de riesgos relevantes para la institución"

Un riesgo es una combinación de las consecuencias que se derivarían de la ocurrencia de un evento no deseado y de la probabilidad de que ocurra el evento. La evaluación de riesgos cuantifica o describe cualitativamente el riesgo y permite a los propietarios de los activos priorizar los riesgos de acuerdo con su gravedad percibida u otros criterios establecidos.

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

riesgos"

La evaluación del riesgo consta de las siguientes actividades:

- Identificación de riesgos
- Análisis de riesgos
- Valoración de riesgos

IDENTIFICACIÓN DEL RIESGO

Consiste en determinar qué puede provocar pérdidas a la institución afectando la consecución de sus objetivos de seguridad de la información. Existen dos enfoques para la identificación del riesgo.

Enfoque basado en eventos: identificar escenarios de alto nivel o estratégicos a través de una consideración de las fuentes de riesgo y como utilizan o impactan a las partes interesadas para alanzar el objetivo deseado de esos riesgos.

Enfoque basado en activos: identificar escenarios operativos, que se detallan en términos de activos, amenazas y vulnerabilidades.

En la presente guía se utiliza el enfoque basado en activos, es decir, los riesgos se identifican y evalúan mediante una inspección de activos, amenazas y vulnerabilidades de acuerdo a los siguientes pasos:

- Identificación de los activos
- Identificación de las amenazas
- Identificación de vulnerabilidades
- Identificación de controles existentes.

Identificación de los activos

Un activo es cualquier cosa que tenga valor para la institución y que, por lo tanto, requiera protección. Para la identificación de los activos se debe tener en cuenta que un sistema de información consiste en algo más que hardware y software.

Se debe identificar un propietario del activo para cada activo, para que se responsabilice y rinda cuentas por el mismo. El propietario del activo tal vez no tenga derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo suele ser la persona más adecuada para determinar el valor que el activo tiene para la organización.

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

De este proceso se genera una lista de los activos que van a estar sometidos a gestión del riesgo, y una lista de los procesos del negocio relacionados con los activos y su importancia. Para realizar la valoración de los activos, es necesario que la institución identifique primero sus activos (con un grado adecuado de detalles). De manera general se pueden diferenciar dos clases de activos:

Los activos primarios:

- Procesos y actividades del negocio.
- Información.

Los activos de soporte (en los que se basan los elementos principales del alcance) de todos los tipos:

- Hardware.
- Software.
- Redes.
- Personal.
- Ubicación.
    - Estructura de la organización.

Ejemplo de identificación de activos:

IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN						
Nro. Activo	**Proceso Macro**	**Subproceso**	**Tipo de Activo**	**Nombre de Activo**	**Descripción del activo**	**Propietario del Activo**
A1	Coordinación General de TIC	Infraestructura	Software	Herramienta de monitoreo ZABBIX	Herramienta Monitoreo Enlaces	Responsable de Infraestructura
A2	Coordinación General de TIC	Infraestructura	Software	Gestión de servicio TI	Herramienta para Gestión de Incidencias	Encargado Centro de servicios
A3	Macro proceso	Subproceso	Software	Portales Institucionales	En este portal se inscriben los niños y se realiza la consulta de la asignación, traslados	Subsecretario / Coordinador / Director Proceso sustantivo
A4	Coordinación General de TIC	Infraestructura	Software	Inicio de sesión único	Manejo de la información del módulo de seguridades	Líder de Proyectos
A5	Coordinación General de TIC	Infraestructura	Hardware	Firewall	Sistema de defensa de que todo el tráfico de entrada o salida a la red, se cuenta con uno de backup	Responsable de Infraestructura
A6	Macro proceso	Subproceso	Software	Business objects	Reportería en Business Objects SAP/ bi	Subsecretario / Coordinador / Director Proceso sustantivo
A7	Coordinación General Administrativa	Instalaciones	Localidad	Datacenter	Equipo de networking para la red ministerial	Responsable de TICs
A8	Coordinación General Administrativa	Talento Humano	Personal	Personal de infraestructura	Administración de la infraestructura tecnológica del ministerio	Responsable de TICs
A9	Coordinación General Administrativa	Talento Humano	Personal	Personal de desarrollo de sistemas	Administración de desarrollo y mantenimiento de software	Responsable de TICs

<u>Valoración de los activos / Ponderación de la criticidad de activos</u>

La ponderación de activos es una etapa en la que participan las unidades del negocio

involucradas con el fin de determinar en términos cualitativos la criticidad de los distintos activos.
Esta ponderación fue realizada en términos de “alto, medio o bajo” donde se asigna un valor cuantitativo a cada valor cualitativo
A continuación, se presentan las referencias para la valoración del impacto en los activos de la información.

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

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

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

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

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

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

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

EVALUACIÓN DE LOS ACTIVOS DE INFORMACIÓN				
Nro. Activo	**Nombre de Activo**	**Tipo de soporte**	**Propietario del Activo**	**Valoración de Impacto (pérdida)**

				C: Confidencialidad	I: Integridad	D: Disponibilidad	
				C	I	D	VA
A1	Herramienta de monitoreo ZABBIX	Virtual	Responsable de Infraestructura	2	3	1	2,00
A2	Gestión de servicio TI	Virtual	Encargado Centro de servicios	2	3	1	2,00
A3	Portales Institucionales	Virtual	Subsecretario / Coordinador / Director Proceso sustantivo	2	3	1	2,00
A4	Inicio de sesión único	Virtual	Líder de Proyectos	3	3	1	2,33
A5	Firewall	Virtual	Responsable de Infraestructura	3	3	3	3,00
A6	Business objects	Virtual	Subsecretario / Coordinador / Director Proceso sustantivo	3	3	3	3,00
A7	Datacenter	Físico y Lógico	Responsable de TICs	1	1	3	1,67
A8	Personal de infraestructura	Físico	Responsable de TICs	1	1	3	1,67
A9	Personal de desarrollo de sistemas	Físico	Responsable de TICs	1	1	3	1,67

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

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

Identificación de Amenazas

Se deben identificar las amenazas y sus orígenes. Una amenaza tiene el potencial de dañar activos como información, procesos y sistemas, por lo tanto, a las organizaciones. Las amenazas pueden ser de origen natural o humano, y pueden ser accidentales o deliberadas.

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

Ejemplo de la identificación de amenazas:

IDENTIFICACIÓN DE AMENAZAS		
Nro. Activo	**Nombre Activo**	**Amenaza**

A1	Herramienta de monitoreo ZABBIX	Mal funcionamiento
		Fallo de los enlaces de comunicación.
		Pérdida de electricidad.
A2	Gestión de servicio TI	Mal funcionamiento
		Destrucción de registros
A3	Portales Institucionales	Accesos a información restringida
		Ataques a las páginas publicadas
		Revelación de información
		Suspensión del servicio
A4	Inicio de sesión único	Acceso inapropiado a los roles definidos para el usuario
		Perder conexión a los usuarios
		Ciber ataques
		Accesos no autorizados, dificultad para identificar actividad
A5	Firewall	Puede acceder ataques cibernéticos
		Comprometer información confidencial.
		Fuga de información.
A6	Business objects	Dificultad al generar reportes de múltiples tablas
		Difusión de información sensible
		Reportes activos para usuarios que ya no pertenezcan a la Institución.
		Dificultad para los usuarios en las actividades propias
A7	Datacenter	Integridad, disponibilidad y confiabilidad de los activos de gestión de información
A8	Personal de infraestructura	Caída de servicios por ausencia de mantenimiento en los equipos físicos y virtuales
A9	Personal de desarrollo de sistemas	Falla en los servicios y suspensión de atención a la ciudadanía

Identificación de Vulnerabilidades

Se debe identificar las vulnerabilidades que puedes ser explotadas por las amenazas, para causar daños a los activos de la institución.

La presencia de una vulnerabilidad no causa daño por sí misma, ya que necesita que exista una amenaza presente para aprovecharla. Una vulnerabilidad que no tiene la amenaza correspondiente puede no requerir la implementación de un control, pero debería reconocerse y monitorearse para detectar cambios. Se debe o es preciso señalar que un control implementado incorrectamente, que funciona mal o un control que se usa incorrectamente, puede ser una vulnerabilidad.

Ejemplo de la identificación de vulnerabilidades:

IDENTIFICACIÓN DE VULNERABILIDADES

Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad
A1	Herramienta de monitoreo ZABBIX	Mal funcionamiento	Herramienta sin licencia
		Fallo de los enlaces de comunicación.	Inadecuada gestión de red.
		Pérdida de electricidad.	Sensibilidad del equipo a los cambios de voltaje.
A2	Gestión de servicio TI	Mal funcionamiento	Herramienta sin licencia
		Destrucción de registros	Respaldo inapropiado o irregular
A3	Portales Institucionales	Accesos a información restringida	Compartir credenciales de acceso
		Ataques a las páginas publicadas	Falta de monitoreo en la red (cloud)
		Revelación de información	Contraseñas no protegidas, claves, certificados
		Suspensión del servicio	Actualización de parches al software base
A4	Inicio de sesión único	Acceso inapropiado a los roles definidos para el usuario	Continua modificación de las reglas del negocio
		Perder conexión a los usuarios	La versión del Aplicativo no controla varias sesiones activas
		Ciber ataques	Falta de monitoreo
		Accesos no autorizados, dificultad para identificar actividad	Compartir credenciales de acceso
A5	Firewall	Puede acceder ataques cibernéticos	Actualización de certificados
		Comprometer información confidencial.	Inadecuada gestión y protección de contraseñas.
		Fuga de información.	interfaces configuras sin revisión
A6	Business objects	Dificultad al generar reportes de múltiples tablas	Interfaz poco amigable
		Difusión de información sensible	Existen reportes que pueden ser visualizado por varias personas sin restricción
		Reportes activos para usuarios que ya no pertenezcan a la Institución.	Usuarios sin depuración
		Dificultad para los usuarios en las actividades propias	Roles desactualizados
A7	Datacenter	Integridad, disponibilidad y confiabilidad de los activos de gestión de información	Infraestructura desactualizada
A8	Personal de infraestructura	Caída de servicios por ausencia de mantenimiento en los equipos físicos y virtuales	Escasos funcionarios para desarrollo de software
A9	Personal de desarrollo de sistemas	Falla en los servicios y suspensión de atención a la ciudadanía	Escasos funcionarios para desarrollo de software

Identificación de Existencia de Controles

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

Se debe identificar los controles existentes para evitar trabajo o costos innecesarios, por ejemplo, en la duplicación de los controles. Además, al identificar los controles existentes, se debe hacer una verificación para asegurarse que los controles funcionan correctamente, una referencia a los reportes de auditoría del SGSI ya existentes debe limitar el tiempo dedicado a esta tarea. Si el control no funciona como se espera, esto puede causar vulnerabilidades.
Ejemplo de la identificación de los controles existentes (implementados):

IDENTIFICACIÓN DE CONTROLES EXISTENTES				Impacto	
Nro. Activo	**Nombre Activo**	**Amenaza**	**Vulnerabilidad**	**CID**	**Controles existentes**
A1	Herramienta de monitoreo ZABBIX	Mal funcionamiento	Herramienta sin licencia	2,00	Monitoreo continuo
		Fallo de los enlaces de comunicación.	Inadecuada gestión de red.	2,00	Monitoreo continuo
		Pérdida de electricidad.	Sensibilidad del equipo a los cambios de voltaje.	2,00	UPS en funcionamiento
A2	Gestión de servicio TI	Mal funcionamiento	Herramienta sin licencia	2,00	Conocimiento del operador
		Destrucción de registros	Respaldo inapropiado o irregular	2,00	Respaldos manuales
A3	Portales Institucionales	Accesos a información restringida	Compartir credenciales de acceso	2,00	Registro de auditoria
		Ataques a las páginas publicadas	Falta de monitoreo en la red (cloud)	2,00	Revisión por parte del proveedor
		Revelación de información	Contraseñas no protegidas, claves, certificados	2,00	Socialización cuidado de credenciales
		Suspensión del servicio	Actualización de parches al software base	2,00	No se ha implementado controles
A4	Inicio de sesión único	Acceso inapropiado a los roles definidos para el usuario	Continua modificación de las reglas del negocio	2,33	Requerimiento funcional
		Perder conexión a los usuarios	La versión del Aplicativo no controla varias sesiones activas	2,33	Socialización de funcionalidad
		Ciber ataques	Falta de monitoreo	2,33	Actualización de la arquitectura
		Accesos no autorizados, dificultad para identificar actividad	Compartir credenciales de acceso	2,33	Socialización de funcionalidad
A5	Firewall	Puede acceder ataques cibernéticos	Actualización de certificados	3,00	Soporte contratado
		Comprometer información confidencial.	Inadecuada gestión y protección de contraseñas.	3,00	Soporte contratado
		Fuga de información.	interfaces configuras sin revisión	3,00	Soporte contratado
A6	Business objects	Dificultad al generar reportes de múltiples tablas	Interfaz poco amigable	3,00	Soporte contratado
		Difusión de información sensible	Existen reportes que pueden ser visualizado por varias personas sin restricción	3,00	Soporte contratado
		Reportes activos para usuarios que ya no pertenezcan a la Institución.	Usuarios sin depuración	3,00	Soporte contratado
		Dificultad para los usuarios en las actividades propias	Roles desactualizados	3,00	Soporte contratado
A7	Datacenter	Integridad, disponibilidad y confiabilidad de los activos de gestión de información	Infraestructura desactualizada	1,67	Soporte contratado

A8	Personal de infraestructura	Caída de servicios por ausencia de mantenimiento en los equipos físicos y virtuales	Escasos funcionarios para desarrollo de software	1,67	Soporte contratado
A9	Personal de desarrollo de sistemas	Falla en los servicios y suspensión de atención a la ciudadanía	Escasos funcionarios para desarrollo de software	1,67	Soporte contratado

Estimación o Análisis del riesgo

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

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

El análisis de riesgos puede llevarse a cabo en diversos grados de detalle dependiendo de la importancia de los activos, la extensión de las vulnerabilidades conocidas e incidentes previos relacionados con la organización. Una metodología de análisis de riesgos puede ser cualitativa o cuantitativa, o una combinación de estos, dependiendo de las circunstancias. En la práctica, el análisis cualitativo a menudo se usa primero para obtener una indicación general del nivel de riesgo y revelar los principales riesgos.

VALORACION DEL RIESGOS

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

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

Criterios de probabilidad de ocurrencia de amenazas:

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

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

Criterio de probabilidad de ocurrencia de vulnerabilidades

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

Criterio de la Evaluación de Riesgos

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

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

Nivel de Riesgo		Acciones
1 - 3	El riesgo es BAJO	Retención y monitoreo del activo
4 - 8	El riesgo es MEDIO	Requiere atención mediante la aplicación de controles que permita disminuir el riesgo, durante un tiempo determinado de acuerdo a la importancia del activo.
9 - 27	El riesgo es ALTO	Requiere atención inmediata, para modificar el riesgo del activo.

Ejemplo del cálculo de la evaluación de riesgos:

Análisis de Riesgos				Evaluación de Riesgos					
				Impacto	Probabilidad				
Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad	controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
A1	Herramienta de monitoreo ZABBIX	Mal funcionamiento	Herramienta sin licencia	2,00	2	2	Monitoreo continuo	8,00	MEDIO
		Fallo de los enlaces de comunicación.	Inadecuada gestión de red.	2,00	1	1	Monitoreo continuo	2,00	BAJO
		Pérdida de electricidad.	Sensibilidad del equipo a los cambios de voltaje.	2,00	1	1	UPS en funcionamiento	2,00	BAJO
A2	Gestión de servicio TI	Mal funcionamiento	Herramienta sin licencia	2,00	2	2	Conocimiento del operador	8,00	MEDIO
		Destrucción de registros	Respaldo inapropiado o irregular	2,00	2	2	Respaldos manuales	8,00	MEDIO
A3	Portales Institucionales	Accesos a información restringida	Compartir credenciales de acceso	2,00	2	2	Registro de auditoria	8,00	MEDIO
		Ataques a las páginas publicadas	Falta de monitoreo en la red (cloud)	2,00	2	1	Revisión por parte del proveedor	4,00	MEDIO
		Revelación de información	Contraseñas no protegidas, claves, certificados	2,00	2	2	Socialización cuidado de credenciales	8,00	MEDIO
		Suspensión del	Actualización de	2,00	1	1		2,00	BAJO

		servicio	parches al software base						
A4	Inicio de sesión único	Acceso inapropiado a los roles definidos para el usuario	Continua modificación de las reglas del negocio	2,33	2	1	Requerimiento funcional	4,67	MEDIO
		Perder conexión a los usuarios	La versión del Aplicativo no controla varias sesiones activas	2,33	2	1	Socialización de funcionalidad	4,67	MEDIO
		Ciber ataques	Falta de monitoreo	2,33	2	1	Actualización de la arquitectura	4,67	MEDIO
		Accesos no autorizados, dificultad para identificar actividad	Compartir credenciales de acceso	2,33	2	2	Socialización de funcionalidad	9,33	ALTO
A5	Firewall	Puede acceder ataques cibernéticos	Actualización de certificados	3,00	2	1	Soporte contratado	6,00	MEDIO
		Comprometer información confidencial.	Inadecuada gestión y protección de contraseñas.	3,00	2	1	Soporte contratado	6,00	MEDIO
		Fuga de información.	interfaces configuras sin revisión	3,00	2	1	Soporte contratado	6,00	MEDIO
A6	Business objects	Dificultad al generar reportes de múltiples tablas	Interfaz poco amigable	3,00	2	1	Soporte contratado	6,00	MEDIO
		Difusión de información sensible	Existen reportes que pueden ser visualizado por varias personas sin restricción	3,00	1	1	Soporte contratado	3,00	BAJO
		Reportes activos para usuarios que ya no pertenezcan a la Institución.	Usuarios sin depuración	3,00	1	2	Soporte contratado	6,00	MEDIO
		Dificultad para los usuarios en las actividades propias	Roles desactualizados	3,00	1	1	Soporte contratado	3,00	BAJO
A7	Datacenter	Integridad, disponibilidad y confiabilidad de los activos de gestión de información	Infraestructura desactualizada	1,67	1	1	Soporte contratado	1,67	BAJO
A8	Personal de infraestructura	Caída de servicios por ausencia de mantenimiento en los equipos físicos y virtuales	Escasos funcionarios para desarrollo de software	1,67	1	1	Soporte contratado	1,67	BAJO
A9	Personal de desarrollo de sistemas	Falla en los servicios y suspensión de atención a la ciudadanía	Escasos funcionarios para desarrollo de software	1,67	1	1	Soporte contratado	1,67	BAJO

TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

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

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

Existen cuatro opciones disponibles para el tratamiento del riesgo:

- Prevención/Evitación del riesgo

- Modificación del riesgo
- Retención/Aceptación del riesgo
- Compartición del riesgo

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

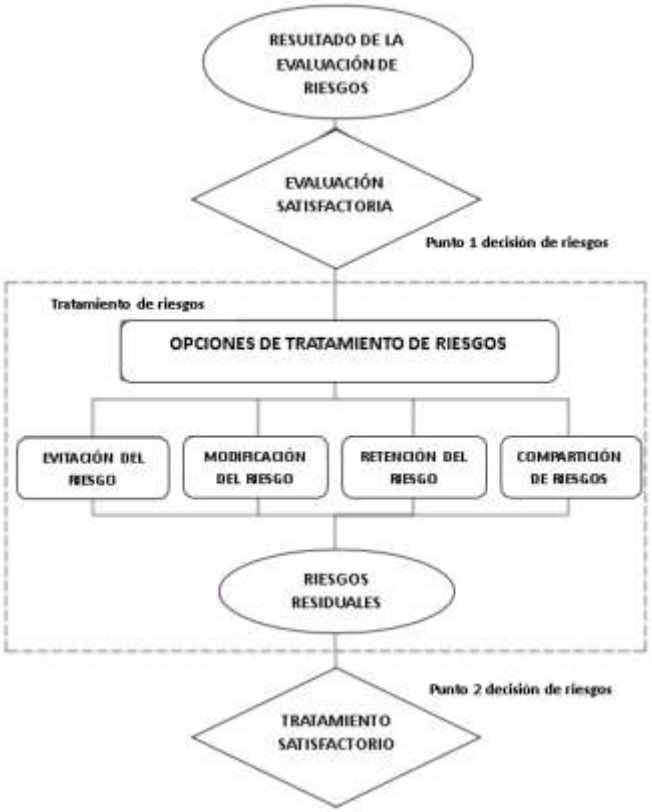

Figura No. 3 ACTIVIDADES PARA EL TRATAMIENTO DE LOS RIESGOS, Fuente: ISO27005

Las opciones para el tratamiento de riesgos se deberían seleccionar en función del resultado de la evaluación de riesgos, el costo esperado para implementar estas opciones y los beneficios esperados de estas opciones.

Cuando se pueden obtener grandes reducciones en los riesgos con un costo relativamente bajo, se deberían implementar esas opciones. Las opciones de mejora pueden ser antieconómicas y es necesario juzgar si son justificables.

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

MODIFICACION DE RIESGOS

Se debe gestionar mediante la implementación de controles (introducción, eliminación o

alteración), para que el riesgo residual se pueda reevaluar como aceptable.

Se debe seleccionar controles apropiados y justificados para cumplir con los requisitos identificados por la evaluación de riesgos y el tratamiento de riesgos. Esta selección también debería tener en cuenta el costo y el plazo para la implementación de controles, o aspectos técnicos, ambientales y culturales. A menudo, es posible reducir el costo total de propiedad de un sistema con controles de seguridad de la información adecuadamente seleccionados.

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

RETENCIÓN / ACEPTACIÓN DEL RIESGO

La decisión sobre la retención del riesgo sin más acción debe tomarse dependiendo de la valoración del riesgo.

Considerar que, si el nivel de riesgo cumple con los criterios de aceptación del riesgo, no es necesario implementar más controles y el riesgo se puede mantener con el monitoreo continuo.

PREVENCIÓN/EVITACION DE RIESGOS

Se debe prevenir o evitar la actividad o condición que da lugar al riesgo particular.

Cuando los riesgos identificados se consideran demasiado altos, o los costos de implementar otras opciones de tratamiento de riesgos exceden los beneficios, se puede tomar una decisión para prevenir el riesgo por completo, al retirarse de una actividad o un conjunto de actividades planificadas o existentes, o al cambiar las condiciones bajo las cuales se opera la actividad.

Por ejemplo, para los riesgos causados por la naturaleza, la alternativa más eficaz en función de los costos puede ser mover físicamente las instalaciones de procesamiento de información a un lugar donde el riesgo no existe o está bajo control.

COMPARTICIÓN DE RIESGOS

El riesgo debe compartirse con otra parte que pueda gestionar de manera más efectiva el riesgo particular dependiendo de la valoración de riesgos; implica la decisión de compartir ciertos riesgos con partes externas. La compartición de riesgos puede crear riesgos nuevos o modificar riesgos existentes e identificados. Por lo tanto, puede ser necesario un tratamiento de riesgos adicional.

Ejemplo del tratamiento de los riesgos:

Evaluación de Riesgos						Tratamiento de Riesgos							Riesgo residual
Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo								
CID	Nivel de amenaza	Nivel de vulnera bilidad				Método de tratamiento de Riesgos	Tipo de control	Control es a Implem entar	Nivel de amenaza	Nivel de vulnera bilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementa do	

2,00	2	2	Monitoreo continuo	8,00	MEDIO	MODIFICAR / PREVENCION / COMPARTIR	CONTROL PREVENTIVO	Proceso para adquirir la licencia	1	1	2,00	BAJO	ACEPTABLE
2,00	1	1	Monitoreo continuo	2,00	BAJO	RETENCIÓN	NO APLICA CONTROL		1	1	2,00	BAJO	ACEPTABLE
2,00	1	1	UPS en funcionamiento	2,00	BAJO	RETENCIÓN	NO APLICA CONTROL		1	1	2,00	BAJO	ACEPTABLE
2,00	2	2	Conocimiento del operador	8,00	MEDIO	MODIFICAR / PREVENCION / COMPARTIR	CONTROL PREVENTIVO	Instalar software gratuito	1	1	2,00	BAJO	ACEPTABLE
2,00	2	2	Respaldos manuales	8,00	MEDIO	MODIFICAR / PREVENCION / COMPARTIR	CONTROL PREVENTIVO	Política de respaldos	1	1	2,00	BAJO	ACEPTABLE
2,00	2	2	Registro de auditoria	8,00	MEDIO	MODIFICAR / PREVENCION / COMPARTIR	CONTROL PREVENTIVO	Doble autenticación	1	1	2,00	BAJO	ACEPTABLE
2,00	2	1	Revisión por parte del proveedor	4,00	MEDIO	MODIFICAR / PREVENCION / COMPARTIR	CONTROL CORRECTIVO	Inclusión en el contrato de servicios	1	1	2,00	BAJO	ACEPTABLE
2,00	2	2	Socialización cuidado de credenciales	8,00	MEDIO	MODIFICAR / PREVENCION / COMPARTIR	CONTROL PREVENTIVO	Plan de socialización	2	1	4,00	MEDIO	INACEPTABLE
2,00	1	1		2,00	BAJO	RETENCIÓN	NO APLICA CONTROL		1	1	2,00	BAJO	ACEPTABLE
2,33	2	1	Requerimiento funcional	4,67	MEDIO	MODIFICAR / PREVENCION / COMPARTIR	CONTROL CORRECTIVO	Soporte contratado	1	1	2,00	BAJO	ACEPTABLE
2,33	2	1	Socialización de funcionalidad	4,67	MEDIO	MODIFICAR / PREVENCION / COMPARTIR	CONTROL CORRECTIVO	Soporte contratado	1	1	2,00	BAJO	ACEPTABLE
2,33	2	1	Actualización de la arquitectura	4,67	MEDIO	MODIFICAR / PREVENCION / COMPARTIR	CONTROL CORRECTIVO	Soporte contratado	1	1	2,00	BAJO	ACEPTABLE
2,33	2	2	Socialización de funcionalidad	9,33	ALTO	MODIFICAR / PREVENCION / COMPARTIR	CONTROL PREVENTIVO	Soporte contratado	1	1	2,00	BAJO	ACEPTABLE
3,00	2	1	Soporte contratado	6,00	MEDIO	MODIFICAR / PREVENCION / COMPARTIR	CONTROL CORRECTIVO	Soporte contratado	1	1	2,00	BAJO	ACEPTABLE
3,00	2	1	Soporte contratado	6,00	MEDIO	MODIFICAR / PREVENCION / COMPARTIR	CONTROL CORRECTIVO	Soporte contratado	1	1	2,00	BAJO	ACEPTABLE

3,00	2	1	Soporte contratado	6,00	MEDIO	MODIFICAR / PREVENCION / COMPARTIR	CONTROL CORRECTIVO	Soporte contratado	1	1	2,00	BAJO	ACEPTABLE
3,00	2	1	Soporte contratado	6,00	MEDIO	MODIFICAR / PREVENCION / COMPARTIR	CONTROL CORRECTIVO	Soporte contratado	1	1	2,00	BAJO	ACEPTABLE
3,00	1	1	Soporte contratado	3,00	BAJO	RETENCIÓN	NO APLICA CONTROL		1	1	2,00	BAJO	ACEPTABLE
3,00	1	2	Soporte contratado	6,00	MEDIO	MODIFICAR / PREVENCION / COMPARTIR	CONTROL PREVENTIVO	Soporte contratado	1	1	2,00	BAJO	ACEPTABLE
3,00	1	1	Soporte contratado	3,00	BAJO	RETENCIÓN	NO APLICA CONTROL		1	1	2,00	BAJO	ACEPTABLE
1,67	1	1	Soporte contratado	1,67	BAJO	RETENCIÓN	NO APLICA CONTROL		1	1	2,00	BAJO	ACEPTABLE
1,67	1	1	Soporte contratado	1,67	BAJO	RETENCIÓN	NO APLICA CONTROL		1	1	2,00	BAJO	ACEPTABLE
1,67	1	1	Soporte contratado	1,67	BAJO	RETENCIÓN	NO APLICA CONTROL		1	1	2,00	BAJO	ACEPTABLE

Aceptación del riesgo de la seguridad de la información

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

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

En algunos casos, el nivel de riesgo residual no cumple con los criterios de aceptación de riesgos porque los criterios que se aplican no tienen en cuenta las circunstancias prevalecientes. Por ejemplo, se puede argumentar que es necesario aceptar los riesgos porque los beneficios que acompañan a los riesgos son muy atractivos o porque el costo de la modificación de riesgos es demasiado alto. La organización debería definir sus propias escalas para los niveles de aceptación del riesgo.

Durante el desarrollo, se deberían considerar los siguientes aspectos:

- Los criterios de aceptación del riesgo pueden incluir umbrales múltiples, con un nivel de riesgo deseado, pero se prevé que la alta dirección acepte riesgos por encima de este nivel en circunstancias definidas

- Los criterios de aceptación de riesgos pueden expresarse como la relación entre el beneficio estimado (u otro beneficio de negocios) y el riesgo estimado;

- Pueden aplicarse diferentes criterios de aceptación de riesgos a diferentes clases de riesgos; por ejemplo, los riesgos que podrían resultar en incumplimiento con reglamentos o leyes, podrían no ser aceptados, aunque se puede permitir la aceptación de riesgos altos, si esto se especifica como un requisito contractual.

- Los criterios de aceptación de riesgos pueden incluir requisitos para futuros tratamientos adicionales, por ejemplo, se puede aceptar un riesgo si hay aprobación y compromiso de tomar medidas para reducirlo a un nivel aceptable dentro de un período de tiempo definido

COMUNICACIÓN Y CONSULTA DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

"La información acerca de los riesgos se debe intercambiar y/o compartir entre el responsable de la toma decisiones y otras partes interesadas."

La comunicación de los riesgos es una actividad para lograr un acuerdo sobre cómo gestionar los riesgos mediante el intercambio y/o el compartir la información sobre el riesgo entre los responsables de la toma de decisiones y otras partes interesadas. La información incluye, entre otros, existencia, naturaleza, forma, probabilidad, gravedad, tratamiento y aceptabilidad de los riesgos.

La comunicación efectiva entre las partes interesadas es importante ya que esto puede tener un impacto significativo sobre las decisiones a tomar. La comunicación asegura que los responsables de implementar la gestión de riesgos y los que tienen un interés personal entiendan la base sobre la cual se toman las decisiones y por qué se requieren acciones particulares. La comunicación es bidireccional.

En consecuencia, la comunicación busca promover la toma de conciencia y la comprensión del riesgo, mientras que la consulta implica obtener retroalimentación e información para apoyar la toma de decisiones.

La comunicación de riesgos debe llevarse a cabo para:

- Asegurar que se consideren de manera apropiada los diferentes puntos de vista cuando se definen los criterios del riesgo y cuando se valoran los riesgos.

- Proporcionar garantías del resultado de la gestión de riesgos de la institución.

- Recopilar información sobre los riesgos.

- Compartir los resultados de la evaluación de riesgos y presentar el plan de tratamiento de riesgos.

- Prevenir o reducir tanto la ocurrencia como la consecuencia de violaciones de seguridad de la información debido a la falta de entendimiento mutuo entre quienes son los responsables de la toma de decisiones y las partes interesadas.

- Soportar la toma de decisiones.

- Obtener nuevos conocimientos sobre la seguridad de la información.

- Coordinar con otras partes y planificar la respuesta para reducir las consecuencias de cualquier incidente.

- Dar a los responsables de la toma de decisiones y a las partes interesadas un sentido de responsabilidad sobre los riesgos.

- Mejorar la toma de conciencia.

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

INFORMACION DOCUMENTADA

Especifica los requisitos para que las instituciones conserven la información documentada, sobre el proceso de evaluación de riesgos su tratamiento, así como sus resultados.

Información documentada sobre procesos

El proceso de evaluación y el tratamiento de riesgos de seguridad, se debe documentar y conservar. Esta información podrá ser utilizada por las partes interesadas o determinada por la institución como necesaria para la efectividad del proceso de evaluación de riesgos de seguridad de la información o del tratamiento de los riesgos.

La información documentada sobre el proceso de evaluación de riesgos debe contener:

- La definición de criterios de riesgo, incluidos los criterios de aceptación del riego y los criterios para realizar la evaluación;
- Razonamiento para la consistencia, validez y comparación de los resultados;
- Descripción del método de identificación del riesgo incluida la identificación de los propietarios del riesgo;
- Descripción del método para analizar los riesgos de seguridad de la información, incluida la evaluación de las posibles consecuencias, la probabilidad real y el nivel de riesgo resultante;
- Descripción del método para comparar los resultados con los criterios de riesgo y priorización de riesgos para el tratamiento de riesgos;

La información documentada sobre el proceso de tratamiento de riesgos, debe contener:

- El método para seleccionar opciones apropiadas de tratamiento de riesgos de seguridad de la información;
- El método para determinar los controles necesarios;
- Revisar los controles que se han pasado por alto sin darse cuenta;
- Como se elaboran los planes de tratamiento de riesgos;
- Como se obtiene la aprobación de los propietarios del riesgo;

Información documentada sobre resultados

La información de los resultados de la evaluación y tratamiento de riesgos de seguridad de la información, debe conservarse.

Las instituciones deben realizar evaluaciones de riesgos en intervalos planificados, cuando lo requieran o cuando ocurran cambios significativos, por lo que es necesario la existencia de un cronograma y de su cumplimiento.

Cuando realmente existe un cambio significativo debe existir evidencia de la evaluación de riesgos realizada y esta deberá contener:

- Los riesgos identificados, sus consecuencias y probabilidad
- La identidad del propietario del riesgo
- Los resultados de la aplicación de los criterios de aceptación de riesgos;
- La prioridad para el tratamiento del riesgo;
- Registrar la justificación de las decisiones de riesgo, para aprender de los errores y facilitar la mejora continua;
- Identificar los controles necesarios;
- Evidencia de que los controles aplicados actúan para modificar los riesgos de manera que cumplan con los criterios de aceptación de riesgos institucionales.

MONITOREO Y REVISIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

MONITOREO Y REVISIÓN DE LOS FACTORES DE RIESGO

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

Esta actividad se puede respaldar en servicios externos que brinden información sobre nuevas amenazas o vulnerabilidades.

Las instituciones deben asegurarse del monitoreo continuo en los siguientes aspectos:

- Activos nuevos que se han incluido en el alcance de la gestión de riesgos.
- Modificaciones necesarias de los valores de los activos, por ejemplo, debido a los requisitos del negocio modificados.
- Nuevas amenazas que podrían estar activas tanto fuera como dentro de la organización y que no han sido evaluadas.
- Probabilidad de que nuevas vulnerabilidades o incrementadas puedan permitir que las amenazas aprovechen estas vulnerabilidades nuevas o modificadas.
- Vulnerabilidades identificadas para determinar a quienes están expuestos a amenazas nuevas o reemergentes.
- El incremento en el impacto o consecuencias de las amenazas evaluadas, las vulnerabilidades y riesgos en conjunto que dan como resultado un nivel inaceptable de riesgos.
- Incidentes de la seguridad de la información.

Los factores que afectan la probabilidad y las consecuencias de las amenazas pueden cambiar, al igual que los factores que afectan la idoneidad o el costo de las diversas opciones

de tratamiento. Los cambios importantes que afectan a la institución deberían ser motivo de una revisión más específica. Por lo tanto, las actividades de monitoreo de riesgos deberían repetirse regularmente y las opciones seleccionadas para el tratamiento de riesgos deberían revisarse periódicamente.

MONITOREO, REVISIÓN Y MEJORA DE LA GESTIÓN DEL RIESGO

"El proceso de gestión de riesgos de seguridad de la información se debe monitorear, revisar y mejorar continuamente, según sea necesario y apropiado".

El monitoreo y la revisión continuos son necesarios para garantizar que el contexto, el resultado de la evaluación y el tratamiento de riesgos, así como los planes de gestión sigan siendo relevantes y apropiados para las circunstancias actuales.
La organización debe garantizar que el proceso de gestión del riesgo de seguridad de la información y las actividades relacionadas continúen siendo apropiadas en las circunstancias actuales y se cumplen. Cualquier mejora acordada para el proceso o las acciones necesarias para mejorar el cumplimiento del proceso, se debería notificar al Comité de Seguridad de la Información, para tener seguridad de que no se omite ni subestima ningún riesgo o elemento del riesgo, y que se toman las acciones necesarias y las decisiones para brindar una comprensión realista del riesgo y la capacidad para responder.

ANEXO C

GUÍA PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN[3]

ANTECEDENTES Y CONTEXTO

Esta guía está diseñada para que las instituciones del Sector Público, usen como referencia a la hora de seleccionar controles dentro del proceso de implementación del Esquema Gubernamental de Seguridad de la Información como un Sistema de Gestión de Seguridad de la Información (SGSI), como documento referencial para instituciones que implementen controles de seguridad de la información comúnmente aceptados.

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

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

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

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

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

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

[3] Basado en la norma NTE-INEN-ISO-IEC-27002:2022

REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN

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

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

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

SELECCIÓN DE CONTROLES

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

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

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

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

ESTRUCTURA DE LOS CONTROLES

Esta guía contiene 4 categorías de controles de seguridad que en conjunto contienen un total de 93 controles.

a) Controles organizacionales (37) Controles diseñados para la gobernanza, toma de decisiones como: políticas de seguridad, roles, responsabilidades, segregación de tareas, cumplimiento legal, etc.

b) Controles de personas (8) Controles deseñados para la intervención del talento humano como: concientización, acuerdos de confidencialidad, proceso disciplinario, teletrabajo, reporte de eventos de SI, etc.

c) Controles físicos (14) Controles diseñados específicamente para el monitoreo y acceso a las instalaciones físicas, protecciones ambientales.

d) Controles tecnológicos (34) Controles en los que intervienen la tecnología

Atributos de los controles:

La institución tiene la capacidad de utilizar atributos para generar diversas perspectivas que categorizan los controles de manera diferente a través de diferentes temas. Estos atributos pueden ser utilizados para filtrar, ordenar o presentar los controles en distintas aristas.

A cada control del anexo EGSI, se asocia cinco atributos, precedidos con (#) que facilita la búsqueda por atributo y son los siguientes:

a)Tipo de control

El atributo del tipo de control se utiliza para analizar los controles desde la perspectiva de cómo y cuándo modifican el riesgo en relación con la aparición de incidentes de seguridad de la información. Los valores atribuidos a este atributo son:

- Preventivo: Actúan sobre la causa de los riesgos, tiene como objetivo disminuir la probabilidad de la ocurrencia de un incidente de seguridad de la información, por consiguiente, elimina la vulnerabilidad o la amenaza de un activo.
- Detectivo: Son controles que constituyen una segunda barrera o capa de seguridad, e control se activa cuando se produce un incidente de seguridad de la información.
- Correctivo: El control actúa después de que ocurra un incidente de seguridad de la información, es decir, elimina la causa para evitar futuras ocurrencias

b) Propiedades de seguridad de la información

Las propiedades de seguridad de la información son otro atributo utilizado para evaluar los controles desde la perspectiva de qué características de la información contribuirán a preservar el control. Los valores atribuidos a este atributo son Confidencialidad, Integridad y Disponibilidad.

- **Confidencialidad**: La información solo tiene que ser accesible o divulgada a aquellos que están autorizados, los controles orientados a la confidencialidad buscan prevenir la divulgación no autorizada de información sensible.

- **Integridad**: La información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros, los controles de integridad buscan proteger la exactitud y la integridad de los datos frente a alteraciones no deseadas o maliciosas.

- **Disponibilidad**: La información debe estar siempre accesible para aquellos que estén autorizados, los controles de disponibilidad buscan prevenir interrupciones o limitaciones en el acceso a la información, asegurando su disponibilidad continua.

Estos valores atribuidos a las propiedades de seguridad de la información ayudan a clasificar y seleccionar los controles adecuados para proteger y preservar cada una de estas características en el manejo de la información

c)Conceptos de ciberseguridad

Los conceptos de ciberseguridad son un atributo que permite observar los controles desde

la perspectiva de cómo se asocian con los conceptos de ciberseguridad definidos en el marco de referencia de ciberseguridad descrito en **ISO/IEC TS 27110**; los valores de los atributos incluyen Identificar, Proteger, Detectar, Responder y Recuperar

1. **Identificar:** El concepto de identificar se enfoca en definir el alcance de las actividades a través de personas, políticas, procesos y tecnología. Las actividades relacionadas con la identificación son fundamentales para la ciberseguridad y pueden abarcar categorías como el entorno empresarial, la evaluación de riesgos, la estrategia de gestión de riesgos, la gobernanza, la gestión de activos y consideraciones de la cadena de suministro; la comprensión obtenida del concepto de identificación permite una visión flexible y repetible de la ciberseguridad, lo que permite que la institución se enfoque y priorice sus esfuerzos, al diseñar el concepto de identificación, es importante considerar la evolución de las amenazas cibernéticas y la tecnología emergente para cumplir con los requisitos futuros en la implementación del esquema gubernamental de seguridad en la información.

2. **Proteger:** El concepto de proteger se centra en desarrollar medidas de seguridad adecuadas para salvaguardar la identidad cibernética de la institución, garantizar el funcionamiento de los controles preventivos y preparar a la institución para brindar servicios críticos y mantener la seguridad de la información; este concepto abarca diversas categorías y actividades relacionadas con la protección de activos contra el mal uso intencional o no intencional, tanto en sistemas de TI tradicionales como en sistemas de control industrial o Internet de las cosas, al desarrollar el concepto de proteger, se consideran aspectos como el control de acceso, la concienciación y capacitación, la seguridad de datos, los procesos y procedimientos de protección de la información, la tecnología de protección, la arquitectura de seguridad, la configuración de activos, la criptografía, la gestión de identidad y acceso, y la seguridad de datos, el creador de un marco de seguridad cibernética debe determinar el alcance del concepto de proteger, considerando enfoques preventivos y orientados a amenazas, y teniendo en cuenta la protección de personas, procesos y tecnología en la implementación del esquema gubernamental de seguridad de la información.

