

REGISTRO OFICIAL[®]

ÓRGANO DE LA REPÚBLICA DEL ECUADOR

MINISTERIO DE
TELECOMUNICACIONES Y
DE LA SOCIEDAD DE LA
INFORMACIÓN:

ACUERDO
No. MINTEL-MINTEL-2026-0008

SE REFORMA EL
ACUERDO MINISTERIAL
No. MINTEL-MINTEL-2024-0003 DE 8
DE FEBRERO DE 2024

ACUERDO Nro. MINTEL-MINTEL-2026-0008**SR. MGS. RICARDO XAVIER GUTIÉRREZ
MINISTRO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA
INFORMACIÓN (E)****CONSIDERANDO:**

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

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

Que, el artículo 227 de la Constitución de la República del Ecuador establece que: *“La Administración Pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación”*;

Que, el primer inciso del artículo 233 de la Constitución de la República del Ecuador dispone: *“Ninguna servidora ni servidor público estará exento de responsabilidades por los actos realizados en el ejercicio de sus funciones, o por sus omisiones, y serán responsables administrativa, civil y penalmente por el manejo y administración de fondos, bienes o recursos públicos (...)”*;

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

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

Que, el artículo 3 de la Ley Orgánica para la Transformación Digital y Audiovisual establece que: *“El ente rector en materia de Telecomunicaciones y de la Sociedad de la Información será la entidad rectora en transformación digital, gobierno digital y ciberseguridad, para lo cual ejercerá atribuciones y responsabilidades, así como emitirá las políticas, directrices, acuerdos, normativa y lineamientos necesarios para su implementación (...)”*.

Que, conforme establece el artículo 7 de la Ley Orgánica para la Transformación Digital y Audiovisual son atribuciones del ente rector de transformación digital: *“(...) b) Emitir políticas públicas, lineamientos, metodologías, regulaciones para la transformación digital, gobierno digital y evaluar su cumplimiento por parte de las entidades del sector público (...)”*;

Que, el artículo 19 de la Ley ibidem establece que: *“Gestión del Marco de Seguridad Digital. - El Marco de Seguridad Digital del Estado se tienen que observar y cumplir con lo siguiente: (...) d. Institucional: Las entidades de la Administración Pública deberán establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información”*;

Que, el artículo 20 de la Ley Orgánica para la Transformación Digital y Audiovisual señala: *“El Marco de Seguridad Digital se articula y sustenta en las normas, procesos, roles, responsabilidades y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información. La Seguridad de la Información se enfoca en la información, de manera independiente de su formato y soporte. La seguridad digital se ocupa de las medidas de la seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando generar confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno”*;

Que, artículo 38 de la Ley Orgánica de Protección de Datos Personales señala: *“El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales. El mecanismo gubernamental de seguridad de la información abarcará y aplicará a todas las instituciones del sector público, contenidas en el artículo 225 de la Constitución de la República de Ecuador, así como a terceros que presten servicios públicos mediante concesión, u otras figuras legalmente reconocidas. Estas, podrán incorporar medidas adicionales al mecanismo gubernamental de seguridad de la información”*;

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

Que, mediante el artículo 1 del Decreto Ejecutivo No. 981 de 28 de enero del 2020 se

dispuso: *“La implementación del gobierno electrónico en la Función Ejecutiva, consiste en el uso de las tecnologías de la información y comunicación por parte de las entidades para transformar las relaciones con los ciudadanos, entre entidades de gobierno y empresas privadas a fin de mejorar la calidad de los servicios gubernamentales a los ciudadanos, promover la interacción con las empresas privadas, fortalecer la participación ciudadana a través del acceso a la información y servicios gubernamentales eficientes y eficaces y coadyuvar con la transparencia, participación y colaboración ciudadana”;*

Que, mediante Decreto Ejecutivo Nro. 438 de 1 de julio de 2026 el Presidente de la República del Ecuador designó al Mgs. Ricardo Xavier Gutiérrez Cevallos como Ministro de Telecomunicaciones y de la Sociedad de la Información, Encargado;

Que, mediante Acuerdo Ministerial No. 15-2019 del 18 de julio de 2019, se expide la Política Ecuador Digital cuyo objeto es transformar al país hacia una economía basada en tecnologías digitales, mediante la disminución de la brecha digital, el desarrollo de la Sociedad de la Información y del Conocimiento, el Gobierno Digital, la eficiencia de la administración pública y la adopción digital en los sectores sociales y económicos;

Que, mediante Acuerdo Ministerial No. 020-2019 de 2 de septiembre de 2019, se expide la Política de seguridad de la información para implementar medidas preventivas y reactivas que permitan resguardar y proteger la información que reposa en las entidades de la administración pública central, institucional y que dependen de la Función Ejecutiva;