3. **Detectar:** Un marco de ciberseguridad debe incluir el concepto detectar, el concepto detectar desarrolla las actividades adecuadas para descubrir eventos de ciberseguridad, las actividades en el concepto de detección brindan a la institución la capacidad de observar de manera proactiva cambios en comportamientos, estados, tráfico, configuración o procesamiento de sus recursos clave, estos cambios pueden ser internos o externos, intencionales o no intencionales; al comprender el panorama cambiante, la institución puede actualizar las políticas, los procedimientos y la tecnología según sea necesario, el concepto de detección puede incluir detección tradicional las categorías pueden incluir: anomalías y eventos, monitoreo continuo de seguridad, proceso de detección, registro, correlación y análisis de registros, búsqueda de amenazas, detección de anomalías, un creador de un marco de seguridad cibernética debe considerar la profundidad y el alcance de los cambios internos y externos que se observarán; el aumento del alcance del concepto de detección puede agregar valor a la seguridad cibernética, algunos marcos de seguridad cibernética pueden centrarse en el nivel de sistema mientras que otros se enfocan en el nivel de proceso al considerar el concepto de detección, los creadores del marco de seguridad cibernética deben determinar el nivel de detalle apropiado para guiar a la institución en la

implementación del esquema gubernamental de seguridad de la información.

4. **Responder:** Un marco de ciberseguridad debe incluir el concepto de responder, el cual se enfoca en desarrollar las actividades adecuadas para responder a eventos de ciberseguridad, estas actividades permiten a la institución calificar, evaluar y abordar los eventos de ciberseguridad en su entorno, el concepto responder abarca la categorización, evaluación y remediación de eventos de ciberseguridad según las necesidades, recursos, partes interesadas y requisitos específicos de la institución, esto incluye la planificación de la respuesta, comunicaciones, análisis, mitigación, mejoras, respuesta a incidentes y eliminación de malware, al crear un marco de seguridad cibernética, es importante considerar aspectos administrativos y de procedimiento en el contexto más amplio del concepto responder, además de la respuesta a incidentes, este concepto puede incorporar la comunicación con partes externas, como la divulgación de vulnerabilidades, informes de amenazas y el intercambio de información con fuentes externas; el creador del marco de seguridad cibernética debe comprender todo el ecosistema en el que se implementará el marco para comprender adecuadamente el concepto responder en la implementación del esquema gubernamental de seguridad de la información.

5. **Recuperación:** Es esencial que un marco de ciberseguridad incluya el concepto de recuperación; el concepto de recuperación engloba las actividades necesarias para restaurar servicios, reparar sistemas y restablecer la reputación, las acciones comprendidas en el concepto de recuperación definen las actividades relacionadas con la restauración y la comunicación después de un evento de ciberseguridad, este concepto no se limita únicamente a ser reactivo, sino que también abarca un enfoque proactivo, la planificación y ejecución eficaces y eficientes de las actividades en el ámbito de recuperación deberían minimizar los daños y ayudar a la institución a reanudar sus operaciones, durante un incidente de ciberseguridad es posible que los servicios se vean afectados negativamente el concepto de recuperación brinda la oportunidad de dar orientación sobre cómo restaurar esos servicios, estos servicios pueden ser tanto de naturaleza técnica como de gestión, asimismo, los activos pueden encontrarse en un estado de funcionamiento no deseado o inoperable. El concepto de recuperación también ofrece la posibilidad de brindar orientación sobre cómo reparar dichos activos, además, la reputación puede haber sido dañada durante un incidente de ciberseguridad, la reputación constituye un factor clave para mantener la cuota de mercado y la confianza de los ciudadanos las categorías que pueden incluirse son: planificación de la recuperación, comunicaciones, mejoras, capacitación en recuperación y ejecución de la recuperación. Al crear un marco de ciberseguridad, es importante que el creador considere diversos factores que influyen en la prioridad de la restauración del servicio estos factores abarcan el impacto comercial, las necesidades de las partes interesadas, los escenarios de implementación y la madurez tecnológica. Aunque algunos marcos de ciberseguridad no incluyen objetivos comerciales, las consecuencias no técnicas de una recuperación pueden ser graves y deben abordarse mediante un marco de ciberseguridad en la implementación del esquema gubernamental de seguridad de la información.

d)Capacidades operativas

Las capacidades operativas representan otro atributo utilizado para analizar los controles

desde la perspectiva de las habilidades y competencias del profesional de seguridad de la información, los valores atribuidos a este atributo incluyen:

1. **Gobernanza**: Se refiere al establecimiento de políticas, estructuras y procesos para garantizar una adecuada dirección y control de la seguridad de la información en la institución.

2. **Gestión de activos**: Se relaciona con la identificación, clasificación y gestión de los activos de información, así como la asignación de responsabilidades para su protección y correcto uso.

3. **Protección de la información**: Se refiere a la implementación de controles y medidas de seguridad para preservar la confidencialidad, integridad y disponibilidad de la información.

4. **Seguridad de recursos humanos**: Implica establecer prácticas y políticas de seguridad para el personal, incluyendo la capacitación en seguridad, la gestión de accesos y los controles relacionados con las actividades del personal.

5. **Seguridad física**: Se centra en la protección de los activos físicos de la institución, como los centros de datos, instalaciones y equipos, mediante medidas de seguridad física apropiadas.

6. **Seguridad de sistemas y redes**: Comprende la implementación de controles de seguridad en los sistemas informáticos y las redes de comunicación para protegerlos contra amenazas y ataques.

7. **Seguridad de aplicaciones**: Se relaciona con la implementación de medidas de seguridad en las aplicaciones de software para prevenir vulnerabilidades y proteger la información procesada por dichas aplicaciones.

8. **Configuración segura**: Implica establecer y mantener una configuración segura en los sistemas y dispositivos, aplicando las mejores prácticas de seguridad y minimizando los riesgos de configuraciones inseguras.

9. **Gestión de identidades y accesos**: Incluye la administración y control de las identidades de los usuarios, así como el acceso a los recursos de información, asegurando que solo se otorguen los privilegios necesarios.

10. **Gestión de amenazas y vulnerabilidades**: Se refiere a la identificación, evaluación y gestión de las amenazas y vulnerabilidades que pueden afectar a los sistemas y la información de la institución.

11. **Continuidad**: Implica la planificación y preparación para mantener la continuidad de las operaciones en caso de incidentes de seguridad o desastres.

12. **Seguridad de las relaciones con proveedores**: Se refiere a la gestión de los riesgos de seguridad asociados a las relaciones con proveedores externos, garantizando la protección de la información compartida y los servicios contratados.

13. **Legal y cumplimiento**: Incluye el cumplimiento de las leyes, regulaciones y normativas aplicables a la seguridad de la información, así como el manejo de

aspectos legales relacionados con incidentes de seguridad.

14. **Gestión de eventos de seguridad de la información**: Comprende la detección, respuesta, investigación y gestión de los eventos de seguridad de la información, incluyendo la generación de registros y la realización de análisis forenses.

15. **Garantía de la seguridad de la información**: Se refiere a la implementación de actividades de control, auditoría y aseguramiento de la seguridad de la información, con el fin de garantizar su efectividad y cumplimiento

Estos valores atribuidos a las capacidades operativas, ayudan a evaluar y seleccionar los controles necesarios para abordar las distintas áreas de la seguridad de la información y asegurar un enfoque integral y adecuado para la protección de los activos de información de la institución.

e)Dominios de seguridad

Los dominios de seguridad representan un atributo para evaluar los controles desde la perspectiva de cuatro áreas principales de la seguridad de la información, estos dominios son:

1. **Gobernanza y ecosistema**: Este dominio abarca la gobernanza de la seguridad del sistema de información y la gestión de riesgos, así como la gestión de la ciberseguridad en el entorno general de la institución, incluyendo las partes interesadas internas y externas.

2. **Protección**: En este dominio se incluyen aspectos como la arquitectura de seguridad de TI, la administración de seguridad de TI, la gestión de acceso e identidad, el mantenimiento de seguridad de TI y la seguridad física y ambiental, se centra en la implementación de medidas y controles para proteger los activos de información.

3. **Defensa**: Este dominio engloba la detección y la gestión de incidentes de seguridad informática, se refiere a la capacidad de identificar y responder ante amenazas y ataques de seguridad, así como la gestión efectiva de los incidentes que puedan surgir.

4. **Resiliencia**: En este dominio se encuentran la continuidad de operaciones y la gestión de crisis, se enfoca en la planificación y preparación para mantener la continuidad de las operaciones de la organización, así como en la gestión de situaciones de crisis que puedan afectar a la seguridad de la información.

Estos dominios de seguridad proporcionan una estructura para categorizar y comprender los diferentes aspectos de la seguridad de la información. Los valores atribuidos a estos dominios son: Gobernanza y ecosistema, Protección, Defensa y Resiliencia.

Los atributos presentados en esta guía se eligen debido a su naturaleza genérica, lo que los hace aplicables a diferentes tipos de instituciones; estas instituciones tienen la flexibilidad de aceptar o ignorar uno o más de los atributos proporcionados según su gestión particular, además, tienen la opción de crear sus propios atributos si consideran que es necesario.

Diseño de los controles

Cada control tiene la siguiente estructura:

1. Título del control: Nombre abreviado del control, que nos da una referencia de su utilidad;
2. Tabla de atributos: Una tabla muestra los valores de cada atributo para el control dado;
3. Control: Cual es el control, descripción de su alcance;
4. Recomendaciones para la implementación: Una selección de las mejores opciones para implementar el control sin ser los únicos, pues cada institución puede tener otras opciones de acuerdo al giro de su negocio.

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

ÍNDICE

1. Controles organizacionales

1.1. Políticas de seguridad de la información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza y ecosistema #Resiliencia

Control

Definir la política de seguridad de la información y las políticas específicas del tema, las mismas deben ser aprobadas por la máxima autoridad y/o el nivel respectivo; publicadas, comunicadas y reconocidas por el personal institucional y las partes interesadas relevantes; estas deben ser revisadas a intervalos planificados y cuando ocurran cambios significativos.

Recomendaciones para la implementación:

a) La máxima autoridad dispondrá la implementación de este Esquema Gubernamental de Seguridad de la Información (EGSI) en la institución; las instituciones de la Administración Pública Central, que generan, utilizan, procesan, comparten y almacenan información en medios electrónicos o escritos, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera.

b) La máxima autoridad de la institución debe aprobar la Política de seguridad de la información (alto nivel) y cualquier cambio, elaborado / coordinado por el oficial de seguridad y revisada por el comité de seguridad de la información, definiendo la directriz necesaria para gestionar la seguridad de la información.

c) La política de seguridad de la información debe tomar en consideración los requisitos derivados de:

- Estrategia de la institución;
- Leyes, reglamentos en general la norma legal vigente.
- Los riesgos y amenazas actuales y proyectadas para la seguridad de la información.

d) La política de seguridad de la información debe contener declaraciones concernientes a:

- Definición de seguridad de la información;
- Objetivos de seguridad de la información o el marco de referencia para establecer objetivos de seguridad de la información:
- Principios para guiar todas las actividades relacionadas con la seguridad de la información;

- Compromiso de satisfacer los requisitos aplicables relacionados con la seguridad de la información:

- Compromiso con la mejora continua del sistema de gestión de seguridad de la información;

- Asignación de responsabilidades para la gestión de seguridad de la información a roles definidos;

- Procedimientos para el manejo de exenciones y excepciones.

e) En un nivel más bajo, la política de seguridad de la información debe estar respaldada por políticas específicas del tema según sea necesario, para una adecuada implementación de los controles de seguridad de la información.

f) Considerar que las políticas de temas específicos generalmente se estructuran para abordar las necesidades de ciertos grupos objetivo dentro de la institución o para cubrir ciertas áreas de seguridad.

g) Las políticas específicas de un tema deben estar alineadas y complementarse con la política de seguridad de la información institucional.

h) La responsabilidad del desarrollo de las políticas específicas del tema debe asignarse al personal pertinente en función de su nivel apropiado de autoridad y competencia técnica de cada área; la revisión y aprobación corresponde al comité de seguridad de la información.

i) El oficial de seguridad de la información realizará el seguimiento respectivo de la implementación de la política de seguridad de la información y las políticas específicas.

j) La política de seguridad de la información y las políticas específicas del tema deben socializarse a los funcionarios de la institución y a las partes interesadas en una forma que sea relevante, accesible y comprensible.

k) La política de seguridad de la información y las políticas específicas del tema pueden estar en un solo documento. La institución puede denominar a estas políticas temáticas como estándares, directivas, políticas u otros.

l) Para garantizar la vigencia de la política de seguridad de la información y las políticas específicas en la institución, estas deben ser revisadas al menos una vez al año y cuando se produzcan cambios significativos a nivel operativo, legal, tecnológico, económico, entre otros; los cuales deben ser documentados, versionados y socializados a las partes interesadas relevantes.

1.2. Roles y responsabilidades de seguridad de la información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad	#Identificar	#Gobernanza	#Gobernanza y ecosistema

	#Disponibilidad			#Protección #Resiliencia

Control

Definir y asignar los roles y responsabilidades de seguridad de la información de acuerdo a las necesidades de la institución.

Recomendaciones para la implementación:

La asignación de roles y responsabilidades de seguridad de la información debe hacerse de acuerdo con la política de seguridad de la información y las políticas específicas del control (ver 1.1).

a) La institución debe definir y gestionar las responsabilidades para, la protección de la información y otros activos asociados, realizar procesos específicos de seguridad de la información, actividades de gestión de riesgos de seguridad de la información y, en particular, aceptación de riesgos residuales (por ejemplo, para los propietarios de riesgos), todo el personal que utiliza la información de la institución y otros activos asociados.

b) Estas responsabilidades deben complementarse, cuando sea necesario, con una guía más detallada para sitios específicos e instalaciones de procesamiento de información.

c) Las personas con responsabilidades de seguridad de la información asignadas pueden asignar tareas de seguridad a otros. Sin embargo, siguen siendo responsables y deben determinar que las tareas delegadas se hayan realizado correctamente.

d) Cada área de seguridad de la cual los individuos son responsables debe definirse, documentarse y comunicarse.

e) Los niveles de autorización deben definirse y documentarse.

f) Las personas que asumen una función específica de seguridad de la información deben ser competentes en el conocimiento y las habilidades requeridas por la función y deben recibir apoyo para mantenerse al día con los desarrollos relacionados con la función y necesarios para cumplir con las responsabilidades de la función.

g) Designar un propietario para cada activo, quien luego se hace responsable de su protección.

h) Realizar el seguimiento de la puesta en marcha de las normas de este documento y disponer la difusión, capacitación y sensibilización del contenido.

1.3. Separación de funciones

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gobernanza #gestión_de_identidad_y_acceso	#Gobernanza y ecosistema

Control

Separar las funciones conflictivas y las áreas conflictivas de responsabilidad.

Recomendaciones para la implementación:

La separación de funciones y áreas de responsabilidad tiene como objetivo separar las funciones en conflicto entre diferentes individuos para evitar que un individuo ejecute funciones potencialmente en conflicto por su cuenta, es decir que no pueda acceder, modificar o utilizar los activos sin autorización o sin que se detecte.

a)La institución debe determinar qué funciones y áreas de responsabilidad necesitan separarse, los siguientes son ejemplos de actividades que pueden requerir separación:

- Iniciar, aprobar y ejecutar un cambio:
- Solicitar, aprobar e implementar derechos de acceso;
- Diseñar, implementar y revisar el código;
- Desarrollar software y administrar sistemas de producción;
- Usar y administrar aplicaciones;
- Utilizar aplicaciones y administrar bases de datos;
- Diseñar, auditar y asegurar los controles de seguridad de la información.

- Las instituciones de acuerdo a su categoría, pueden encontrar difícil lograr la segregación de funciones, en caso de no ser posible, considerar implementar otros controles, como el seguimiento de las actividades, las pistas de auditoría y la supervisión de la gestión.

1.4. Responsabilidades de la dirección

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza ecosistema

Control

La máxima autoridad debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos en la institución.

Recomendaciones para la implementación:

La máxima autoridad de la institución debe demostrar su apoyo, soporte a la política de

seguridad de la información, las políticas, los procedimientos y los controles de seguridad de la información específicos de cada tema.

Las responsabilidades de las autoridades deben incluir asegurar que el personal:

a)Este debidamente informado sobre sus roles y responsabilidades de seguridad de la información, a través del respectivo acuerdo de confidencialidad, antes de que se le conceda acceso a la información de la institución y otros activos asociados:

b)Cuente con directrices que establecen las expectativas de seguridad de la información de su rol dentro de la institución;

c) Tiene la obligación de cumplir con la política de seguridad de la información y las políticas de temas específicos de la institución;

d) Logre un nivel de conciencia de seguridad de la información relevante para sus roles y responsabilidades dentro de la institución (ver 2.3);

e)Acuerde el cumplimiento de los términos y condiciones laborales de acuerdo a la norma legal vigente y la relación laboral existente, incluida la política de seguridad de la información de la institución y los métodos de trabajo apropiados;

f) Continúe teniendo las habilidades, conocimiento y calificaciones apropiadas en seguridad de la información a través de la educación profesional.

g)Cuando sea factible, cuenten con un canal confidencial para denunciar violaciones de la política de seguridad de la información, políticas de temas específicos o procedimientos para la seguridad de la información ("denuncia"). Esto puede permitir informes anónimos o tener disposiciones para asegurar que el conocimiento de la identidad del denunciante sea conocido solo por aquellos que necesitan tratar con dichos informes.

h) Cuenten con los recursos adecuados y tiempo de planificación de proyectos para implementar los procesos y controles relacionados con la seguridad de la información de la institución.

1.5. Contacto con las autoridades

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Responder #Recuperar	#Gobernanza	#Defensa #Resiliencia

Control

La institución debe establecer y mantener contacto con las autoridades relevantes.

Recomendaciones para la implementación:

a) Establecer un procedimiento que especifique el contacto con autoridades a las cuales se reportarán incidentes derivados del incumplimiento de la política de seguridad o por acciones

de seguridad de cualquier origen (ej. fiscalía, policía, bomberos, 911, servicios públicos, servicios básicos, energía eléctrica, salud, otros). Todo incidente de seguridad de la información que sea considerado crítico deberá ser reportado al oficial de seguridad y este a su vez al comité de seguridad y la máxima autoridad según los casos.

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

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

d) Las instituciones bajo ataque pueden solicitar a las autoridades de acuerdo a la norma legal vigente que tomen medidas contra la fuente del ataque.

e) Mantener dichos contactos puede ser un insumo para respaldar la gestión de incidentes de seguridad de la información o los procesos de planificación de contingencia y continuidad del negocio

1.6. Contacto con grupos de interés especial

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder #Recuperar	#Gobernanza	#Defensa

Control

Establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales especializadas en seguridad de la información para mejorar el conocimiento.

Recomendaciones para la implementación:

La pertenencia a grupos o foros de intereses especiales deben considerarse como un medio para:

a) Mejorar el conocimiento sobre las mejores prácticas y mantenerse actualizado con la información de seguridad relevante;

b) Asegurarse de que la comprensión del entorno de seguridad de la información esté actualizada;

c) Recibir avisos tempranos de alertas, asesoramiento y parches relacionados con ataques a las vulnerabilidades de la institución, por parte de instituciones públicas, privadas y académicas reconocidas por su aporte en la gestión de la seguridad de la información;

d) Obtener acceso a asesoramiento especializado en seguridad de la información con otras instituciones;

e) Compartir e intercambiar información sobre nuevas tecnologías, productos, servicios, amenazas o vulnerabilidades entre las instituciones públicas que implementan el EGSI;

f) Proporcionar puntos de enlace adecuados cuando se trate de incidentes de seguridad de la información (ver 1.24 a 1.28).

1.7. Inteligencia de amenazas

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Detectar #Responder	#Gestión_amenazas_y_vulnerabilidades	#Defensa #Resiliencia

Control

La información relacionada con las amenazas a la seguridad de la información se debe recopilar y analizar para generar información sobre amenazas.

Recomendaciones para la implementación:

El objetivo primordial de este control es proporcionar conciencia del entorno de amenazas de la organización para que se puedan tomar las medidas de mitigación adecuadas, de acuerdo a las siguientes recomendaciones:

a) La información sobre amenazas existentes o emergentes se recopila y analiza para:

- Facilitar acciones informadas para evitar que las amenazas causen daño a la institución;
- Reducir el impacto de tales amenazas.

b) La inteligencia de amenazas se puede dividir en tres capas, todas las cuales deben tenerse en cuenta:

- Inteligencia de amenazas estratégicas: intercambio de información de alto nivel sobre el cambiante panorama de amenazas (por ejemplo, tipos de atacantes o tipos de ataques):
- Inteligencia de amenazas tácticas; información sobre las metodologías, herramientas y tecnologías involucradas del atacante:
- Inteligencia de amenazas operativas: detalles sobre ataques específicos, incluidos indicadores técnicos.

c) La inteligencia de amenazas debe ser:

- Relevante (es decir, relacionado con la protección de la institución);
- Perspicaz (es decir, proporcionando a la institución una comprensión precisa y

detallada del panorama de amenazas);

- Contextual, para brindar conciencia situacional (es decir, agregar contexto a la información en función del momento de los eventos, dónde ocurren, experiencias previas y prevalencia en instituciones similares);

- Procesable (es decir, la institución puede actuar sobre la información de manera rápida y efectiva).

d) Las actividades de inteligencia de amenazas deben incluir:

- Establecer objetivos para la producción de inteligencia sobre amenazas:
- Identificar, examinar y seleccionar fuentes de información internas y externas que sean necesarias y apropiadas para proporcionar la información requerida para la producción de inteligencia sobre amenazas;

- Recopilar información de fuentes seleccionadas, que pueden ser internas y externas:

- Tratar la información recopilada para prepararla para el análisis (por ejemplo, traduciendo, formateando o corroborando la información);

- Analizar la información para comprender cómo se relaciona y es significativa para la institución;

- Comunicar y compartir con personas relevantes en un formato que pueda ser comprensible.

e) La inteligencia de amenazas debe analizarse y utilizarse posteriormente:

- Implementando procesos para incluir información recopilada de fuentes de inteligencia de amenazas en los procesos de gestión de riesgos de seguridad de la información de la institución;

- Como entrada adicional a controles técnicos preventivos y de detección como firewalls, sistema de detección de intrusos o soluciones antimalware;

- Como entrada a los procesos y técnicas de prueba de seguridad de la información.

- La institución debe compartir la inteligencia sobre amenazas con otras instituciones responsables (Cert, cirt etc.) de forma mutua para mejorar la inteligencia sobre amenazas en general.

f) La inteligencia de amenazas a menudo la proporcionan proveedores o asesores independientes, agencias gubernamentales o grupos colaborativos de inteligencia de amenazas.

La eficacia de controles como 1.25, 4.7, 4.16 y 4.23 depende de la calidad de la inteligencia de amenazas disponible.

1.8. Seguridad de la información en la Gestión de proyectos

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Gobernanza	#Gobernanza_y_Ecosistema #Protección

Control

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

Recomendaciones para la implementación:

a) La gestión de proyectos en uso debe exigir que:

- Los riesgos de seguridad de la información se evalúen y traten en una etapa temprana y periódicamente como parte de los riesgos del proyecto a lo largo del ciclo de vida del proyecto;
- Los requisitos de seguridad de la información (Los requisitos de seguridad de la aplicación (4.26), los requisitos para cumplir con los derechos de propiedad intelectual (1.32), etc.) se abordan en las primeras etapas de los proyectos;
- Los riesgos de seguridad de la información asociados con la ejecución de proyectos, como la seguridad de los aspectos de comunicación interna y externa, se consideran y tratan a lo largo del ciclo de vida del proyecto;
- Se revisa el progreso en el tratamiento de riesgos de seguridad de la información y se evalúa y prueba la eficacia del tratamiento.

b) Los requisitos de seguridad de la información deben determinarse para todos los tipos de proyectos, no solo para los proyectos de desarrollo de TIC. También se deben considerar lo siguiente al determinar estos requisitos:

- Qué información está involucrada (determinación de la información), cuáles son las necesidades de seguridad de la información correspondientes (clasificación; ver 1.12) y el impacto potencial del negocio negativo que puede resultar de la falta de seguridad adecuada;
- Las necesidades de protección requeridas de la información y otros activos asociados involucrados, particularmente en términos de confidencialidad, integridad y disponibilidad;
- El nivel de confianza o seguridad requerido con respecto a la identidad reclamada de las entidades para derivar los requisitos de autenticación;
- Procesos de aprovisionamiento y autorización de acceso, para clientes y otros

usuarios potenciales de la institución, así como para usuarios privilegiados o técnicos, como miembros relevantes del proyecto, personal de operación potencial o proveedores externos;

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

- Requisitos derivados de los procesos de negocios, como registro y monitoreo de transacciones, requisitos de no repudio;

- Requisitos exigidos por otros controles de seguridad de la información, por ejemplo, interfaces para registro y monitoreo o sistemas de detección de fuga de datos;

- Cumplimiento del entorno legal, de acuerdo a norma legal vigente en el que opera la institución.

- El nivel de confianza o garantía requerido para que terceras partes cumplan con la política de seguridad de la información de la institución y las políticas específicas del tema, incluidas los capítulos de seguridad relevantes en cualquier acuerdo, contratos o norma legal vigente.

1.9. Inventario de información y otros activos asociados

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gestión_de_activos	#Gobernanza_y_Ecosistema #Protección

Control

Elaborar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.

Recomendaciones para la implementación:

<u>Inventario</u>

a) La institución debe identificar su información y otros activos asociados y determinar su importancia en términos de seguridad de la información. La documentación debe mantenerse en un lugar dedicado o inventarios existentes, según corresponda.
b) Inventariar los activos primarios, en formatos físicos y/o electrónicos

- Los procesos estratégicos, claves y de apoyo de la institución, activos de información.
- Las normas y reglamentos que son la razón de ser de la institución.
- Planes estratégicos y operativos de la institución y áreas específicas.
- Los archivos generados por los servidores públicos, tanto de manera física como electrónica, razón de ser de la función que desempeñan en la institución.

- Los manuales e instructivos de sistemas informáticos: instalación, guía de usuario, operación, administración, mantenimiento, entre otros.
- De la operación de los aplicativos informáticos de los servicios informáticos: datos y meta-datos asociados, archivos de configuración, código fuente, respaldos, versiones, etc.
- Del desarrollo de aplicativos de los servicios informáticos: actas de levantamiento de requerimientos, documento de análisis de requerimientos, modelos entidad - relación, diseño de componentes, casos de uso, diagramas de flujo y estado, casos de prueba, etc.
- Del soporte de aplicativos de los servicios informáticos: tickets de soporte, reportes físicos y electrónicos, evaluaciones y encuestas, libros de trabajo para capacitación, etc.
- De la imagen corporativa de la institución: manual corporativo (que incluye manual de marca y fuentes en formato electrónico de logos), archivos multimedia, tarjetas de presentación, volantes, banners, trípticos, etc.

c) Inventariar los activos de soporte de Hardware

- Equipos móviles: teléfono celular, tableta, computador portátil, etc.
- Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, etc.
- Periféricos de entrada: teclado, ratón, micrófono, escáner plano, escáner de mano, cámara digital, cámara web, lápiz óptico, pantalla táctil, etc.
- Periféricos de salida: monitor, proyector, audífonos, parlantes, impresora láser, impresora de inyección de tinta, impresoras, plóter, etc.
- Periféricos y dispositivos de almacenamiento: sistema de almacenamiento (NAS, SAN), librería de cintas, cintas magnéticas, disco duro externos, memoria USB, etc.
- Periféricos de comunicaciones: tarjeta USB para redes inalámbricas (Wi-Fi, Bluetooth),
- Tableros: de transferencia (bypass) de la unidad ininterrumpible de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc.
- Sistemas: de control de accesos, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión, etc.

d) Inventariar los activos de soporte de Software

- Sistemas operativos.
- Software de servicio, mantenimiento o administración de: gabinetes de servidores de cuchilla, servidores (estantería/rack, torre, virtuales), sistema de redes de datos, sistemas de almacenamiento (NAS, SAN), telefonía, sistemas (de UPS, grupo electrógeno, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión), etc.
- Paquetes de software o software base de: suite de ofimática, navegador de Internet, cliente de correo electrónico, mensajería instantánea, edición de imágenes, vídeo conferencia, servidor (proxy, de archivos, de correo electrónico, de impresiones, de mensajería instantánea, de aplicaciones, de base de datos), etc.
- Aplicativos informáticos del negocio.

e) Inventariar los activos de soporte de redes.

- Panel de conexión (patch panel), tomas o puntos de red, racks (cerrado o abierto, de piso o pared), etc.
- Switchs (de centros de datos, de acceso, de borde, de gabinete de servidores, access-point, transceiver, equipo terminal de datos, etc.).
- Ruteador (router), cortafuego (firewall), controlador de red inalámbrica, etc.
- Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, balanceador de carga, switch de contenido, etc.

f) Inventariar los activos referentes a la estructura organizacional

- Estructura organizacional de la institución, que incluya todas las unidades administrativas con los cargos y nombres de las autoridades.
- Estructura organizacional del área de las TIC, con los cargos y nombres del personal: administrador (de servidores, de redes de datos, de respaldos de la información, de sistemas de almacenamiento, de bases de datos, de seguridades, de aplicaciones del negocio, de recursos informáticos, etc.), líder de proyecto, personal de capacitación, personal de mesa de ayuda, personal de aseguramiento de calidad, programadores).
- Inventario referente a los sitios y edificaciones de la institución: dirección, correo electrónico, guía institucional, planos arquitectónicos, estructurales, eléctricos, sanitarios, de datos, etc.
- De los servicios esenciales: número de teléfono fijo y/o celular del proveedor de servicios de Internet, transmisión de datos, suministro de energía eléctrica, suministro de agua potable, etc.

g) Realizar revisiones periódicas de la información identificada y otros activos asociados contra el inventario de activos;

h) Hacer cumplir automáticamente una actualización de inventario en el proceso de instalación, cambio o eliminación de un activo.

Cada activo debe clasificarse de acuerdo con la clasificación de la información (ver 1.12) asociada a ese activo.

Propiedad

a) Para la información identificada y otros activos asociados, la propiedad del activo debe asignarse a un individuo o grupo y se debe identificar la clasificación (ver 1.12, 1.13).

b) Se debe implementar un proceso para asegurar la asignación oportuna de la propiedad de los activos.

c) La propiedad debe asignarse cuando se crean los activos o cuando se transfieren los activos a la institución.

d) La propiedad de los activos debe reasignarse según sea necesario cuando los propietarios actuales de los activos se van o cambian de puesto.

Deberes del propietario

El propietario del activo debe ser responsable de la gestión adecuada de un activo durante todo el ciclo de vida del activo, asegurando que:

a) Se inventarían la información y otros activos asociados;

b) La información y otros activos asociados estén debidamente clasificados y protegidos;

c) La clasificación se revisa periódicamente de acuerdo a la necesidad institucional;

d) Se enumeran y vinculan los componentes que respaldan los activos tecnológicos, como bases de datos, almacenamiento, componentes y subcomponentes de software;

e) Se establecen los requisitos para el uso aceptable de la información y otros activos asociados (ver 1.10);

f) Las restricciones de acceso correspondan con la clasificación y que sean efectivas y sean revisadas periódicamente;

g) La información y otros activos asociados, cuando se eliminen, se manejen de manera segura y se eliminen del inventario;

h) Estén involucrados en la identificación y gestión de riesgos asociados con su(s) activo(s);

i) Apoyan al personal que tiene los roles y responsabilidades de administrar su información.

Los activos de información deberán ser actualizados al menos una vez al año o ante cualquier modificación.

1.10. Uso aceptable de la información y otros activos asociados

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos #Información_protección	#Gobernanza_y_Ecosistema #Protección

Control

Identificar, documentar e implementar reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.

Recomendaciones para la implementación:

Los usuarios internos y externos que utilicen o tengan acceso a la información de la institución y otros activos asociados deben conocer los requisitos de seguridad de la información para proteger y manejar la información de la institución y otros activos asociados.

a) La institución debe establecer una política específica de un tema para el uso aceptable de

la información y otros activos asociados y comunicarla a las partes interesadas.

La política específica del tema debería establecer:

- comportamientos esperados e inaceptables de las personas desde una perspectiva de seguridad de la información;
- Uso permitido y prohibido de información y otros activos asociados;
- Las actividades de monitoreo que realiza la institución.

b) Se debe elaborar procedimientos de uso aceptable para todo el ciclo de vida de la información de acuerdo a su clasificación (ver 1.12) y riesgos determinados. Se deben considerar los siguientes elementos:

- Restricciones de acceso que respaldan los requisitos de protección para cada nivel de clasificación;
- Mantenimiento de un registro de los usuarios autorizados de información y otros activos asociados;
- Protección de copias temporales o permanentes de información a un nivel consistente con la protección de la información original;
- Almacenamiento de activos asociados con la información de acuerdo con las especificaciones de los fabricantes (ver 3.8):
- Marcado claro de todas las copias de los medios de almacenamientos (electrónicos o físicos) para la atención del destinatario autorizado (ver 3.10);
- Autorización de eliminación de información y otros activos asociados y método(s) de eliminación admitidos (ver 4.10).
- El Oficial de Seguridad de la Información es el encargado de asegurar que los lineamientos para la utilización de los recursos de las Tecnologías de la Información contemplen los requerimientos de seguridad establecidos, según la criticidad de la información que procesan
- Reglamentar el uso de correo electrónico institucional:
    - Este servicio debe utilizarse exclusivamente para las tareas propias de las funciones que se desarrollan en la institución y no debe utilizarse para ningún otro fin.
    - Cada persona es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte.
    - Todos los mensajes deben poder ser monitoreados y respaldados.
    - Toda cuenta de correo electrónico debe estar asociada a una cuenta de usuario.
    - Debe definirse un espacio de almacenamiento de acuerdo a los recursos existentes y a la necesidad definida por la institución.
    - Todo sistema debe contar con las facilidades automáticas que notifiquen al

usuario cuando un mensaje enviado por él no es recibido correctamente por el destinatario, describiendo detalladamente el motivo del error.
- Deben utilizarse programas que monitoreen el accionar de virus informáticos tanto en mensajes como en archivos adjuntos, antes de su ejecución.
- Todo usuario es responsable por la destrucción de los mensajes con origen desconocido, y asume la responsabilidad por las consecuencias que pueda ocasionar la ejecución de los archivos adjuntos, en estos casos, no deben contestar dichos mensajes y deben enviar una copia al Oficial de Seguridad de la Información para que efectúe el seguimiento y la investigación necesaria.
- Para el envío y la conservación de la información, debe implementarse el cifrado (criptografía) de datos.
- Todo usuario es responsable de la cantidad y tamaño de mensajes que envíe. Debe controlarse el envío no autorizado de correos masivos.
- Para evitar la fuga de información sensible se debe bloquear y prohibir el acceso y uso de servicios de correo electrónico de libre uso tales como: Gmail, Hotmail, Yahoo, entre otros.

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

    - El Oficial de Seguridad de la Información en coordinación con el área tecnológica, debe elaborar, poner en marcha y controlar la aplicación de un procedimiento institucional para acceso y uso de la Internet y la Web por parte de todo funcionario sin excepción, y en el cual se acepten las condiciones aquí especificadas y otras que la institución considere apropiadas.
    - Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la institución, y no debe utilizarse para ningún otro fin.
    - Cada usuario es responsable de la información y contenidos a los que accede y de aquella que copia para conservación en los equipos de la institución.
    - Debe limitarse a los usuarios el acceso a portales, aplicaciones o servicios de la Internet y la Web que pudieren perjudicar los intereses y la reputación de la institución. Específicamente, se debe bloquear el acceso por medio de dispositivos fijos y/o móviles a aquellos portales, aplicaciones o servicios de la Internet y la Web sobre pornografía, racismo, violencia, delincuencia o de contenidos ofensivos y contrarios a los intereses, entre otros, y valores de la institución o que impacten negativamente en la productividad y trabajo de la institución (ej., mensajería instantánea-chats, redes sociales, video, otros) y particularmente a los que atenten a la ética y moral.
    - Todos los accesos deben poder ser sujetos de monitoreo y conservación permanente por parte de la institución.
    - El Oficial de Seguridad de la Información, puede acceder a los contenidos monitoreados, con el fin de asegurar el cumplimiento de las medidas de seguridad.
    - La institución podrá en cualquier momento bloquear o limitar el acceso y uso de la Internet a los funcionarios o a terceros que accedan tanto por medio alámbrico como inalámbrico.

- Reglamentar el uso de los sistemas de video-conferencia:

    - Definir un responsable para administrar el sistema de video-conferencia.
    - Crear contraseñas para el ingreso a la configuración de los equipos y/o para las

salas virtuales de video-conferencia.
- Deshabilitar la respuesta automática de los equipos de video-conferencia y todo procedimiento que sea necesario para mantener la seguridad del tráfico.

1.11. Devolución de activos

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos	#Protección

Control

El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la institución que estén en su poder al cambiar o terminar su relación laboral, contrato o acuerdo; **asegurándose por parte del Nivel jerárquico Superior el cumplimiento**

Recomendaciones para la implementación:

a) El proceso de cambio o terminación se debe formalizar para incluir la devolución de todos los activos físicos y electrónicos emitidos anteriormente que sean propiedad de la institución o estén encomendados a ella.

b) En los casos en que el personal y otras partes interesadas compren el equipo de la institución o usen su propio equipo personal, se deben seguir los procedimientos para asegurar que toda la información relevante sea rastreada y transferida a la institución y eliminada de manera segura del equipo (ver 3.14).

c) En los casos en que el personal y otras partes interesadas tengan conocimientos que sean importantes para las operaciones en curso, esa información debe documentarse y transferirse a la institución.

d) Durante el periodo de notificación y posteriormente, la institución debe evitar la copia no autorizada de información relevante (por ejemplo, propiedad intelectual) por parte del personal bajo notificación de terminación de la relación laboral.

La institución debe identificar y documentar claramente toda la información y otros activos asociados que se devolverán, que pueden incluir:

a) Dispositivos de punto extremo de usuario;

b) Dispositivos portátiles de almacenamiento;

c) Equipo especializado;

d) Hardware de autenticación (por ejemplo, llaves mecánicas, fichas físicas y tarjetas inteligentes) para sistemas de información, sitios y archivos físicos:

e) Copias físicas de la información.

a) En el caso de ser difícil devolver la información que se tiene sobre los activos que no son propiedad de la organización. En tales casos, es necesario restringir el uso de la información utilizando otros controles de seguridad de la información, como la gestión de derechos de acceso (1.18) o el uso de criptografía (4.24).

1.12. Clasificación de la información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Información_protección	#Protección #Defensa

Control

La información se debe clasificar de acuerdo con las necesidades de seguridad de la información de la institución, normativa legal vigente en función de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.

Recomendaciones para la implementación:

a) La institución debe establecer una política específica sobre la clasificación de la información y comunicarla a todas las partes interesadas relevantes.

b) Elaborar y aprobar un catálogo de clasificación de la información, se la deberá clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la institución.

c) La institución debe tener en cuenta los requisitos de confidencialidad, integridad y disponibilidad en el esquema de clasificación.

d) Las clasificaciones y los controles de protección asociados para la información deben tener en cuenta las necesidades de negocios para compartir o restringir la información.

e) La institución debe proteger la integridad de la información y asegurar la disponibilidad, así como los requisitos legales relacionados con la confidencialidad, integridad o disponibilidad de la información.

f) Los activos distintos de la información también pueden clasificarse de acuerdo con la clasificación de la información, que se almacena, procesa o maneja o protege de otro modo por el activo.

g) Los propietarios de la información deben ser responsables de su clasificación, con el apoyo del área jurídica.

h) El esquema de clasificación debe incluir reuniones para la clasificación y criterios para la revisión de la clasificación a lo largo del tiempo.

i) Los resultados de la clasificación deben actualizarse de acuerdo con los cambios del valor, la sensibilidad y la criticidad de la información a lo largo de su ciclo de vida.

j) El esquema debe estar alineado con la política específica del tema sobre el control de acceso y debe poder abordar las necesidades de negocios específicos de la institución.

k) La clasificación puede ser determinada por el nivel de impacto que el compromiso de la información tendría para la institución. Cada nivel definido en el esquema debe recibir un nombre que tenga sentido en el contexto de la aplicación del esquema de clasificación.

l) El esquema debe ser consistente en toda la institución e incluirse en sus procedimientos para que todos clasifiquen la información y otros activos asociados aplicables de la misma manera.

1.13. Etiquetado de la información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operacionales	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Protección	#Información_protección	#Protección #Defensa

Control

Desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la institución.

Recomendaciones para la implementación:

Los procedimientos deben dar orientación sobre dónde y cómo se colocan las etiquetas teniendo en cuenta cómo se accede a la información o cómo se manejan los activos según los tipos de medios de almacenamiento.

a) Los procedimientos para el etiquetado de la información deben cubrir la información y otros activos asociados en todos los formatos de ser necesario. El etiquetado debe reflejar el esquema de clasificación establecido en 1.12

b) Las etiquetas deben ser fácilmente reconocibles

c) Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la institución.

d) Definir procedimientos en casos en los que se omite el etiquetado (por ejemplo, etiquetado de información no confidencial para reducir la carga de trabajo);

e) Etiquetar la información enviada o almacenada en medios electrónicos o físicos, o cualquier otro formato;

f) Cómo manejar los casos en los que el etiquetado no es posible (por ejemplo, debido a restricciones técnicas).

g) En caso de destrucción de un activo, la etiqueta asociada a éste debe mantenerse en el inventario respectivo con los registros de las acciones realizadas

Los ejemplos de técnicas de etiquetado incluyen:

a) Etiquetas físicas;

b) Encabezados y pies de página;

c) Metadatos;

d) Marca de agua;

e) Sellos de caucho.

La información digital debe utilizar metadatos para

a) Identifican gestionar y controlar la información, especialmente en lo que respecta a la confidencialidad. Los metadatos también deben permitir una búsqueda eficiente y correcta de información, los metadatos deben facilitar que los sistemas interactúen y tomen decisiones en función de las etiquetas de clasificación asociadas.

b) Los procedimientos deben describir cómo adjuntar metadatos a la información, qué etiquetas usar y cómo se deben manejar los datos, de acuerdo con el modelo de información y la arquitectura de TIC de la institución.

c) Los sistemas deben agregar metadatos adicionales relevantes cuando procesan información según sus propiedades de seguridad de la información.

d) El personal y otras partes interesadas deben conocer los procedimientos de etiquetado. Todo el personal debe recibir la capacitación necesaria para asegurar que la información esté correctamente etiquetada y manejada en consecuencia.

e) Los resultados de los sistemas que contienen información clasificada como confidencial o crítica deben llevar una etiqueta de clasificación adecuada.

f)El etiquetado de la información clasificada es un requisito clave para el intercambio de información.

1.14. Transferencia de información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Protección	#Gestión_de_activos #Información_protección	#Protección

Control

Elaborar y documentar, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la institución y terceros.

Recomendaciones para la implementación:

General

La institución debe establecer y comunicar una política específica del tema sobre la transferencia de información a todas las partes interesadas relevantes. Normas, procedimientos y acuerdos para proteger la información en tránsito debe reflejar la clasificación de la información involucrada. Cuando la información se transfiera entre la institución y terceros, los acuerdos de transferencia (incluida la autenticación del destinatario) deben ser establecido y mantenido para proteger la información en todas sus formas en tránsito (ver 1.10)

La transferencia de información puede ocurrir a través de transferencia electrónica, transferencia de medios de almacenamiento físico y transferencia verbal.

Para todo tipo de transferencia de información, las reglas, procedimientos y acuerdos deben incluir:

a) Controles diseñados para proteger la información transferida de la intercepción, el acceso no autorizado, la copia, la modificación, el enrutamiento incorrecto, la destrucción y la denegación de servicio, incluidos los niveles de control de acceso acordes con la clasificación de la información involucrada y cualquier control especial que se requiera para proteger la información confidencial, como el uso de técnicas criptográficas (ver 4.24);

b) Controles para asegurar la trazabilidad y el no repudio, incluido el mantenimiento de una cadena de custodia de la información durante el tránsito;

c) Identificación de los contactos apropiados relacionados con la transferencia, incluidos los propietarios de la información, los propietarios del riesgo, los oficiales de seguridad y los custodios de la información, según corresponda;

d) Responsabilidades y obligaciones en caso de incidentes de seguridad de la información, como la pérdida de medios físicos de almacenamiento o datos:

e) Uso de un sistema de etiquetado acordado para información sensible o critica, asegurando que el significado de las etiquetas se comprenda de inmediato y que la información esté debidamente protegida (ver 1.13);

f) Confiabilidad y disponibilidad del servicio de transferencia;

g) La política o lineamientos específicos del tema sobre el uso aceptable de las instalaciones de transferencia de información (ver 1.10);

h) Directrices de retención y eliminación para todos los registros de negocios, incluidos los mensajes; pueden existir leyes y reglamentos propios con respecto a la retención y eliminación de registros de negocios.

i) La consideración de cualquier otro requisito legal, estatutario, reglamentario y contractual relevante (ver 1.31, 1.32, 1.33, 1.34) relacionado con la transferencia de información (por ejemplo, requisitos para firmas electrónicas).

Transferencia electrónica

Las reglas, los procedimientos y los acuerdos también deben considerar los siguientes

elementos al utilizar las instalaciones de comunicación electrónica para la transferencia de información:

a) Detección y protección contra malware que puede transmitirse mediante el uso de comunicaciones electrónicas (ver 4.7);

b) Protección de la información electrónica sensible comunicada que se encuentra en forma de archivo adjunto;

c) Prevención contra el envío de documentos y mensajes en las comunicaciones a la dirección o número equivocado;

d) Obtener aprobación antes de utilizar servicios públicos externos, como mensajería instantánea, redes sociales, uso compartido de archivos o almacenamiento en la nube;

e) Niveles más fuertes de autenticación al transferir información a través de redes de acceso público;

f) Restricciones asociadas con las instalaciones de comunicación electrónica (por ejemplo, impedir el reenvío automático de correo electrónico a direcciones de correo externas);

g) Advertir al personal y otras partes interesadas que no envíen servicios de mensajes cortos (SMS) o mensajes instantáneos con información crítica ya que estos pueden ser leídos en lugares públicos (y por lo tanto por personas no autorizadas) o almacenados en dispositivos no protegidos adecuadamente;

h) Tomar en cuenta consideraciones legales como la de firmas electrónicas.

i) Asesorar al personal y otras partes interesadas sobre los problemas de uso de máquinas o servicios de fax, según:

   1) acceso no autorizado a los almacenes de mensajes incorporados para recuperar mensajes:

   2) programación deliberada o accidental de máquinas para enviar mensajes a números específicos.

<u>Transferencia de medios de almacenamiento físico</u>

Al transferir medios físicos de almacenamiento (incluido el papel), las reglas, los procedimientos y los acuerdos también deben incluir:

a) Responsabilidades de control y notificación de la transmisión, despacho y recepción;

b) Asegurar el correcto direccionamiento y transporte del mensaje;

c) Embalaje que proteja el contenido de cualquier daño físico que pueda surgir durante el tránsito y de acuerdo con las especificaciones de los fabricantes, por ejemplo, protegiendo contra cualquier factor ambiental que pueden reducir la eficacia de la restauración de los medios de almacenamiento, como la exposición al calor, la humedad o los campos

electromagnéticos; utilizar estándares técnicos mínimos para el embalaje y la transmisión (por ejemplo, el uso de sobres opacos);

d)Una lista de mensajeros confiables autorizados acordados por las autoridades;

e)Normas de identificación del mensajero;

f) Según el nivel de clasificación de la información en los medios de almacenamiento que se transportarán, utilizar controles a prueba de manipulaciones o inviolables (por ejemplo, bolsas, contenedores);

g)Procedimientos para verificar la identificación de los mensajeros;

h) Lista aprobada de terceras partes que prestan servicios de transporte o mensajería según la clasificación de la información;

i) Llevar registros para identificar el contenido de los medios de almacenamiento, la protección aplicada, así como registrar la lista de destinatarios autorizados, los tiempos de transferencia a los custodios de tránsito y la recepción en destino.

Transferencia verbal

Para proteger la transferencia verbal de información, se debe recordar al personal y otras partes interesadas que deben:

a) No tener conversaciones verbales confidenciales en lugares públicos o por canales de comunicación inseguros, ya que pueden ser escuchadas por personas no autorizadas;

b) No dejar mensajes que contengan información confidencial en contestadores automáticos o mensajes de voz, ya que estos pueden ser reproducidos por personas no autorizadas, almacenados en sistemas comunales o almacenados incorrectamente como resultado de una marcación incorrecta;

c) Ser proyectado al nivel apropiado para escuchar la conversación;

d) Asegurarse de que se implementen los controles de sala apropiados (por ejemplo, insonorización, puerta cerrada);

e) Comenzar cualquier conversación delicada con un descargo de responsabilidad para que los presentes sepan el nivel de clasificación y los requisitos de manejo de lo que están a punto de escuchar.

1.15. Control de acceso

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Protección	#Gestión_de_identidad_acceso	#Protección

Control

Elaborar, implementar y socializar la política para controlar el acceso físico y lógico a la información y otros activos asociados en función de los requisitos institucionales y de seguridad de la información.

Recomendaciones para la implementación:

Los propietarios de la información y otros activos asociados deben determinar la seguridad de la información y los requisitos de negocios relacionados con el control de acceso, debe definirse una política de tema específico sobre control de acceso que tenga en cuenta estos requisitos y debe comunicarse a todas las partes interesadas relevantes.

Estos requisitos y la política específica del tema deben considerar lo siguiente

a) Determinar qué entidades requieren qué tipo de acceso a la información y otros activos asociados;

b) Seguridad de las aplicaciones (ver 4.26);

c) Acceso físico, que debe estar respaldado por controles de entrada físicos apropiados (ver 3.2, 3.3, 3.4);

d) Diseminación y autorización de la información (por ejemplo, el principio de necesidad de saber) y niveles de seguridad de la información y clasificación de la información (ver 1.10, 1.12, 1.13);

e) Restricciones al acceso privilegiado (ver 4.2);

f) Separación de funciones (ver 1.3);

g) La legislación, los reglamentos y las obligaciones contractuales pertinentes con respecto a la limitación del acceso a datos o servicios (ver 1.31, 1.32, 1.33, 1.34, 4.3);

h) Separación de funciones de control de acceso (por ejemplo, solicitud de acceso, autorización de acceso, administración de acceso);

i) Autorización formal de solicitudes de acceso (ver 1.16 y 1.18);

j) La gestión de los derechos de acceso (ver 1.18);

k) Registro (ver 4.15).

l) Las reglas de control de acceso deben implementarse definiendo y mapeando los derechos y restricciones de acceso apropiados para las entidades relevantes (ver 1.16).

m) Una entidad puede representar tanto a un usuario humano como a un elemento técnico o lógico (por ejemplo, una máquina, un dispositivo o un servicio).

n) Para simplificar la gestión del control de acceso, se pueden asignar roles específicos a grupos de entidades.

Se debe tener en cuenta lo siguiente al definir e implementar reglas de control de acceso:

a) Coherencia entre los derechos de acceso y la clasificación de la información;

b) Coherencia entre los derechos de acceso y las necesidades y requisitos de seguridad del perímetro físico;

c) Considerar todos los tipos de conexiones disponibles en entornos distribuidos para que las entidades solo tengan acceso a la información y otros activos asociados, incluidas las redes y la red servicios, que estén autorizados a utilizar;

d) Considerar cómo se pueden reflejar los elementos o factores relevantes para el control de acceso dinámico

e) Considerar la norma legal vigente sobre el acceso a datos o servicios.

A menudo se utilizan principios generales en el contexto del control de acceso dos de los principios más utilizados son:

a) Necesidad de saber: una entidad solo tiene acceso a la información que esa entidad requiere para realizar sus tareas (diferentes tareas o roles significan diferente información de necesidad de saber y, por lo tanto, diferentes perfiles de acceso);

b) Necesidad de uso: a una entidad solo se le asigna acceso a la infraestructura de tecnologías de la información cuando existe una necesidad clara.

Se debe tener cuidado al especificar reglas de control de acceso para considerar:

a) Establecer reglas basadas en la premisa del privilegio mínimo, “En general, todo está prohibido a menos que esté expresamente permitido", en lugar de la regla más débil, “En general, todo está permitido a menos que esté expresamente prohibido;

b) Cambios en las etiquetas de información (ver 1.13) que son iniciados automáticamente por las instalaciones de tratamiento de información y aquellos iniciados a discreción de un usuario;

c) Cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos iniciados por un administrador;

d) Cuando definir y revisar periódicamente la aprobación.

1.16. Gestión de identidad

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Protección	#Gestión_de_identidad_acceso	#Protección

Control

Elaborar, implementar y socializar el procedimiento para gestionar el ciclo de vida completo de las identidades, entendiéndose como identidad la identificación única de personas y sistemas que acceden a la información de la institución y otros activos asociados y permitir la asignación adecuada de derechos de acceso.

Recomendaciones para la implementación:

Los procesos utilizados en el contexto de la gestión de la identidad deben asegurar que:

a) Para las identidades asignadas a personas, una identidad específica solo se vincula a una sola persona para poder responsabilizar a la persona por las acciones realizadas con esta identidad específica;

b) Las identidades asignadas a varias personas (por ejemplo, identidades compartidas) solo se permiten cuando son necesarias por razones de negocios u operativas y están sujetas a aprobación y documentación especificas;

c) Las identidades asignadas a entidades no humanas están sujetas a una aprobación segregada adecuada y a una supervisión continua independiente;

d) Las identidades se deshabilitan o eliminan de manera oportuna si ya no son necesarias (por ejemplo, si sus entidades asociadas se eliminan o ya no se usan, o si la persona vinculada a una entidad ha dejado la institución, ha cambiado de función o por ausencia temporal);

e) En un dominio específico, una sola identidad se asigna a una sola entidad, [es decir, se evita el mapeo de múltiples identidades a la misma entidad dentro del mismo contexto (identidades duplicadas)]:

f) Se mantengan registros de todos los eventos importantes relacionados con el uso y la gestión de las identidades de los usuarios y de la información de autenticación.

g) Mantener un registro de la gestión de accesos a aplicaciones, redes, que evidencie, fecha de creación, eliminación, suspensión, activación o eliminación del acceso; al igual que de cada identidad, disponer de los permisos de acceso que han sido asignados

h) Crear los accesos para los usuarios, para lo cual la institución debe generar convenios de confidencialidad y responsabilidad con el usuario solicitante; además, validar que el usuario tenga los documentos de ingreso con Recursos Humanos (o quien haga estas funciones) en orden y completos

i) La institución debe contar con un proceso de soporte para manejar los cambios en la información relacionada con las identidades de los usuarios Estos procesos pueden incluir la re verificación de documentos confiables relacionados con una persona.

j) Al utilizar identidades proporcionadas o emitidas por terceras partes (por ejemplo, credenciales de redes sociales), la institución debe asegurarse de que las identidades de terceras partes provean el nivel de confianza requerido y que los riesgos asociados se conozcan y se traten adecuadamente. Esto puede incluir controles relacionados con terceras partes (ver 1.19), así como controles relacionados con la información de autenticación asociada (ver 1.17).

1.17. Información de autenticación

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Protección	#Gestión_de_identidad_acceso	#Protección

Control

Elaborar, implementar y socializar la asignación y gestión de la información de autenticación, esta debe controlarse mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.

Recomendaciones para la implementación:

Asignación de información de autenticación

El proceso de asignación y gestión debe asegurar que:

a) Las contraseñas personales o los números de identificación personal (PIN) generados automáticamente durante los procesos de enrolamiento, ya que la información de autenticación secreta temporal no se puede adivinar y es única para cada persona, y que los usuarios están obligados a cambiarlos después del primer uso;

b) Se establecen procedimientos para verificar la identidad de un usuario antes de proporcionar información de autenticación nueva, de reemplazo o temporal;

c) La información de autenticación, incluida la información de autenticación temporal, se transmite a los usuarios de manera segura (por ejemplo, a través de un canal autenticado y protegido) y se evita el uso de mensajes de correo electrónico sin protección (texto claro) para este fin;

d)Los usuarios acusan recibo de la información de autenticación;

e) La información de autenticación predeterminada predefinida o proporcionada por los proveedores se cambia inmediatamente después de la instalación de sistemas o software;

f) Se mantienen registros de los eventos importantes concernientes con la asignación y gestión de la información de autenticación y se garantiza su confidencialidad, y se aprueba el método de mantenimiento de registros (por ejemplo, mediante el uso de una herramienta de bóveda de contraseñas aprobada).

Responsabilidades del usuario

Cualquier persona que tenga acceso o utilice información de autenticación debe ser advertida de que se asegure de que:

a) La información de autenticación secreta, como las contraseñas, se mantiene confidencial. La información de autenticación secreta personal no debe compartirse con nadie. La

información de autenticación secreta utilizada en el contexto de identidades vinculadas a múltiples usuarios o vinculadas a entidades no personales se comparte únicamente con personas autorizadas (Ej. acuerdos de confidencialidad específicos, otros);

b)La información de autenticación afectada o comprometida se cambia inmediatamente después de la notificación o cualquier otra indicación de un compromiso;

c) Cuando se utilizan contraseñas como información de autenticación, se seleccionan contraseñas seguras de acuerdo con las recomendaciones de las mejores prácticas, por ejemplo:

1) Las contraseñas no se basan en nada que otra persona pueda adivinar u obtener fácilmente utilizando información relacionada con la persona (por ejemplo, nombres, números de teléfono y fechas de nacimiento);

2) Las contraseñas no se basan en palabras del diccionario o combinaciones de las mismas (palabras o secuencias ordinarias);

3) Use frases de contraseñas fáciles de recordar e intente incluir caracteres alfanuméricos y especiales;

4) Las contraseñas tienen una longitud mínima (16 caracteres);

d)Las mismas contraseñas no se utilizan en distintos servicios y sistemas;

e)La obligación de seguir estas reglas también está incluida en los términos y condiciones del funcionario en el acuerdo de confidencialidad (ver 2.2).

Sistema de gestión de contraseñas

Cuando se utilizan contraseñas como información de autenticación, el sistema de administración de contraseñas debe:

a) Permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para abordar los errores de entrada;

b) Aplicar contraseñas seguras de acuerdo con las recomendaciones de buenas prácticas;

c) Obligar a los usuarios a cambiar sus contraseñas en el primer inicio de sesión;

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

e) Hacer cumplir los cambios de contraseña según sea necesario, por ejemplo, después de un incidente de seguridad, o al terminar o cambiar de empleo cuando un usuario tiene contraseñas conocidas para identidades que permanecen activas (por ejemplo, identidades compartidas);

f) Evitar la reutilización de contraseñas anteriores;

g) Evitar el uso de contraseñas de uso común y nombres de usuario comprometidos, combinaciones de contraseñas de sistemas pirateados;

h)No mostrar contraseñas en la pantalla cuando se ingresan;

i) Almacenar y transmitir contraseñas en forma protegida.

El cifrado y el hashing de contraseñas deben realizarse de acuerdo con las técnicas criptográficas aprobadas para contraseñas (ver 4.24).

1.18. Derechos de acceso

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Protección	#Gestión_de_identidad_acceso	#Protección

Control

Revisar, modificar y eliminar los derechos de acceso a la información y otros activos asociados, de acuerdo con la política y reglas de control de acceso específicas de la institución.

Recomendaciones para la implementación:

El proceso de aprovisionamiento para asignar o revocar los derechos de acceso físico y lógico otorgados a la identidad autenticada de una entidad debe incluir:

Concesión y revocación de los derechos de acceso

a) Obtener autorización del propietario de la información y otros activos asociados para el uso de la información y otros activos asociados (ver 1.9). Aprobación separada de los derechos de acceso por la gestión también puede ser adecuada;

b) Considerando los requisitos de negocios y la política y las reglas específicas del tema de la institución sobre el control de acceso;

c) Considerar la separación de funciones, incluida la separación de las funciones de aprobación e implementación de los derechos de acceso y la separación de roles en conflicto;

d) Asegurar que los derechos de acceso se eliminen cuando alguien no necesite acceder a la información y otros activos asociados, en particular asegurar que los derechos de acceso de los usuarios que han dejado la institución se eliminen de manera oportuna;

e) Considerar otorgar derechos de acceso temporal por un período de tiempo limitado y revocarlos en la fecha de vencimiento, en particular para el personal temporal o el acceso temporal requerido por el personal;

f) Verificar que el nivel de acceso otorgado esté de acuerdo con las políticas específicas del tema sobre control de acceso (ver 1.15) y sea consistente con otros requisitos de

seguridad de la información, como la separación de funciones (ver 1.3);

g) Asegurar que los derechos de acceso se activen (por ejemplo, por parte de los proveedores de servicios) solo después de que los procedimientos de autorización se completen con éxito;

h) Mantener un registro central de los derechos de acceso otorgados a un identificador de usuario (ID, lógico o físico) para acceder a la información y otros activos asociados;

i) Modificar los derechos de acceso de los usuarios que han cambiado de rol o trabajo:

j) Eliminar o ajustar los derechos de acceso físico y lógico, lo que puede hacerse mediante la eliminación, revocación o reemplazo de claves, información de autenticación, tarjetas de identificación o suscripciones:

k) Mantener un registro de cambios en los derechos de acceso lógico y físico de los usuarios

l) Cambiar las contraseñas de autenticación siempre que haya indicios de su posible divulgación

Revisión de los derechos de acceso

Las revisiones regulares de los derechos de acceso físico y lógico deben considerar lo siguiente:

a) Actualizar los derechos de acceso de los usuarios después de cualquier cambio dentro de la misma institución (por ejemplo, cambio de trabajo, promoción, descenso) o terminación del empleo (ver 2.1 a 2.5);

b)Autorizaciones de derechos de acceso privilegiado.

Consideración antes del cambio o terminación del empleo

Los derechos de acceso de un usuario a la información y otros activos asociados deben revisarse y ajustarse o eliminarse antes de cualquier cambio o terminación del empleo en función de la evaluación de factores de riesgo tales:

a)Los derechos de acceso de un usuario a la información y otros activos asociados se deben revisar y ajustar o eliminar antes de cualquier cambio o terminación del empleo en función de la evaluación de factores de riesgo.

b)Si la terminación o cambio es iniciado por el usuario o por la gestión y el motivo de la terminación;

c)Las responsabilidades actuales del usuario;

d)El valor de los activos actualmente accesibles.

Se debe considerar incluir cláusulas en los contratos de personal y de servicio que especifiquen sanciones si el personal intenta acceder sin autorización (ver 1.20, 2.2, 2.4, 2.6).

1.19. Seguridad de la información en las relaciones con proveedores

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Proveedor_relación_buques_seguridad	#Gobernanza_y_ecosistema #Protección

Control

Elaborar, Implementar y socializar la política, procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.

Recomendaciones para la implementación:

Estos procesos y procedimientos deben incluir aquellos que debe implementar la institución, así como aquellos que la institución requiere que el proveedor implemente para el inicio del uso de los productos o servicios de un proveedor o para la terminación del uso de los productos y servicios de un proveedor, tales como:

a) La institución debe identificar e implementar procesos y procedimientos para abordar los riesgos de seguridad asociados con el uso de productos y servicios proporcionados por los proveedores.

b) Esto también debe aplicarse al uso que hace la institución de los recursos de los proveedores de servicios en la nube.

c) Estos procesos y procedimientos deben incluir aquellos que debe implementar la institución, así como aquellos que la institución requiere que el proveedor implemente para el inicio del uso de los productos o servicios de un proveedor o para la terminación del uso de los productos y servicios de un proveedor.

d) Identificar y documentar los tipos de proveedores a los cuales la institución permitirá acceder a su información (por ejemplo, servicios de TIC, logística, servicios públicos, servicios financieros, componentes de infraestructura de TIC) que pueden afectar la confidencialidad, integridad y disponibilidad de la información de la institución;

e) Establecer cómo evaluar y seleccionar proveedores de acuerdo con la sensibilidad de la información, productos y servicios (por ejemplo, con análisis de mercado, referencias de clientes, revisión de documentos, evaluaciones in situ, certificaciones);

f) Evaluar y seleccionar productos o servicios del proveedor que cuenten con controles de seguridad de la información adecuados y revisamos; en particular, la exactitud e integridad de los controles implementados por el proveedor que asegure la integridad de la información y el tratamiento de la información del proveedor y, por lo tanto, la seguridad de la información de la institución:

g) Definir la información de la institución, los servicios TIC y la infraestructura física a la que los proveedores pueden acceder, monitorear, controlar o usar;

h) Definir los tipos de componentes y servicios de infraestructura TIC proporcionados por los proveedores que pueden afectar la confidencialidad, integridad y disponibilidad de la información de la institución;

i) Evaluar y gestionar los riesgos de seguridad de la información asociados con:

1) El uso por parte de los proveedores de la información de la institución y otros activos asociados, incluidos los riesgos que se originan del personal del proveedor potencialmente malicioso;

2) Mal funcionamiento o vulnerabilidades de los productos (incluidos los componentes y subcomponentes de software utilizados en estos productos) o servicios proporcionados por los proveedores;

j) Monitorear el cumplimiento de los requisitos de seguridad de la información establecidos para cada tipo de proveedor y tipo de acceso, incluida la revisión por terceras partes y la validación del producto;

k) Mitigar el incumplimiento de un proveedor, ya sea que este haya sido detectado a través del monitoreo o por otros medios;

l) El manejo de incidentes y contingencias asociadas con los productos y servicios del proveedor, incluidas las responsabilidades tanto de la institución como de los proveedores;

m) Resiliencia y, si es necesario, medidas de recuperación y contingencia para garantizar la disponibilidad de la información del proveedor y el tratamiento de información y, por lo tanto, la disponibilidad de la información de la institución;

n) Concienciación y formación para el personal de la institución que interactúa con el personal del proveedor con respecto a las reglas de participación apropiadas, políticas, procesos y procedimientos específicos del tema y comportamiento en función del tipo de proveedor y el nivel de acceso del proveedor a los sistemas y la información de la institución;

o) Administrar la transferencia necesaria de información, otros activos asociados y cualquier otra cosa que deba cambiarse y asegurar que la seguridad de la información se mantenga durante todo el período de transferencia;

p) Requisitos para asegurar una terminación segura de la relación con el proveedor, incluyendo:

1) Desaprovisionamiento de los derechos de acceso;

2) Manejo de la información;

3) Determinar la propiedad de la propiedad intelectual desarrollada durante la relación contractual;

4) Portabilidad de la información en caso de cambio de proveedor o internalización;

5) Gestión de registros;

6) Devolución de bienes;

7) Eliminación segura de información y otros activos asociados;

8) Requisitos continuos de confidencialidad;

q) Nivel de seguridad personal y seguridad física que se espera del personal y las instalaciones del proveedor.

r) Se deben considerar los procedimientos para continuar con el tratamiento de la información en caso de que el proveedor no pueda suministrar sus productos o servicios (por ejemplo, debido a un incidente, porque el proveedor ya no está en el negocio o ya no proporciona algunos componentes debido a los avances tecnológicos) para evitar cualquier retraso en la institución de productos o servicios de reemplazo (por ejemplo, identificar un proveedor alternativo por adelantado o utilizar siempre proveedores alternativos).

1.20. Abordar la seguridad de la información en los acuerdos con proveedores

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Proveedor_relación_buques_seguridad	#Gobernanza_y_ecosistema #Protección

Control

Los requisitos de seguridad de la información pertinentes, deben establecerse, documentarse y acordarse con cada proveedor en función del tipo de relación con el proveedor, antes que pueda ingresar, procesar, almacenar, comunicar o proporcionar componentes de TI que dan soporte a la información de la institución.

Recomendaciones para la implementación:

Los acuerdos con los proveedores se deben establecer y documentar para asegurar que haya una comprensión clara entre la institución y el proveedor con respecto a las obligaciones de ambas partes para cumplir con los requisitos de seguridad de la información relevantes.

Se puede considerar la inclusión de los siguientes términos en los acuerdos para satisfacer los requisitos de seguridad de la información identificados:

a) Descripción de la información que se proporcionará o se acceden y los métodos para proporcionar o acceder a la información;

b) Clasificación de la información de acuerdo con el esquema de clasificación de la institución (ver 1.10, 1.12, 1:13);

c) Mapeo entre el esquema de clasificación propio de la institución y el esquema de clasificación del proveedor;

d) Requisitos legales, estatutarios, reglamentarios y contractuales, incluida la protección de datos, el manejo de información personal identificable (PII), los derechos de propiedad intelectual y los derechos de autor y una descripción de cómo se asegurará que se cumplan;

e) La obligación de cada pase contratante de implementar un conjunto de controles acordado, incluido el control de acceso, la revisión del desempeño, el seguimiento, la presentación de informes y la auditoria, y las obligaciones del proveedor de cumplir con los requisitos de seguridad de la información de la institución;

f) Reglas de uso aceptable de la información y otros activos asociados, incluido el uso inaceptable si es necesario;

g) Procedimientos o condiciones para la autorización y revocación de la autorización para el uso de la información de la institución y otros activos asociados por parte del personal del proveedor (por ejemplo, a través de una lista explicita del personal del proveedor autorizado para usar la información de la institución y otros activos asociados);

h) Requisitos de seguridad de la información con respecto a la infraestructura TIC del proveedor; en particular, requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso a servir como base para acuerdos de proveedores individuales basados en las necesidades de negocios de la institución y los criterios de riesgo;

i) Indemnizaciones y remediación por incumplimiento de la relación contractual por parte del contratista;

j) Requisitos y procedimientos de gestión de incidentes (especialmente notificación y colaboración durante la remediación de incidentes);

k) Requisitos de capacitación y concientización para procedimientos específicos y requisitos de seguridad de la información (por ejemplo, para respuesta a incidentes, procedimientos de autorización);

l) Disposiciones pertinentes para la subcontratación, incluidos los controles que deben implementarse, como un acuerdo sobre el uso de subproveedores (por ejemplo, exigir que tengan las mismas obligaciones del proveedor, exigiendo tener una lista de subproveedores y notificación antes de cualquier cambio);

m) Contactos relevantes, incluida una persona de contacto para cuestiones de seguridad de la información;

n) Cualquier requisito de evaluación, cuando sea legalmente permisible, para el personal del proveedor, incluidas las responsabilidades de realizar los procedimientos de evaluación y notificación si la evaluación no se ha completado o si los resultados generan dudas o inquietudes;

o) Los mecanismos de evidencia y aseguramiento de certificaciones de terceras partes para los requisitos de seguridad de la información relevantes relacionados con los procesos del proveedor y un informe independiente sobre la efectividad de controles;

p) Derecho a auditar los procesos y controles del proveedor relacionados con el contrato;

q) La obligación del proveedor de entregar periódicamente un informe sobre la efectividad de los controles y el acuerdo sobre la corrección oportuna de los problemas relevantes planteados en el informe;

r) Procesos de resolución de defectos y resolución de conflictos;

s) Proporcionar respaldo alineado con las necesidades de las instituciones (en términos de frecuencia y tipo y ubicación de almacenamiento);

t) Asegurar la disponibilidad de una instalación alternativa (es decir, un sitio de recuperación ante desastres) que no esté sujeta a las mismas amenazas que la instalación principal y las consideraciones para los controles de respaldo (controles alternativos) en los controles primarios del evento fallan;

u) tener un proceso de gestión de cambios que asegure la notificación previa a la institución y la posibilidad de que la institución no acepte cambios:

v) controles de seguridad física acordes con la clasificación de la información;

w) Controles de transferencia de información para proteger la información durante la transferencia física o transmisión lógica;

x) Cláusulas de rescisión al concluir el contrato, incluida la gestión de registros, la devolución de activos, la eliminación segura de información y otros activos asociados, y cualquier confidencialidad en curso que produzca obligaciones;

y) Provisión de un método para destruir de forma segura la información de la institución almacenada por el proveedor tan pronto como ya no sea necesaria;

z) Asegurar, al final del contrato, la entrega del apoyo a otro proveedor o a la propia institución.

La institución debe establecer y mantener un registro de acuerdos con partes externas (por ejemplo, contratos, memorandos de acuerdos de comprensión de acuerdos de intercambio de información) para realizar un seguimiento de adónde va su información. La institución también debe revisar, validar y actualizar regularmente sus acuerdos con partes externas para garantizar que aún sean necesarios y adecuados para su propósito con los capítulos de seguridad de la información relevantes.

a) Registrar y mantener las terceras partes vinculadas a la institución considerando los siguientes tipos:
    1. Proveedores de servicios (ej., Internet, proveedores de red, servicios telefónicos, servicios de mantenimiento, energía eléctrica, agua, entre otros);
    2. Servicios de seguridad;
    3. Contratación externa de proveedores de servicios y/u operaciones;
    4. Asesores y auditores externos;
    5. Limpieza, alimentación y otros servicios de soporte contratados externamente;
    6. Personal temporal (estudiantes, pasantes, funcionarios públicos externos);
    7. Otros

1.21. Gestión de seguridad de la información en la cadena de suministro de las TIC

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Proveedor_relación_buques_seguridad	#Gobernanza_y_ecosistema #Protección

Control

Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.

Recomendaciones para la implementación:

a) Definir los requisitos de seguridad de la información que se aplicarán a la adquisición de productos o servicios de TIC;

b) Exigir que los proveedores de servicios de TIC propaguen los requisitos de seguridad de la institución a lo largo de la cadena de suministro si subcontratan partes del servicio de TIC proporcionado a la institución;

c) Exigir que los proveedores de productos TIC informen prácticas de seguridad adecuadas a lo largo de la cadena de suministro si estos productos incluyen componentes comprados o adquiridos de otros proveedores u otras entidades (por ejemplo, desarrolladores de software subcontratados y proveedores de componentes de hardware);

d) Solicitar que los proveedores de productos TIC proporcionen información que describa los componentes de software utilizados en los productos;

e) Solicitar que los proveedores de productos TIC proporcionen información que describa las funciones de seguridad implementadas de su producto y la configuración requerida para su operación segura;

f) Implementar un proceso de monitoreo y métodos aceptables para validar que los productos y servicios de TIC entregados cumplan con los requisitos de seguridad establecidos. Ejemplos de dicha revisión de proveedores los métodos pueden incluir pruebas de penetración y prueba o validación de certificaciones de terceras partes para las operaciones de seguridad de la información del proveedor;

g) Implementar un proceso para identificar y documentar los componentes del producto o servicio que son críticos para mantener la funcionalidad y, por lo tanto, requieren mayor atención, escrutinio y seguimiento adicional cuando se construyen fuera de la institución, especialmente si el proveedor subcontrata aspectos de los componentes del producto o servicio a otros proveedores;

h) Obtener la seguridad de que los componentes críticos y su origen pueden rastrearse a lo largo de la cadena de suministro;

i) Obtener la seguridad de que los productos TIC entregados funcionan como se espera sin

características inesperadas o no deseadas;

j)Implementar procesos para garantizar que los componentes de los proveedores sean genuinos y no se alteren sus especificaciones. Las medidas de ejemplo incluyen etiquetas antimanipulación, verificaciones hash criptográficas o firmas digitales La supervisión del desempeño fuera de las especificaciones puede ser un indicador de manipulación o falsificación. La prevención y detección de la manipulación debe implementarse durante varias etapas del ciclo de vida del desarrollo del sistema, incluido el diseño, el desarrollo, la integración, las operaciones y el mantenimiento;

k) Obtener garantías de que los productos TIC alcancen los niveles de seguridad requeridos, por ejemplo, a través de una certificación formal o un esquema de evaluación como el Acuerdo de Reconocimiento de Criterios Comunes;

l) Definir reglas para compartir información sobre la cadena de suministro y cualquier posible problema y compromiso entre la institución y los proveedores;

m) Implementar procesos específicos para gestionar el ciclo de vida y la disponibilidad de los componentes TIC y los riesgos de seguridad asociados. Esto incluye gestionar los riesgos de que los componentes ya no estén disponibles debido a que los proveedores ya no están en el negocio o los proveedores ya no proporcionan estos componentes debido a los avances tecnológicos. Se debe considerar la identificación de un proveedor alternativo y el proceso para transferir el software y la competencia al proveedor alternativo.

n) Se aconseja a las instituciones que trabajen con los proveedores para comprender la cadena de suministro de las TIC y cualquier asunto que tenga un efecto importante en los productos y servicios que se proporcionan. La institución puede influir en las prácticas de seguridad de la información de la cadena de suministro de TIC aclarando en los acuerdos con sus proveedores los asuntos que deben abordar otros proveedores en la cadena de suministro de TIC.

o) Las TIC deben adquirirse de fuentes acreditadas La confiabilidad del software y el hardware es una cuestión de control de calidad. Si bien generalmente no es posible que una institución inspeccione los sistemas de control de calidad de sus proveedores, puede hacer juicios confiables basados en la reputación del proveedor.

1.22. Monitoreo, revisión y gestión de cambios de servicios de proveedores

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Proveedor_relación_buques_seguridad	#Gobernanza_y_ecosistema #Protección #Defensa Información_seguridad_garantia

Control

La institución debe monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios

Recomendaciones para la implementación:

a) El monitoreo, la revisión y la gestión de cambios de los servicios del proveedor deben asegurar que se cumplan los términos y condiciones de seguridad de la información de los acuerdos, que los incidentes y problemas de seguridad de la información se gestionen adecuadamente y que los cambios en los servicios del proveedor o el estado de negocios no afecten la prestación del servicio.

b) Monitorear los niveles de desempeño del servicio para verificar el cumplimiento de los acuerdos;

c) Controlar los cambios realizados por los proveedores, incluidos:

1) Mejoras a los servicios actuales ofrecidos;

2) Desarrollo de nuevas aplicaciones y sistemas;

3) Modificaciones o actualizaciones de las políticas y procedimientos del proveedor;

4) Controles nuevos o modificados para resolver incidentes de seguridad de la información y mejorar la seguridad de la información;

d) Monitorear los cambios en los servicios del proveedor, incluyendo:

1) Cambios y mejoras a las redes;

2) Uso de nuevas tecnologías;

3) Adopción de nuevos productos o versiones o lanzamientos más nuevos;

4) Nuevas herramientas y entornos de desarrollo;

5) Cambios en la ubicación física de las instalaciones de servicio;

6) Cambio de subproveedores;

7) Subcontratación a otro proveedor;

e) Revisar los informes de servicio producidos por el proveedor y organizar reuniones regulares de progreso según lo requieran los acuerdos;

f) Realizar auditorías de proveedores y subproveedores, junto con la revisión de los informes de los Auditores independientes, si están disponibles, y dar seguimiento a los problemas identificados;

g) Proporcionar información sobre incidentes de seguridad de la información y revisar esta información según lo requieran los acuerdos y cualquier guía y procedimiento de soporte;

h) Revisar las pistas de auditoría del proveedor y los registros de eventos de seguridad de la información, problemas operativos, fallas, rastreo de fallas e interrupciones relacionadas con el servicio prestado;

i) Responder y gestionar cualquier evento o incidente de seguridad de la información identificado;

j) Identificar vulnerabilidades de seguridad de la información y gestionarlas;

k) Revisar los aspectos de seguridad de la información de las relaciones del proveedor con sus propios proveedores;

l) Asegurarse de que el proveedor mantenga suficiente capacidad de servicio junto con planes viables diseñados para asegurar que se mantengan los niveles de continuidad del servicio acordados después de fallas importantes en el servicio o desastres (ver 1.29, 1.30, 1.35, 1.36, 4.14);

m) Asegurar que los proveedores asignen responsabilidades para revisar el cumplimiento y hacer cumplir los requisitos de los acuerdos;

n) Evaluar periódicamente que los proveedores mantienen niveles adecuados de seguridad de la información.

o) La responsabilidad de administrar el contrato y las relaciones con los proveedores debe asignarse a un individuo o equipo designado.

p) Se deben poner a disposición suficientes habilidades técnicas y recursos para monitorear que se cumplan los requisitos del acuerdo, en particular los requisitos de seguridad de la información.

q) Se deben tomar las acciones apropiadas cuando se observen deficiencias en la prestación del servicio.

1.23. Seguridad de la información para el uso de servicios en la nube

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Proveedor_relación_buques_seguridad	#Gobernanza_y_ecosistema #Protección

Control

Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer de acuerdo con los requisitos de seguridad de la información de la institución.

Recomendaciones para la implementación:

La institución debe definir:

a) Todos los requisitos de seguridad de la información pertinentes asociados con el uso de los servicios en la nube;

b) Criterios de selección del servicio en la nube y alcance del uso del servicio en la nube;

c) Funciones y responsabilidades relacionadas con el uso y la gestión de los servicios en la nube;

d) Qué los controles de seguridad de la información gestionan el proveedor de servicios en la nube y cuáles gestiona la institución como cliente del servicio en la nube:

e) Cómo obtener y utilizar las capacidades de seguridad de la información proporcionadas por el proveedor de servicios en la nube;

f) Cómo obtener garantías sobre los controles de seguridad de la información implementados por los proveedores de servicios en la nube;

g) Cómo administrar los controles, las interfaces y los cambios en los servicios cuando una institución utiliza múltiples servicios en la nube, particularmente de diferentes proveedores de servicios en la nube;

h) Procedimientos para el manejo de incidentes de seguridad de la información que se produzcan en relación con el uso de los servicios en la nube;

i) Su enfoque para monitorear, revisar y evaluar el uso continuo de los servicios en la nube para administrar los riesgos de seguridad de la información;

j) Cómo cambiar o detener el uso de los servicios en la nube, incluidas las estrategias de salida para los servicios en la nube.

k) Para todos los servicios en la nube, la institución debe revisar los acuerdos de servicios en la nube con los proveedores de servicios en la nube. Un acuerdo de servicio en la nube debe abordar los requisitos de confidencialidad, integridad, disponibilidad y manejo de la información de la institución, con objetivos de nivel de servicio en la nube y objetivos cualitativos de servicio en la nube apropiados.

l) La institución también debe realizar evaluaciones de riesgos relevantes para identificar los riesgos asociados con el uso del servicio en la nube. Cualquier riesgo residual relacionado con el uso del servicio en la nube debe ser claramente identificado y aceptado por los responsables en la administración por parte de la institución.

Un acuerdo entre el proveedor de servicios en la nube y la institución, que actúa como cliente del servicio en la nube, debe incluir las siguientes disposiciones contractuales de ser el caso para la protección de los datos de la institución y la disponibilidad de los servicios:

a) Proporcionar soluciones basadas en normas aceptadas por la industria para la arquitectura y la infraestructura;

b) Administrar los controles de acceso del servicio en la nube para cumplir con los requisitos de la institución;

c) Implementar soluciones de protección y monitoreo de malware;

d) Tratar y almacenar la información confidencial de la institución en ubicaciones aprobadas legalmente (por ejemplo, un país o una región en particular) o dentro o sujeto a una

jurisdicción en particular;

e) Brindar soporte dedicado en caso de un incidente de seguridad de la información en el entorno del servicio en la nube;

f) Asegurar que se cumplan los requisitos de seguridad de la información de la institución en caso de que los servicios en la nube se subcontraten a un proveedor externo (o se prohíba la subcontratación de los servicios en la nube);

g) Soportar a la institución en la recopilación de evidencia digital, teniendo en cuenta las leyes y regulaciones para evidencia digital en diferentes jurisdicciones;

h) Proporcionar soporte y disponibilidad de servicios apropiados durante un período de tiempo apropiado cuando la institución desee o tenga que salir del servicio en la nube:

i) Proporcionar la copia de seguridad necesaria de los datos y la información de configuración y gestionar de forma segura las copias de seguridad, según corresponda, en función de las capacidades del proveedor de servicios en la nube utilizado por la institución, actuar como cliente del servicio en la nube;

j) Proporcionar y devolver información como archivos de configuración, código fuente y datos que son propiedad de la institución, actuando como cliente del servicio en la nube, cuando se solicite durante la prestación del servicio o al finalizar el servicio.