Que, mediante Acuerdo Ministerial No. MINTEL-MINTEL-2022-0031 de 2 de noviembre de 2022 se emitió la Política para la Transformación Digital del Ecuador 2022-2025, con el objetivo de: *“establecer los lineamientos para fomentar la Transformación Digital del Ecuador, considerando la investigación, desarrollo e innovación sobre infraestructuras y capacidades digitales, así como la digitalización de las empresas y servicios públicos, fomentando el uso de tecnologías emergentes, gestión de datos, seguridad de la información e interoperabilidad hacia todos los sectores sociales del país, considerando el desarrollo de un entorno normativo, regulatorio e institucional”;*

Que, mediante Acuerdo Ministerial No. MINTEL-MINTEL-2024-0003 de 8 de febrero de 2024 se expidió el Esquema Gubernamental de Seguridad de la Información -EGSI-, el cual es de implementación obligatoria en las entidades, organismos e instituciones del sector público, de conformidad con lo establecido en el artículo 225 de la Constitución de la República del Ecuador y los artículos 7 literal o), y 20 de la Ley Orgánica para la Transformación Digital y Audiovisual; y, además, es de implementación obligatoria para terceros que presten servicios públicos mediante concesión, u otras figuras legalmente reconocidas, quienes podrán incorporar medidas adicionales de seguridad de la información;

Que, mediante Memorando Nro. MINTEL-SGERC-2026-0106-M de 31 de julio de 2026, el Subsecretario de Gobierno Electrónico y Registro Civil, remitió al señor Ministro de Telecomunicaciones y de la Sociedad de la Información Encargado, el INFORME TÉCNICO QUE MOTIVA LA REFORMA DEL ACUERDO MINISTERIAL Nro.

MINTEL-MINTEL-2024-0003, ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN -EGSI-“SGERC-DIISIRC-0004-2026”, aprobado por el señor Viceministro de Tecnologías de la Información y Comunicación;

En ejercicio de las atribuciones que le confieren el numeral 1 del artículo 154 de la Constitución de la República del Ecuador; los artículos 65 y 67 del Código Orgánico Administrativo; artículos 3 y 7 de la Ley Orgánica para la Transformación Digital y Audiovisual, y el artículo 17 del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva;

ACUERDA:

Reformar el Acuerdo Ministerial No. MINTEL-MINTEL- 2024-0003 de 8 de febrero de 2024, mediante el cual se expidió el Esquema Gubernamental de Seguridad de la Información – EGSÍ.

Artículo 1.- Sustitúyase el artículo 8, por el siguiente texto:

“Artículo 8. – La máxima autoridad designará al interior de su Institución a un Oficial de Seguridad de la Información (OSI), el cual deberá tener formación y experiencia de al menos 2 años en áreas de seguridad de la información y ciberseguridad.

El OSI 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.

La designación del OSI deberá ser comunicada inmediatamente a la Subsecretaría de Gobierno Electrónico y Registro Civil del Ministerio de Telecomunicaciones y de la Sociedad de la Información, a través de las herramientas que para el efecto se utilicen”.

Artículo 2.- Sustitúyanse los anexos A) B) y C) del Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 de 8 de febrero de 2024, por los que se encuentran como anexos al presente Acuerdo Ministerial.

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

Dado en Quito, D.M. , a los 31 día(s) del mes de Julio de dos mil veintiséis.

Documento firmado electrónicamente

SR. MGS. RICARDO XAVIER GUTIÉRREZ
MINISTRO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA
INFORMACIÓN (E)



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
RICARDO XAVIER
GUTIERREZ CEVALLOS

ANEXO

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)

Versión 3.0

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

INTRODUCCIÓN

La masificación de los servicios apoyados con tecnologías de la información ha transformado a la información 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 de los servicios institucionales.

En ejercicio de sus competencias, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) ha desarrollado el Esquema Gubernamental de Seguridad de la Información (EGSI v3), como un marco técnico orientado a fortalecer la gestión de la seguridad de la información en el sector público, promoviendo un enfoque de mejora continua.

Este esquema responde a la necesidad de articular la seguridad de la información con la ciberseguridad y la protección de datos personales, permitiendo a las instituciones adoptar mecanismos efectivos para la protección de la información y el fortalecimiento de la confianza en los servicios públicos.

En este sentido, el EGSI constituye una norma técnica estructurada que establece lineamientos para la gestión de riesgos, la definición de políticas y la implementación de controles, fomentando una cultura institucional orientada a la seguridad.