La institución, actuando como cliente del servicio en la nube, debe considerar si el acuerdo debe exigir a los proveedores de servicios en la nube que proporcionen una notificación previa antes de que se realicen cambios sustanciales que afecten al cliente en la forma en que se entrega el servicio a la institución, incluido:

a) cambios en la infraestructura técnica (por ejemplo, reubicación, reconfiguración o cambios en el hardware o el software) que afecten o modifiquen la oferta de servicios en la nube;

b) Tratar o almacenar información en una nueva jurisdicción geográfica o legal;

c) uso de proveedores de servicios en la nube similares u otros subcontratistas (incluido el cambio de partes existentes o el uso de nuevas partes).

d) La institución que utiliza servicios en la nube debe mantener un estrecho contacto con sus proveedores de servicios en la nube. Estos contactos permiten el intercambio mutuo de información sobre la seguridad de la información para el uso de los servicios en la nube, incluido un mecanismo para que tanto el proveedor del servicio en la nube como la institución, que actúa como cliente del servicio en la nube, monitoreen cada característica del servicio e informen los incumplimientos de los compromisos contenidos en los acuerdos.

1.24. Planificación y preparación de la gestión de incidentes de seguridad de la información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Correctivo	#Confidencialidad #Integridad	#Responder #Recuperar	#Gobernanza #Gestión_de_ev	#Defensa

	#Disponibilidad		entos_de_seguridad_de_la_información	

Control

La institución debe planificar y prepararse para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, funciones y responsabilidades de gestión de incidentes de seguridad de la información.

Recomendaciones para la implementación:

Funciones y responsabilidades

a) La institución debe establecer procesos apropiados de gestión de incidentes de seguridad de la información.
b) Debe determinarse las funciones y responsabilidades para llevar a cabo los procedimientos de gestión de incidentes y comunicada efectivamente a las partes interesadas internas y externas relevantes.

c) Establecer un método común para reportar eventos de seguridad de la información, incluido el punto de contacto (ver 2.8);

d) Establecer un proceso de gestión de incidentes para proporcionar a la institución la capacidad de gestionar incidentes de seguridad de la información, incluida la administración, documentación, detección, clasificación, priorización, análisis, comunicación y coordinación de las partes interesadas;

e) Establecer un proceso de respuesta a incidentes para proporcionar a la institución la capacidad de evaluar, responder y aprender de los incidentes de seguridad de la información;

f) Solo permitir que personal competente maneje los problemas relacionados con los incidentes de seguridad de la información dentro de la institución. Dicho personal debe contar con documentación de procedimientos y capacitación periódica;

g) Establecer un proceso para identificar la capacitación, la certificación y el desarrollo profesional continuo necesarios para el personal de respuesta a incidentes.

Procedimientos de gestión de incidentes

a) Los objetivos para la gestión de incidentes de seguridad de la información se deben acordar con las autoridades responsables de los activos y se debe asegurar que los responsables de la gestión de incidentes de seguridad de la información entiendan las prioridades de la institución para manejar los incidentes de seguridad de la información, incluido el marco de tiempo de resolución basado en las posibles consecuencias y gravedad. Se deben implementar procedimientos de gestión de incidentes para cumplir con estos objetivos y prioridades.

b) La máxima autoridad o su delegado junto al comité de seguridad de la información y el oficial de seguridad de la información deben asegurarse de que se cree un plan de gestión

de incidentes de seguridad de la información considerando diferentes escenarios.

c) Evaluación de eventos de seguridad de la información según criterios de lo que constituye un incidente de seguridad de la información;

d)Monitorear (ver 4.15 y 4.16), detectar (ver 4.16), clasificar (ver 1.25), analizar y reportar (ver 2.8) de eventos e incidentes de seguridad de la información por medios humanos o automáticos;

e)Gestionar los incidentes de seguridad de la información hasta su conclusión, incluyendo respuesta y escalamiento (ver 1.26), según el tipo y la categoría del incidente, posible activación de gestión de crisis y activación de planes de continuidad, recuperación controlada de un incidente y comunicación a internos y partes interesadas externas;

f) Coordinación con partes interesadas internas y externas tales como autoridades, grupos de interés y foros externos, proveedores y clientes (ver 1.5 y 1.6);

g)Registrar las actividades de gestión de incidentes;

h) Manejo de evidencia (ver 1.28);

i) Análisis de causa raíz o procedimientos post-mortem;

j) Identificación de las lecciones aprendidas y de las mejoras a los procedimientos de gestión de incidentes o controles de seguridad de la información en general que se requieran.

Procedimientos de notificación

Los procedimientos de notificación deben incluir:

a) Acciones a tomar en caso de un evento de seguridad de la información (por ejemplo, tomar nota de todos los detalles pertinentes de inmediato, como el mal funcionamiento y los mensajes en la pantalla, informar de inmediato al punto de contacto y solo tomando acciones coordinadas):

b) Uso de formularios de incidentes para ayudar al personal a realizar todas las acciones necesarias al informar incidentes de seguridad de la información:

c) Procesos de retroalimentación adecuados para asegurar que aquellas personas que reporten eventos de seguridad de la información sean notificadas, en la medida de lo posible, de los resultados después de que el problema haya sido abordado y cerrado;

d) Elaboración de informes de incidencias.

e) Mantener contactos efectivos con las autoridades, grupos de interés internos y externos, (Cert, Csirt, Soc, otros); que tratan asuntos relacionados con los incidentes de seguridad de la información.

f) Cualquier requisito externo sobre el informe de incidentes a las partes interesadas relevantes dentro del marco de tiempo definido (por ejemplo, requisitos de notificación de

incumplimiento a los reguladores) debe considerarse cuando implementar procedimientos de gestión de incidentes.

1.25. Evaluación y decisión sobre eventos de seguridad de la información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

La institución debe evaluar los eventos de seguridad de la información y decidir si se clasificarán como incidentes de seguridad de la información.

Recomendaciones para la implementación:

a) Se debe acordar un esquema de categorización y priorización de incidentes de seguridad de la información para la identificación de las consecuencias y prioridad de un incidente.

b) El esquema debe incluir los criterios para clasificar los eventos como incidentes de seguridad de la información.

c) El punto de contacto debe evaluar cada evento de seguridad de la información utilizando el esquema acordado.

d) El personal responsable de coordinar y responder a los incidentes de seguridad de la información debe realizar la evaluación y tomar una decisión sobre los eventos de seguridad de la información.

e) Los resultados de la evaluación y la decisión deben registrarse en detalle para fines de futura referencia y verificación.

1.26. Respuesta a incidentes de seguridad de la información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.

Recomendaciones para la implementación:

La institución debe establecer y comunicar procedimientos sobre la respuesta a incidentes de seguridad de la información a todas las partes interesadas pertinentes.

Los incidentes de seguridad de la información deben ser respondidos por un equipo designado con la competencia requerida (ver 1.24).

La respuesta debe incluir lo siguiente:

a) Contener, si las consecuencias del incidente pueden extenderse, los sistemas afectados por el incidente;

b)Recolectar evidencia (ver 1.28) tan pronto como sea posible después de la ocurrencia;

- Clasificar el incidente de acuerdo al tipo de servicio afectado y al nivel de severidad.
- Asignar una prioridad de atención al incidente en el caso de que se produjeran varios en forma simultánea.
- Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas.

c) Escalada, según sea necesario, incluidas las actividades de gestión de crisis y posiblemente invocando planes de continuidad del negocio (ver 1.29 y 1.30);

d) Asegurar que todas las actividades de respuesta involucradas se registren correctamente para su posterior análisis;

e) Comunicar la existencia del incidente de seguridad de la información o cualquier detalle relevante del mismo al oficial de seguridad y a todas las partes interesadas internas y externas pertinentes siguiendo el principio de necesidad de saber;

f) Coordinarse con partes internas y externas, como autoridades, grupos y foros de interés externos, proveedores y clientes, para mejorar la eficacia de la respuesta y ayudar a minimizar las consecuencias para otras organizaciones;

g)Una vez solucionado satisfactoriamente el incidente, cerrarlo formalmente y registrarlo;
h)Realizar análisis forenses de seguridad de la información, según se requiera (ver 1.28):

i) Realizar un análisis posterior al incidente para identificar la causa raíz. Asegúrese de que esté documentado y comunicado de acuerdo con los procedimientos definidos (ver 1.27);

j) Identificar y gestionar las vulnerabilidades y debilidades de la seguridad de la información, incluidas las relacionadas con los controles que han causado, contribuido o fallado en prevenir el incidente.

1.27. Aprendiendo de los incidentes de seguridad de la información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

Utilizar el conocimiento obtenido de los incidentes de seguridad de la información para fortalecer y mejorar los controles de seguridad de la información, así como también analizar y resolver incidentes en el futuro.

Recomendaciones para la implementación:

La institución debe establecer procedimientos para cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información.

La información obtenida de la evaluación de incidentes de seguridad de la información debe utilizarse para:

a) Mejorar el plan de gestión de incidentes, incluidos los escenarios y procedimientos de incidentes (ver 1.24);

b) Identificar incidentes recurrentes o graves y sus causas para actualizar la evaluación de riesgos de seguridad de la información de la institución y determinar e implementar los controles adicionales necesarios para reducir la probabilidad o las consecuencias de futuros incidentes similares. Los mecanismos para habilitar eso incluyen recopilar, cuantificar y monitorear información sobre tipos de incidentes, volúmenes y costos;

    - Determinar el número de incidentes por tipo, el número de incidentes graves, el tiempo medio de resolución de incidentes.
    - Determinar el costo promedio por incidente.
    - Determinar el número de incidentes recurrentes.
    - Determinar la frecuencia de un incidente recurrente.

c) Mejorar la concienciación y la formación de los usuarios (ver 2.3) proporcionando ejemplos de lo que puede suceder, cómo responder a tales incidentes y cómo evitarlos en el futuro.

1.28. Recopilación de evidencias

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

Establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información, de acuerdo a norma legal vigente.

Recomendaciones para la implementación:

Debe ser posible demostrar que:

Se debe desarrollar y seguir procedimientos internos al tratar con evidencia relacionada con eventos de seguridad de la información con el propósito de acciones disciplinarias y legales.

En general, estos procedimientos para la gestión de evidencias deben proporcionar instrucciones para la identificación, recopilación, adquisición y conservación de evidencias de acuerdo con los diferentes tipos de medios de almacenamiento, dispositivos y estado de los dispositivos (es decir, encendido o apagado), por lo general, las evidencias deben recopilarse de una manera que sea admisible en los tribunales de justicia, nacionales correspondientes u otro foro disciplinario.

Debería ser posible demostrar que:

a)Los registros están completos y no han sido manipulados de ninguna manera;

b)Las copias de las pruebas electrónicas probablemente sean idénticas a los originales;

c) Cualquier sistema de información a partir del cual se hayan recopilado evidencias funcionaba correctamente en el momento en que se registraron las evidencias.

Cuando esté disponible, se debe buscar la certificación u otros medios relevantes legales de calificación del personal y las herramientas, para fortalecer el valor de la evidencia preservada; además aplicar procedimientos adecuados para mantener la cadena de custodia, de acuerdo a lo que dispone la norma legal vigente

La evidencia digital puede trascender los límites institucionales o jurisdiccionales. En tales casos, se debe asegurar que la institución tenga derecho a recopilar la información requerida como evidencia digital.

1.29. Seguridad de la información durante la interrupción

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Continuidad	#Protección #Resiliencia

Control

Documentar los procesos de gestión de la continuidad del negocio, que incluya los requisitos de seguridad de la información, para planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción.

Recomendaciones para la implementación:

La institución debe determinar sus requisitos para adaptar los controles de seguridad de la información durante la interrupción. Los requisitos de seguridad de la información deben incluirse en los procesos de gestión de la continuidad del negocio.

Los planes se deben desarrollar, implementar, probar, revisar y evaluar para mantener o restaurar la seguridad de la información de los procesos de negocios críticos luego de una interrupción o falla. La seguridad de la información debe restaurarse al nivel requerido y en los plazos requeridos.

La institución debe implementar y mantener:

a) Controles de seguridad de la información, sistemas y herramientas de soporte dentro de los planes de continuidad del negocio y continuidad de las TIC;

b) Procesos para mantener los controles de seguridad de la información existente durante la interrupción;

c) Controles de compensación para los controles de seguridad de la información que no se pueden mantener durante la interrupción.

La institución debe verificar permanentemente los controles de continuidad de la seguridad de la información establecida e implementada, para lo cual se debe considerar lo siguiente:

a) Evaluar la capacidad de respuesta ante desastres verificando los tiempos de respuesta, validez de los procedimientos y capacidad de los responsables. Los resultados obtenidos permitirán actualizar y mantener los planes establecidos.
b) Ejecutar autoevaluaciones del plan de continuidad, estrategias y procesos generados.
c) Ejecutar y probar la funcionalidad de los procesos, procedimientos y controles para la continuidad de la seguridad de la información asegurando la consistencia con los objetivos planteados.
d) Realizar auditorías tanto internas como externas, identificando el tipo y alcance de la auditoría a realizar, se entregará un plan de medidas correctivas para llevar a cabo las recomendaciones acordadas.
e) Realizar pruebas de:

- Validez: revisar y discutir el plan;
- Simulación: escenario que permitirá verificar el plan de continuidad;
- Actividades críticas: pruebas en un entorno controlado sin poner en peligro la operación de los servicios informáticos;
- Completa: interrupción real y aplicación del plan de continuidad.

1.30. Preparación de las TIC para la continuidad del negocio

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Correctivo	#Disponibilidad	#Responder	#Continuidad	#Resiliencia

Control

La preparación de las TIC debe planificarse, documentarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.

Recomendaciones para la implementación:

La preparación de las TIC para la continuidad del negocio es un componente importante en la gestión de la continuidad del negocio y la gestión de la seguridad de la información para garantizar que los objetivos de la institución puedan seguir cumpliéndose durante la interrupción.

Los requisitos de continuidad de las TIC son el resultado del análisis de impacto del negocio (BIA). El proceso BIA debe utilizar tipos y criterios de impacto para evaluar los impactos a lo largo del tiempo que resultan de la interrupción de las actividades comerciales que entregan productos y servicios. La magnitud y la duración del impacto resultante deben usarse para identificar actividades prioritarias a las que se les debe asignar un objetivo de tiempo de recuperación (RTO - Recovery Time Objective). El BIA debe entonces determinar qué recursos se necesitan para apoyar las actividades priorizadas. También se debe especificar un RPO (Recovery point Objective) para estos recursos. Un subconjunto de estos recursos debe incluir servicios de TIC.

El BIA relacionado con los servicios de TIC se puede ampliar para definir los requisitos de desempeño y capacidad de los sistemas de TIC y los objetivos de punto de recuperación (RPO) de la información necesaria para respaldar las actividades durante la interrupción.

Con base en los resultados del BIA y la evaluación de riesgos relacionados con los servicios de TIC, la institución debe identificar y seleccionar estrategias de continuidad de las TIC que consideren opciones para antes, durante y después de la interrupción. Las estrategias de continuidad del negocio pueden comprender una o más soluciones. Con base en las estrategias, los planes deben desarrollar, implementar y probar para cumplir con el nivel de disponibilidad requerido de los servicios de TIC y en los plazos requeridos luego de la interrupción o falla de los procesos críticos.

La institución debe asegurarse de que:

a) Existe una estructura organizativa adecuada para preparar, mitigar y responder a una interrupción con el soporte de personal con la responsabilidad, autoridad y competencias necesarias;

b) Los planes de continuidad de las TIC, incluidos los procedimientos de respuesta y recuperación que detallan cómo la institución planea gestionar una interrupción del servicio de TIC, son;

   1) Evaluado regularmente a través de ejercicios y pruebas;

   2) Aprobado por la gerencia;

c) Los planes de continuidad TIC incluyen la siguiente información de continuidad TIC:

1) Especificaciones de rendimiento y capacidad para cumplir con los requisitos y objetivos de continuidad del negocio como se especifica en el BIA;

2) RTO de cada servicio TIC priorizado y los procedimientos para restaurar esos componentes;

3) RPO de los recursos TIC priorizados definidos como información y los procedimientos para restaurar la información.

La gestión de la continuidad de las TIC constituye una parte clave de los requisitos de continuidad del negocio en relación con la disponibilidad para poder:

a) Responder y recuperarse de la interrupción de los servicios de TIC, independientemente de la causa;
b) Garantizar que la continuidad de las actividades prioritarias este respaldada por los servicios de TIC requeridos;
c) Responder antes de que ocurra una interrupción de los servicios de TIC, y al detectar al menos un incidente que puede resultar en una interrupción de los servicios de TIC.

1.31. Requisitos legales, estatutarios, reglamentarios y contractuales

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Legal_y_cumplimiento	#Gobernanza_y_ecosistema #Protección

Control

Identificarse, documentarse y mantenerse actualizados los requisitos legales, estatutarios, reglamentarios, contractuales y toda norma legal vigente relevante para la seguridad de la información y el enfoque de la institución para cumplir con estos requisitos.

Recomendaciones para la implementación:

Generalidades

Los requisitos externos, incluidos los requisitos legales, estatutarios, reglamentarios, contractuales y toda norma legal vigente, deben tenerse en cuenta para:

a) Desarrollar políticas y procedimientos de seguridad de la información;

b) Diseñar, implementar o cambiar los controles de seguridad de la información:

c) Clasificar la información y otros activos asociados como parte del proceso para establecer requisitos de seguridad de la información para necesidades internas o para acuerdos con proveedores;

d) Realizar evaluaciones de riesgos de seguridad de la información y determinar las actividades de tratamiento de riesgos de seguridad de la información;

e) Determinar los procesos junto con las funciones y responsabilidades relacionadas con la seguridad de la información;

f) Determinar los requisitos contractuales de los proveedores relevantes para la institución y el alcance del suministro de productos y servicios.

Legislación y reglamentos

La institución debe:

a) Identificar toda legislación, reglamentos pertinentes y toda norma legal vigente y nueva que pueda publicarse, relacionada a la seguridad de la información de la institución para conocer los requisitos para su gestión, entre otras:

- Constitución de la República del Ecuador
- Ley de Comercio Electrónico, Firmas y Mensajes de Datos
- Ley Orgánica de Transparencia y Acceso a la Información Pública
- Ley orgánica de protección de datos personales
- Ley orgánica para la transformación, digital y audiovisual
- Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva
- Ley Orgánica y Normas de Control de la Contraloría General del Estado
- Leyes y normas de control del sistema financiero
- Leyes y normas de control de empresas públicas
- Ley del Sistema Nacional de Archivos
- Código orgánico de la economía social de los conocimientos, creatividad e innovación
- Otras normas cuya materia trate sobre la seguridad de la información.

b) Observar el cumplimiento de la normativa de otros países al tener relación con ellos.

c) revisar periódicamente la legislación, reglamentos identificados y toda norma legal vigente para mantenerse al día con los cambios e identificar nueva legislación;

d) Definir y documentar los procesos específicos y las responsabilidades individuales para cumplir con los requisitos.

Criptografía

Se debe tener en cuenta el cumplimiento de los acuerdos, leyes y reglamentos relevantes relacionados con los siguientes elementos

a) Restricciones a la importación o exportación de hardware y software informático para realizar funciones criptográficas;

b) Restricciones a la importación o exportación de hardware y software informático que esté diseñado para tener funciones criptográficas añadidas;

c) Restricciones en el uso de criptografía;

d) Métodos obligatorios o discrecionales de acceso por parte de las autoridades de los países a la información cifrada;

e)Vigencia de firmas digitales, sellos y certificados.

Se recomienda buscar asesoramiento legal al asegurar el cumplimiento de la legislación y las reglamentaciones relevantes, especialmente cuando la información cifrada o las herramientas criptográficas se mueven a través de las fronteras jurisdiccionales.

Contratos

a)Contratos con clientes;

b)Contratos con proveedores (ver 1.20);

c)Contratos de seguro.

1.32. Derechos de propiedad intelectual

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Legal_y_cumplimiento	#Gobernanza_y_ecosistema

Control

Documentar, Implementar y socializar procedimientos apropiados para proteger los derechos de propiedad intelectual y el uso de productos patentados.

Recomendaciones para la implementación:

Para garantizar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos patentados.

Se deben considerar las siguientes directrices para proteger cualquier material que pueda considerarse propiedad intelectual:

a) Definir y comunicar una política específica sobre la protección de los derechos de propiedad intelectual y las acciones disciplinarias para los funcionarios que la infrinjan;

b)Publicar procedimientos para el cumplimiento de los derechos de propiedad intelectual que definan el uso conforme de software y productos de información;

c) Adquirir software solo a través de fuentes conocidas y acreditadas, para asegurar que no se infrinjan los derechos de autor, si el Software es Libre Opensource se considerará los términos de las licencias públicas generales;

d)Mantener registros de activos apropiados e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual, se aplica tanto al software libre como al privativo;

e)Mantener prueba y evidencia de propiedad de licencias, manuales, etc.;

f) asegurar que cualquier número máximo de usuarios o recursos, por ejemplo, unidades centrales de procesamiento (CPU) permitidas dentro de la licencia:

g) Llevar a cabo revisiones para asegurar que solo se instalen software autorizado y productos con licencia;

h)Proporcionar procedimientos para mantener las condiciones apropiadas de la licencia y/o suscripción;

i) Disponer a los funcionarios que utilicen solo software desarrollado, provisto o aprobado por la institución

j)Proporcionar procedimientos para desechar o transferir software a otros;

k) Cumplir con los términos y condiciones del software y la información obtenida de redes públicas y fuentes externas;

l) No duplicar, convertir a otro formato o extraer de grabaciones de negocios (video, audio) que no sea lo permitido por la ley de derechos de autor o las licencias aplicables;

m) No copiar, total o parcialmente, normas (por ejemplo, normas internacionales), libros, artículos, informes u otros documentos, salvo lo permitido por la ley de derechos de autor o las licencias aplicables.

n)Los derechos de propiedad intelectual incluyen derechos de autor de software o documentos, derechos de diseño, marcas registradas, patentes y licencias de código fuente.

o)Registrar el software desarrollado por la institución o contratado a terceros como desarrollo, para proteger la propiedad intelectual.

1.33. Protección de registros

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Legal_y_cumplimiento #Gestión_de_activos #Información_protección	#Defensa

Control

Implementar el procedimiento adecuado para proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada, de acuerdo a la norma legal vigente.

Recomendaciones para la implementación:

La institución debe tomar los siguientes pasos para proteger la autenticidad, confiabilidad, integridad y usabilidad de los registros, ya que su contexto comercial y los requisitos para su gestión cambian con el tiempo:

a) Emitir directrices sobre el almacenamiento, el manejo de la cadena de custodia y la eliminación de registros, lo que incluye la prevención de la manipulación de registros. Estas directrices deben estar alineadas con la política del tema específico de la gestión institucional.

b) Elaborar un calendario de conservación que defina los registros y el período de tiempo durante el cual deben conservarse.

c) Asegurar la identificación de los registros y de su periodo de retención teniendo en cuenta la norma legal vigente, tanto nacional como internacional, y toda normativa, así como las expectativas de la comunidad o la sociedad, si corresponde. Este sistema de almacenamiento y manejo debe permitir la destrucción adecuada de registros después de ese período si la institución lo considera.

d) Considerar su clasificación de seguridad de la información correspondiente, con base en el esquema de clasificación de la institución, al decidir sobre la protección de registros institucionales específicos. Los registros deben clasificarse en tipos de registros sean registros contables, registros de transacciones comerciales, registros de personal, registros legales, cada uno con detalles de los periodos de retención y el tipo de medio de almacenamiento permitido, que puede ser físico o electrónico.

e) Elegir los sistemas de almacenamiento de datos de manera que los registros requeridos puedan recuperarse en un marco de tiempo y formato aceptables, según los requisitos que se deban cumplir.

f) Establecer procedimientos para asegurar la capacidad de acceder a los registros (tanto los medios de almacenamiento como la legibilidad del formato) durante todo el período de retención para salvaguardar contra pérdidas debido a futuros cambios tecnológicos, cuando se elijan medios de almacenamiento electrónico. Todas las claves criptográficas relacionadas y los programas asociados con archivos cifrados o firmas digitales también deben conservarse para permitir el descifrado de los registros por el tiempo que se retienen los registros (ver 4.24).

g) Implementar los procedimientos de almacenamiento y manipulación de acuerdo con las recomendaciones proporcionadas por los fabricantes de los medios de almacenamiento. Se deben considerar la posibilidad de deterioro de los medios utilizados para el almacenamiento de registros, Los procedimientos de almacenamiento y manipulación se deberán implementar según las recomendaciones del fabricante. Para almacenamiento a largo plazo, se recomienda considerar el uso de cintas y discos digitales utilizando formatos de archivos y datos abiertos.

1.34. Privacidad y protección de PII

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Identificar #Proteger	#información_protección	#Protección

	#Integridad #Disponibilidad		#Legal_y_cumplimiento	

Control

Identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la PII (Información personal identificable) de acuerdo con las leyes, reglamentos aplicables, norma legal vigente y los requisitos contractuales necesarios.

Recomendaciones para la implementación:

a) La institución debe elaborar y socializar la política de privacidad y protección de PII específica del tema a todas las partes interesadas pertinentes.

b) La institución debe desarrollar e implementar procedimientos para la preservación de la privacidad y la protección de la PII. Estos procedimientos deben comunicarse a todas las partes interesadas relevantes involucradas en el tratamiento de información de identificación personal

c) El cumplimiento de estos procedimientos y de toda la legislación y los reglamentos concernientes con la preservación de la privacidad y la protección de la PII requiere roles, responsabilidades y controles apropiados. Se debe nombrar a una persona responsable, como el oficial de privacidad o el **delegado de protección de datos,** que debe brindar orientación a los funcionarios, los proveedores de servicios y otras partes interesadas sobre sus responsabilidades individuales y los procedimientos específicos que se deben seguir; que no podrá ser el Oficial de Seguridad de la Información.

d) La responsabilidad por el manejo de la PII se debe abordar teniendo en cuenta las leyes y los reglamentos pertinentes.

e) Se deben implementar medidas técnicas y organizativas apropiadas para proteger la PII.

1.35. Revisión independiente de seguridad de la información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#información_seguridad_garantía	#Gobernanza_y_Ecosistema

Control

Revisar de forma independiente al menos una vez al año o cuando se produzcan cambios significativos, la gestión de la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías

Recomendaciones para la implementación:

a) La máxima autoridad o su delegado junto al comité de seguridad de la información y el oficial de seguridad de la información, deben planificar e iniciar revisiones periódicas

independientes. Las revisiones deben incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoqué de la seguridad de la información, incluida la política de seguridad de la información, las políticas de temas específicos y otros controles.
b) Las revisiones deben ser realizadas por personas independientes del área bajo revisión (por ejemplo, la función de auditoría interna, un gerente independiente o una organización externa especializada en tales revisiones.

c) Las personas que lleven a cabo estas revisiones deben tener la competencia adecuada. La persona que realiza las revisiones no debe estar en la línea de autoridad para garantizar que tenga la independencia para realizar una evaluación.

d) Los resultados de las revisiones independientes deben informarse al comité de seguridad de la información y si procede a la máxima autoridad. Estos registros deben mantenerse.

e) Si las revisiones independientes identifican que el enfoque y la implementación de la institución para gestionar la seguridad de la información son inadecuados [por ejemplo, los objetivos y requisitos documentados no se cumplen o no cumplen con la dirección para la seguridad de la información establecida en la política de seguridad de la información y las políticas específicas del tema (ver 1.1)], el comité debe iniciar acciones correctivas.

f) La institución debería considerar la realización de revisiones independientes cuando:

- Las leyes y reglamentos afecten el cambio de la institución;
- Ocurren incidentes significativos;
- La institución cambia sus competencias;
- La institución comienza a usar un nuevo producto o servicio, o cambia el uso de un producto o servicio actual;
- La institución cambia significativamente los controles y procedimientos de seguridad de la información.

1.36. Cumplimiento de políticas, reglas y normas de seguridad de la información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Legal_y_cumplimiento #Información_seguridad_garantía	#Gobernanza_y_Ecosistema

Control

Revisar periódicamente el cumplimiento de la política de seguridad de la información de la institución, las políticas, las reglas y las normas del tema específico, bajo la responsabilidad de las autoridades institucionales.

Recomendaciones para la implementación:

El nivel jerárquico superior, propietarios de servicios, productos o información deben identificar cómo revisar que se cumplan los requisitos de seguridad de la información definidos en la política de seguridad de la información. Las políticas específicas del tema, las reglas, los estándares y otras reglamentaciones aplicables. Se deben considerar herramientas automáticas de medición y generación de informes para una revisión periódica eficiente.

Si se encuentra algún incumplimiento como resultado de la revisión, el jerárquico superior debe:

a)Identificar las causas del incumplimiento;

b)Evaluar la necesidad de acciones correctivas para lograr el cumplimiento;

c)Implementar acciones correctivas apropiadas;

d) Revisar las acciones correctivas tomadas para verificar su efectividad e identificar cualquier deficiencia o debilidad.

e) Los resultados de las revisiones y acciones correctivas llevadas a cabo por las autoridades, propietarios de servicios, productos o información deben registrarse y estos registros deben mantenerse.

f) Informar los resultados a las personas que realizan revisiones independientes (ver 1.35) cuando se lleva a cabo una revisión independiente en el área de su responsabilidad.

Las acciones correctivas deben completarse de manera oportuna según corresponda al riesgo, si no se completa para la próxima revisión programada, el progreso debe al menos abordarse en esa revisión.

1.37. Procedimientos documentados operativos

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Recuperar	#Gestión de activos #Seguridad física #Sistema_y_seguridad_de_la_red #Appplication_security #Configuración_segura #Identidad_y_acceso_administración #Gestión_de_amenazas_y_vulnerabilidades #Continuidad #Gestión_de_eventos_de_seguridad_de_la_información	#Gobernanza_y_Ecosistema #Protección #Defensa

Control

Documentar, implementar y socializar los procedimientos operativos para las instalaciones de tratamiento de información, y ponerse a disposición de los usuarios, para garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.

Recomendaciones para la implementación:

Se deben preparar procedimientos documentados para las actividades operativas de la institución asociadas con la seguridad de la información, por ejemplo:

a) Cuando la actividad necesite ser realizada de la misma manera por muchas personas;

b) Cuando la actividad se realiza con poca frecuencia y cuando se realiza la próxima vez es probable que se haya olvidado el procedimiento;

c) Cuando la actividad sea nueva y presente un riesgo si no se realiza correctamente;

d) Antes del traspaso de la actividad al nuevo personal.

Los procedimientos operativos deben especificar:

a) Las personas responsables;

b) La instalación y configuración segura de sistemas;

c) Tratamiento y manejo de información, tanto automatizado como manual;

d) Respaldo (ver 4.13) y resiliencia;

e) Requisitos de programación, incluidas las interdependencias con otros sistemas;

f) Instrucciones para el manejo de errores u otras condiciones excepcionales [por ejemplo, restricciones en el uso de programas de utilidad (ver 4.18)], que pueden surgir durante la ejecución del trabajo;

g) Contactos de soporte y escalamiento, incluidos contactos de soporte externo en caso de dificultades operativas o técnicas inesperadas;

h) Instrucciones de manejo de medios de almacenamiento (ver 3.10 y 3.14);

i) Procedimientos de reinicio y recuperación del sistema para su uso en caso de falla del sistema;

j) La gestión de la pista de auditoría y la información de registro del sistema (ver 4.15 y 4.17) y los sistemas de monitoreo de video (ver 3.4);

k) Procedimientos de monitoreo tales como capacidad, desempeño y seguridad (ver 4.6 y 4.16);

l) Instrucciones de mantenimiento.

Los procedimientos operativos documentados deben revisarse y actualizarse cuando sea necesario. Los cambios a los procedimientos operativos documentados deben ser autorizados.

Cuando sea técnicamente factible, los sistemas de información deben administrarse de manera consistente, utilizando los mismos procedimientos, herramientas y utilidades.

2. Control de personas

2.1. Selección

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_recursos_humanos	#Gobernanza_y_Ecosistema

Control

Verificar los antecedentes de todos los candidatos a funcionarios deben llevarse a cabo antes de unirse a la institución y de manera continua, teniendo en cuenta la norma legal vigente y ética aplicable, deben ser proporcionales a los requisitos institucionales, la clasificación de la información a la que se accede y los riesgos percibidos.

Recomendaciones para la implementación:

Se debe realizar un proceso de selección para todo el personal, incluido el personal a tiempo completo, a tiempo parcial y temporal. Cuando estas personas sean contratadas a través de proveedores de servicios, los requisitos de selección deben incluirse en los acuerdos contractuales entre la institución y los proveedores.

La información sobre todos los candidatos que se están considerando para puestos dentro de la institución se debe recopilar y manejar teniendo en cuenta la norma legal vigente.

La verificación debe tener en cuenta toda la legislación relevante sobre privacidad, protección de PII y basada en el empleo y, cuando esté permitido, debe incluir lo siguiente:

a) Disponibilidad de referencias satisfactorias (por ejemplo, referencias de negocios y personales):

b) Una verificación (de integridad y precisión) del curriculum vitae del solicitante;

c) Confirmación de las calificaciones académicas y profesionales reclamadas;

d) Verificación de identidad independiente (por ejemplo, pasaporte u otro documento aceptable emitido por las autoridades correspondientes);

e) Verificación más detallada, como revisión de crédito o revisión de antecedentes penales si el candidato asume un papel crítico.

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

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

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

c) Considerar más verificaciones y detalladas cuando el trabajo, ya sea en el nombramiento inicial o en la promoción, implique que la persona tenga acceso a instalaciones de tratamiento de información y, en particular, si esto implica el manejo de información confidencial (por ejemplo, información financiera, información personal o información de atención médica).

d) Definir los criterios y las limitaciones para las revisiones de verificación en los procedimientos, determinar quién es elegible para evaluar a las personas y cómo y cuándo y por qué se lleva a cabo las revisiones de verificación.

En situaciones en las que la verificación no se puede completar de manera oportuna, se deben implementar controles de mitigación hasta que se haya terminado la revisión, por ejemplo:

- Incorporación retrasada;
- Retraso en el despliegue de los activos corporativos;
- Embarque con acceso reducido;
- Terminación del empleo.

Los controles de verificación deben repetirse periódicamente para confirmar la idoneidad continua del personal, según la importancia del perfil de una persona.

2.2. Términos y condiciones de empleo

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_recursos_humanos	#Gobernanza_y_Ecosistema

Control

Los procesos contractuales de trabajo deben establecer las responsabilidades del personal y de la institución con respecto a la seguridad de la información y de acuerdo a la normativa legal vigente.

Recomendaciones para la implementación:

Las obligaciones contractuales para el personal deben tener en cuenta la política de seguridad de la información de la institución y las políticas de temas específicos relevantes, Además, se pueden aclarar y señalar los siguientes puntos:

a) Acuerdos de confidencialidad o de no divulgación que el personal al que se le da acceso a información confidencial debe firmar antes de que se le dé acceso a la información y otros activos asociados (ver 2.6);

b) Responsabilidades y derechos legales, por ejemplo, en relación con las leyes de derechos de autor o la legislación de protección de datos (ver 1.32 y 1.34);

c) Responsabilidades para la clasificación de la información y la gestión de la información de la institución y otros activos asociados, instalaciones de tratamiento de información y servicios de información manipulado por el personal (ver 1.9 a 1.13);

d) Responsabilizar por el manejo de la información recibida de las partes interesadas;

e) Comunicar a las partes interesadas las acciones legales a tomar si el personal ignora los requisitos de seguridad de la institución (ver 2.4) de acuerdo a norma legal vigente.

f) Las funciones y responsabilidades de seguridad de la información deben comunicarse a los candidatos durante el proceso previo al ingreso a la institución.

g) La organización debe asegurarse de que el personal esté de acuerdo con los términos y condiciones relacionados con la seguridad de la información.

h) Los términos y condiciones deben ser apropiados para la naturaleza y el grado de acceso que tendrán a los activos de la organización asociados con los sistemas y servicios de información.

i) Los términos y condiciones relacionados con la seguridad de la información deben revisarse cuando cambien las leyes, los reglamentos, la política de seguridad de la información o las políticas específicas de un tema.

j) Asegurar que el personal y las partes interesadas relevantes conozcan y cumplan con sus responsabilidades de seguridad de la información. 1.32 y 1.34)];

k) Las responsabilidades contenidas en los términos y condiciones de empleo deben continuar durante un período definido después de la terminación del empleo (ver 2.5).

2.3. Concienciación, educación y formación en seguridad de la información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_recursos_humanos	#Gobernanza_y_Ecosistema

Control

Los funcionarios de la institución y las partes interesadas relevantes deben recibir la concienciación, educación y formación adecuadas sobre la seguridad de la información y actualizaciones regulares de la política de seguridad de la información de la institución, las políticas y los procedimientos de temas específicos, según sea relevante para su función laboral.

Recomendaciones para la implementación:

General

a) Se debe establecer un plan de concienciación, educación y formación en seguridad de la información de acuerdo con la política de seguridad de la información de la institución, las políticas de temas específicos y los procedimientos relevantes sobre seguridad de la información, teniendo en cuenta la información de la institución que debe protegerse y los controles de seguridad de la información que se han implementado para proteger la información.

b) La concienciación, la educación y la formación en seguridad de la información deben llevarse a cabo periódicamente. La concienciación, la educación y la formación iniciales pueden aplicarse al personal nuevo y a aquellos que se transfieran a nuevos puestos o roles con requisitos de seguridad de la información sustancialmente diferentes.

c) La comprensión del personal debe evaluarse al final de una actividad de concienciación, educación o formación para probar la transferencia de conocimientos y la eficacia del programa de concienciación, educación y formación.

Concienciación

Un plan de concienciación sobre la seguridad de la información debe tener como objetivo que el personal sea consciente de sus responsabilidades con respecto a la seguridad de la información y los medios por los cuales se cumplen esas responsabilidades.

La concientización sobre la seguridad de la información debe cubrir aspectos generales tales como:

a) El compromiso de la máxima autoridad con la seguridad de la información en toda la institución;

b) Las necesidades de familiarización y cumplimiento concernientes a las reglas y obligaciones de seguridad de la información aplicables, teniendo en cuenta la política de seguridad de la información y las políticas, normas, leyes, estatutos, reglamentos, contratos y acuerdos de temas específicos de acuerdo a norma legal vigente:

c) Responsabilidad personal por las propias acciones e inacciones, y responsabilidades generales para asegurar o proteger la información que pertenece a la institución y las partes interesadas;

d) Procedimientos básicos de seguridad de la información, informes de eventos de seguridad

de la información (2.8) y controles de referencia, seguridad de contraseñas (1.17), controles de malware y mesas despejadas;

e) puntos de contacto y recursos para obtener información adicional y asesoramiento sobre asuntos de seguridad de la información, incluidos más materiales de concientización sobre la seguridad de la información.

Educación y entrenamiento

a) La institución debe identificar, preparar e implementar un plan de capacitación adecuado para los equipos técnicos cuyas funciones requieren conjuntos de habilidades y experiencia específicos.

b) Los equipos técnicos deben tener las habilidades para configurar y mantener el nivel de seguridad requerido para dispositivos, sistemas, aplicaciones y servicios. Si faltan habilidades, la institución debe tomar medidas y adquirirlas.

c) El programa de educación y capacitación debe considerar diferentes formas [por ejemplo, conferencias o autoestudios, ser asesorado por personal experto o consultores (capacitación en el trabajo), rotar a los miembros del personal para seguir diferentes actividades, reclutar personas ya capacitadas y contratar consultores]. Puede usar diferentes medios de entrega, incluidos el aprendizaje en el aula, a distancia, basado en la web, a su propio ritmo y otros.

d) El personal técnico debe mantener actualizados sus conocimientos suscribiéndose a boletines y revistas o asistiendo a congresos y eventos destinados a la mejora técnica y profesional.

2.4. Proceso disciplinario

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Seguridad_de_recursos_humanos	#Gobernanza_y_Ecosistema

Control

Formalizar y comunicar un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación de la política de seguridad de la información, de acuerdo a la norma legal vigente.

Recomendaciones para la implementación:

El proceso disciplinario no debe iniciarse sin la verificación legal previa de que se ha producido una violación de la política de seguridad de la información (ver 1.28).

a) El proceso disciplinario formal debe prever una respuesta graduada que tenga en cuenta factores tales como:
   - La naturaleza (quién, qué, cuándo, cómo) y la gravedad del incumplimiento y sus

consecuencias;

- Si el delito fue intencional (malicioso) o no intencional (accidental);
- Si se trata o no de una primera o reiterada infracción;
- Si el infractor fue debidamente capacitado o no.

b) La respuesta debe tener en cuenta la norma legal vigente, los requisitos legales, estatutarios, reglamentarios, contractuales pertinentes, así como otros factores que sean necesarios.

c) El proceso disciplinario también debe usarse como elemento disuasorio para evitar que el personal y otras partes interesadas relevantes violen la política de seguridad de la información, las políticas y los procedimientos de temas específicos para la seguridad de la información.

d) Las violaciones deliberadas de la política de seguridad de la información deben requerir acciones inmediatas.

2.5. Responsabilidades después de la terminación o cambio de empleo

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_recursos_humanos #Gestión_de_activos	#Gobernanza_y_Ecosistema

Control

Definir, aplicar y comunicar al personal relevante y otras partes interesadas, las responsabilidades y deberes de seguridad de la información que siguen siendo válidas después de la terminación de la relación laboral o el cambio de puesto.

Recomendaciones para la implementación:

a) El proceso para gestionar la terminación de la relación laboral o el cambio de puesto en la institución debe definir qué responsabilidades y deberes de seguridad de la información deben permanecer vigentes después de la terminación o el cambio, esto puede incluir la confidencialidad de la información, la propiedad intelectual y otros conocimientos obtenidos, así como las responsabilidades contenidas en cualquier otro acuerdo de confidencialidad (ver 2.6).

b) Las responsabilidades y deberes que sigan vigentes después de la terminación del empleo o contrato deben estar contenidos en los términos y condiciones de empleo (ver 2.2), contrato o acuerdo de la persona.

c) Otros contratos o acuerdos que continúan por un periodo definido después del final de la

relación laboral del funcionario también pueden contener responsabilidades de seguridad de la información.

d) Los cambios de responsabilidad o empleo deben gestionarse como la terminación de la responsabilidad o cargo actual combinada con el inicio de la nueva responsabilidad o cargo.

e) Los roles y responsabilidades de seguridad de la información que tenga cualquier persona que deje o cambie de puesto se deben identificar y transferir a otra persona

f) Se debe establecer un proceso para la comunicación de los cambios y de los procedimientos operativos al personal, a otras partes interesadas y a las personas de contacto pertinentes como clientes y proveedores.

g) El proceso de terminación o cambio de cargo también se debe aplicar al personal externo (es decir, proveedores) cuando se produce una terminación de la relación laboral con la institución, o cuando hay un cambio de puesto dentro de la institución;

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

i) Previa la terminación de un contrato se deberá realizar la transferencia de la documentación e información de la que fue responsable al nuevo funcionario a cargo, en caso de ausencia, al jefe inmediato o quien haga sus veces.

2.6. Acuerdos de confidencialidad o no divulgación

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Seguridad_de_recursos_humanos #Información_protección #Relaciones_con_proveedores	#Gobernanza_y_Ecosistema

Control

Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la institución para la protección de la información deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas relevantes de acuerdo a la necesidad de la institución.

Recomendaciones para la implementación:

a) Los acuerdos de confidencialidad o de no divulgación deben abordar el requisito de proteger la información confidencial utilizando términos legalmente exigibles.

b) Los acuerdos de confidencialidad o no divulgación son aplicables a las partes interesadas y al personal de la institución.

c) En función de los requisitos de seguridad de la información de una institución, los términos de los acuerdos deben determinarse teniendo en cuenta el tipo de información que se manejaré, su nivel de clasificación, su uso y el acceso permitido por la otra parte.

d) Para identificar los requisitos para los acuerdos de confidencialidad o no divulgación, se debe considerar los siguientes elementos:

- Una definición de la información a proteger de acuerdo a la clasificación de la misma;
- La duración esperada de un acuerdo de confidencialidad, incluidos los casos en que puede ser necesario mantener la confidencialidad indefinidamente o hasta que la información esté disponible públicamente de acuerdo a la normativa legal vigente;
- las acciones requeridas cuando se termina un acuerdo;
- Las responsabilidades y acciones de los signatarios para evitar la divulgación de información no autorizada;
- La propiedad de la información y la propiedad intelectual, y cómo esto se relaciona con la protección de la información confidencial;
- Implementar políticas para el uso permitido de la información confidencial y los derechos del firmante para usar la información;
- El derecho a auditar y monitorear actividades que involucren información confidencial para circunstancias altamente sensibles;
- El proceso de notificación y reporte de divulgación no autorizada o fuga de información confidencial:
- Definir los términos para la devolución o destrucción de la información al término del contrato;
- Definir las acciones previstas a tomar en caso de incumplimiento del acuerdo.

e) La institución debe tener en cuenta el cumplimiento de los acuerdos de confidencialidad y no divulgación para el área al que se aplican (ver 1.31, 1.32, 1.33, 1.34).

f) Los requisitos para los acuerdos de confidencialidad y no divulgación deben revisarse periódicamente y cuando ocurran cambios legales que influyan en estos requisitos.

2.7. Trabajo remoto

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos #Información_protección #Seguridad_física #Sistema_y_seguridad_de_la_red	#Protección

Control

Implementar políticas y medidas de seguridad cuando el personal trabaja de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la institución.

Recomendaciones para la implementación:

El trabajo remoto ocurre cuando el personal de la institución trabaja desde un lugar fuera de las instalaciones de la institución, accediendo a la información ya sea en forma impresa o electrónica a través de equipos de TIC; los entornos de trabajo remoto incluyen los denominados "teletrabajo", "trabajo desde casa (telecommuting)", "lugar de trabajo flexible", "entornos de trabajo virtuales" y "mantenimiento remoto".

Las instituciones que permiten actividades de trabajo a distancia deben emitir una política específica sobre el tema del trabajo a distancia que defina las condiciones y restricciones pertinentes. Cuando se considere aplicable, se deben considerar los siguientes asuntos:

a) La seguridad física existente o propuesta del sitio de trabajo remoto, teniendo en cuenta la seguridad física del lugar y el entorno local, incluidos los diferentes sitios donde se encuentra el personal;

b) Reglas y mecanismos de seguridad para el entorno físico remoto, como archivadores con cerradura, transporte seguro entre ubicaciones y reglas para el acceso remoto, puesto despejado, impresión y eliminación de información y otros activos asociados, e informes de eventos de seguridad de la información (ver 2.8);

c) Los entornos físicos de trabajo remoto esperados;

d) Los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas de la institución, la sensibilidad de la información a la que se accederá y pasará por el enlace de comunicación y la sensibilidad de los sistemas y aplicaciones;

e) El uso de acceso remoto, como acceso de escritorio virtual que admita el tratamiento y almacenamiento de información en equipos de propiedad privada;

f) La amenaza de acceso no autorizado a información o recursos de otras personas en el lugar de trabajo remoto (por ejemplo, familiares y amigos);

g) La amenaza de acceso no autorizado a información o recursos de otras personas en lugares públicos;

h) El uso de redes domiciliarias y redes públicas, y requisitos o restricciones en la configuración de servicios de redes inalámbricas;

j) Uso de medidas de seguridad, como firewalls y protección contra malware;

k) Mecanismos seguros para implementar e inicializar sistemas de forma remota;

l) Mecanismos seguros de autenticación y habilitación de privilegios de acceso teniendo en cuenta la vulnerabilidad de los mecanismos de autenticación de un solo factor donde se permite el acceso remoto a la red de la institución.

Las directrices y medidas a considerar deben incluir:

a) La provisión de equipos y muebles de almacenamiento adecuados para las actividades de trabajo remoto, donde no se permite el uso de equipos de propiedad privada que no estén bajo el control de la institución, de ser posible;

b) Una definición del trabajo permitido, la clasificación de la información que puede ser mantenida y los sistemas y servicios internos a los que el trabajador remoto está autorizado a acceder;

c) La provisión de capacitación para quienes trabajan a distancia y quienes brindan apoyo, esto debe incluir cómo realizar negocios de manera segura mientras se trabaja de forma remota:

d) La provisión de equipos de comunicación adecuados, incluidos los métodos para asegurar el acceso remoto, como los requisitos sobre bloqueos de pantalla del dispositivo y temporizadores de inactividad; la habilitación del seguimiento de la ubicación del dispositivo; instalación de capacidades de borrado remoto;

e) Seguridad física;

f) Normas y orientaciones sobre el acceso de familiares y visitantes a equipos e información;

g) La provisión de soporte y mantenimiento de hardware y software;

h) La provisión de seguros;

i) Los procedimientos de respaldo y continuidad del negocio;

j) Auditoría y monitoreo de la seguridad;

k) Revocación de facultades y derechos de acceso y devolución de equipos cuando finalicen las actividades de trabajo remoto.

2.8. Reporte de eventos de seguridad de la información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Detective	#Confidencialidad #Integridad #Disponibilidad	#Detectar	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

Proporcionar un procedimiento para que el personal informe eventos de seguridad de la información observados o sospechados a través de los canales apropiados de manera oportuna.

Recomendaciones para la implementación:

Todo el personal y los usuarios deben ser conscientes de su responsabilidad de informar los eventos de seguridad de la información lo más rápido posible para prevenir o minimizar el efecto de los incidentes de seguridad de la información.

También deben conocer el procedimiento para informar eventos de seguridad de la información y el punto de contacto al que se debe informar los eventos, el mecanismo de presentación de informes debe ser lo más fácil, accesible y disponible posible. Los eventos de seguridad de la información incluyen incidentes, violaciones y vulnerabilidades.

Establecer un punto de contacto para el reporte de los eventos de seguridad de la información. Es conveniente garantizar que este punto de contacto sea conocido en toda la institución, siempre esté disponible y puede suministrar respuesta oportuna y adecuada. Todas las partes interesadas deberán tener conciencia de su responsabilidad para reportar todos los eventos de seguridad de la información lo más pronto posible, este proceso será liderado por el Oficial de Seguridad de la Información.

El responsable de llevar este reporte denominado "Reporte de vulnerabilidades o debilidades de la seguridad de la información" es el Oficial de Seguridad de la Información. El Oficial de Seguridad de la Información coordinará con el responsable de la información y el área de tecnología a fin tomar las medidas pertinentes para prevenir o eliminar la vulnerabilidad o debilidad detectada.

Las situaciones a considerar para comunicar los eventos de seguridad de la información incluyen:

a) Controles de seguridad de la información ineficaces;

b) Incumplimiento de las expectativas de confidencialidad, integridad o disponibilidad de la información:

c) Errores humanos;

d) Incumplimiento de la política de seguridad de la información, políticas de temas específicos o normas aplicables:

e) Incumplimientos de las medidas de seguridad física;

f) Cambios en el sistema que no han pasado por el proceso de control y gestión de cambios;

g) Mal funcionamiento u otro comportamiento anómalo del sistema de software o hardware,

h) Infracciones de acceso;

i) Vulnerabilidades;

j) Sospecha de infección por malware.

Se debe advertir al personal y a los usuarios que no intenten probar vulnerabilidades de seguridad de la información sospechosas, las vulnerabilidades de prueba pueden interpretarse como un mal uso potencial del sistema y también pueden causar daños al sistema o servicio de información, y pueden corromper u ocultar la evidencia digital. En última instancia, esto puede resultar en responsabilidad legal para la persona que realiza la prueba.

El responsable de llevar el "Reporte de vulnerabilidades o debilidades de la seguridad de la información" es el Oficial de Seguridad de la Información, el mismo que deberá tomar las medidas pertinentes para tratar la vulnerabilidad o debilidad detectada.

3. Controles físicos

3.1. Perímetros de seguridad física

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física	#Protección

Control

Los perímetros de seguridad se deben definir y utilizar para proteger las áreas que contienen información y otros activos asociados, para evitar el acceso físico no autorizado, el daño y la interferencia a la información de la institución.

Recomendaciones para la implementación:

Las siguientes directrices se deben considerar e implementar cuando corresponda para los perímetros de seguridad física:

a) Definir y documentar los perímetros de seguridad, la ubicación y fortaleza de cada uno de los perímetros de acuerdo con los requisitos de seguridad de la información relacionados con los activos dentro del perímetro;

b) Tener perímetros físicamente sólidos para un edificio o sitio que contenga instalaciones de tratamiento de información (es decir, no debe haber espacios en el perímetro o áreas donde un allanamiento pueda ocurrir fácilmente). Los techos, paredes y pisos exteriores del sitio deben ser de construcción sólida y todas las puertas externas deben estar adecuadamente protegidas contra el acceso no autorizado con mecanismos de control como rejas, alarmas, cerraduras. Las puertas y ventanas deben cerrarse con llave cuando estén desatendidas y se debe considerar la protección externa para las ventanas, particularmente a nivel del suelo; también se deben considerar los puntos de ventilación;

c) Alarmar, monitorear y probar todas las puertas contra incendios en un perímetro de seguridad junto con las paredes para establecer el nivel requerido de resistencia de acuerdo

con los estándares adecuados, deben operar a manera a prueba de fallas;

d) Disponer de alarmas de incendio y puertas de evacuación debidamente monitoreadas que cumplan normas nacionales e internacionales;

3.2. Entrada física

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_identidad_y_acceso	#Protección

Control

Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados, para garantizar que solo el personal autorizado dispone de permiso de acceso.

Recomendaciones para la implementación:

Generalidades

Los puntos de acceso como las áreas de entrega, carga y otros puntos donde personas no autorizadas pueden ingresar a las instalaciones deben controlarse y si es posible, aislarse de las instalaciones de tratamiento de información para evitar el acceso no autorizado.

Se deben considerar las siguientes directrices:

a) Restringir el acceso a los sitios y edificios al personal no autorizado. El proceso de gestión de los derechos de acceso a las áreas físicas debe incluir el otorgamiento, revisión periódica, actualización y revocación de las autorizaciones (ver 1.18);

b) Mantener y monitorear de forma segura un libro de registro físico o un registro de auditoria electrónico de todos los accesos y proteger todos los registros (ver 1.33) y la información de autenticación confidencial;

c) Establecer e implementar un proceso y mecanismos técnicos para la gestión del acceso a las áreas donde se procesa o almacena la información. Los mecanismos de autenticación incluyen el uso de tarjetas de acceso, biometría o autenticación de dos factores, como una tarjeta de acceso y un PIN secreto. Se deben considerar puertas dobles de seguridad para el acceso a áreas sensibles;

d) Establecer un área de recepción monitoreada por personal u otros medios para controlar el acceso físico al sitio o edificio;

e) Inspeccionar y examinar los efectos personales del personal y de los interesados a la entrada y salida, de acuerdo a la norma legal vigente.

f) Requerir que todo el personal y las partes interesadas usen algún tipo de identificación

visible y que notifiquen de inmediato al personal de seguridad si encuentran visitantes sin escolta y cualquier persona que no use una identificación visible. Se deben considerar insignias fácilmente distinguibles para identificar mejor a los empleados permanentes, proveedores y visitantes;

g) Otorgar acceso restringido al personal del proveedor a áreas seguras o instalaciones de tratamiento de información solo cuando sea necesario. Este acceso debe ser autorizado y monitoreado;

h) Prestar especial atención a la seguridad del acceso físico en el caso de edificios que contengan activos para múltiples organizaciones;

i) Diseñar medidas de seguridad física para que puedan reforzarse cuando aumente la probabilidad de incidentes físicos;

j) Proteger otros puntos de entrada, como salidas de emergencia, del acceso no autorizado;

k) Establecer un proceso de gestión de claves para garantizar la gestión de las claves físicas o la información de autenticación (por ejemplo, códigos de bloqueo, cerraduras de combinación para oficinas, salas e instalaciones, como armarios de llaves) y asegurar un libro de registro o una auditoría anual de claves y que el acceso a las claves físicas o se controle la información de autenticación (ver 1.17 para obtener más orientación sobre la información de autenticación).

Visitantes

Se deben considerar las siguientes directrices:

a) Autenticar la identidad de los visitantes por un medio apropiado;

b) Registrar la fecha y hora de entrada y salida de los visitantes;

c) Permitir el acceso de visitantes únicamente para fines específicos, autorizados y con instrucciones sobre los requisitos de seguridad del área y sobre los procedimientos de emergencia;

d) Supervisar a todos los visitantes, a menos que se conceda una excepción explicita.

Zonas de entrega y carga y entrada de material

Se deben considerar las siguientes directrices:

a) Restringir el acceso a las áreas de carga y entrega desde el exterior del edificio al personal identificado y autorizado;

b) Diseñar las áreas de entrega y carga para que las entregas puedan cargarse y descargarse sin que el personal de entrega obtenga acceso no autorizado a otras partes del edificio;

c) Asegurar las puertas externas de las áreas de carga y entrega cuando se abren las puertas de las áreas restringidas;

d) Inspeccionar y examinar las entregas entrantes en busca de explosivos, productos u otros materiales peligrosos antes de que se muevan de las áreas de entrega y carga;

e) Registrar las entregas entrantes de acuerdo con los procedimientos de gestión de activos (ver 1.9 y 3.10) al ingresar al sitio;

f) Separar físicamente los envíos entrantes y salientes, cuando sea posible;

g) Inspeccionar las entregas entrantes en busca de evidencia de manipulación en el camino. Si se descubre una manipulación, se debe informar de inmediato al personal de seguridad.

3.3. Seguridad de oficinas, despachos e instalaciones

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección

Control

Diseñar, documentar e implementar la seguridad física de oficinas, despachos e instalaciones.

Recomendaciones para la implementación:

Se deben considerar las siguientes recomendaciones para asegurar oficinas, salas e instalaciones:

a) Ubicar las instalaciones criticas seguras para evitar el acceso del público;

b) Cuando corresponda, asegurarse de que los edificios sean seguros y den una indicación mínima de su propósito, sin señales obvias, fuera o dentro del edificio, que identifiquen la presencia de actividades de tratamiento de información;

c) Configurar instalaciones para evitar que la información o actividades confidenciales sean visibles y audibles desde el exterior. El blindaje electromagnético también se debe considerar apropiado;

d) No poner a disposición de cualquier persona no autorizada directorios, guías telefónicas internas y mapas accesibles en línea que identifiquen ubicaciones de instalaciones de tratamiento de información confidencial;

e) Ubicar los equipos de reproducción de documentos sensibles como impresoras, copiadoras y otros, en un área protegida.

3.4. Monitoreo de seguridad física

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad_física	#Protección #Defensa

Control

Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados.

Recomendaciones para la implementación:

Las instalaciones físicas deben ser monitoreadas por sistemas de vigilancia, que pueden incluir guardias, alarmas contra intrusos, sistemas de video vigilancia como un circuito cerrado de televisión y software de gestión de información de seguridad física, ya sea administrado internamente o por un proveedor de servicios de monitoreo.

El acceso a los edificios que albergan sistemas críticos se debe monitorear continuamente para detectar accesos no autorizados o comportamientos sospechosos mediante:

a) Instalar sistemas de vigilancia por video, como un circuito cerrado de televisión, para ver y registrar el acceso a áreas sensibles dentro y fuera de las instalaciones de la institución;

b) Instalar, de acuerdo con las normas relevantes aplicables, y probar periódicamente detectores de contacto, sonido o movimiento para activar una alarma de intrusión, tales como:

1) Instalar detectores de contacto que activen una alarma cuando se haga o se rompa un contacto en cualquier lugar donde se pueda hacer o romper un contacto (como ventanas, puertas y debajo de objetos) para usar como alarma de pánico;

2) Detectores de movimiento basados en tecnología infrarroja que activan una alarma cuando un objeto pasa por su campo de visión:

3) Instalar sensores sensibles al sonido de cristales rotos que puedan usarse para activar una alarma para alertar al personal de seguridad;

c) usar esas alarmas para cubrir todas las puertas exteriores y ventanas accesibles. Las áreas desocupadas deben estar alarmadas en todo momento; También se debe proporcionar cobertura para otras áreas (por ejemplo, salas de computadoras o de comunicaciones).

d) El diseño de los sistemas de monitoreo se debe mantener confidencial porque la divulgación puede facilitar robos no detectados.

e) Los sistemas de monitoreo se deben proteger contra el acceso no autorizado para evitar que personas no autorizadas accedan a la información de vigilancia, como transmisiones

de video, o que los sistemas se deshabiliten de forma remota.

f) El panel de control del sistema de alarma se debe colocar en una zona de alarma y, para las alarmas de seguridad, en un lugar que permita una ruta de salida fácil para la persona que activa la alarma.

g) El panel de control y los detectores deben tener mecanismos a prueba de manipulaciones. El sistema se debe probar periódicamente para asegurar de que funciona según lo previsto, especialmente si sus componentes funcionan con baterías.

Cualquier mecanismo de monitoreo y registro se debe usar teniendo en cuenta las leyes y regulaciones locales, incluida la protección de datos y la legislación de protección de PII, especialmente con respecto al monitoreo de personal y periodos de retención de videos grabados.

3.5. Protección contra las amenazas externas y ambientales

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física	#Protección

Control

Diseñar e implementar la protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.

Recomendaciones para la implementación:

Las evaluaciones de riesgos para identificar las posibles consecuencias de las amenazas físicas y ambientales se deben realizar antes de comenzar las operaciones críticas en un sitio físico y en intervalos regulares. Se debe implementar las salvaguardas necesarias y se debe monitorear los cambios en las amenazas. Se debe obtener asesoramiento especializado sobre cómo gestionar los riesgos derivados de las amenazas físicas y ambientales tales como incendios, inundaciones, terremotos, explosiones, disturbios civiles, desechos tóxicos, emisiones ambientales y otras formas de desastres naturales o desastres causados por seres humanos.

La localización y la construcción de las instalaciones físicas deben tener en cuenta:

a)Topografía local, como elevación adecuada, masas de agua y fallas tectónicas;

b) Amenazas urbanas, como lugares con un alto perfil para atraer disturbios políticos, actividad criminal o ataques terroristas.

Con base en los resultados de la evaluación de riesgos, se deben identificar las amenazas físicas y ambientales relevantes y se deben considerar los controles apropiados en los siguientes contextos como ejemplo:

a) Incendio: instalar y configurar sistemas capaces de detectar incendios en una etapa temprana para enviar alarmas o activar sistemas de supresión de incendios para evitar que el fuego dañe los medios de almacenamiento y los sistemas de tratamiento de información relacionados.

b) Inundaciones: instalar sistemas capaces de detectar inundaciones en una etapa temprana bajo los pisos de áreas que contienen medios de almacenamiento o sistemas de tratamiento de información. Las bombas de agua o medios equivalentes deben estar fácilmente disponibles en caso de que ocurra una inundación;

c) Sobrecargas eléctricas: adoptar sistemas capaces de proteger los sistemas de información del servidor y del cliente contra sobrecargas eléctricas o eventos similares para minimizar las consecuencias de tales eventos;

d) Explosivos y armas: realizar inspecciones aleatorias para detectar la presencia de explosivos o armas en el personal, vehículos o bienes que ingresan a las instalaciones de tratamiento de información sensible.

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

Realizar mantenimientos de las instalaciones eléctricas, UPS; así como de los sistemas de climatización, ductos de ventilación y todo lo que se considere necesario.

3.6. Trabajo en áreas seguras

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física	#Protección

Control

Elaborar, implementar y socializar procedimientos de seguridad para trabajar en zonas seguras, y proteger la información y otros activos asociados contra daños e interferencias no autorizadas por parte del personal que trabaja en estas áreas.

Recomendaciones para la implementación:

Las medidas de seguridad para trabajar en áreas seguras se deben aplicar a todo el personal y cubrir todas las actividades que se desarrollen en el área segura.

Se debe considerar las siguientes directrices:

a) Hacer que el personal sea consciente de la existencia o de las actividades dentro de un área segura únicamente según sea necesario:

b) Evitar el trabajo sin supervisión en áreas seguras tanto por razones de seguridad como para reducir las posibilidades de actividades maliciosas;

c) Cerrar físicamente e inspeccionar periódicamente las áreas seguras vacantes;

d) No permitir equipos fotográficos, de video, de audio u otros equipos de grabación, como cámaras en los dispositivos finales del usuario, a menos que esté autorizado;

e) Controlar adecuadamente el transporte y uso de los dispositivos de punto final del usuario en áreas seguras;

f) Socializar y Publicar los procedimientos de emergencia de manera fácilmente visible o accesible.

3.7. Puesto de trabajo despejado y pantalla limpia

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Seguridad_física	#Protección

Control

Definir y aplicar adecuadamente reglas de puesto despejado para documentos y medios de almacenamiento extraíbles y reglas de pantalla limpia para las instalaciones de tratamiento de información.

Recomendaciones para la implementación:

La institución debe establecer y comunicar una política de tema específicos sobre puesto despejado y pantalla limpia a todas las partes interesadas relevantes.

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

Se deben considerar las siguientes recomendaciones:

a) Guardar bajo llave la información confidencial o crítica (por ejemplo, en papel o en medios de almacenamiento electrónicos) (idealmente en una caja fuerte, gabinete u otro tipo de mueble de seguridad cuando no sea necesario, especialmente cuando la oficina esté desocupada;

b) Proteger los dispositivos de punto final del usuario mediante cerraduras con llave u otros medios de seguridad cuando no estén en uso o desatendidos;

c) Dejar los dispositivos de punto final de usuarios desconectados de la red o protegidos con un mecanismo de bloqueo de pantalla y teclado controlado por un mecanismo de autenticación de usuario cuando están desatendidos. Todas las computadoras y sistemas

se deben configurar con una función de tiempo de espera o cierre de sesión automático;

d) Hacer que el creador recopile los resultados de las impresoras o dispositivos multifunción de inmediato. El uso de impresoras con una función de autenticación, de modo que los creadores sean los únicos que puedan obtener sus impresiones y solo cuando estén parados al lado de la impresora;

e) Almacenar de forma segura documentos y medios de almacenamiento extraíbles que contengan información confidencial y, cuando ya no se necesiten, desecharlos utilizando mecanismos seguros de eliminación;

f) Establecer y comunicar reglas y orientación para la configuración de ventanas emergentes en las pantallas (por ejemplo, apagar las nuevas ventanas emergentes de correo electrónico y mensajería, si es posible, durante presentaciones, pantallas compartidas o en un área pública);

g) Borrar información sensible o crítica en pizarras y otros tipos de pantallas cuando ya no se necesiten.

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

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

j) Tener procedimientos implementados al desocupar las instalaciones, incluida la realización de un barrido final antes de irse para asegurar que los activos de la institución no se queden atrás (por ejemplo, documentos caídos detrás de cajones o muebles).

3.8. Ubicación y protección de equipos

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección

Control

Los equipos que procesan información deben estar ubicados de forma segura y protegida, para reducir los riesgos de las amenazas, peligros ambientales y de oportunidades de acceso no autorizado.

Recomendaciones para la implementación:

Se deben considerar las siguientes recomendaciones para proteger el equipo:

a) Ubicar de forma segura el equipo para minimizar el acceso innecesario a las áreas de trabajo y evitar el acceso no autorizado;

b) Ubicar cuidadosamente las instalaciones de tratamiento de información que manejan datos confidenciales para reducir el riesgo de que personas no autorizadas vean la

información durante su uso;

c) Adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales, por ejemplo, robo, fuego, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo.

d) Establecer directrices para evitar comer, beber y fumar en las proximidades de las instalaciones de tratamiento de información;

e) Monitorear las condiciones ambientales, como la temperatura y la humedad, en busca de condiciones que puedan afectar negativamente la operación de las instalaciones de tratamiento de información:

f) Aplicar protección contra rayos a todos los edificios y colocar filtros de protección contra rayos en todas las líneas eléctricas y de comunicaciones entrantes;

g) Considerar el uso de métodos de protección especiales, como membranas de teclado, para equipos en ambientes industriales;

h) Proteger los equipos que tratan información confidencial para minimizar el riesgo de fuga de información debido a la emanación electromagnética;

i) Separar físicamente las instalaciones de tratamiento de información gestionadas por la institución de aquellas que no son gestionadas por la institución.

j) Aislar los elementos que requieran protección especial para reducir el nivel de protección general requerido

3.9. Seguridad de los activos fuera de las instalaciones

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección

Control

Aplicar medidas de seguridad a los equipos ubicados afuera de las instalaciones de la institución, considerando los riesgos que surgen el trabajar fuera de las mismas, para evitar la pérdida, el daño, el robo o el compromiso de los dispositivos externos y la interrupción de las operaciones.

Recomendaciones para la implementación:

Se deben considerar las siguientes directrices para la protección de dispositivos que almacenan o procesan información fuera de las instalaciones de la institución:

a) Cualquier dispositivo utilizado fuera de las instalaciones de la institución que almacene o procese información (por ejemplo, dispositivo móvil), incluidos los dispositivos de propiedad de la institución y los dispositivos de propiedad privada y utilizados en nombre de la institución (traiga su propio dispositivo - BYOD) necesita protección.

b) El uso de estos dispositivos debe ser autorizado por la autoridad del área responsable del activo;

c) No dejar desatendidos equipos y medios de almacenamiento fuera de las instalaciones en lugares públicos y no seguros;

d) Observar las instrucciones de los fabricantes para proteger el equipo en todo momento (por ejemplo, protección contra la exposición a campos electromagnéticos fuertes, agua, calor, humedad, polvo);

e) Cuando se transfieren equipos fuera de las instalaciones entre diferentes personas o partes interesadas, mantener un registro que defina la cadena de custodia del equipo, incluidos al menos los nombres y las instituciones de quienes son responsables del equipo. La información que no necesita transferirse con el activo se debe eliminar de forma segura antes de la transferencia;

f) Cuando sea necesario y práctico, solicitar autorización para retirar equipos y medios de las instalaciones de la institución y llevar un registro de tales retiros para mantener un registro de auditoría (ver 1.14):

g) Protección contra la visualización de información en un dispositivo (por ejemplo, un teléfono móvil o una computadora portátil) en el transporte público, y los riesgos asociados con el movimiento de la persona;

h) Implementar el seguimiento de la ubicación y la capacidad de borrar dispositivos de forma remota;

i) Establecer una cobertura adecuada del seguro, para proteger los equipos que se encuentran fuera de las instalaciones,

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

La instalación permanente de equipos fuera de las instalaciones de la institución, como antenas y cajeros automáticos (ATM), puede estar sujeta a un mayor riesgo de daño, robo o escuchas ilegales. Estos riesgos pueden variar considerablemente entre ubicaciones y se deben tener en cuenta al determinar las medidas más apropiadas; considerar las siguientes directrices al colocar este equipo fuera de las instalaciones de la institución:

a) Monitoreo de la seguridad física (ver 3.4);

b) Protección contra amenazas físicas y ambientales (ver 3.5);

c) Controles de acceso físico y a prueba de manipulaciones;

d) Controles de acceso lógico.

3.10. Medios de almacenamiento

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección

Control

Implementar procedimientos para la gestión de los medios de almacenamiento a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la institución.

Recomendaciones para la implementación:

Se deben considerar las siguientes recomendaciones para la gestión de medios de almacenamiento extraíbles:

Medios de almacenamiento extraíbles

a) Establecer una política de temas específicos sobre la gestión de medios de almacenamiento extraíbles y socializar dicha política de temas específicos a cualquier persona que use o manipule medios de almacenamiento extraíbles;

b) Cuando sea necesario y práctico, solicitar autorización para que los medios de almacenamiento se retiren de la institución y mantener un registro de tales retiros para mantener un registro de auditoría;

c) Almacenar todos los medios de almacenamiento en un entorno seguro y protegido de acuerdo con su clasificación de información y protegerlos contra amenazas ambientales como calor, humedad, campo electrónico o envejecimiento, de acuerdo con las especificaciones de los fabricantes;

d) Si la confidencialidad o la integridad de la información son consideraciones importantes, usar técnicas criptográficas para proteger la información en medios de almacenamiento extraíbles;

e) Modificar el riesgo de que los medios de almacenamiento se degraden mientras aún se necesita la información almacenada, transfiriendo la información a nuevos medios de almacenamiento antes de que se vuelva ilegible;

f) Almacenar múltiples copias de información valiosa en medios de almacenamiento separados para reducir aún más el riesgo de daño o pérdida de información coincidente;

g) Considerar el registro de medios de almacenamiento extraíbles para limitar la posibilidad de pérdida de información;

h) Solo habilitar puertos de medios de almacenamiento extraíbles, por ejemplo, ranuras para tarjetas digitales seguras (sd) y puertos de bus serie universal (usb), si existe una razón institucional para su uso;

i) Cuando sea necesario utilizar medios de almacenamiento extraíbles, monitorear la transferencia de información a dichos medios de almacenamiento;

j) La información puede ser vulnerable al acceso no autorizado, mal uso o corrupción durante el transporte físico, por ejemplo, cuando se envían medios de almacenamiento a través del servicio postal o de mensajería.

En este control, los medios incluyen documentos en papel. Al transferir medios físicos de almacenamiento, aplique las medidas de seguridad de 1.14.

Reutilización o eliminación segura

Se deben establecer procedimientos para la reutilización o eliminación segura de los medios de almacenamiento para minimizar el riesgo de fuga de información confidencial a personas no autorizadas. Los procedimientos para la reutilización segura o la eliminación de medios de almacenamiento que contengan información confidencial deben ser proporcionales a la criticidad de la información; se deben considerar los siguientes elementos:

a) Si los medios de almacenamiento que contienen información confidencial se deben reutilizar dentro de la institución, eliminar datos de forma segura o formatear los medios de almacenamiento antes de su reutilización (ver 4.10);

b) Deshacerse de medios de almacenamiento que contengan información confidencial de forma segura cuando ya no se necesiten, por ejemplo, destruyendo, triturando o eliminando de forma segura el contenido;

c) Contar con procedimientos para identificar los activos que pueden requerir una eliminación segura;

d)Muchas instituciones ofrecen servicios de recogida y eliminación de medios de almacenamiento. Se debe tener cuidado al seleccionar un proveedor externo adecuado con controles y experiencia adecuados;

e)Registrar la eliminación de elementos sensibles para mantener un registro de auditoria;

f) Al acumular medios de almacenamiento para su eliminación, teniendo en cuenta el efecto de agregación, que puede hacer que una gran cantidad de información no sensible se vuelva sensible;

g) Realizar una evaluación de riesgos con los dispositivos dañados que contengan datos confidenciales para determinar si los elementos se deben destruir físicamente en lugar de enviar a reparar o desechar (ver 3.14)

3.11. Servicios de soporte

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo	#Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad_física	#Protección

Control

Las instalaciones de tratamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de soporte.

Recomendaciones para la implementación:

Las instituciones dependen de los servicios públicos, por ejemplo, electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado para respaldar sus instalaciones de tratamiento de información. Por lo tanto, la institución debería:

a) Asegurarse de que el equipo de soporte de los servicios públicos (UPS, generador eléctrico y otros) esté configurado, operado y mantenido de acuerdo con las especificaciones del fabricante correspondiente;

b) Asegurarse de que el equipo de soporte a los servicios públicos, sea inspeccionados y probados periódicamente para asegurar su correcto funcionamiento;

c) Si es necesario y de ser posible, activar alarmas para detectar fallas en los servicios públicos;

d) Si es necesario, asegúrese de que las empresas de servicios públicos tengan múltiples alimentaciones con diversas rutas físicas;

e)Asegurarse de que el equipo de soporte a los servicios públicos, esté en una red separada de las instalaciones de tratamiento de información si está conectado a una red o de acuerdo a la estructura de la institución para mantener la infraestructura funcionando hasta tomar las decisiones pertinentes;

f) Asegurarse de que el equipo que respalda a los servicios públicos esté conectado a internet, solo cuando sea necesario y solo de manera segura.

g) Proporcionar iluminación de emergencia y comunicaciones; los interruptores y válvulas de emergencia para cortar la energía, el agua, el gas u otros servicios públicos debe ubicarse cerca de las salidas de emergencia o las salas de equipos.

h) Los detalles de los contactos de emergencia deben registrarse y estar disponibles para el personal en caso de un apagón.

3.12. Seguridad del cableado

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencial #Disponibilidad	#Proteger	#Seguridad_física	#Protección

Control

Los cables que transportan energía, datos o servicios de información de soporte se deben proteger contra intercepciones, interferencias o daños.

Recomendaciones para la implementación:

Se deben considerar las siguientes directrices para la seguridad del cableado:

a) Las líneas eléctricas y de telecomunicaciones a las instalaciones de tratamiento de información sean subterráneas cuando sea posible, o estén sujetas a una protección alternativa adecuada, como protectores de cables de piso y postes de servicios públicos; si los cables son subterráneos, protegerlos de cortes accidentales con conductos blindados o señales de presencia:

b) Separar los cables de alimentación de los cables de comunicaciones para evitar interferencias;

c) Para sistemas sensibles o críticos, los controles adicionales a considerar incluyen:

1) instalación de conductos blindados y cuartos o cajas cerradas y alarmas en los puntos de inspección y terminación;

2) Uso de blindaje electromagnético para proteger los cables;

3) Barridos técnicos periódicos e inspecciones físicas para detectar dispositivos no autorizados conectados a los cables;

4) Acceso controlado a paneles de conexión y salas de cables (por ejemplo, con llaves mecánicas o PIN):

5) Uso de cables de fibra óptica;

d) Etiquetar los cables en cada extremo con suficientes detalles de origen y destino para permitir la identificación física y la inspección del cable.

e) Buscar el asesoramiento de especialistas sobre cómo gestionar los riesgos derivados de incidentes o mal funcionamiento del cableado.

3.13. Mantenimiento de equipo

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad

#Preventivo	#Confidencial #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión de activos	#Protección #Resiliencia

Control

Elaborar, implementar, socializar y evaluar el plan de mantenimiento de los equipos para asegurar la disponibilidad, integridad y confidencialidad de la información.

Recomendaciones para la implementación:

Se deben considerar las siguientes recomendaciones para el mantenimiento de los equipos:

a) Brindar Mantenimientos periódicos a los equipos y dispositivos de acuerdo a las especificaciones de servicio recomendadas por el proveedor;

b) Implementación y monitoreo de un programa de mantenimiento por parte de la institución;

c) Controlar que solo personal calificado este autorizado para realizar reparaciones y mantenimiento en el equipo;

d) Mantener registros de todas las fallas sospechadas o reales, y de todo mantenimiento preventivo y correctivo;

e) Implementar controles apropiados para realizar mantenimientos programados y emergentes, considerando el tratamiento de la información sensible, teniendo en cuenta si este mantenimiento es realizado por personal en el sitio o externo a la institución; someter al personal de mantenimiento a un adecuado acuerdo de confidencialidad;

f) Gestionar mantenimientos planificados con hora de inicio, fin, impacto y responsables y poner previamente en conocimiento de administradores y usuarios finales;

g) Supervisar al personal de mantenimiento al realizar el mantenimiento en el sitio;

h) Autorizar y controlar el acceso para el mantenimiento remoto;

i) Aplicar medidas de seguridad para los activos fuera de las instalaciones (ver 3.9) si el equipo que contiene información se retira de las instalaciones para su mantenimiento;

j) Cumplir con todos los requisitos de mantenimiento impuestos por el seguro;

k) Antes de volver a poner en funcionamiento el equipo después del mantenimiento, inspeccionarlo para asegurarse de que el equipo no haya sido manipulado y funcione correctamente;

l) Aplicar medidas para la eliminación segura o la reutilización del equipo (ver 3.14) si se determina que el equipo debe ser eliminado.

3.14. Eliminación segura o reutilización de equipos

Tipo de	Propiedades de	Conceptos de	Capacidades	Dominios de

Control	la SI	Ciberseguridad	operativas	seguridad
#Preventivo	#Confidencial	#Proteger	#Seguridad_física #Gestión de activos	#Protección

Control

Los elementos del equipo que contengan medios de almacenamiento se deben verificar para asegurar que todos los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

Recomendaciones para la implementación:

El equipo se debe verificar para asegurar si los medios de almacenamiento están contenidos o no antes de su eliminación o reutilización.

Los medios de almacenamiento que contengan información confidencial o con derechos de autor se deben destruir físicamente o la información se debe destruir, eliminar o sobrescribir utilizando técnicas para hacer que la información original no se pueda recuperar en lugar de utilizar la función de eliminación estándar. (Ver 3.10) para obtener orientación detallada sobre la eliminación segura de medios de almacenamiento y (4.10) para obtener orientación sobre la eliminación de información.

La institución debe considerar la eliminación de los controles de seguridad, como los controles de acceso o el equipo de vigilancia, al final del contrato de arrendamiento o al mudarse de las instalaciones. Esto depende de factores como:

a) Su contrato de arrendamiento para devolver la instalación a su condición original, de ser el caso;

b) Modificar el riesgo de dejar sistemas con información confidencial para el próximo usuario, por ejemplo, listas de acceso de usuarios, archivos de video o imagen;

c) La capacidad de reutilizar los controles en la siguiente instalación.

d) Las llaves de cifrado se mantienen confidenciales (por ejemplo, nunca se almacenan en el mismo disco).

4. Controles tecnológicos

4.1. Dispositivos de usuario final

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencial #Integridad #Disponibilidad	#Proteger	#Gestión de activos #Información_protección	#Protección

Control

Implementar y socializar una política para el manejo seguro de la información almacenada, en los dispositivos de usuario final.

Recomendaciones para la implementación:

Generalidades

La política específica del tema debe comunicarse a todo el personal pertinente y considerar lo siguiente:

a) El tipo de información y el nivel de clasificación que los dispositivos de punto final del usuario pueden manejar, procesar, almacenar o soportar;

b) Registro de dispositivos de punto final de usuario;

c) Registro de dispositivos móviles, debidamente autorizados

d) Requisitos de protección física;

e) Restricción de la instalación de software, por ejemplo, controlado de forma remota por los administradores del sistema;

f) Requisitos para el software del dispositivo de punto final del usuario (incluidas las versiones de software) y para aplicar actualizaciones, por ejemplo, actualización automática activa;

g) Reglas para la conexión a servicios de información, redes públicas o cualquier otra red fuera de las instalaciones, por ejemplo, que requiera el uso de un firewall personal;

h) Controles de acceso;

i) Cifrado del dispositivo de almacenamiento;

j) Protección contra malware;

k) Deshabilitación, borrado o bloqueo remoto;

l) Copias de seguridad;

m) Uso de servicios web y aplicaciones web;

n) Análisis del comportamiento del usuario final (ver 4.16);

o) El uso de dispositivos extraíbles, incluidos los dispositivos de memoria extraíbles, y la posibilidad de desactivar puertos físicos (por ejemplo, puertos usb);

p) La separación del uso de los dispositivos con fines privados respecto a los de la institución, incluyendo el uso de software de soporte para permitir dicha separación y proteger los datos de la institución en un dispositivo privado;

Responsabilidad del usuario

a) Cerrar sesiones activas y cancelar servicios cuando ya no se necesiten;

b) Proteger los dispositivos de punto final del usuario de uso no autorizado con un control físico (por ejemplo, bloqueo de teclas o bloqueos especiales) y un control lógico (por ejemplo, acceso con contraseña) cuando no estén en uso (Ej. No mayor a 10 minutos); no deje los dispositivos que llevan información de negocios importante, sensible o crítica desatendida;

c) Use dispositivos con especial cuidado en lugares públicos, oficinas abiertas, lugares de reunión y otras áreas no protegidas (por ejemplo, evite leer información confidencial si las personas pueden leer por detrás, use privacidad filtros de pantalla);

d) Proteger físicamente los dispositivos de punto final del usuario contra el robo (por ejemplo, en automóviles y otras formas de transporte, habitaciones de hotel, centros de conferencias y lugares de reunión).

e) Se debe establecer un procedimiento específico que tenga en cuenta los requisitos legales, estatutarios, reglamentarios, contractuales incluidos los seguros y otros requisitos de seguridad de la institución para los casos de robo o pérdida de dispositivos de punto final del usuario.