El EGSI v3 se compone de tres guías fundamentales:

- 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 27001:2022).
- 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 27005:2022 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 27002:2023).

El EGSi es un recurso 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 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 PÚBLICO.

La asignación de responsabilidades se definió en los artículos 5, 6, 7, 8 y 9 del Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, sin embargo, en esta guía se aclaran 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 con 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).

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, al igual que el Delegado de Protección de Datos Personales, asistirán a las reuniones del Comité de Seguridad de la Información (CSI) 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 CSI 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 líderes/responsables de las áreas, con el fin de estimular la aprobación de políticas y normativas en relación a la Seguridad de la Información en cada institución; en las siguientes reuniones el enfoque puede orientarse a la planificación estratégica y gestión de aspectos vinculados a la seguridad de la información, por lo que se podría delegar la participación a los representantes de las respectivas áreas involucradas.

El Comité tendrá como principales responsabilidades:

- a) Establecer los objetivos de seguridad de la información, alineados a los objetivos institucionales.
 - Los objetivos de seguridad de la información deberán definirse de manera que estén alineados con los indicadores clave (KPIs) establecidos para medir la eficacia de las medidas de seguridad implementadas, garantizando así que las métricas seleccionadas respalden el logro de los objetivos organizacionales en materia de seguridad de la información.
- 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 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 EGSÍ.
- 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 EGSÍ; 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.

Oficial de Seguridad de la Información (OSI)

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

El responsable de la implementación y mejora continua del EGSÍ, 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 y experiencia de al menos 2 años en áreas de seguridad de la información y ciberseguridad.

El OSI 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.

Dentro de sus principales responsabilidades se encuentra:

- a) Identificar y conocer la estructura organizacional de la institución (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 EGSÍ:

- Identificar convenientemente las partes interesadas relacionadas con el negocio y en especial con 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 el 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 le 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 continuas relacionadas con la concienciación.*
 - *Planificar charlas de Seguridad de Información para nuevos funcionarios.*
 - *Plan de medidas disciplinarias para violaciones a la seguridad de la Información.*
- 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 políticos 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 ante el Ministerio de Telecomunicaciones y de la Sociedad de la Información.

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.

PRINCIPIOS

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

¹ Basado en la NTE-INEN-ISO-IEC-27001:2022



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 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.

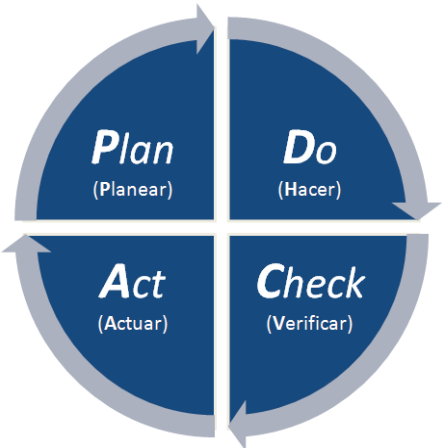


Figura No. 2 MODELO PDCA, Fuente: <https://www.jacquelinebetancourt.com/single-post/2019/03/04/Mejora-Continua-Excelencia-a-nuestro-alcance>

La relación que existe entre el modelo PDCA y la ISO 27001:2022 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	Tratamiento de riesgos de seguridad de la Información	Revisión de la Dirección	
			Información Documentada			

Figura No. 3 ESTRUCTURA PDCA-ISO27001:2022, Fuente: elaboración propia.