Uso De Dispositivos Personales

a) Separación del uso personal y de negocio de los dispositivos, incluido el uso de software para respaldar dicha separación y proteger los datos de negocios en un dispositivo privado;

b) Proporcionar acceso a la información de negocio solo después de que los usuarios hayan reconocido sus deberes (protección física, actualización de software, etc.), renunciar a la propiedad de los datos de la institución, permitir que la institución borre datos de forma remota en caso de robo o pérdida del dispositivo o cuando ya no está autorizado a utilizar el servicio. En tales casos, se debe considerar la norma legal de protección de datos personales e identificables PII;

c) Políticas y procedimientos de temas específicos para prevenir disputas concernientes con los derechos de propiedad intelectual desarrollados en equipos de propiedad privada;

d) Acceso a equipos de propiedad privada (para verificar la seguridad de la máquina o durante una investigación), que puede ser impedido por la normativa legal;

e) Acuerdos de licencia de software que la institución puede ser responsable en la autorización de licencias de software de cliente, en dispositivos de propiedad privada del personal o usuarios externos.

Conexiones inalámbricas

La institución debe establecer procedimientos para:

a) La configuración de conexiones inalámbricas en dispositivos (por ejemplo, deshabilitar protocolos vulnerables);

b) Usar conexiones inalámbricas o por cable con el ancho de banda adecuado de acuerdo con las políticas de temas específicos (por ejemplo, porque se necesitan copias de

seguridad o actualizaciones de software).

4.2. Derechos de acceso privilegiado

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencial #Integridad #Disponibilidad	#Proteger	#Gestión_de_identidad_y_acceso	#Protección

Control

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

Recomendaciones para la implementación:

La asignación de derechos de acceso privilegiado se debe controlar a través de un proceso de autorización de acuerdo con la política de temas específicos de control de accesos relevantes (ver 1.15). Se debe considerar lo siguiente:

a) Identificar a los usuarios que necesitan derechos de acceso privilegiado para cada sistema o proceso como sistemas operativos, sistemas de gestión de bases de datos y aplicaciones;

b) Mantener un registro documentado de identificación de los usuarios y sus privilegios especiales asociados con cada servicio o sistema operativo, sistema de gestión de base de datos, aplicaciones y otros;

c) Asignar derechos de acceso privilegiados a los usuarios según sea necesario y en función de cada caso, de acuerdo con la política específica de control de acceso (ver en 1.15), es decir, sólo a las personas con la competencia necesaria para llevar a cabo las actividades que requieren un acceso privilegiado y sobre la base de los requisitos mínimos para sus roles funcionales;

d) Mantener un proceso de autorización, es decir, determinar quién puede aprobar los derechos de acceso privilegiado o no, conceder derechos de acceso privilegiados hasta que se complete el proceso de autorización y un registro de todos los privilegios asignados;

e) Definir y aplicar los requisitos de caducidad de los derechos de acceso privilegiados

f) Tomar medidas para asegurar que los usuarios son conscientes de sus derechos de acceso privilegiado y de cuándo están en modo de acceso privilegiado. Las medidas posibles incluyen el uso de identidades de usuario específicas, la configuración de la interfaz de usuario o incluso equipos específicos;

g) Los requisitos de autenticación para los derechos de acceso privilegiado pueden ser mayores que los requisitos para los derechos de acceso normales. Puede ser necesaria una reautenticación o un paso de autenticación antes de realizar trabajos con derechos de acceso privilegiados;

h) Revisar periódicamente, y después de cualquier cambio organizativo, a los usuarios que

trabajen con derechos de acceso privilegiados para verificar si sus funciones, roles, responsabilidades y competencias siguen calificando para trabajar con derechos de acceso privilegiados (ver 1.18):

i) Establecer reglas específicas para evitar el uso de identificadores de administración genéricos (como "root"), en función de las capacidades de configuración de los sistemas. Gestionar y proteger la autenticación de dichas identidades (ver 1.17);

j) Conceder acceso privilegiado temporal sólo durante el tiempo necesario para implementar los cambios o actividades aprobadas cambios o actividades aprobadas (por ejemplo, para actividades de mantenimiento o algunos cambios críticos), en lugar de conceder permanentemente derechos de acceso privilegiados;

k) Registrar todos los accesos privilegiados a los sistemas con fines de auditoría;

l) No compartir o vincular identidades con derechos de acceso privilegiado a múltiples personas, asignadas a cada uno (no compartir o vincular identidades con derechos de acceso privilegiados a múltiples personas, asignando a cada persona una identidad separada que permita asignar derechos de acceso privilegiados específicos. Las identidades pueden agruparse (por ejemplo, definiendo un grupo de administradores) para simplificar la gestión de derechos de acceso privilegiados;

l) Utilizar únicamente las credenciales con derechos de acceso privilegiados para realizar tareas administrativas y no para las tareas generales del día a día, es decir, consultar el correo electrónico, acceder a la web (los usuarios deberían tener una identidad de red normal separada para estas actividades).

Los derechos de acceso privilegiado son derechos de acceso proporcionados a una identidad, un rol o un proceso que permite realizar actividades que los usuarios o procesos típicos no pueden realizar. Los roles de administrador del sistema generalmente requieren derechos de acceso privilegiado.

4.3. Restricción de acceso a la información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencial #Integridad #Disponibilidad	#Proteger	#Gestión_de_identidad_y_acceso	#Protección

Control

El acceso a la información y otros activos asociados debe estar restringido de acuerdo con la política de temas específicos establecida sobre control de acceso.

Recomendaciones para la implementación:

El acceso a la información y otros activos asociados debe estar restringido de acuerdo con las políticas de temas específicos establecidas. Se debe considerar lo siguiente para respaldar los requisitos de restricción de acceso:

a) No permitir el acceso a información sensible por parte de usuarios con identidades desconocidas o de forma anónima. El acceso público o anónimo solo se debe otorgar a ubicaciones de almacenamiento que no contengan información confidencial;

b) Proporcionar mecanismos de configuración para controlar el acceso a la información en sistemas, aplicaciones y servicios;

c) Controlar a qué datos puede acceder un usuario en particular, determinar sus perfiles;

d) controlar qué identidades o grupo de identidades tienen acceso, como lectura, escritura, eliminación y ejecución;

e) Proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, datos de aplicaciones o sistemas.

Además, se deben considerar técnicas y procesos de gestión de acceso dinámico para proteger información confidencial que tiene un gran valor para la institución cuando la institución:

a) Necesita un control granular sobre quién puede acceder a dicha información durante qué período y de qué manera;

b) Quiere compartir dicha información con personas ajenas a la institución y mantener el control sobre quién puede acceder a ella;

c) Quiere gestionar dinámicamente, en tiempo real, el uso y distribución de dicha información;

d) Quiere proteger dicha información contra cambios no autorizados, copia y distribución (incluida la impresión);

e) Quiere monitorear el uso de la información;

f) Desea registrar cualquier cambio en dicha información que tenga lugar en caso de que se requiera una investigación futura.

Las técnicas de gestión de acceso dinámico deben proteger la información a lo largo de su ciclo de vida (es decir, creación, tratamiento, almacenamiento, transmisión y eliminación), incluyendo:

a) Establecer reglas sobre la gestión del acceso dinámico en función de casos de uso específicos considerando:

   1) Otorgar permisos de acceso en función de la identidad, el dispositivo, la ubicación o la aplicación;

   2) Aprovechar el esquema de clasificación para determinar qué información debe protegerse con técnicas de gestión de acceso dinámico;

b) Establecer procesos operativos, de seguimiento y de presentación de informes e infraestructura técnica de soporte.

Los sistemas de gestión de acceso dinámico deben proteger la información mediante:

a) Exigir autenticación, credenciales apropiadas o un certificado para acceder a la información:

b) Restringir el acceso, por ejemplo, a un período de tiempo específico (por ejemplo, después de una fecha determinada o hasta una fecha determinada);

c) Usar cifrado para proteger la información;

d) Definir los permisos de impresión de la información;

e) Registrar quién accede a la información y cómo se utiliza la información;

f) Generar alertas si se detectan intentos de mal uso de la información.

Las técnicas de gestión de acceso dinámico y otras tecnologías de protección de información dinámica pueden respaldar la protección de la información incluso cuando los datos se comparten más allá de la institución de origen, donde no se pueden aplicar los controles de acceso tradicionales. Se puede aplicar a documentos, correos electrónicos u otros archivos que contengan información para limitar quién puede acceder al contenido y de qué manera. Puede ser a nivel granular y adaptarse a lo largo del ciclo de vida de la información.

4.4. Acceso al código fuente

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencial #Integridad #Disponibilidad	#Proteger	#Gestión_de_identidad_y_acceso #Seguridad_de_aplicaciones #Configuración_segura	#Protección

Control

Restringir el acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software a los usuarios autorizados, debe administrarse adecuadamente, de acuerdo a las políticas establecidas por la institución.

Recomendaciones para la implementación:

El acceso al código fuente y elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) y herramientas de desarrollo (por ejemplo, compiladores, constructores, herramientas de integración, plataformas y entornos de prueba) se debe controlar estrictamente.

Para el código fuente, esto se puede lograr controlando el almacenamiento central de dicho código, preferiblemente en el sistema de gestión de código fuente.

El acceso de lectura y el acceso de escritura al código fuente pueden diferir según la función del personal. Por ejemplo, el acceso de lectura al código fuente puede proporcionarse

ampliamente dentro de la institución, pero el acceso de escritura al código fuente solo está disponible para personal privilegiado o propietarios designados. Cuando los componentes del código son utilizados por varios desarrolladores dentro de una institución.

a) Se debe implementar el acceso de lectura a un repositorio de código centralizado. Además, si dentro de una institución se utiliza código fuente abierto a componentes de código de terceras partes, el acceso de lectura a dichos repositorios de código externos puede proporcionarse ampliamente. Sin embargo, el acceso aún debería estar restringido.

b) Asignar a un administrador del código fuente de programas, software, quien tendrá en custodia los mismos y deberá considerar las siguientes recomendaciones para controlar el acceso a las bibliotecas de programas fuente, a fin de reducir la posibilidad de alterar los programas informáticos:

1) Administrar el acceso al código fuente del programa y las bibliotecas fuente del programa de acuerdo con los procedimientos establecidos;

2) Otorgar acceso de lectura y escritura al código fuente en función de las necesidades de negocio y administrado para abordar los riesgos de alteración o uso indebido y de acuerdo con los procedimientos establecidos;

3) Actualización del código fuente y elementos asociados y otorgamiento de acceso al código fuente de acuerdo con los procedimientos de control de cambios (ver 4.32) y solo realizarlo después de que se haya recibido la autorización correspondiente:

4) No otorgar a los desarrolladores acceso directo al repositorio del código fuente, sino a través de herramientas para desarrolladores que controlan las actividades y autorizaciones en el código fuente (administrador de versiones);

5) Mantener las listas de programas en un entorno seguro, donde el acceso de lectura y escritura se debe administrar y asignar adecuadamente;

6) Mantener un registro de auditoría de todos los accesos y de todos los cambios en el código fuente;

7) Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos como respaldos de información;

8) Considerar controles adicionales para asegurar su integridad (por ejemplo, firma digital), si se pretende publicar el código fuente del programa.

4.5. Autenticación segura

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencial #Integridad #Disponibilidad	#Proteger	#Gestión_de_identidad_y_acceso	#Protección

Control

Establecer las tecnologías y los procedimientos de autenticación segura, se deben

implementar en función de las restricciones de acceso a la información y la política del tema específico sobre el control de acceso.

Recomendaciones para la implementación:

Se debe elegir una técnica de autenticación adecuada para corroborar la identidad reclamada de un usuario, software, mensajes y otras entidades.

La fuerza de la autenticación debe ser adecuada para la clasificación de la información a la que se accede. Cuando se requiera una fuerte autenticación y verificación de identidad, los métodos de autenticación se deben utilizar alternativas a las contraseñas, como certificados digitales, tarjetas inteligentes, tokens o medios biométricos.

La información de autenticación debe ir acompañada de factores de autenticación adicionales para acceder a los sistemas de información crítica también conocida como autenticación de múltiples factores. Usando una combinación de múltiples factores de autenticación, como lo que sabes, lo que tienes y lo que eres, reduce las posibilidades de accesos no autorizados.

La autenticación multifactor se puede combinar con otras técnicas para requerir factores adicionales en circunstancias específicas, en función de reglas y patrones predefinidos, como el acceso desde una ubicación inusual, desde un dispositivo inusual o en un momento inusual.

La información de autenticación biométrica debe invalidarse si alguna vez se ve comprometida. La autenticación biométrica puede no estar disponible según las condiciones de uso (por ejemplo, humedad o envejecimiento). Para prepararse para estos problemas, la autenticación biométrica debe ir acompañada de al menos una técnica de autenticación alternativa.

El procedimiento para iniciar sesión en un sistema o aplicación debe estar diseñado para minimizar el riesgo de acceso no autorizado. Los procedimientos y tecnologías de inicio de sesión deben implementarse teniendo en cuenta lo siguiente:

a) No mostrar información confidencial del sistema o de la aplicación hasta que el proceso de inicio de sesión se haya completado con éxito para evitar proporcionar asistencia innecesaria a un usuario no autorizado;

b) Exhibir un aviso general advirtiendo que el sistema o la aplicación o el servicio solo deben ser accedidos por usuarios autorizados;

c) no proporcionar mensajes de ayuda durante el procedimiento de inicio de sesión que ayudarían a un usuario no autorizado si surge una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecto;

d) Validar la información de inicio de sesión solo al completar todos los datos de entrada;

e) Protección contra intentos de inicio de sesión de fuerza bruta en nombres de usuario y contraseñas, usando la prueba de *Turing* pública completamente automatizada para diferenciar a las computadoras de los humanos (CAPTCHA), requiriendo restablecer

contraseña después de un número predefinido de intentos fallidos o bloquear al usuario después de un número máximo de errores:

f) Registro de intentos fallidos y exitosos;

g) Generar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de inicio de sesión, enviar una alerta al usuario y a los administradores del sistema de la institución cuando se ha alcanzado el número de intentos de contraseña incorrectos;

h) Mostrar o enviar la siguiente información en un canal separado al completar un inicio de sesión exitoso:

1) Fecha y hora del inicio de sesión exitoso anterior;

2) Detalles de cualquier intento fallido de inicio de sesión desde el último inicio de sesión exitoso;

i) No mostrar una contraseña en texto claro cuando se ingresa; en algunos casos, puede ser necesario desactivar esta funcionalidad para facilitar el inicio de sesión del usuario por razones de accesibilidad o para evitar el bloqueo de usuarios debido a errores repetidos;
j) No transmitir contraseñas en texto claro a través de una red para evitar ser capturado por un programa "sniffer" de la red;

k) Finalizar sesiones inactivas después de un periodo definido de inactividad, especialmente en ubicaciones de alto riesgo (ejemplo 10 minutos), como áreas públicas o externas fuera de la gestión de seguridad de la institución o en los dispositivos de punto final del usuario;

l) Restringir los tiempos de duración de la conexión para proporcionar seguridad adicional para aplicaciones de alto riesgo y reducir la ventana de oportunidad para el acceso no autorizado.

4.6. Gestión de la capacidad

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo	#Integridad #Disponibilidad	#Identificar #Proteger #Detectar	#Continuidad	#Gobernanza_y_ecosistema #Protección

Control

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

Recomendaciones para la implementación:

Se debe identificar los requisitos de capacidad para las instalaciones de tratamiento de información, recursos humanos, oficinas y otras instalaciones, teniendo en cuenta la

importancia de negocios de los sistemas y procesos en cuestión, considerar lo siguiente:

a) Se debe aplicar el ajuste y el monitoreo del sistema para asegurar y, cuando sea necesario, mejorar la disponibilidad y la eficiencia de los sistemas.

b) La institución debe realizar pruebas de estrés stress-tests de los sistemas y servicios para confirmar que hay suficiente capacidad del sistema disponible para cumplir con los requisitos de rendimiento máximo.

c) Se debe establecer controles de detección para indicar los problemas a su debido tiempo, las proyecciones de los futuros requisitos de capacidad deben tener en cuenta los nuevos requisitos del negocio y del sistema y las tendencias actuales y proyectadas en las capacidades de tratamiento de información de la institución.

d) Se debe prestar especial atención a cualquier recurso con largos plazos de entrega o altos costos, por lo tanto, los gerentes, propietarios de servicios o productos deben monitorear la utilización de los recursos clave del sistema.

e) Las autoridades deben usar la información de capacidad para identificar y evitar posibles limitaciones de recursos y dependencia del personal clave que pueden representar una amenaza para la seguridad del sistema o los servicios y planificar la acción apropiada.

Se puede lograr proporcionar capacidad suficiente aumentando la capacidad o reduciendo la demanda. Se debe considerar lo siguiente para aumentar la capacidad:

a) Contratación de nuevo personal;

b) Obtención de nuevas instalaciones o espacio de disco;

c) Adquirir recursos necesarios, memoria y almacenamiento más potentes;

d) Hacer uso de la computación en la nube, que tiene características inherentes que abordan directamente cuestiones de capacidad. La computación en la nube tiene elasticidad y escalabilidad que permiten una rápida expansión y reducción bajo demanda de los recursos disponibles para aplicaciones y servicios particulares.

Se debe considerar lo siguiente para reducir la demanda de los recursos de la institución:

a) Eliminación de datos obsoletos (espacio en disco);

b) Eliminación de registros impresos que hayan cumplido su periodo de retención (liberar espacio en los estantes);

c) Desmantelamiento de aplicaciones, sistemas, bases de datos o entornos innecesarios;

d) Optimizar procesos por lotes y cronogramas;

e) Optimizar el código de la aplicación o las consultas de la base de datos:

f) Denegar o restringir el ancho de banda para servicios que consumen recursos si estos no

son críticos (por ejemplo, transmisión de video).

g) Considerar un plan de gestión de capacidad documentado para los sistemas de misión crítica.

4.7. Protección contra malware

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Sistema_y_seguridad_de_la_red Información_protección	#Defensa #Protección

Control

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

Recomendaciones para la implementación:

La protección contra el malware debe basarse en el software de detección y reparación de malware, la conciencia de seguridad de la información, el acceso adecuado al sistema y los controles de gestión de cambios.

El uso de software de detección y reparación de malware por sí solo no suele ser adecuado. Se debe considerar la siguiente orientación:

a) Elaborar Implementar y socializar una política formal, con reglas y controles que prevengan o detecten el uso de software no autorizado, por ejemplo, lista de aplicaciones permitidas; es decir, usar una lista que proporciona aplicaciones permitidas (ver 4.19 y 4.32):

b) Implementar controles que eviten o detecten el uso de sitios web maliciosos conocidos o sospechosos, por ejemplo, listas de bloqueo;

c) Reducir las vulnerabilidades que pueden ser explotadas por malware, por ejemplo, a través de la gestión técnica de vulnerabilidades (ver 4.8 y 4.19);

d) Llevar a cabo una validación automatizada periódica del software y el contenido de datos de los sistemas, especialmente para los sistemas que soportan procesos de negocios críticos; investigar la presencia de archivos no aprobados o rectificaciones no autorizadas:

e) Establecer medidas de protección contra los riesgos asociados con la obtención de archivos y software ya sea desde o a través de redes externas o en cualquier otro medio;

f) Instalar y actualizar regularmente software de detección y reparación de malware para escanear computadoras y medios de almacenamiento electrónico (antivirus). Realización de escaneos regulares que incluyen:

1) Escanear cualquier dato recibido a través de redes o mediante cualquier forma de medio de almacenamiento electrónico, en busca de malware antes de su uso;

2) Escanear archivos adjuntos y descargas de correo electrónico y mensajería

instantánea en busca de malware antes de su uso. Llevar a cabo este escaneo en diferentes lugares, por ejemplo, en servidores de correo electrónico, computadoras de escritorio y al ingresar a la red de la institución;

3) Escanear páginas web en busca de malware cuando se accede a ellas;

g) Determinar la ubicación y configuración de las herramientas de detección y reparación de malware en función de los resultados de la evaluación de riesgos y considerando:

1) Principios de defensa en profundidad donde serían más efectivos. Por ejemplo, esto puede conducir a detección de malware en una puerta de enlace de red (en varios protocolos de aplicación, como correo electrónico, transferencia de archivos y web), así como en dispositivos y servidores de punto final de usuario;

2) Las técnicas evasivas de los atacantes, por ejemplo, el uso de archivos cifrados para entregar malware o el uso de protocolos de cifrado para transmitir malware;

h) Tener cuidado de protegerse contra la introducción de malware durante los procedimientos de mantenimiento y emergencia, que pueden eludir los controles normales contra el malware,

i) Implementar un proceso para autorizar la desactivación temporal o permanente de algunas o todas las medidas contra el malware, incluidas las autoridades de aprobación de excepciones responsables de los activos, la justificación documentada y la fecha de revisión. Esto puede ser necesario cuando la protección contra malware provoca la interrupción de las operaciones normales;

j) Preparar planes de continuidad del negocio apropiados para recuperarse de ataques de malware, incluidas todas las copias de seguridad de datos y software necesarias incluidas las copias de seguridad en línea y fuera de línea y las medidas de recuperación (ver 4.13);

k) Aislar entornos donde puedan ocurrir consecuencias catastróficas;

l) Definir procedimientos y responsabilidades para tratar la protección contra malware en los sistemas, incluida la capacitación en su uso, informes y recuperación de ataques de malware,

m) Concientizar (ver 2.3) a todos los usuarios sobre cómo identificar y mitigar potencialmente la recepción, el envío o la instalación de correos electrónicos, archivos o programas infectados con malware, [la información recopilada en n) y o) puede usarse para asegurar que la concienciación y la formación se mantengan actualizadas];

n) Implementar procedimientos para recopilar regularmente información sobre un nuevo malware, como suscribirse a listas de correo o revisar sitios web relevantes:

o) Verificar que la información relacionada con el malware, como los boletines de advertencia, provenga de fuentes calificadas y acreditadas como sitios de Internet confiables o proveedores de software de detección de malware y que sea precisa e informativa.

4.8. Gestión de vulnerabilidades técnicas

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos #Información_protección	#Protección

Control

Realizar las actividades necesarias para obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la institución a tales vulnerabilidades y se debe tomar las medidas apropiadas.

Recomendaciones para la implementación:

Identificación de vulnerabilidades técnicas

La institución debe tener un inventario preciso de los activos (ver 1.9 a 1.14) como requisito previo para la gestión eficaz de la vulnerabilidad técnica.

El inventario debe incluir el proveedor de software, el nombre del software, los números de versión, el estado actual de implementación qué software está instalado en qué sistemas y la(s) persona(s) dentro de la institución responsables del software.

Para identificar vulnerabilidades técnicas, la institución debe considerar:

a) Definir y establecer los roles y responsabilidades asociados con la gestión técnica de vulnerabilidades, incluido el monitoreo de vulnerabilidades, la evaluación de riesgos de vulnerabilidades, la actualización, el seguimiento de activos y cualquier responsabilidad de coordinación requerida;

b) Para el software y otras tecnologías (basado en la lista de inventario de activos, ver 1.9), identificar los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas relevantes y mantener la concienciación sobre ellas. Actualizar la lista de recursos de información en función de los cambios en el inventario o cuando se encuentren otros recursos nuevos o útiles;

c) Exigir a los proveedores de sistemas de información (incluidos sus componentes) que aseguren la notificación, el manejo y la divulgación de vulnerabilidades, incluidos los requisitos de los contratos aplicables (ver 1.20);

d) Usar herramientas de escaneo de vulnerabilidades adecuadas para las tecnologías en uso para identificar vulnerabilidades y verificar si la reparación de vulnerabilidades fue exitosa;

e) Realizar pruebas de penetración planificadas, documentadas y repetibles o evaluaciones de vulnerabilidad por parte de personas competentes y autorizadas para respaldar la identificación de vulnerabilidades, tener precaución ya que tales actividades pueden comprometer la seguridad del sistema;

f) Rastrear el uso de bibliotecas de terceras partes y código fuente en busca de vulnerabilidades. Esto se debe incluir en la codificación segura (ver 4.28).

La institución debe desarrollar procedimientos y capacidades para:

a) Detectar la existencia de vulnerabilidades en sus productos y servicios incluyendo cualquier componente externo utilizado en estos;

b) Recibir informes de vulnerabilidad de fuentes internas o externas.

La institución debe proporcionar un punto de contacto público (OSI) como parte de una política del tema específico sobre la divulgación de vulnerabilidades para que los investigadores y otras personas puedan informar problemas. La institución debe establecer procedimientos de notificación de vulnerabilidades, formularios de notificación en línea y hacer uso de inteligencia de amenazas o foros de intercambio de información apropiados. La institución también debe compartir información con otras instituciones de la función ejecutiva u otras partes interesadas (Cert, Csirt entre otros).

Evaluación de vulnerabilidades técnicas

Para evaluar las vulnerabilidades técnicas identificadas, se debe considerar la siguiente guía:

a) Analizar y verificar los informes para determinar qué actividad de respuesta y remediación se necesita;

b) Una vez identificada una potencial vulnerabilidad técnica, identificar los riesgos asociados y las acciones a tomar, tales acciones pueden implicar la actualización de sistemas vulnerables o la aplicación de otros controles.

Tomar las medidas apropiadas para abordar las vulnerabilidades técnicas

Se debe implementar un proceso de administración de actualizaciones de software para asegurar que se instalen los parches aprobados y las actualizaciones de aplicaciones más actualizados para todo el software autorizado, si es necesario realizar cambios, se debe conservar el software original y aplicar los cambios a una copia designada, todos los cambios deben probarse y documentarse por completo, de modo que puedan volver a aplicarse, si es necesario, a futuras actualizaciones de software.

Si es necesario, las modificaciones deben ser probadas y validadas por un organismo de evaluación independiente.

Se debe considerar la siguiente orientación para abordar las vulnerabilidades técnicas:

a) Tomar medidas apropiadas y oportunas en respuesta a la identificación de posibles vulnerabilidades técnicas; definir un cronograma para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes;

b) Según la urgencia con la que se deba abordar una vulnerabilidad técnica, realizando la acción de acuerdo con los controles relacionados con la gestión de cambios (ver 4.32) o

siguiendo los procedimientos de respuesta a incidentes de seguridad de la información (ver 1.26);

c) Utilizar únicamente actualizaciones de fuentes legítimas que pueden ser internas o externas a la institución;

d) Probar y evaluar las actualizaciones antes de instalarlas para asegurar que sean efectivas y que no produzcan efectos secundarios que no se puedan tolerar, es decir, si hay una actualización disponible, evaluar los riesgos asociados con la instalación de la actualización, los riesgos que plantea la vulnerabilidad deben compararse con el riesgo de instalar la actualización:

e) Abordar primero los sistemas de alto riesgo;

f) Desarrollar soluciones (por lo general, actualizaciones o parches de software):

g) Prueba para confirmar si la remediación o mitigación es efectiva;

h) Proporcionar mecanismos para verificar la autenticidad de la remediación:

i) Si no hay ninguna actualización disponible o no se puede instalar la actualización, considerar otros controles, tales como:

1) Aplicar cualquier solución alternativa sugerida por el proveedor de software u otras fuentes relevantes;

2) Apagar servicios o capacidades relacionadas con la vulnerabilidad;

3) Adaptar o agregar controles de acceso (por ejemplo, firewalls) en la frontera de la red (ver 4.20 a 4.22);

4) Proteger los sistemas, dispositivos o aplicaciones vulnerables de los ataques mediante la implementación de filtros de tráfico adecuados;

5) Aumentar el monitoreo para detectar ataques reales;

6) Concienciación sobre la vulnerabilidad.

Para el software adquirido, si los proveedores publican regularmente actualizaciones de seguridad para su software y se puede instalar dichas actualizaciones automáticamente, la institución debe decidir si usar la actualización automática o no.

Un proceso eficaz de gestión de vulnerabilidades técnicas debe estar alineado con las actividades de gestión de incidentes, para comunicar datos sobre vulnerabilidades a la función de respuesta a incidentes y proporcionar procedimientos técnicos que se llevarán a cabo en caso de que ocurra un incidente.

4.9. Gestión de la configuración

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad

#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración_ segura	#Protección

Control

Documentar, implementar, monitorear y revisar las configuraciones de seguridad de hardware, software, servicios y redes.

Recomendaciones para la implementación:

Generalidades

La institución debe definir e implementar procesos y herramientas para hacer cumplir las configuraciones definidas (incluidas las configuraciones de seguridad) para el hardware, el software, los servicios (por ejemplo, servicios en la nube) y las redes, tanto para los sistemas recién instalados como para los sistemas operativos durante su vida útil.

Deben existir roles, responsabilidades y procedimientos para asegurar un control satisfactorio de todos los cambios de configuración.

Plantillas normalizadas

Se deben definir plantillas normalizadas para la configuración segura de hardware, software, servicios y redes:

a) Usar orientación disponible públicamente (por ejemplo, plantillas predefinidas de proveedores y de organizaciones de seguridad);

b) Considerar el nivel de protección necesario para determinar un nivel suficiente de seguridad;

c) Respaldar la política de seguridad de la información de la institución, las políticas de temas específicos, las normalizaciones y otros requisitos de seguridad;

d) Considerar la viabilidad y aplicabilidad de las configuraciones de seguridad en el contexto de la institución.

e) Las plantillas se deben revisar periódicamente y actualizar cuando sea necesario abordar nuevas amenazas o vulnerabilidades, o cuando se introduzcan nuevas versiones de software o hardware

Se debe considerar lo siguiente para establecer plantillas normalizadas para la configuración segura de hardware, software, servicios y redes:

a) Minimizar el número de credenciales con derechos de acceso privilegiados o de nivel de administrador;

b) Deshabilitar credenciales innecesarias, no utilizadas o inseguras;

c) Deshabilitar o restringir funciones y servicios innecesarios;

d) Restringir el acceso a poderosos programas de utilidades y configuraciones de parámetros del host;

e) Sincronización de relojes;

f) Cambiar la información de autenticación predeterminada del proveedor, como las contraseñas predeterminadas, inmediatamente después de la instalación y revisar otros parámetros importantes relacionados con la seguridad predeterminada;

g) Invocar las instalaciones de tiempo de espera que cierran automáticamente la sesión de los dispositivos informáticos después de un periodo predeterminado de inactividad;

h) Verificar que se hayan cumplido los requisitos de la licencia (ver 1.32).

Administrar configuraciones

a) Las configuraciones establecidas de hardware, software, servicios y redes se deben registrar y debe mantener un registro de todos los cambios de configuración.

b) Los registros se deben almacenar de forma segura. Esto se puede lograr de varias maneras, como bases de datos de configuración o plantillas de configuración.

c) Los cambios en las configuraciones deben seguir el proceso de gestión de cambios (ver 4.32).

Los registros de configuración pueden contener según corresponda:

a) Información actualizada del propietario o punto de contacto del activo:

b) Fecha del último cambio de configuración;

c) Versión de la plantilla de configuración;

d) Relación con configuraciones de otros activos.

Monitoreo de configuraciones

a)Las configuraciones se deben monitorear, un conjunto integral de herramientas de gestión del sistema (por ejemplo, utilidades de mantenimiento, soporte remoto, herramientas de gestión del negocio, software de copia de seguridad y restauración).

b)Revisar las configuraciones periódicamente para verificar los ajustes de configuración, evaluar la fortaleza de las contraseñas y evaluar las actividades realizadas.

c)Las configuraciones reales se pueden comparar con las plantillas de destino definidas. Cualquier desviación se debe abordar, ya sea mediante la aplicación automática de la configuración objetivo-definida o mediante el análisis manual de la desviación seguido de acciones correctivas.

d)La documentación de los sistemas a menudo registra detalles sobre la configuración tanto del hardware como del software.

e)El endurecimiento del sistema es una parte típica de la gestión de la configuración.

f) La gestión de la configuración se puede integrar con los procesos de gestión de activos y las herramientas asociadas.

4.10. Eliminación de información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Información_protección #Legal_y_cumplimiento	#Protección

Control

La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento debe ser eliminada cuando ya no sea necesaria.

Recomendaciones para la implementación:

General

La información sensible no se debe conservar más tiempo del necesario para reducir el riesgo de divulgación no deseada, de acuerdo a la norma legal vigente institucional.

Al eliminar información sobre sistemas, aplicaciones y servicios, se debe considerar lo siguiente:

a) Seleccionar un método de eliminación (por ejemplo, sobreescritura electrónica o borrado Criptográfico) de acuerdo con los requisitos del negocio y teniendo en cuenta las leyes y reglamentos relevantes;

b) Registrar los resultados de la eliminación como evidencia;

c) Al utilizar proveedores de servicios de eliminación de información, obtener evidencia de la eliminación de información de ellos.

d) Cuando terceras partes almacenen la información de la institución en su nombre, la institución debe considerar la inclusión de requisitos sobre la eliminación de información en los acuerdos con las terceras partes para hacerlo cumplir durante y después de la terminación de tales servicios.

Métodos de eliminación

De acuerdo con la política del tema específico de la institución sobre retención de datos y teniendo en cuenta la legislación y las reglamentaciones relevantes, la información sensible debe eliminarse cuando ya no se necesite:

a) Configurar sistemas para destruir de forma segura la información cuando ya no se necesite (por ejemplo, después de un período sujeto a la política del tema específico sobre retención de datos o por solicitud de acceso del sujeto):

b) Eliminar versiones obsoletas, copias y archivos temporales dondequiera que se encuentren;

c) Usar un software de eliminación seguro y aprobado para eliminar información de forma permanente para ayudar a asegurar que la información no se pueda recuperar mediante el uso de herramientas forenses o de recuperación especializadas;

d) Usar proveedores aprobados y certificados de servicios de eliminación segura;

e) Utilizar mecanismos de eliminación apropiados para el tipo de medio de almacenamiento que se va a eliminar unidades de disco duro desmagnetizadas y otros medios de almacenamiento magnético.

Cuando se utilizan servicios en la nube, la institución debe verificar si el método de eliminación proporcionado por el proveedor de servicios en la nube es aceptable y, de ser así, la institución debe usarlo o solicitar que el proveedor de servicios en la nube elimine la información. Estos procesos de eliminación se deben automatizar de acuerdo con las políticas del tema específico, cuando estén disponibles y sean aplicables. Dependiendo de la confidencialidad de la información eliminada, los registros pueden rastrear o verificar que estos procesos de eliminación hayan ocurrido.

Para evitar la exposición no intencional de información sensible cuando el equipo se devuelve a los proveedores, la información sensible se debe proteger eliminando los almacenamientos auxiliares unidades de disco duro y la memoria antes de que el equipo abandone las instalaciones de la institución.

Teniendo en cuenta que la eliminación segura de algunos dispositivos (por ejemplo, teléfonos inteligentes) solo se puede lograr mediante la destrucción o el uso de las funciones integradas en estos dispositivos (por ejemplo, "restaurar la configuración de fábrica"), la institución debe elegir el método apropiado de acuerdo con la clasificación de la información manejada por tales dispositivos.

Se deben aplicar las medidas de control descritas en 3.14 para destruir físicamente el dispositivo de almacenamiento y eliminar simultáneamente la información que contiene.

Un registro oficial de borrado de información es útil a la hora de analizar la causa de un posible evento de fuga de información.

4.11. Enmascaramiento de datos

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Información_ protección	#Protección

Control

Elaborar, implementar y socializar con las partes interesadas, una política de enmascaramiento de datos de acuerdo a la política específica de control de acceso y otros temas relacionados considerando los requisitos del negocio y la norma legal vigente.

Recomendaciones para la implementación:

Cuando la protección de datos confidenciales (por ejemplo, PII) sea una preocupación, la institución debe considerar ocultar dichos datos mediante el uso de técnicas como el enmascaramiento de datos, la seudonimización o la anonimización.

Las técnicas de seudonimización o anonimización pueden ocultar la PII, disfrazar la verdadera identidad de los titulares de la PII u otra información confidencial, y desconectar el vínculo entre la PII y la identidad del titular de la PII o el vínculo entre otra información confidencial.

Cuando se utilicen técnicas de seudonimización o anonimización, se debe verificar que los datos hayan sido adecuadamente seudonimizados o anonimizados.

La anonimización de datos debe considerar todos los elementos de la información sensible para que sea eficaz. A modo de ejemplo, si no se considera adecuadamente, se puede identificar a una persona incluso si se anonimizan los datos que pueden identificar directamente a esa persona, por la presencia de otros datos que permitan identificar indirectamente a la persona.

Las técnicas adicionales para el enmascaramiento de datos incluyen:

a) Encriptación (que requiere que los usuarios autorizados tengan una clave);

b) Anular o eliminar caracteres (evitando que los usuarios no autorizados vean los mensajes completos);

c) Números y fechas variables;

d) Sustitución (cambiar un valor por otro para ocultar datos sensibles);

e) Reemplazar valores con su hash

Se debe considerar lo siguiente al implementar técnicas de enmascaramiento de datos:

a) No otorgar a todos los usuarios acceso a todos los datos, por lo tanto, diseñar consultas y máscaras para mostrar solo los datos mínimos requeridos al usuario;

b) Hay casos en los que algunos datos no deben ser visibles para el usuario para algunos registros de un conjunto de datos; en este caso, diseñar e implementar un mecanismo para la ofuscación de datos (por ejemplo, si un paciente no quiere que el personal del hospital pueda ver todos sus registros, incluso en caso de emergencia, entonces el personal del hospital recibe datos parcialmente ofuscados y los datos solo pueden ser accedidos por personal con roles específicos si contienen información útil para un tratamiento adecuado);

c) Cuando los datos están ofuscados, dando al principal de PII la posibilidad de exigir que los usuarios no puedan ver si los datos están ofuscados (ofuscación de la ofuscación; esto se usa en los centros de salud, por ejemplo, si el paciente no quiere que el personal vea esa información confidencial, como embarazos o resultados de exámenes de sangre ha sido ofuscado);

d) Cualquier requisito legal o reglamentario (por ejemplo, exigir el enmascaramiento de la información de las tarjetas de pago durante el tratamiento o el almacenamiento).

Se debe tener en cuenta lo siguiente al utilizar el enmascaramiento de datos, la seudonimización o la anonimización:

a) Nivel de fuerza del enmascaramiento de datos, seudonimización o anonimización según el uso de los datos procesados;

b) Controles de acceso a los datos procesados;

c) Acuerdos o restricciones en el uso de los datos procesados;

d) Prohibir cotejar los datos procesados con otra información para identificar al principal de la PII;

e) Realizar un seguimiento del suministro y recepción de los datos tratados;

La anonimización altera irreversiblemente la PII de tal manera que el principal de la PII ya no se puede identificar directa o indirectamente:

a) La seudonimización reemplaza la información de identificación con un alias. El conocimiento del algoritmo (a veces denominado "información adicional") utilizado para realizar la seudonimización permite al menos alguna forma de identificación del principal de PII. Por lo tanto, dicha "información adicional" debe mantenerse separada y protegida.

b) Si bien la seudonimización es, por lo tanto, más débil que la anonimización, los conjuntos de datos seudonimizados pueden ser más útiles en la investigación estadística.

c) El enmascaramiento de datos es un conjunto de técnicas para ocultar, sustituir u ofuscar elementos de datos confidenciales. El enmascaramiento de datos puede ser estático (cuando los elementos de datos se enmascaran en la base de datos original), dinámico (usando automatización y reglas para proteger los datos en tiempo real) o sobre la marcha (con datos enmascarados en la memoria de una aplicación).

4.12. Prevención de fuga de datos

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos #Información_protección	#Protección

Control

Elaborar, implementar y socializar la política para la prevención de fuga de datos, las medidas deben aplicar a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.

Recomendaciones para la implementación:

La institución debería considerar lo siguiente para reducir el riesgo de fuga de datos:

a) Identificar y clasificar la información para protegerla contra fugas (por ejemplo, información personal, proyectos en gestión, contratación pública en proceso):

b) Monitorear los canales de fuga de datos (por ejemplo, correo electrónico, transferencias de archivos, dispositivos móviles y dispositivos portátiles de almacenamiento);

c) Actuar para evitar que se filtre información (por ejemplo, poner en cuarentena correos electrónicos que contengan información confidencial)

Las herramientas de prevención de fuga de datos se deben utilizar para:

a) Identificar y controlar la información confidencial en riesgo de divulgación no autorizada (por ejemplo, en datos no estructurados en el sistema de un usuario);

b) Detectar la divulgación de información confidencial (por ejemplo, cuando la información se carga en servicios en la nube de terceras partes no confiables o se envía por correo electrónico);

c) Bloquear las acciones de los usuarios o las transmisiones de la red que expongan información confidencial (por ejemplo, evitando que se copien las entradas de la base de datos en una hoja de cálculo).

La institución debe determinar si es necesario restringir la capacidad de un usuario para copiar y pegar o cargar datos en servicios, dispositivos y medios de almacenamiento fuera de la institución. Si ese es el caso, la institución debería implementar tecnología como herramientas de prevención de fuga de datos o la configuración de herramientas existentes que permitan a los usuarios ver y manipular datos almacenados de forma remota, pero evitar copiar y pegar fuera del control de la institución.

Si se requiere la exportación de datos, se debe permitir que el propietario de los datos apruebe la exportación y responsabilice a los usuarios por sus acciones.

La toma de capturas de pantalla o fotografías de la pantalla se debe abordar a través de los términos y condiciones de uso, capacitación y auditoria.

Cuando se realiza una copia de seguridad de los datos, se debe tener cuidado para asegurar que la información confidencial esté protegida mediante medidas como el cifrado, el control de acceso y la protección física de los medios de almacenamiento que contienen la copia de seguridad.

También se debería considerar la prevención de fuga de datos para protegerse las contra acciones de inteligencia de un adversario de obtener información confidencial o secreta

(geopolítica, humana, financiera, comercial, científica o cualquier otra) que puede ser de interés para el espionaje o puede ser crítica para la comunidad. Las acciones de prevención de fuga de datos deben estar orientadas a confundir las decisiones del adversario, por ejemplo, reemplazando información auténtica con información falsa, ya sea como una acción independiente o como respuesta a las acciones de inteligencia del adversario. Ejemplos de este tipo de acciones son la ingeniería social inversa o el uso de honeypots para atraer a los atacantes.

Las herramientas de prevención de fuga de datos están diseñadas para identificar datos, monitorear el uso y el movimiento de datos y tomar medidas para evitar la fuga de datos (por ejemplo, alertar a los usuarios sobre su comportamiento de riesgo y bloquear la transferencia de datos a dispositivos portátiles de almacenamiento).

La prevención de la fuga de datos involucra inherentemente el monitoreo de las comunicaciones del personal y las actividades en línea y, por extensión, los mensajes de terceros, lo que genera inquietudes legales que deben tenerse en cuenta antes de implementar las herramientas de prevención de la fuga de datos. Existe una variedad de norma legal relacionada con la privacidad, la protección de datos, el empleo, la interceptación de datos y las telecomunicaciones que es aplicable al monitoreo y tratamiento de datos en el contexto de la prevención de fugas de datos.

4.13. Copia de seguridad de la información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Correctivo	#Integridad #Disponibilidad	#Recuperar	#Continuidad	#Protección

Control

Elaborar, implementar y socializar la política de respaldos que incluyen la información, el software y los sistemas; se deben mantener y probarse regularmente para verificar su validez.

Recomendaciones para la implementación:

Se debe establecer una política sobre copias de seguridad para abordar los requisitos de seguridad de la información y retención de datos de la institución.

Se deben proporcionar instalaciones de respaldo adecuadas para asegurar que toda la información y el software esenciales se puedan recuperar después de un incidente, falla o pérdida de medios de almacenamiento.

Se deben desarrollar e implementar planes sobre cómo la institución respaldará la información, el software y los sistemas, para abordar la política del tema específico sobre respaldo.

Al diseñar un plan de respaldo, se deben tener en cuenta los siguientes elementos:

a) Los responsables del área de Tecnologías de la Información, Oficial de Seguridad de la Información junto con el propietario de la información, determinarán los procedimientos formales para el respaldo, resguardo y contención de la información

b) La producción de registros precisos y completos de las copias de seguridad y los procedimientos de restauración documentados:

c) Reflejar los requisitos de la institución (por ejemplo, el objetivo del punto de recuperación, ver 1.30), los requisitos de seguridad de la información involucrada y la criticidad de la información para la operación continua de la institución en la medida (por ejemplo, respaldo completo o diferencial) y frecuencia de las copias de seguridad;

d) Almacenar las copias de seguridad en una localización remota segura y protegida, a una distancia suficiente para escapar de cualquier daño de un desastre en el sitio principal;

e) Considerar los respaldos a medios de almacenamiento y en el mismo sitio si se tiene suficientes recursos, ya que, en caso de mantenimientos de los sistemas de información, es más rápida su recuperación.

f) Dar a la información de respaldo un nivel adecuado de protección física y ambiental (ver Capítulo 3 y 4.1) consistente con las normas aplicados en el sitio principal;

g) Probar regularmente los medios de respaldo para asegurar que se pueda confiar en ellos para uso de emergencia cuando sea necesario.

h) Probar la capacidad de restaurar datos respaldados en un sistema de prueba, sin sobrescribir los medios de almacenamiento originales en caso de que el proceso de respaldo o restauración falle y cause daños o pérdidas irreparables de datos;

i) Proteger las copias de seguridad mediante encriptación de acuerdo con los riesgos identificados (por ejemplo, en situaciones donde la confidencialidad es importante);

j) Asegurar de que se detecte la pérdida inadvertida de datos antes de realizar la copia de seguridad.

k) Monitorear la ejecución de las copias de seguridad y abordar las fallas de las copias de seguridad programadas para asegurar la integridad de las copias de seguridad de acuerdo con la política del tema específico sobre las copias de seguridad.

l) Probar regularmente las medidas de respaldo para sistemas y servicios individuales, para asegurar que cumplan con los objetivos de respuesta a incidentes y planes de continuidad del negocio (ver 1.30). Esto se debe combinar con una prueba de los procedimientos de restauración y comparar con el tiempo de restauración requerido por el plan de continuidad del negocio. En el caso de sistemas y servicios críticos, las medidas de respaldo deben cubrir toda la información del sistema, las aplicaciones y los datos necesarios para recuperar el sistema completo en caso de desastre.

m) Realizar copias de seguridad de la información, las aplicaciones y los sistemas de la institución en el entorno del servicio en la nube (cuando la institución utiliza un servicio en la nube). La institución debe determinar si se cumplen los requisitos de copia de seguridad y se cumplen cuando se utiliza el servicio de copia de seguridad de la información proporcionado como parte del servicio en la nube.

n) Determinar el periodo de retención de la información del negocio esencial, teniendo en cuenta cualquier requisito para la retención de copias de archivo. La institución debe

considerar la eliminación de la información (ver 4.10) en los medios de almacenamiento utilizados para la de seguridad una vez que expire el período de retención de la información y debe tener en cuenta la norma legal vigente.

4.14. Redundancia de las instalaciones de tratamiento de información

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Correctivo	#Disponibilidad	#Proteger	#Continuidad #Gestión_de_activos	#Protección #Resiliencia

Control

La institución debe implementar la redundancia necesaria en las instalaciones de procesamiento de información, de acuerdo a los requisitos de disponibilidad.

Recomendaciones para la implementación:

La institución debe identificar los requisitos para la disponibilidad de los servicios de negocio y los sistemas de información; la institución debe diseñar e implementar una arquitectura de sistemas con la redundancia adecuada para cumplir con estos requisitos.

La organización debe considerar lo siguiente al implementar sistemas redundantes:

a) Contratar con dos o más proveedores de redes e instalaciones críticas de tratamiento de información, como proveedores de servicios de Internet;

b) Usar redes redundantes;

c) Utilizar dos centros de datos separados geográficamente con sistemas duplicados;

d) Utilizar suministros o fuentes de alimentación físicamente redundantes;

e) Uso de múltiples instancias paralelas de componentes de software, con equilibrio de carga automática entre ellas (entre instancias en el mismo centro de datos o en diferentes centros de datos);

f) Tener componentes duplicados en los sistemas (por ejemplo, CPU, discos duros, memorias) o en redes (por ejemplo, cortafuegos, enrutadores, conmutadores).

g) Cuando corresponda, preferiblemente en modo de producción, los sistemas de información redundantes se deben probar para asegurar que la conmutación por error de un componente a otro funcione como se espera.

4.15. Registro de eventos

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Detectivo	#Confidencialidad	#Detectar	#Gestión_de_evento	#Protección

	#Integridad #Disponibilidad		s_de_la_seguridad_ de_la_información	#Defensa

Control

Implementar el procedimiento para generar, almacenar, proteger y analizar periódicamente los registros de las actividades de los usuarios, excepciones, fallas y eventos de seguridad de la información.

Recomendaciones para la implementación:

Generalidades

La institución debe determinar el propósito para el cual se crean los registros, qué datos se recopilan y registran y cualquier requisito específico del registro para proteger y manejar los datos de registro.

Los registros de eventos deben incluir para cada evento, según corresponda:

a) Identificaciones de usuario;

b) Actividades del sistema:

c) Fechas, horas y detalles de eventos relevantes (por ejemplo, inicio y cierre de sesión);

d) Identidad del dispositivo, identificador del sistema y ubicación;

e) Direcciones de red y protocolos.

Los siguientes eventos deben ser considerados para el registro:

a) Intentos de acceso al sistema exitoso y rechazado;

b) Datos exitosos y rechazados y otros intentos de acceso a recursos;

c) Cambios en la configuración del sistema;

d) Uso de privilegios;

e) Uso de programas de servicios y aplicaciones;

f) Los archivos a los que se accede y el tipo de acceso, incluida la eliminación de archivos de datos importantes;

g) Alarmas emitidas por el sistema de control de acceso;

h) Activación y desactivación de sistemas de seguridad, como sistemas antivirus y sistemas de detección de intrusos;

i) Creación, modificación o supresión de credenciales de acceso:

j) Transacciones ejecutadas por los usuarios en las aplicaciones. En algunos casos, las

aplicaciones son un servicio o producto proporcionado o ejecutado por una tercera parte.

Es importante que todos los sistemas tengan fuentes de tiempo sincronizadas (ver 4.17), ya que esto permite la correlación de registros entre sistemas para el análisis, alerta e investigación de un incidente.

Protección de registros

a) Los usuarios, incluidos aquellos con derechos de acceso privilegiados, no deben tener permiso para eliminar o desactivar registros de sus propias actividades.

b) Potencialmente pueden manipular los registros en las instalaciones de tratamiento de la información bajo su control directo, por lo tanto, es necesario proteger y revisar los registros para mantener la responsabilidad de los usuarios privilegiados, mantener un adecuado registro de auditoría.

c) Registrar, proteger y revisar regularmente de acuerdo a las necesidades de la institución; las actividades del administrador y del operador del sistema, se debe incluir al registro:

- La hora en la que ocurrió el evento.
- La información sobre el evento.
- La cuenta de administrador y operador que estuvo involucrado.
- Los procesos que estuvieron implicados

Los controles deben tener como objetivo proteger contra cambios no autorizados en la información de registro y problemas operativos con la instalación de registro de auditoría, incluidos:

a) Alteraciones en los tipos de mensajes que se registran;

b) Archivos de registro que se están editando o eliminando;

c) Falla en el registro de eventos o sobre escritura de eventos pasados registrados si se excede el medio de almacenamiento que contiene un archivo de registro.

Para la protección de los registros, se debe considerar el uso de las siguientes técnicas: hashing criptográfico, registro en un archivo de solo lectura y solo para agregar, registro en un archivo de transparencia pública.

Es posible que se requiera archivar algunos registros de auditoría debido a los requisitos sobre la retención de datos o los requisitos para recopilar y retener evidencia (ver 1.28).

Los registros de eventos pueden contener datos confidenciales e información de identificación personal. Se debe tomar las medidas apropiadas de protección de la privacidad (ver 1.34).

Análisis de registro

a) El análisis de registros debe cubrir el análisis y la interpretación de los eventos de seguridad de la información, para ayudar a identificar actividades inusuales o comportamientos anómalos, que pueden representar indicadores de compromiso.

b) Considerar las habilidades necesarias para los expertos que realizan el análisis;

c)Determinar el procedimiento de análisis de registros;

d) Los atributos requeridos de cada evento relacionado con la seguridad;

e) Excepciones identificadas mediante el uso de reglas predeterminadas [por ejemplo, información de seguridad y gestión de eventos (SIEM) o reglas de cortafuegos, y sistemas de detección de intrusos (IDS) o firmas de malware];

f) Patrones de comportamientos conocidos y tráfico de red en comparación con actividad y comportamiento anómalos [análisis de comportamiento de usuarios y entidades (UEBA)];

g) Resultados del análisis de tendencias o patrones (por ejemplo, como resultado del uso de análisis de datos, técnicas de big data y herramientas de análisis especializadas);

h) Inteligencia de amenazas disponible.

El análisis de registros debe estar respaldado por actividades de monitoreo específicas para ayudar a identificar y analizar el comportamiento anómalo, que incluye:

a) Revisar los intentos exitosos y fallidos de acceder a los recursos protegidos (por servidores de sistemas de nombres de dominio (DNS), portales web y recursos compartidos de archivos;

b) Verificar los registros de DNS para identificar conexiones de red salientes a servidores maliciosos, como los asociados con servidores de comando y control de botnet,

c) Examinar los informes de uso de los proveedores de servicios (por ejemplo, facturas o informes de servicios) en busca de actividad inusual dentro de los sistemas y redes (por ejemplo, mediante la revisión de patrones de actividad);

d) Incluir registros de eventos de monitoreo físico, como entrada y salida, para asegurar una detección y un análisis de incidentes más precisos;

e) Correlación de registros para permitir un análisis eficiente y altamente preciso.

Los incidentes de seguridad de la información presuntos y reales deben identificarse (por ejemplo, infección de malware o sondeo de cortafuegos) y estar sujetos a una mayor investigación (por ejemplo, como parte de un proceso de gestión de incidentes de seguridad de la información, ver 1.25).

4.16. Actividades de monitoreo

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión_de_eventos_de_la_seguridad_de_la_información	#Defensa

Control

Las redes, los sistemas y las aplicaciones se deben monitorear para detectar comportamientos anómalos y se debe tomar las medidas apropiadas para evaluar posibles incidentes de seguridad de la información.

Recomendaciones para la implementación:

El alcance y el nivel de monitoreo se debe determinar de acuerdo con los requisitos de seguridad de la información y del negocio y teniendo en cuenta las leyes y reglamentos pertinentes, los registros de seguimiento se deben mantener durante periodos de retención definidos, de acuerdo a la norma legal vigente.

Lo siguiente debe ser considerado para su inclusión dentro del sistema de monitoreo:

a) Considerar el tráfico de red, sistema y aplicación entrante y saliente;

b) Acceso a sistemas, servidores, equipos de red, sistema de monitoreo, aplicaciones críticas, etc.;

c) Archivos de configuración de red y sistema de nivel crítico o administrativo;

d) Registros de herramientas de seguridad, por ejemplo, antivirus, ids, sistema de prevención de intrusos (ips), filtros web, firewalls, prevención de fuga de datos;

e) Registros de eventos relacionados con la actividad del sistema y de la red:

f) Comprobar que el código que se está ejecutando está autorizado para ejecutarse en el sistema y que no ha sido manipulado (por ejemplo, mediante una recopilación para agregar código adicional no deseado):

g) Uso de los recursos (por ejemplo, CPU, discos duros, memoria, ancho de banda) y su desempeño.

La institución debe establecer una línea de base de comportamiento normal y monitorear contra esta línea de base para detectar anomalías. Al establecer una línea de base, se debe considerar lo siguiente:

a) Revisar la utilización de los sistemas en periodos normales y pico;

b) Hora habitual de acceso, lugar de acceso, frecuencia de acceso para cada usuario o grupo de usuarios

El sistema de monitoreo se debe configurar contra la línea de base establecida para identificar comportamientos anómalos, tales como:

a) terminación no planificada de procesos o aplicaciones;

b) actividad típicamente asociada con malware o tráfico que se origina en direcciones IP o dominios de red maliciosos conocidos, por ejemplo, aquellos asociados con servidores de comando y control de botnet,

c) Características de ataque conocidos, por ejemplo, denegación de servicio y desbordamiento de buffer,

d) Comportamiento inusual del sistema, por ejemplo, registro de pulsaciones de teclas, inyección de procesos y desviaciones en el uso de protocolos normalizados;

e) Cuellos de botella y sobrecargas, por ejemplo, colas de la red, niveles de latencia y fluctuaciones de la red;

f) Acceso no autorizado (real o intentado) a sistemas o información;

g) Escaneo no autorizado de aplicaciones de negocios, sistemas y redes;

h) Intentos exitosos y fallidos de acceder a recursos protegidos, por ejemplo, servidores DNS, portales web y sistemas de archivos;

i) comportamiento inusual del usuario y del sistema en relación con el comportamiento esperado.

Se debe utilizar un monitoreo continuo a través de una herramienta de monitoreo, el monitoreo se debe hacer en tiempo real o en intervalos periódicos, sujeto a las necesidades y capacidades de la institución, las herramientas de monitoreo deben incluir la capacidad de manejar grandes cantidades de datos, adaptarse a un panorama de amenazas en constante cambio y permitir la notificación en tiempo real. Las herramientas también deben poder reconocer firmas y datos específicos o patrones de comportamiento de la red o la aplicación.

El software de monitoreo automatizado se debe configurar para generar alertas (por ejemplo, a través de consolas de administración, mensajes de correo electrónico o sistemas de mensajería instantánea) en función de umbrales predefinidos.

El sistema de alerta se debe ajustar y capacitar en la línea de base de la institución para minimizar los falsos positivos.

El personal debe estar dedicado a responder a las alertas y debe estar debidamente capacitado para interpretar con precisión los posibles incidentes, debe haber sistemas y procesos redundantes para recibir y responder a las notificaciones de alerta.

Los eventos anormales deben comunicarse a las partes relevantes para mejorar las siguientes actividades: auditoría, evaluación de seguridad, exploración y monitoreo de vulnerabilidades (ver 1.25).

Deben existir procedimientos para responder a los indicadores positivos del sistema de monitoreo de manera oportuna, a fin de minimizar el efecto de los eventos adversos (ver 1.26) en la seguridad de la información.

También se deben establecer procedimientos para identificar y abordar los falsos positivos, incluido el ajuste del software de monitoreo para reducir la cantidad de falsos positivos en el futuro.

El monitoreo de la seguridad se puede mejorar mediante:

a) Aprovechar los sistemas de inteligencia de amenazas (ver 1.7);

b) Aprovechar las capacidades de aprendizaje automático e inteligencia artificial;

c) Usar listas de bloqueo o listas de permitidos;

d) Realizar una serie de evaluaciones técnicas de seguridad (por ejemplo, evaluaciones de vulnerabilidad, pruebas de penetración, simulaciones de ataques cibernéticos y ejercicios de respuesta cibernética) y utilizar los resultados de estas evaluaciones para ayudar a determinar las líneas de base o el comportamiento aceptable;

e) Utilizar sistemas de seguimiento del desempeño para ayudar a establecer y detectar comportamientos anómalos;

f) Aprovechamiento de registros en combinación con sistemas de seguimiento.

Las actividades de monitoreo a menudo se realizan utilizando software especializado, como los sistemas de detección de intrusos. Estos se pueden configurar a una línea base de actividades normales, aceptables y esperadas del sistema y de la red.

4.17. Sincronización del reloj

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Detectivo	#Integridad	#Proteger #Detectar	#Gestión_de_eventos_de_la_seguridad_de_la_información	#Protección #Defensa

Control

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

Recomendaciones para la implementación:

Se debe considerar las recomendaciones siguientes:

a) Los requisitos externos e internos para la representación del tiempo, la sincronización confiable y la precisión deben documentarse e implementarse.

b) Se Debe utilizar protocolos como el protocolo de tiempo de red (NTP) o el protocolo de tiempo de precisión (PTP) para mantener todos los sistemas en red sincronizados con un reloj de referencia.

c) La institución puede usar dos fuentes de tiempo externas al mismo tiempo para mejorar la confiabilidad de los relojes externos y administrar adecuadamente cualquier variación.

d) La sincronización del reloj puede ser difícil cuando se usan múltiples servicios en la

nube o cuando se usan tantos servicios en la nube como locales. En este caso, se debe monitorear el reloj de cada servicio y registrar la diferencia para mitigar los riesgos derivados de las diferencias.

e) Verificar y corregir cualquier variación significativa de los relojes sobre todo en sistemas de procesamiento donde el tiempo es un factor clave.

f) Garantizar que la marca de tiempo refleja la fecha/hora real considerando especificaciones locales (por ejemplo, el horario de Galápagos o de países en donde existen representaciones diplomáticas del país, turistas extranjeros, entre otros).

g) Garantizar la configuración correcta de los relojes para la exactitud de los registros de auditoría o control de transacciones y evitar repudio de las mismas debido a aspectos del tiempo.

h) La configuración correcta de los relojes de las computadoras es importante para garantizar la precisión de los registros de eventos, que pueden ser necesarios para investigaciones o como evidencia en casos legales y disciplinarios.

4.18. Uso de programas de utilidad privilegiados

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Sistema_y_seguridad_de_la_red #Configuración_segura #Seguridd_de_aplicaciones	#Protección

Control

El uso de programas utilitarios que puedan anular los controles del sistema y de las aplicaciones se debe restringir y controlar estrictamente.

Recomendaciones para la implementación:

Se deben considerar las siguientes recomendaciones para el uso de programas de utilidad que pueden anular los controles del sistema y de la aplicación:

a) Limitación del uso de programas utilitarios al número mínimo práctico de usuarios autorizados de confianza (ver 4.2);

b) Uso de procedimientos de identificación, autenticación y autorización para programas utilitarios, incluida la identificación única de la persona que usa el programa utilitario;

c) Definición y documentación de niveles de autorización para programas utilitarios;

d) Autorización para uso adecuado de programas utilitarios;

e) No poner programas utilitarios a disposición de los usuarios que tienen acceso a aplicaciones en sistemas donde se requiere separación de funciones;

f) Eliminar o deshabilitar todos los programas utilitarios innecesarios;

g) Como mínimo, separación lógica de los programas utilitarios del software de aplicación. Cuando sea práctico, segregar las comunicaciones de red para tales programas del tráfico de aplicaciones:

h) Limitación de la disponibilidad de los programas utilitarios (por ejemplo, durante la duración de un cambio autorizado);

i) Registro de todos los usos de los programas utilitarios.

La mayoría de los sistemas de información tienen uno o más programas utilitarios que pueden anular los controles del sistema y de las aplicaciones, por ejemplo, diagnósticos, parches, antivirus, desfragmentadores de disco, depuradores, copias de seguridad y herramientas de red.

4.19. Instalación de software en sistemas operativos

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración_segura #Seguridad_de_aplicaciones	#Protección

Control

Implementar y documentar procedimientos para gestionar de forma segura la instalación de software en los sistemas operativos.

Recomendaciones para la implementación:

Se deben considerar las siguientes recomendaciones para administrar de forma segura los cambios y la instalación de software en los sistemas operativos:

a) Realizar actualizaciones del software operativo solo por parte de administradores capacitados con la autorización de gestión apropiada (ver 4.5);

b) Asegurar que solo se instale código ejecutable aprobado y ningún código de desarrollo o compiladores en los sistemas operativos;

c) Solo instalar y actualizar el software después de pruebas extensas y exitosas (ver 4.29 y 4.31);

d) Actualizar todas las bibliotecas fuente de programas correspondientes;

e) Usar un sistema de control de configuración para mantener el control de todo el software operativo, así como la documentación del sistema;

f) Definir una estrategia de reversión antes de que se implementen los cambios;

g) Mantener un registro de auditoría de todas las actualizaciones del software operativo;

h) Archivar versiones antiguas de software, junto con toda la información y parámetros requeridos, procedimientos, detalles de configuración y software de soporte como medida de contingencia, y durante el tiempo que se requiera que el software sea o procese datos archivados.

i) Cualquier decisión de actualizar a una nueva versión debe tener en cuenta los requisitos de negocios para el cambio y la seguridad de la versión, por ejemplo, la introducción de una nueva funcionalidad de seguridad de la información o el número y la gravedad de las vulnerabilidades de seguridad de la información que afectan a la versión actual.

j) Los parches de software se deben aplicar cuando pueden ayudar a eliminar o reducir las vulnerabilidades de seguridad de la información (ver 4.8 y 4.19).

k) El software informático puede basarse en software y paquetes suministrados externamente, por ejemplo, programas de software que utilizan módulos alojados en sitios externos, que se deben monitorear y controlar para evitar cambios no autorizados, ya que pueden introducir vulnerabilidades de seguridad de la información.

l) El software suministrado por el proveedor que se utiliza en los sistemas operativos se debe mantener en un nivel respaldado por el proveedor. Con el tiempo, los proveedores de software dejarán de admitir versiones anteriores de software.

m)La institución debe considerar los riesgos de depender de software sin soporte.

n) El software de código abierto utilizado en los sistemas operativos se debe mantener hasta la última versión adecuada del software. Con el tiempo, el código fuente abierto puede dejar de mantenerse, pero aún está disponible en un repositorio de software de código abierto.

o) La institución también debe considerar los riesgos de confiar en software de código abierto sin mantenimiento cuando se utiliza en sistemas operativos.

p) Cuando los proveedores estén involucrados en la instalación o actualización de software, el acceso físico o lógico solo debe otorgarse cuando sea necesario y con la debida autorización. Las actividades del proveedor deben ser monitoreadas (ver 1.22).

q) La institución debe definir y hacer cumplir reglas estrictas sobre qué tipos de software pueden instalar los usuarios.

r) El principio de privilegio mínimo se debe aplicar a la instalación de software en sistemas operativos.

s) La institución debe identificar qué tipos de instalaciones de software estén permitidas, por ejemplo, actualizaciones y parches de seguridad para el software existente y qué tipos de instalaciones están prohibidas, por ejemplo, software que es solo para uso personal y software cuya naturaleza con respecto a ser potencialmente malicioso es desconocida para sospechar.

t) Estos privilegios se deben otorgar en función de las funciones de los usuarios en cuestión.

4.20. Seguridad de redes

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Sistema_y_seguridad_de_la_red	#Protección

Control

Proteger, administrar y controlar las redes y los dispositivos de red, para proteger la información en los sistemas y aplicaciones institucionales.

Recomendaciones para la implementación:

Se deben implementar controles para asegurar la seguridad de la información en las redes y para proteger los servicios conectados del acceso no autorizado, en particular, se deben considerar los siguientes elementos:

a) El tipo y nivel de clasificación de la información que la red puede soportar;

b) Establecer responsabilidades y procedimientos para la gestión de equipos y dispositivos de red;

c) Mantener la documentación actualizada, incluidos los diagramas de red y los archivos de configuración de los dispositivos, por ejemplo, enrutadores, conmutadores;

d) Separar la responsabilidad operativa de las redes de las operaciones del sistema Tic cuando corresponda (ver 1.3);

e) Establecer controles para salvaguardar la confidencialidad e integridad de los datos que pasan por redes públicas, redes de terceras partes o redes inalámbricas y para proteger los sistemas y aplicaciones conectados (ver 1.22, 4.24, 1.14 y 2.6). También se pueden requerir controles adicionales para mantener la disponibilidad de los servicios de red y las computadoras conectadas a la red;

f) Registro y monitoreo adecuados para permitir el registro y la detección de acciones que pueden afectar o son relevantes para la seguridad de la información (ver 4.16 y 4.15);

g) Coordinar estrechamente las actividades de gestión de la red tanto para optimizar el servicio a la institución como para asegurar que los controles se apliquen de forma coherente en toda la infraestructura de tratamiento de la información;

h) Sistemas de autenticación en la red;

i) Restringir y filtrar la conexión de los sistemas a la red (por ejemplo, usando firewalls);

j) Detectar, restringir y autenticar la conexión de equipos y dispositivos a la red;

k) Endurecimiento de los dispositivos de red;

l) Segregar los canales de administración de red de otro tráfico de red:

m) Aislar temporalmente subredes críticas, si la red está bajo ataque;

n) Deshabilitar protocolos de red vulnerables.

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

4.21. Seguridad de los servicios de red

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Sistema_y_seguridad_de_la_red	#Protección

Control

Los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red se deben identificar, implementar y monitorear, independientemente de si estos servicios se entregan de manera interna o están externalizados. (SLA´s).

Recomendaciones para la implementación:

Las medidas de seguridad necesarias para servicios particulares, tales como características de seguridad, niveles de servicio y requisitos de servicio, deben ser identificadas e implementadas por proveedores de servicios de red internos o externos. La institución debe asegurarse de que los proveedores de servicios de red implementen estas medidas.

La Capacidad del proveedor de servicios de red para gestionar los servicios acordados de forma segura se debe determinar y controlar periódicamente, el derecho a la auditoria se debe acordar entre la institución y el proveedor. La institución también debe considerar las certificaciones de terceras partes proporcionadas por los proveedores de servicios para demostrar que mantienen las medidas de seguridad adecuadas.

Las reglas sobre el uso de redes y servicios de red deben formularse e implementarse para cubrir:

a) Las redes y los servicios de red a los que se permite acceder;

b) Requisitos de autenticación para acceder a diversos servicios de red;

c) Procedimientos de autorización para determinar quién puede acceder a qué redes y servicios en red;

d) Administración de redes y controles tecnológicos y procedimientos para proteger el acceso a conexiones de red y servicios de red;

e) Los medios utilizados para acceder a las redes y servicios de red, por ejemplo, uso de red privada virtual (VPN) o red inalámbrica;

f) Hora, ubicación y otros atributos del usuario al momento del acceso;

g) Seguimiento del uso de los servicios de red.

Se debe considerar las siguientes características de seguridad de los servicios de red:

a) Tecnología aplicada para la seguridad de los servicios de red, como autenticación, encriptación y controles de conexión a la red;

b) Parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las normas de seguridad y conexión a la red;

c) Almacenamiento en caché (por ejemplo, en una red de entrega de contenido) y sus parámetros que permiten a los usuarios elegir el uso del almacenamiento en caché de acuerdo con los requisitos de rendimiento, disponibilidad y confidencialidad;

d) procedimientos para el uso de servicios de red para restringir el acceso a servicios o aplicaciones de red, cuando sea necesario.

4.22. Separación en las redes

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Sistema_y_seguridad_de_la_red	#Protección

Control

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

Recomendaciones para la implementación:

Se deben considerar las siguientes recomendaciones para la implementación:

a) La institución debe considerar la gestión de la seguridad de las grandes redes dividiéndolas en dominios de red separados y separándolas de la red pública (es decir, Internet), documentar la división de red identificando las direcciones IP que se encuentran en cada segmento de red;

b) Los dominios se pueden elegir en función de los niveles de confianza, criticidad y sensibilidad, por ejemplo, dominio de acceso público, dominio de escritorio, dominio de servidor, sistemas de alto y bajo riesgo, junto con unidades organizativas, por ejemplo, recursos humanos, finanzas o alguna combinación, por ejemplo, dominio de servidor que se conecta a varias unidades organizativas;

c) La separación se puede realizar usando redes físicamente diferentes o usando diferentes redes lógicas (VLAN);

d) El perímetro de cada dominio debe estar bien definido;

e) Si se permite el acceso entre dominios de red, se debe controlar en el perímetro mediante una puerta de enlace, por ejemplo, un cortafuegos, un enrutador de filtrado de contenido, los criterios para la separación en las redes en dominios y el acceso permitido a través de las puertas de enlace se deben basar en una evaluación de los requisitos de seguridad de cada dominio;

f) La evaluación debe estar de acuerdo con la política del tema específico sobre control de acceso (ver 1.15), requisitos de acceso, valor y clasificación de la información procesada y tener en cuenta el costo relativo y el impacto en el rendimiento de incorporar tecnología de puerta de enlace adecuada;

g) Las redes inalámbricas requieren un tratamiento especial por su cobertura y la posibilidad de quedar al alcance de usuarios maliciosos;

h) Se debe considerar el ajuste de la cobertura de radio para la separación en las redes inalámbricas.;

i) Para entornos sensibles, se debe considerar tratar todos los accesos inalámbricos como conexiones externas y segregar este acceso de las redes internas hasta que el acceso haya pasado a través de una puerta de enlace de acuerdo con los controles de la red (ver 4.20) antes de otorgar acceso a los sistemas internos;

j) La red de acceso inalámbrico para invitados se debe separar de las del personal, si el personal solo usa dispositivos de punto final de usuario controlados que cumplen con las políticas de temas específicos de la institución.

k) El WIFI para invitados debe tener al menos las mismas restricciones que el WiFi para el personal, a fin de desalentar el uso del WiFi de invitados por parte del personal.

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

4.23. Filtrado web

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Sistema_y_seguridad_de_la_red	#Protección

Control

El acceso a sitios web externos se debe administrar para reducir la exposición a contenido malicioso, autorizado por la autoridad respectiva.

Recomendaciones para la implementación:

Antes de implementar este control, la institución debe establecer reglas para el uso seguro y apropiado de los recursos en línea, incluida cualquier restricción a sitios web y aplicaciones basadas en la web indeseables o inapropiados. Las reglas deben mantenerse actualizadas.

La institución debe reducir los riesgos de que su personal acceda a sitios web que contengan información ilegal o que se sepa que contienen virus o material de phishing. Una técnica para lograr esto funciona bloqueando la dirección IP o el dominio de los sitios web en cuestión. Algunos navegadores y tecnologías antimalware hacen esto automáticamente o pueden configurarse para hacerlo.

La institución debe identificar los tipos de sitios web a los que el personal debe o no tener acceso. La institución debe considerar bloquear el acceso a los siguientes sitios web maliciosos:

a) Sitios web que tienen una función de carga de información a menos que esté permitido por razones de negocios válidos:

b) Sitios web maliciosos conocidos o sospechosos (por ejemplo, aquellos que distribuyen malware o contenido de phishing),

c) Servidores de mando y control;

d) Sitio web malicioso adquirido de inteligencia de amenazas (ver 1.7);

e) Sitios web que comparten contenido ilegal.

Se debe brindar capacitación al personal sobre el uso seguro y apropiado de los recursos en línea, incluido el acceso a la web.

La capacitación debe incluir las políticas de seguridad de la institución, el punto de contacto para plantear problemas de seguridad y el proceso de excepción cuando se necesita acceder a recursos web restringidos por razones comerciales legítimas.

También se debe capacitar al personal para asegurar de que no invalide ningún aviso del navegador que informe que un sitio web no es seguro, pero permite que el usuario continúe.

4.24. Uso de criptografía

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración_segura	#Protección

Control

Elaborar, implementar y socializar reglas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas, de acuerdo a la necesidad de la institución.

Recomendaciones para la implementación:

Generalidades

Al usar criptografía, se debe considerar lo siguiente:

a) Definir la política institucional sobre criptografía, incluidos los principios generales para la protección de la información. Es necesaria una política específica sobre el uso de la criptografía para maximizar los beneficios y minimizar los riesgos del uso de técnicas criptográficas y para evitar el uso inapropiado o incorrecto, esta política debe ser periódicamente revisada y actualizada.

b) Identificar el nivel de protección requerido y la clasificación de la información y en consecuencia establecer el tipo, fortaleza y calidad de los algoritmos criptográficos requeridos;

c) El uso de criptografía para la protección de la información contenida en los dispositivos móviles o medios de almacenamiento de los usuarios y transmitida a través de redes a dichos dispositivos o medios de almacenamiento;

d) La gestión de claves, incluidos los métodos para gestionar la generación y protección de claves criptográficas y la recuperación de información cifrada en caso de pérdida o daño de claves;

e) Roles y responsabilidades para:

1) La implementación de las reglas para el uso efectivo de la criptografía;

2) La gestión de claves, incluida la generación de claves (ver 4.24);

f) Las normas a ser adoptadas, así como los algoritmos criptográficos, la fuerza del cifrado, las soluciones criptográficas y las prácticas de uso que sean aprobadas o requeridas para su uso en la institución;

g) El impacto del uso de información cifrada en los controles que se basan en la inspección de contenido, por ejemplo, detección de malware o filtrado de contenido.

Al implementar las reglas de la institución para el uso eficaz de la criptografía, se debe tener en cuenta las reglamentaciones y restricciones nacionales que pueden aplicarse al uso de técnicas criptográficas. (ver 1.31).

El contenido de los acuerdos o contratos de nivel de servicio con proveedores externos de servicios criptográficos, por ejemplo, con una autoridad de certificación debe cubrir cuestiones de responsabilidad, confiabilidad de los servicios y respuesta de tiempos para la prestación de los servicios (ver 1.22).

Gestión de claves

La gestión adecuada de claves requiere procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir claves criptográficas.

Un sistema de gestión de claves se debe basar en un conjunto acordado de normas, procedimientos y métodos seguros para:

a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones;

b) Emitir y obtener certificados de clave pública;

c) Distribuir claves a las entidades previstas, incluido cómo activar las claves cuando se reciben;

d) Almacenar claves, incluida la forma en que los usuarios autorizados obtienen acceso a las claves;

e) Cambiar o actualizar las claves, incluidas las reglas sobre cuándo cambiar las claves y cómo se hará;

f) Tratar con claves comprometidas;

g) Revocación de claves, incluido cómo retirar o desactivar claves, por ejemplo, cuando las claves se han visto comprometidas o cuando un usuario deja una institución (en cuyo caso las claves también deben archivarse);

h) Recuperar claves pérdidas o corruptas;

i) Realizar copias de seguridad o archivar claves;

j) Destrucción de llaves;

k) Registro y auditoría de actividades clave relacionadas con la gestión;

l) Establecer fechas de activación y desactivación de claves para que las claves solo se puedan usar durante el período de tiempo de acuerdo con las reglas de la institución sobre administración de claves;

m) Gestionar solicitudes legales de acceso a claves criptográficas (por ejemplo, se puede exigir que la información cifrada esté disponible sin cifrar como prueba en un caso judicial).

Todas las claves criptográficas se deben proteger contra modificaciones y pérdidas. Además, las claves secretas y privadas necesitan protección contra el uso no autorizado y la divulgación, el equipo utilizado para generar, almacenar y archivar claves se debe proteger físicamente.

Además de la integridad para muchos casos de uso también se debe considerar la autenticidad de las claves públicas.

La autenticidad de las claves públicas generalmente se aborda mediante procesos de gestión de claves públicas que utilizan autoridades de certificación y certificados de clave pública, pero también es posible abordarla mediante el uso de tecnologías como la aplicación de procesos manuales para claves de números pequeños.

La criptografía se puede utilizar para lograr diferentes objetivos de seguridad de la información, por ejemplo:

a) Confidencialidad: uso de cifrado de información para proteger información sensible o crítica, ya sea almacenada o transmitida;

b) Integridad o autenticidad: uso de firmas digitales o códigos de autenticación de mensajes para verificar la autenticidad o integridad de la información sensible o crítica almacenada o transmitida. Usar algoritmos con el fin de verificar la integridad de los archivos;

c) No repudio: uso de técnicas criptográficas para proporcionar evidencia de la ocurrencia o no ocurrencia de un evento o acción;

d) Autenticación: uso de técnicas criptográficas para autenticar usuarios y otras entidades del sistema que solicitan acceso o realizan transacciones con usuarios, entidades y recursos del sistema.

Para el uso de firma electrónica considerar:

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

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

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

4.25. Ciclo de vida de desarrollo seguro

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_Aplicaciones #Sistema_y_seguridad_de_la_red	#Protección

Control

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

Recomendaciones para la implementación:

El desarrollo seguro es un requisito para crear un servicio, una arquitectura, un software y un sistema seguro.

Para lograrlo, se deben considerar los siguientes aspectos:

a) Separación de los entornos de desarrollo, prueba y producción (ver 4.31);

b) Orientación sobre la seguridad en el ciclo de vida del desarrollo de software:

1) Seguridad en la metodología de desarrollo de software (ver 4.28 y 4.27);

2) Directrices de codificación segura para cada lenguaje de programación utilizado (ver 4.28);

c) Requisitos de seguridad en la fase de especificación y diseño (ver 1.8);

d) Puntos de control de seguridad en proyectos (ver 1.8);

e) Pruebas del sistema y seguridad, como pruebas de regresión, escaneo de código y pruebas de penetración (ver 4.29);

f) Repositorios seguros para el código fuente y la configuración (ver 4.4 y 4.9);

g) Seguridad en el control de versiones (ver 4.32);

h) Conocimiento y capacitación en seguridad de la aplicación requeridos (ver 4.28);

i) Control de calidad de software.

j) La capacidad de los desarrolladores para prevenir, encontrar y corregir vulnerabilidades (ver 4.28);

k) Requisitos de licencia y alternativas para garantizar soluciones rentables y evitar futuros problemas de licencia (ver 1.32).

l) Si se subcontrata el desarrollo, la institución se debe asegurar de que el proveedor cumpla con las especificaciones técnicas de la institución para el desarrollo (ver 4.30).

4.26. Requisitos de seguridad de la aplicación

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_Aplicaciones #Sistema_y_seguridad_de_la_red	#Protección #Defensa

Control

Identificar, especificar y aprobar los requisitos de seguridad de la información para desarrollar o adquirir aplicaciones.

Recomendaciones para la implementación:

Generalidades

Se debe identificar y especificar los requisitos de seguridad de las aplicaciones, estos requisitos generalmente se determinan a través de una evaluación de riesgos. Los requisitos se deben desarrollar con el soporte de especialistas en seguridad de la información.

Los requisitos de seguridad de la aplicación pueden cubrir un amplio rango de temas, según el propósito de la aplicación.

Los requisitos de seguridad de la aplicación deben incluir, según corresponda:

a) Nivel de confianza en la identidad de los usuarios, por ejemplo, mediante autenticación (ver 1.17, 4.2 y 4.5);

b) Identificar el tipo de información y el nivel de clasificación a ser procesado por la aplicación;

c) Necesidad de separación de acceso y nivel de acceso a datos y funciones en la aplicación;

d) Resiliencia contra ataques maliciosos o interrupciones no intencionales, por ejemplo, protección contra desbordamiento de búfer o inyecciones de lenguaje de consulta estructurado (SQL);

e) Requisitos legales, estatutarios y reglamentarios en la jurisdicción donde se genera, procesa, completa o almacena la transacción;

f) Necesidad de privacidad asociada con todas las partes involucradas;

g) Los requisitos de protección de cualquier información confidencial;

h) Protección de datos en proceso, en tránsito y en reposo;

i) Necesidad de cifrar de forma segura las comunicaciones entre todas las partes involucradas;

j) Controles de entrada, incluidas verificaciones de integridad y validación de entrada;

k) Controles automatizados, por ejemplo, límites de aprobación o aprobaciones dobles;

l) Controles de salida, considerando también quién puede acceder a las salidas y su autorización;

m) Restricciones en torno al contenido de los campos de "texto libre", ya que pueden conducir al almacenamiento no controlado de datos confidenciales, por ejemplo, datos personales;

n) Requisitos derivados del proceso de negocio, tales como registro y seguimiento de transacciones, requisitos de no repudio;

o) Requisitos exigidos por otros controles de seguridad, por ejemplo, interfaces para registro y monitoreo o sistemas de detección de fuga de datos;

p) Manejo de mensajes de error.

Servicios transaccionales

Para las aplicaciones que ofrecen servicios transaccionales entre la institución y las partes interesadas, se debe considerar lo siguiente al identificar los requisitos de seguridad de la información:

a) El nivel de confianza que cada parte requiere en la identidad reclamada de cada una;

b) El nivel de confianza requerido en la integridad de la información intercambiada o procesada y los mecanismos para la identificación de la falta de integridad, por ejemplo, verificación de redundancia cíclica, hashing, firmas digitales;

c) Procesos de autorización asociados con quién puede aprobar contenidos, emitir o firmar documentos transaccionales clave;
d) Confidencialidad, integridad, prueba de envío y recepción de documentos clave y no repudio, por ejemplo, contratos asociados a procesos de licitación y contratación;

e) La confidencialidad e integridad de cualquier transacción, por ejemplo, pedidos, detalles de la dirección de entrega y confirmación de recibos;

f) Requisitos sobre cuánto tiempo mantener la confidencialidad de una transacción;

g) Seguros y otros requisitos contractuales.