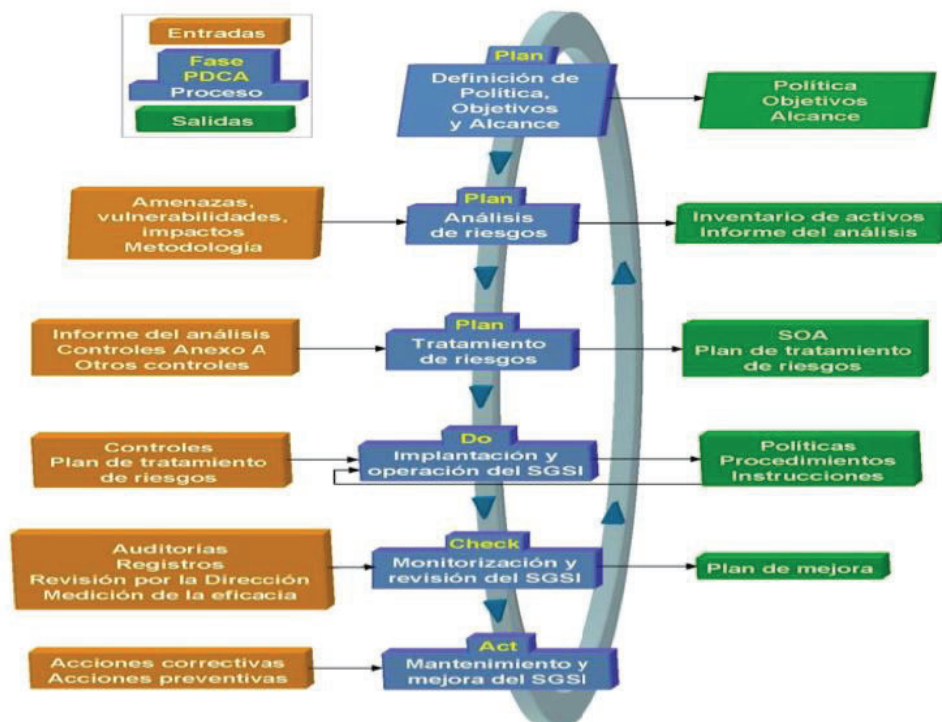
PROCESO PDCA ASOCIADO AL ESTANDAR INTERNACIONAL ISO 27001

Figura No. 4 PROCESO PDCA-ISO27001:2022, 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, iniciarán 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

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 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 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”.

El presente anexo es una guía que le proporciona a la institución una metodología para realizar la gestión de los riesgos de seguridad de la información, la cual contiene conceptos básicos y una serie de pasos o actividades que se deben realizar, esta guía se basa en la NTE INEN ISO/IEC 27005:2022 y la metodología MAGERIT.

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 uno o varios de sus principios de seguridad de la información (CID):

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

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



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

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

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.
- **Impacto:** Es la consecuencia de la materialización de una amenaza sobre un activo. El costo para la institución de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros (ejemplo: 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 SEGURIDAD DE LA INFORMACIÓN

El proceso de gestión del riesgo de 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.

El proceso de la gestión de riesgos es un proceso iterativo para las actividades de evaluación y tratamiento del riesgo, que le permitirá a la institución aumentar la probabilidad de alcanzar los objetivos planteados, cumplir con los requisitos legales y reglamentarios y a tomar decisiones adecuadas, este proceso iterativo incrementa la profundidad y el detalle de la evaluación en cada iteración.

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 riesgos².

Es posible que el tratamiento de los riesgos no conduzca inmediatamente a un nivel aceptable de riesgos residuales. En esta situación, se puede realizar otro intento para encontrar un tratamiento adicional de los riesgos, o puede haber otra iteración de la evaluación de riesgos, ya sea en su totalidad o en partes³.

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 riesgos⁴.

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

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

Tabla 1. PASOS DE LAS ACTIVIDADES DEL PROCESO DE GESTIÓN DEL RIESGO, Fuente: elaboración propia.