Aplicaciones de pago y pedidos electrónicos

Además, para aplicaciones que involucren pedidos y pagos electrónicos, se debe considerar lo siguiente:

a) Requisitos para mantener la confidencialidad e integridad de la información de la orden;

b) El grado de verificación apropiado para verificar la información de pago proporcionada por un cliente;

c) Evitar la pérdida o duplicación de información de transacciones:

d) Almacenar los detalles de la transacción fuera de cualquier entorno de acceso público, por ejemplo, en una plataforma de almacenamiento existente en la intranet de la institución, y no retenida ni expuesta en medios de almacenamiento electrónico accesibles directamente desde Internet;

e) Cuando se utiliza una autoridad de confianza, por ejemplo, con el fin de emitir y mantener firmas digitales o certificados digitales, la seguridad se integra y se incorpora a lo largo de todo el proceso de gestión de firmas o certificados de extremo a extremo

Varias de las consideraciones anteriores pueden abordarse mediante la aplicación de la criptografía (ver 4.24), teniendo en cuenta los requisitos legales (ver 1.31 a 1.36, especialmente (ver 1.31) para la legislación criptográfica).

4.27. Arquitectura del sistema seguro y principios de ingeniería

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_Aplicaciones #Sistema_y_seguridad_de_la_red	#Protección

Control

Los principios para diseñar sistemas seguros se deben establecer, documentar, mantener y aplicar a cualquier actividad de desarrollo de sistemas de información, socializar al área respectiva.

Recomendaciones para la implementación:

Los principios de ingeniería de seguridad se deben establecer, documentar y aplicar a las actividades de ingeniería de sistemas de información. La seguridad se debe diseñar en todas las capas de la arquitectura (negocios, datos, aplicaciones y tecnología) La nueva tecnología debe analizar en busca de riesgos de seguridad y el diseño, revisar frente a patrones de ataque conocidos.

Los principios de ingeniería segura proveen orientación sobre las técnicas de autenticación de usuarios, el control seguro de sesiones y la validación y desinfección de datos.

Los principios de ingeniería de sistemas seguros deben incluir el análisis de:

a) La gama completa de controles de seguridad necesarios para proteger la información y los sistemas contra las amenazas identificadas;

b) Las capacidades de los controles de seguridad para prevenir, detectar o responder a eventos de seguridad;

c) Los controles de seguridad específicos requeridos por procesos de negocios particulares, por ejemplo, cifrado de información confidencial, verificación de integridad y firma digital de información:

d) Considerar dónde y cómo se aplicarán los controles de seguridad, por ejemplo, mediante la integración con una arquitectura de seguridad y la infraestructura técnica;

e) Considerar cómo los controles de seguridad individuales (manuales y automatizados) funcionan juntos para producir un conjunto integrado de controles.

Los principios de ingeniería de seguridad deben tener en cuenta:

a)La necesidad de integrarse con una arquitectura de seguridad;

b) Infraestructura de seguridad técnica, por ejemplo, infraestructura de clave pública (PKI), gestión de identidad y acceso (IAM), prevención de fuga de datos y gestión de acceso dinámico;

c) Capacidad de la institución para desarrollar y soportar la tecnología elegida;

d) Costo, tiempo y complejidad de cumplir con los requisitos de seguridad;

e) Buenas prácticas actuales.

f) La información almacenada en dispositivos móviles debería ser la mínima, y más si se trata de contraseñas o datos de sesión. Este tipo de dispositivos son los más propensos a desaparecer y por lo tanto su información puede ser expuesta más fácilmente

La ingeniería de sistemas seguros debe implicar:

a) El uso de principios de arquitectura de seguridad, tales como "seguridad por diseño", "defensa en profundidad", "seguridad por defecto", "denegación predeterminada", "fallo seguro", "desconfiar de la entrada de aplicaciones externas", "seguridad en implementación", “asumir incumplimiento, “privilegio mínimo", “facilidad de uso y administración” y “funcionalidad mínima”;

b) Una revisión del diseño orientada a la seguridad para ayudar a identificar las vulnerabilidades de la seguridad de la información, asegurar que se especifiquen los controles de seguridad y cumplir con los requisitos de seguridad;

c) Documentación y reconocimiento formal de los controles de seguridad que no cumplen plenamente los requisitos (por ejemplo, debido a requisitos de seguridad superiores);

d) Endurecimiento de los sistemas.

La institución debe considerar principios de "confianza cero" tales como:

a) suponiendo que los sistemas de información de la institución ya han sido violados y, por lo tanto, no dependen solo de la seguridad del perímetro de la red;

b) Emplear un enfoque de "nunca confiar y siempre verificar" para el acceso a los sistemas de información;

c) Asegurar que las solicitudes a los sistemas de información estén encriptadas de extremo a extremo;

d) Verificar cada solicitud a un sistema de información como si se originara en una red externa abierta, incluso si estas solicitudes se originaron internamente en la institución, es decir, no confiar automáticamente en nada dentro o fuera de sus perímetros;

e) Utilizando técnicas de control de acceso dinámico y de "privilegio mínimo" (ver 1.15, 1.18 y 4.2). Esto incluye autenticar y autorizar solicitudes de información o a sistemas basados en información contextual como información de autenticación (ver 1.17), identidades de usuario (ver 1.16), datos sobre el dispositivo de punto final del usuario y clasificación de datos (ver 1.12):

f) Siempre autenticar a los solicitantes y siempre validar las solicitudes de autorización a los sistemas de información en función de la información, incluida la información de

autenticación (ver 1.17) y las identidades de los usuarios (1.16), datos sobre el dispositivo de punto final del usuario y clasificación de datos (ver 1.12), por ejemplo, hacer cumplir una autenticación fuerte, por ejemplo, multifactor, (ver 4.5).

Los principios de ingeniería de seguridad establecidos se deben aplicar, cuando corresponda, al desarrollo subcontratado de sistemas de información a través de contratos y otros acuerdos vinculantes entre la institución y el proveedor a quien la institución subcontrata. La institución se debe asegurar de que las prácticas de ingeniería de seguridad de los proveedores se alineen con las necesidades de la institución.

Los principios de ingeniería de seguridad y los procedimientos de ingeniería establecidos se deben revisar periódicamente para asegurar que contribuyan efectivamente a mejorar las normas de seguridad dentro del proceso de ingeniería, también se deben revisar periódicamente para asegurar que permanezcan actualizados en términos de combatir cualquier nueva amenaza potencial y seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican.

4.28. Codificación segura

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_Aplicaciones #Sistema_y_seguridad_de_la_red	#Protección

Control

Los principios de codificación segura deben aplicarse al desarrollo de software, para garantizar que el software se escriba de forma segura, reduciendo así la cantidad de posibles vulnerabilidades de seguridad de la información en el software.

Recomendaciones para la implementación:

Generalidades

La institución debe establecer procesos para proporcionar una buena gobernanza para la codificación segura, se debe establecer y aplicar una línea de base segura mínima, además, dichos procesos y gobernanza deben extenderse para cubrir los componentes de software de terceras partes y el software de código abierto.

La institución debe monitorear las amenazas del mundo real y actualizar el asesoramiento y la información sobre las vulnerabilidades del software para guiar los principios de codificación segura de la institución a través de la mejora y el aprendizaje continuo, esto puede ayudar a asegurar que se implementen prácticas de codificación segura y efectiva para combatir el panorama de amenazas que cambia rápidamente.

Planificación antes de codificar

Los principios de codificación segura deben usarse tanto para nuevos desarrollos como en escenarios de reutilización, estos principios deben aplicarse a las actividades de desarrollo tanto dentro de la institución como para los productos y servicios suministrados por la

institución a otros, la planificación y los pre-requisitos antes de la codificación deben incluir:

a) expectativas específicas de la institución y principios aprobados para la codificación segura que se utilizará para desarrollos de código internos y externos;

b) Prácticas y defectos de codificaciones comunes e históricas que conducen a vulnerabilidades de seguridad de la información;

c) Configurar herramientas de desarrollo, como entornos de desarrollo integrados (IDE), para ayudar a hacer cumplir la creación de código seguro:

d) Seguir la orientación emitida por los proveedores de herramientas de desarrollo y entornos de ejecución, según corresponda;

e) Mantenimiento y uso de herramientas de desarrollo actualizadas, por ejemplo, compiladores;

f) Calificación de los desarrolladores en la escritura de código seguro;

g) Diseño y arquitectura seguros, incluido el modelado de amenazas;

h) Normas de codificación segura y, cuando corresponda, exigir su uso;

i) Uso de ambientes controlados para el desarrollo.

Durante la codificación

Las consideraciones durante la codificación deben incluir:

a) Prácticas de codificación seguras específicas para los lenguajes y técnicas de programación que se utilizan;

b) Utilizar técnicas de programación seguras, como programación en pares, refactorización, revisión por pares, iteraciones de seguridad y desarrollo basado en pruebas:

c) Utilizar técnicas de programación estructurada;

d) Documentar el código y eliminar los defectos de programación, lo que puede permitir que se exploten las vulnerabilidades de seguridad de la información;

e) Prohibir el uso de técnicas de diseño inseguras (por ejemplo, el uso de contraseñas codificadas, ejemplos de código no aprobados y servicios web no autenticados).

Las pruebas deben realizarse durante y después del desarrollo (ver 4.29).

Los procesos de prueba de seguridad de aplicaciones estáticas (SAST) pueden identificar vulnerabilidades de seguridad en el software.

Antes de que el software entre en funcionamiento, se debe evaluar lo siguiente:

a) Superficie de ataque y el principio de privilegio mínimo;

b) Realizar un análisis de los errores de programación más comunes y documentar que estos han sido mitigados.

Revisión y mantenimiento

Después de que el código se haya hecho operativo:

a) Las actualizaciones se deben empaquetar e implementar de forma segura;

b) Se deben manejar las vulnerabilidades de seguridad de la información reportadas (ver 4.8);

c) Los errores y los ataques sospechosos se deben registrar y los registros se deben revisar periódicamente para hacer los ajustes necesarios al código:

d) El código fuente se debe proteger contra el acceso no autorizado y la manipulación, por ejemplo, mediante el uso de herramientas de gestión de la configuración, que suelen proporcionar funciones como control de acceso y control de versiones.

Si utiliza herramientas y bibliotecas externas, la institución debe considerar:

a) asegurar que las bibliotecas externas se gestionen (por ejemplo, manteniendo un inventario de las bibliotecas utilizadas y sus versiones) y se actualicen regularmente con los ciclos de publicación:

b) Selección, autorización y reutilización de componentes bien examinados, en particular componentes de autenticación y criptográficos;

c) La licencia, seguridad e historial de los componentes externos;

d) Asegurar que el software se pueda mantener, rastrear y provenir de fuentes comprobadas y confiables;

e) Disponibilidad a largo plazo de recursos y artefactos para el desarrollo.

Cuando sea necesario modificar un paquete de software, se debe considerar los siguientes puntos:

a) El riesgo de que los controles incorporados y los procesos de integridad se vean comprometidos;

b) Si se debería obtener el consentimiento del vendedor;

c) La posibilidad de obtener los cambios necesarios del proveedor como actualizaciones estándar del programa;

d) El impacto si la institución se hace responsable del mantenimiento futuro del software como resultado de los cambios;

e) compatibilidad con otro software en uso.

4.29. Pruebas de seguridad en el desarrollo y la aceptación

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_de_Aplicaciones #Información_seguridad_garantía #Sistema_y_seguridad_de_la_red	#Protección

Control

Definir, documentar e implementar los procesos de prueba de seguridad en el ciclo de vida del desarrollo.

Recomendaciones para la implementación:

Los nuevos sistemas de información, las actualizaciones y las nuevas versiones se deben probar y verificar minuciosamente durante los procesos de desarrollo. Las pruebas de seguridad deben ser una parte integral de las pruebas de sistemas o componentes.

Las pruebas de seguridad se deben realizar frente a un conjunto de requisitos, que pueden expresarse como funcionales o no funcionales. Las pruebas de seguridad deben incluir pruebas de:

a) Funciones de seguridad como autenticación de usuarios (ver 4.5), restricción de acceso (ver 4.3) y uso de criptografía (ver 4.24);

b) Codificación segura (ver 4.28);

c) Configuraciones seguras (ver 4.9, 4.20 y 4.22) incluyendo la de sistemas operativos, firewalls y otros componentes de seguridad.

Los planes de prueba deben determinarse utilizando un conjunto de criterios. El alcance de las pruebas debe ser proporcional a la importancia, la naturaleza del sistema y el impacto potencial del cambio que se está introduciendo. El plan de prueba debe incluir:

a) Cronograma detallado de actividades y pruebas;

b) Insumos y productos esperados bajo una variedad de condiciones;

c) Criterios para evaluar los resultados;

d) Decisión de acciones adicionales según sea necesario.

La institución puede aprovechar las herramientas automatizadas, como las herramientas de análisis de código o los escáneres de vulnerabilidades, y debe verificar la corrección de los defectos relacionados con la seguridad.

Para los desarrollos internos, estas pruebas deben ser realizadas inicialmente por el equipo de desarrollo. Luego se deben realizar pruebas de aceptación independientes para garantizar que el sistema funcione como se espera (ver 1.8). Se debe considerar lo siguiente:

a) Realizar actividades de revisión de código como un elemento relevante para probar las leyes de fallas de seguridad, incluidas las entradas y condiciones imprevistas;

b) Realizar un escaneo de vulnerabilidades para identificar configuraciones inseguras y vulnerabilidades del sistema:

c) Realizar pruebas de penetración para identificar código y diseño inseguro.

Para los componentes de compra y desarrollo subcontratados, se debe seguir un proceso de adquisición, los contratos con el proveedor deben abordar los requisitos de seguridad identificados (ver 1.20), los productos y servicios deben evaluarse según estos criterios antes de la adquisición.

Las pruebas se deben realizar en un entorno de prueba que coincida lo más posible con el entorno de producción objetivo para asegurar que el sistema no introduzca vulnerabilidades en el entorno de la institución y que las pruebas sean confiables (ver 4.31).

4.30. Desarrollo subcontratado

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Detectar	#Sistema_y_red_seguridad #Seguridad_de_aplicaciones #Relaciones_con_proveedores_seguridad	#Protección

Control

La institución debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados, de acuerdo a las especificaciones determinadas en el contrato.

Recomendaciones para la implementación:

Cuando se subcontrata el desarrollo del sistema, la institución debe comunicar y acordar los requisitos y expectativas, monitorear y revisar continuamente si la entrega del trabajo subcontratado cumple con las especificaciones técnicas del contrato, se debe considerar los siguientes puntos en toda la cadena de suministro externa a la institución:

a) Acuerdos de licencia, propiedad del código y derechos de propiedad intelectual relacionados con el contenido subcontratado (ver 1 32);

b) Requisitos contractuales para prácticas seguras de diseño, codificación y pruebas (ver 4.25 a 4.29);

c) Provisión del modelo de amenaza a considerar por desarrolladores externos;

d) Pruebas de aceptación para la calidad y exactitud de los entregables (ver 4.29):

e) Provisión de evidencia de que se han establecido niveles mínimos aceptables de seguridad y capacidades de privacidad, por ejemplo, informes de aseguramiento;

f) Provisión de evidencia de que se han aplicado suficientes pruebas para protegerse contra la presencia de contenido malicioso tanto intencional como no intencional en el momento de la entrega;

g) Provisión de evidencia de que se han aplicado pruebas suficientes para protegerse contra la presencia de vulnerabilidades conocidas;

h) Acuerdos de depósito en garantía para el código fuente del software, por ejemplo, si el proveedor cierra;

i) Derecho contractual a auditar procesos y controles de desarrollo:

j) Requisitos de seguridad para el entorno de desarrollo (ver 4.31);

k) Teniendo en cuenta la legislación aplicable, por ejemplo, sobre protección de datos personales.

4.31. Separación de los entornos de desarrollo, prueba y producción

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones #Sistema_y_seguridad_de_la_red	#Protección

Control

Los entornos de desarrollo, prueba y producción deben estar separados y protegidos, para reducir los riesgos de acceso no autorizados.

Recomendaciones para la implementación:

Se debe identificar e implementar el nivel de separación entre los entornos de producción, prueba y desarrollo que es necesario para evitar problemas de producción.

Se debe considerar los siguientes elementos:

a) Separar adecuadamente los sistemas de desarrollo y producción y operarlos en diferentes dominios (por ejemplo, en entornos físicos o virtuales separados);

b) Definir, documentar e implementar reglas y autorizaciones para el despliegue de software desde el estado de desarrollo hasta el de producción;

c) Probar los cambios en los sistemas de producción y las aplicaciones en un entorno de pruebas o etapas antes de aplicarlos a los sistemas de producción (ver 4.29);

d) No realizar pruebas en entornos de producción excepto en circunstancias que hayan sido definidas y aprobadas;

e) Compiladores, editores y otras herramientas de desarrollo o programas de utilidad que no sean accesibles desde los sistemas de producción cuando no se requieran;

f) Mostrar etiquetas de identificación del entorno adecuadas en los menús para reducir el riesgo de error;

g) No copiar información confidencial en los entornos del sistema de desarrollo y prueba a menos que se proporcionen controles equivalentes para los sistemas de desarrollo y prueba.

En todos los casos, los entornos de desarrollo y pruebas deben protegerse teniendo en cuenta:

a) Aplicación de parches y actualización de todas las herramientas de desarrollo, integración y prueba (incluidos constructores, integradores, compiladores, sistemas de configuración y bibliotecas);

b) Configuración segura de sistemas y software,

c) Control de acceso a los ambientes;

d) Monitoreo de cambios en el entorno y código almacenado en el mismo;

e) Monitoreo seguro de los ambientes;

f) Realizar copias de seguridad de los entornos.

Una sola persona no debe tener la capacidad de realizar cambios tanto en el desarrollo como en la producción sin una revisión y aprobación previas. Esto se puede lograr, por ejemplo, mediante la separación de los derechos de acceso o mediante reglas supervisadas.

En situaciones excepcionales, se deben implementar medidas adicionales como registro detallado y monitoreo en tiempo real para detectar y actuar sobre cambios no autorizados.

4.32. Gestión de cambios

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones #Sistema_y_seguridad_de_la_red	#Protección

Control

Definir, documentar e implementar un proceso formal de gestión de cambios para las

instalaciones de tratamiento de información y los sistemas de información, para preservar la seguridad de la información al ejecutar cambios.

Recomendaciones para la implementación:

La introducción de nuevos sistemas y cambios importantes en los sistemas existentes deben seguir reglas acordadas y un proceso formal de documentación, especificación, prueba, control de calidad e implementación administrada, deben existir responsabilidades y procedimientos de gestión para asegurar un control satisfactorio de todos los cambios.

Los procedimientos de control de cambios se deben documentar y aplicar para asegurar la confidencialidad, integridad y disponibilidad de la información en las instalaciones de tratamiento de información y los sistemas de información, para todo el ciclo de vida de desarrollo del sistema desde las primeras etapas de diseño hasta todos los esfuerzos de mantenimiento posteriores.

Siempre que sea factible, deben integrarse los procedimientos de control de cambios para la infraestructura y el software de las TIC.

Los procedimientos de control de cambios deben incluir:

a) Planificar y evaluar el impacto potencial de los cambios considerando todas las dependencias;

b) Autorización de cambios;

c) Comunicar los cambios a las partes interesadas pertinentes documentadamente;

d) Pruebas y aceptación formal de pruebas para los cambios (ver 4.29);

e) Aplicación de cambios, incluidos los planes de despliegue;

f) Consideraciones de emergencia y contingencia, incluidos los procedimientos de roll-back;

g) Mantener registros de cambios que incluyan todo lo anterior;

h) Asegurar que la documentación operativa (ver 1.37) y los procedimientos del usuario se cambien según sea necesario para seguir siendo apropiados;

i) Asegurar que los planes de continuidad de las TIC y los procedimientos de respuesta y recuperación (ver 1.30) se modifiquen según sea necesario para seguir siendo apropiados.

El control inadecuado de los cambios en las instalaciones de procesamiento de información y los sistemas de información es una causa común de fallas en el sistema o la seguridad. Los cambios en el entorno de producción, especialmente cuando se transfiere software del entorno de desarrollo al operativo, pueden afectar la integridad y disponibilidad de las aplicaciones.

El oficial de seguridad de la información (OSI), supervisará el cumplimiento de las etapas de la gestión de cambios, en aquellos cambios que afecten a la seguridad de la información.

4.33. Información de prueba

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad	#Proteger	#Información_ protección	#Protección

Control

La información de las pruebas debe seleccionarse, protegerse y gestionarse adecuadamente; para garantizar la relevancia de las pruebas y la protección de la información operativa utilizada para las pruebas.

Recomendaciones para la implementación:

La información de prueba se debe seleccionar para asegurar la confiabilidad de los resultados de las pruebas y la confidencialidad de la información operativa relevante. La información confidencial (incluida la información de identificación personal) no se debe copiar en los entornos de desarrollo y prueba (ver 4.31).

Se deben aplicar las siguientes recomendaciones para proteger las copias de la información operativa, cuando se utilizan con fines de prueba, ya sea que el entorno de prueba se construya internamente o en un servicio en la nube:

a) Aplicar los mismos procedimientos de control de acceso a los entornos de prueba que los que se aplican a los entornos operativos;

b) Tener una autorización separada cada vez que se copia información operativa a un entorno de prueba;

c) Registrar la copia y el uso de información operativa para proporcionar una pista de auditoria;

d) Proteger la información confidencial mediante eliminación o enmascaramiento (ver 4.11) si se usa para pruebas;

e) Eliminar correctamente (ver 4.10) la información operativa de un entorno de prueba inmediatamente después de que se complete la prueba para evitar el uso no autorizado de la información de la prueba.

f) Identificar por cada sistema, los datos que pueden ser copiados de un ambiente de producción a un ambiente de pruebas.

Almacenar de forma segura, para evitar la manipulación, que de lo contrario puede generar resultados no válidos y solo se debería usar para propósitos de prueba

4.34. Protección de los sistemas de información durante las pruebas de auditoría

Tipo de Control	Propiedades de la SI	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	Proteger	#Sistema_y_red_seguridad #Información_protección	#Gobernanza_y_ecosistema #Protección

Control

Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas en producción, se deben planificar, documentar y acordar entre el evaluador y el responsable del proceso correspondiente; para minimizar el impacto de la auditoría y otras actividades de aseguramiento.

Recomendaciones para la implementación:

Se deben observar las siguientes recomendaciones:

a) Considerar acordar solicitudes de auditoria para el acceso a sistemas y datos con la gestión adecuada;

b) Considerar acordar y controlar el alcance de las pruebas de auditoría técnica, asegurar que la persona que realiza la auditoría sea independiente de las actividades auditadas;

c) Limitar las pruebas de auditoria al acceso de solo lectura al software y los datos. Si el acceso de solo lectura no está disponible para obtener la información necesaria, ejecutar la prueba por un administrador experimentado que tenga los derechos de acceso necesarios en nombre del auditor;

d) Si se otorga el acceso, establecer y verificar los requisitos de seguridad, por ejemplo, antivirus y parches, de los dispositivos utilizados para acceder a los sistemas, por ejemplo, computadoras portátiles o tabletas, antes de permitir el acceso;

e) Solo permitir el acceso que no sea de solo lectura para copias aisladas de archivos del sistema, eliminándolos cuando se complete la auditoría, o brindándoles la protección adecuada si existe la obligación de mantener dichos archivos bajo los requisitos de documentación de auditoria;

f) Identificar y acordar solicitudes de tratamiento especial o adicional, como ejecutar herramientas de auditoría;

g) Ejecutar pruebas de auditoría que puedan afectar la disponibilidad del sistema fuera del horario de negocio:

h) Monitorear y registrar todos los accesos para fines de auditoría y prueba.

Las pruebas de auditoría y otras actividades de aseguramiento también pueden ocurrir en los sistemas de prueba y desarrollo, donde dichas pruebas pueden afectar, por ejemplo, la

integridad del código o conducir a la divulgación de cualquier información confidencial que se encuentre en dichos entornos.

Anexo (informativo)

Correspondencia del EGSI v3 con el EGSI v2

El propósito de este anexo es proporcionar compatibilidad con la versión anterior del EGSI V2 para las instituciones de la APC.

Tabla de referencia controles EGSI V3 con los controles del EGSI V2

Identificador de control EGSI V3	Identificador de control EGSI V2	Nombre del Control
1.1	1.1.1, 1.1.2	Políticas de seguridad de la información
1.2	2.1.1	Roles y responsabilidades de seguridad de la información
1.3	2.1.2	Separación de funciones
1.4	3.2.1	Responsabilidades de la dirección
1.5	2.1.3	Contacto con las autoridades
1.6	2.1.4	Contacto con los grupos de interés especial
1.7	Nuevo	Inteligencia de amenazas
1.8	2.1.5, 10.1.1	Gestión de proyectos de seguridad de la información
1.9	4.1.1, 4.1.2	Inventario de información y otros activos asociados
1.10	4.1.3, 4.2.3	Uso aceptable de la información y otros activos asociados
1.11	4.1.4	Devolución de Bienes
1.12	4.2.1	Clasificación de la información
1.13	4.2.2	Etiquetado de la información
1.14	9.2.1, 9.2.2, 9.2.3	Transferencia de información
1.15	5.1.1, 5.1.2	Control de acceso
1.16	5.2.1	Gestión de identidad
1.17	5.2.4, 5.3.1, 5.4.3	Información de autenticación
1.18	5.2.2, 5.3.1, 5.2.6	Derechos de acceso
1.19	11.1.1	Seguridad de la información en las relaciones con los proveedores
1.20	11.1.2	Abordar la seguridad de la información en los acuerdos con los proveedores
1.21	11.1.3	Gestión de la seguridad de la información en la cadena de suministro de las TIC
1.22	11.2.1, 11.2.2	Monitoreo, revisión y gestión de cambios de servicios de proveedores
1.23	Nuevo	Seguridad de la información para el uso de servicios en la nube
1.24	12.1.1	Planificación y preparación de la gestión de incidentes de seguridad de la información

1.25	12.1.4	Evaluación y decisión sobre eventos de seguridad de la información
1.26	12.1.5	Respuesta a incidentes de seguridad de la información
1.27	12.1.6	Aprendiendo de los incidentes de seguridad de la información
1.28	12.1.7	Recopilación de evidencia
1.29	13.1.1, 13.1.2, 13.1.3	Seguridad de la información durante la interrupción
1.30	Nuevo	Preparación de las TIC para la continuidad del negocio
1.31	14.1.1, 14.1.5	Requisitos legales, estatutarios, reglamentarios y contractuales
1.32	14.1.2	Derechos de propiedad intelectual
1.33	14.1.3	Protección de los registros
1.34	14.1.4	Privacidad y protección de PII
1.35	14.2.1	Revisión independiente de seguridad de la información
1.36	14.2.2, 14.2.3	Cumplimiento de políticas, reglas y normas de seguridad de la información
1.37	8.1.1	Procedimientos operativos documentados
2.1	3.1.1	Selección
2.2	3.1.2	Términos y condiciones de empleo
2.3	3.2.2	Concienciación, educación y formación en seguridad de la información
2.4	3.2.3	Proceso disciplinario
2.5	3.3.1	Responsabilidades después de la terminación o cambio de empleo
2.6	9.2.4	Acuerdos de confidencialidad o no divulgación
2.7	2.2.2	Trabajo remoto
2.8	12.1.2, 12.1.3	Reporte de eventos de seguridad de la información
3.1	7.1.1	Perímetros de seguridad física
3.2	7.1.2, 7.1.6	Entrada física
3.3	7.1.3	Seguridad de oficinas, despachos e instalaciones
3.4	Nuevo	Monitoreo de seguridad física
3.5	7.1.4	Protección contra las amenazas externas y ambientales
3.6	7.1.5	Trabajo en áreas seguras
3.7	7.2.9	Puesto de trabajo despejado y pantalla limpia
3.8	7.2.1	Ubicación y protección de equipos
3.9	7.2.6	Seguridad de los activos fuera de las instalaciones
3.10	4.3.1, 4.3.2, 4.3.3, 7.2.5	Medios de almacenamiento
3.11	7.2.2	Instalaciones de suministro
3.12	7.2.3	Seguridad del cableado
3.13	7.2.4	Mantenimiento de equipo

3.14	7.2.7	Eliminación segura o reutilización de equipos
4.1	2.2.1, 7.2.8	Dispositivos de usuario final
4.2	5.2.3	Derechos de acceso privilegiado
4.3	5.4.1	Restricción de acceso a la información
4.4	5.4.5	Acceso al código fuente
4.5	5.4.2	Autenticación segura
4.6	8.1.3	Gestión de capacidades
4.7	8.2.1	Protección contra malware
4.8	8.6.1, 14.2.3	Gestión de vulnerabilidades técnicas
4.9	Nuevo	Gestión de la configuración
4.10	Nuevo	Eliminación de información
4.11	Nuevo	Enmascaramiento de datos
4.12	Nuevo	Prevención de fuga de datos
4.13	8.3.1	Copia de seguridad de la información
4.14	13.2.1	Redundancia de las instalaciones de tratamiento de información
4.15	8.4.1, 8.4.2, 8.4.3	Registro de eventos
4.16	Nuevo	Actividades de monitoreo
4.17	8.4.4	Sincronización de reloj
4.18	5.4.4	Uso de programas de utilidad privilegiados
4.19	8.5.1, 8.6.2	Instalación de software en sistemas operativos
4.20	9.1.1	Seguridad en redes
4.21	9.1.2	Seguridad de los servicios de red.
4.22	9.1.3	Separación en las redes
4.23	Nuevo	Filtrado web
4.24	6.1.1, 6.1.2	Uso de criptografía
4.25	10.2.1	Ciclo de vida de desarrollo seguro
4.26	10.1.2, 10.1. 3	Requisitos de seguridad de la aplicación
4.27	10.2.5	Arquitectura del sistema seguro y principios de ingeniería
4.28	Nuevo	Codificación segura
4.29	10.2.8, 10.2.9	Pruebas de seguridad en desarrollo y aceptación.
4.30	10.2.7	Desarrollo subcontratado
4.31	8.1.4, 10.2.6	Separación de los entornos de desarrollo, prueba y producción
4.32	8.1.2, 10.2.2, 10.2.3, 10.2.4	Gestión de cambios
4.33	10. 3.1	Información de prueba
4.34	8 .7.1	Protección de los sistemas de información durante las pruebas de auditoría

GLOSARIO DE TÉRMINOS

Lista de términos relacionados en el contexto del Esquema Gubernamental de la Seguridad de la Información:

A.

Activo de información. - En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la institución.

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

Análisis de riesgos. - proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Aplicación. – solución de TI, incluyendo programas de aplicación, datos de aplicaciones y procedimientos diseñados para ayudar a los usuarios de las organizaciones a realizar tareas específicas o manejar tipos específicos de problemas de TI, automatizando un proceso o función del negocio

Ataque. - intento de destruir, exponer, alterar, deshabilitar, robar o lograr acceso no autorizado o hacer uso no autorizado de un activo.

Autenticación. - Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autenticidad. - Propiedad de que una entidad es lo que afirma ser.

C.

Cadena de custodia. - Posesión demostrable, movimiento, manejo y localización de material de un punto en el tiempo a otro

Comité de Seguridad de la información (CSI). – se encarga de gestionar la implementación y mejora continua del Esquema Gubernamental de Seguridad de la Información.

Comportamiento de los riesgos. – El comportamiento de los riesgos se manifiesta de diversas formas a lo largo del tiempo debido a la evolución constante de las amenazas y del entorno en el que opera la institución.

Confidencialidad. - Propiedad de que la información no esté disponible o no sea divulgada a personas, entidades o procesos no autorizados.

Contenidos maliciosos. - aplicaciones, documentos, archivos, datos u otros recursos que tienen características o capacidades maliciosas incrustadas, disfrazadas o escondidas en ellos.

Control. - Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Control de acceso. - Medios para asegurar que el acceso físico y lógico a los activos esté autorizado y restringido en función de los requisitos de seguridad de negocios y de la información

Control contramedida. - los medios de gestión de riesgos, que incluyen las políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden ser de carácter administrativo, técnico, de gestión o de carácter legal.

D.

Declaración de responsabilidad. – Se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio.

Directiva o directriz. - Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad. - Propiedad de estar disponible y utilizable en el momento que sea requerido por una entidad autorizada.

Dispositivo de punto final del usuario. - Dispositivo de punto final utilizado por los usuarios para acceder a los servicios de tratamiento de información.

Dispositivo de punto final. - Dispositivo de hardware de tecnología de la información y la comunicación (TIC) conectado a la red, punto final puede referirse a computadoras de escritorio, portátiles, teléfonos inteligentes, tablets, clientes ligeros, impresoras u otro hardware especializado, incluidos medidores inteligentes y dispositivos de Internet de las cosas (IoT).

Documentación esencial. – Considerada documentación esencial las siguientes:

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

E.

Estudio de gestión de riesgos. - El estudio de gestión de riesgos en el EGSI, es un proceso estructurado y sistemático que tiene como objetivo identificar, evaluar y gestionar los riesgos relacionados con la seguridad de la información en la institución; que podrían comprometer la confidencialidad, integridad y disponibilidad de la información.

EGSI. - Esquema Gubernamental de Seguridad de la Información para las instituciones de la APCID para preservar la integridad, disponibilidad y confidencialidad de la

información.

Encargado de PII. - Parte interesada de la privacidad que trata la información personal identificable (PII) en nombre y de acuerdo con las instrucciones de un responsable de PII.
Entidad. - Elemento relevante para el propósito de la operación de un dominio que tiene una existencia reconociblemente distinta, puede tener una realización física o lógica; como una persona, una institución, un dispositivo, un grupo de tales elementos, un suscriptor humano de un servicio de telecomunicaciones, una tarjeta SIM, un pasaporte, una tarjeta de interfaz de red, una aplicación de software, un servicio de un sitio web.
Evaluación del impacto en la privacidad PIA. - Proceso general de identificación, análisis, evaluación, consulta, comunicación y planificación del tratamiento de posibles impactos en la privacidad con respecto al tratamiento de información personal identificable (PII) (3 1 21), enmarcado dentro del marco de referencia más amplio de gestión de riesgos de una institución

Evaluación de riesgos. - Proceso global de identificación, análisis y estimación de riesgos.

Evento de seguridad de la información. - Ocurrencia que indica una posible violación de seguridad de la información o falla de los controles.

F.

Fiabilidad. - Propiedad de comportamiento y resultados consistentes previstos

G.

Gestión de claves. - Controles referidos a la gestión de claves criptográficas.

Gestión de incidentes de seguridad de la información. - Procesos para detectar, reportar, evaluar, responder, tratar y aprender para el majeo de los incidentes de seguridad de la información.

Gestión de riesgos. - Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

I.

Identificación de riesgos. - Proceso de encontrar, reconocer y describir riesgos.

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

Incidente de seguridad de la información. - Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Es uno de los activos más importantes de las instituciones, en las formas que esta se manifieste: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, magnético, papel, electrónico, computadoras, audiovisual y otros.

Información confidencial. - Información que no está destinada a estar disponible o

divulgarse a personas, entidades o procesos no autorizados.

Información personal identificable PII. - Cualquier información que (a) pueda utilizarse para establecer un vínculo entre la información y la persona física a la que se refiere dicha información, o (b) esté o pueda estar vinculada directa o indirectamente a una persona física.

Información sensible. - Información que necesita protegerse de la falta de disponibilidad, el acceso no autorizado, la modificación o la divulgación pública debido a posibles efectos adversos en un individuo, institución, seguridad nacional o seguridad pública.
Instalación de tratamiento de información. - Cualquier sistema, servicio o infraestructura de tratamiento de información, o la localización física que lo alberga.

Institución. - Grupo de personas e instalaciones con una disposición de responsabilidades, autoridades y relaciones.

Integridad. - Propiedad de proteger la precisión y completitud de los activos.

Internet (red interconectada), interconexión de redes. - una colección de redes interconectadas.

La internet. - sistema global de redes interconectadas de dominio público”

Inventario de activos. - Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

N.

No repudio. - Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

M.

Malware, software malicioso. - Software diseñado con malas intenciones que contiene características o capacidades que potencialmente pueden causar daño directamente o indirectamente al usuario y/o al sistema informático del usuario.

O.

Objetivo. - Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

Oficial de Seguridad de la Información (OSI). - Es el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento del Esquema

P.

Parte interesada. - <gestión de riesgos> persona u organización que puede afectar, verse afectada por, o percibirse a sí misma como afectada por una decisión o actividad.

Phishing (engaño técnico). - proceso fraudulento o intento de adquirir información privada o confidencial de manera enmascarada haciéndose pasar por una entidad confiable en una comunicación electrónica.

Plan de concienciación. – Plan orientado a crear conciencia y educar a los funcionarios y a las partes interesadas sobre la importancia de la seguridad de la información y cómo contribuir a su éxito.

Plan de continuidad del negocio. - Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos. - Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política. - Intenciones y dirección de una institución, expresadas formalmente por su alta dirección.

Política de escritorio despejado. - La política de la empresa que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.

Principal de PII. - Persona natural a la que se refiere la información personal identificable (PII).

Proceso. - Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Propietario del activo. - puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la institución.

Propietario de la Información. - es el responsable de clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

Propietario del riesgo. - persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Proveedor de servicios de Internet. - organización que presta servicios de Internet a un usuario y permite a sus clientes acceder a Internet.

Punto de recuperación objetivo RPO. - Momento en el que se recuperarán los datos después de que se haya producido una interrupción.

R.

Registro. - Información creada, recibida y mantenida como evidencia y como activo por una institución o persona, en cumplimiento de obligaciones legales o en la transacción de negocios.

Regla. -Principio aceptado o instrucción que establece las expectativas de la institución

sobre lo que se requiere hacer, lo que está permitido o no permitido.

Resiliencia. - Capacidad de los activos institucionales, para regresar a su forma original.

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

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

Ruptura. - Incidente, ya sea anticipado o no, que causa una desviación negativa no planificada de la entrega esperada de productos y servicios de acuerdo con los objetivos de la institución.

S.

Seguridad de la información. - conjunto de medidas preventivas y reactivas de las instituciones y de los sistemas tecnológicos que permiten la preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de información. - Aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento

Software engañoso (spyware). - que recopila información privada o confidencial de un usuario de computador.

Software potencialmente no deseado. - software engañoso, incluyendo el malware y no malicioso, que exhibe las características de software engañoso.

Spam (correo basura). - abuso de los sistemas de mensajería electrónica para enviar indiscriminadamente mensajes masivos no solicitados.

T.

Tiempo objetivo de recuperación RTO. - Periodo de tiempo dentro del cual los niveles mínimos de servicios y/o productos y los sistemas de soporte, las aplicaciones o funciones deben recuperarse después de que se haya producido una interrupción.

Tratamiento de riesgos. - Proceso de modificar el riesgo, mediante la implementación de controles.

Trazabilidad. - Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Troyano, caballo de Troya. - software malintencionado que aparece para realizar una función deseable.

U.

Usuario. - Parte interesada con acceso a los sistemas de información de la institución, como personal, clientes, proveedores.

V.

Violación de seguridad de la información. - Compromiso de seguridad de la información que conduce a la destrucción, pérdida, alteración, divulgación o acceso no deseados a la información protegida transmitida, almacenada o procesada de otro modo
Vulnerabilidad. - Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Términos Abreviados

ABAC	Control de acceso basado en atributos
ACL	Lista de control de acceso
BIA	Análisis de impacto del negocio
APC	Administración pública central
BYOD	Trae tu propio dispositivo
CAPTCHA	Prueba de Turing pública completamente automatizada para diferenciar a las computadoras de los humanos
CPU	Unidad central de proceso
DAC	Control de acceso discrecional
DNS	Sistema de nombres de dominio
GPS	Sistema de posicionamiento global
IAM	Gestión de acceso e identidad
TIC	Tecnología de la información y la comunicación
ID	Identificación
IDE	Entorno de desarrollo integrado
IDS	Sistema de detección de intrusos
IoT	Internet de las cosas
IP	Protocolo de internet
IPS	Sistema de prevención de intrusiones
TI	Tecnologías de la información
SGSI	Sistema de gestión de seguridad de la información
MAC	Control de acceso obligatorio
NTP	Protocolo de tiempo de red
PIA	Evaluación de impacto de privacidad
PII	Información personal identificable
PIN	Número de identificación personal
PKI	Infraestructura de clave pública
PTP	Protocolo de tiempo de precisión

RBAC	Control de acceso basado en roles
RPO	Punto de recuperación objetivo
RTO	Tiempo objetivo de recuperación
SAST	Pruebas de seguridad de aplicaciones estáticas
SD	Seguro digital
SDN	Redes definidas por software
SD-WAN	Red de área amplia definida por software
SIEM	Gestión de eventos e información de seguridad
SMS	Servicio de mensajes cortos
SQL	Lenguaje de consulta estructurado
SSO	Inicio de sesión único
SWID	Identificación del software
UEBA	Análisis de comportamiento de usuarios y entidades
UPS	Fuente de alimentación ininterrumpida
URL	Localizador uniforme de recursos
USB	Bus serie universal
VM	Máquina virtual
VPN	Red privada virtual
WIFI	Fidelidad inalámbrica

FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN

	Nombre / Cargo	Firma
Elaborado por:	Marcelo Guerrero / **Especialista de Seguridad de la Información**	Firmado electrónicamente por: MARCELO EDUARDO GUERRERO FLORES
	Maribel Martínez / **Analista Senior en Seguridad de la Información**	Firmado electrónicamente por: MARIBEL ALEXANDRA MARTINEZ CARRILLO
	Luis Gualotuña / **Analista Senior en Seguridad de la Información**	Firmado electrónicamente por: LUIS IVAN GUALOTUÑA GUALOTUÑA
Revisado por:	Giovanny Jami / **Director de Infraestructura, Interoperabilidad, Seguridad de la Información y Registro Civil**	Firmado electrónicamente por: GIOVANNY ERNESTO JAMI TAPIA
Aprobado por:	José Luis Nath / **Subsecretario de Gobierno Electrónico y Registro Civil**	Firmado electrónicamente por: JOSE LUIS NATH NIETO