² Basado en la NTE-INEN-ISO-IEC-27005:2022

³ Basado en la NTE-INEN-ISO-IEC-27005:2022

⁴ Basado en la NTE-INEN-ISO-IEC-27005:2022

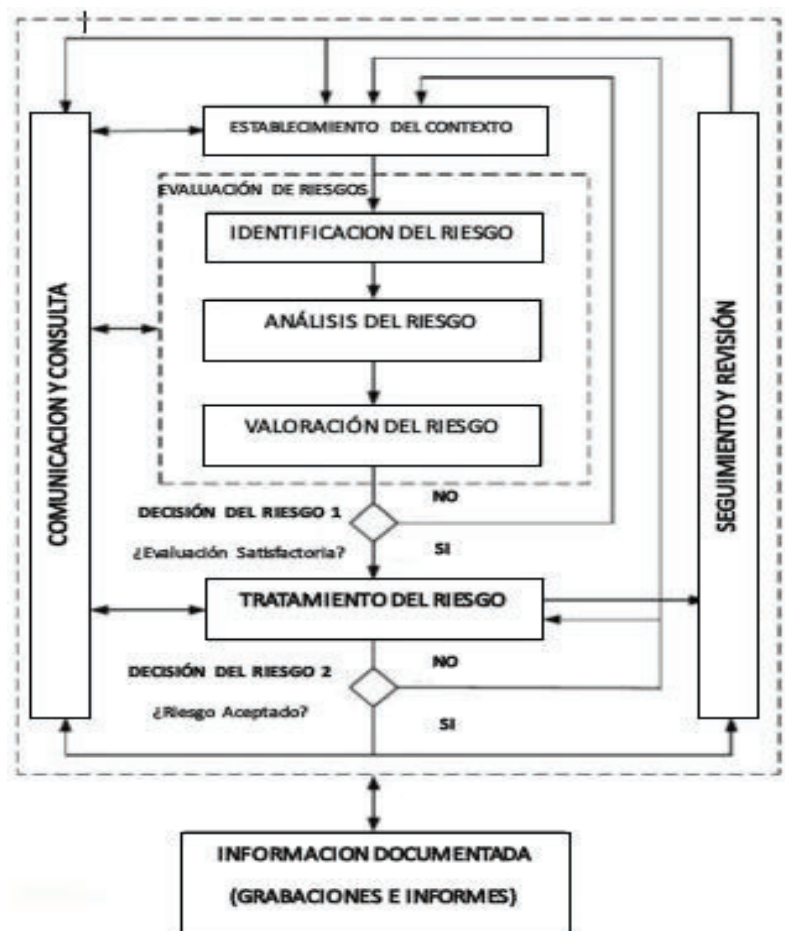


Figura No. 2 PROCESO DE GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN,
Fuente: NTE INEN ISO/IEC 27005:2022

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”.

El contexto interno y externo comprende el entorno en el que se relaciona la institución busca lograr sus objetivos.

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 seguridad de la información de la institución.

Criterios de impacto o de consecuencia

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. Además, se debe basar en el apetito de riesgo que la institución está dispuesta a retener o asumir.

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: se centra en el panorama general de amenazas de la institución, identifica eventos y sus consecuencias (activos primarios) identifica 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 alcanzar el objetivo deseado de esos riesgos. La institución se enfoca en el tratamiento de los riesgos críticos, no se realiza una identificación de activos a detalle.

Enfoque basado en activos: se centra en identificar amenazas y vulnerabilidades de los activos de soporte o apoyo, identificar escenarios operativos, es decir, la institución se enfoca en el tratamiento de riesgos a un nivel detallado.

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 con 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 software⁵.

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.

⁵ Basado en la NTE-INEN-ISO-IEC-27005:2022

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: Activos de valor para la institución

- Procesos y actividades del negocio.
- Información.

Los activos de soporte: Activos de valor en los que se soportan o residen los activos primarios:

- Hardware.
- Software.
- Redes.
- Personal.
- Ubicación.
- 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	Gestión de la infraestructura tecnológica	Monitoreo y Control	Software	Herramienta de monitoreo ZABBIX	Herramienta de monitoreo de enlaces	Director(a) de Infraestructura
A2	Coordinación General Administrativa	Unidad de Gestión Tecnológica	Software	Solución para la gestión de servicios de TI (OTRS)	Herramienta para Gestión de Incidencias, soporte técnico.	Responsable de la Unidad de Gestión Tecnológica
A3	Gestión de comunicación social	Administración y Gestión de la página web institucional	Software	Portal web institucional	Plataforma en línea para el acceso público a información relevante acerca de la institución, sus servicios, proyectos, noticias y eventos.	Director(a) de Comunicación Social
A4	Coordinación Nacional de datos ciudadanos	Dirección de cedulación	Software	Sistema de registro nacional de identificación (RENI)	Sistema que almacena los registros de los documentos de identificación	Director(a) de cedulación
A5	Gestión de la infraestructura tecnológica	Implementación de controles de seguridad informática	Hardware	Firewall	Dispositivo que monitorea y filtra el tráfico entre dos o más redes basado en políticas de seguridad.	Director(a) de Infraestructura
A6	Gestión del Talento Humano	Proceso de control interno	Software	Archivo de procesos disciplinarios	Expedientes electrónicos que contienen registros de hechos, pruebas y decisiones sobre la conducta de servidores, que son esenciales para la transparencia, la rendición de cuentas, la toma de decisiones	Director(a) de Talento Humano

					y el cumplimiento de normativas dentro de la institución.	
A7	Coordinación General Administrativa	Instalaciones	Localidad	Centro de datos	Instalación física que alberga la infraestructura de procesamiento, almacenamiento y red de la institución	Responsable de TI
A8	Coordinación General Administrativa	Talento Humano	Personal	Personal de infraestructura	Administración de la infraestructura tecnológica del ministerio	Responsable de TI
A9	Coordinación General Administrativa	Talento Humano	Personal	Personal de desarrollo de sistemas	Administración de desarrollo y mantenimiento de software	Responsable de TI

Tabla 2. IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN (Ejemplo), Fuente: elaboración propia.

Valoración de los activos / Ponderación de la criticidad de activos

La ponderación de activos es una etapa en la que participan las unidades del negocio involucradas con el fin de determinar en términos cualitativos la criticidad de los distintos activos. Esta ponderación fue realizada en términos de “alto, medio o bajo” donde se asigna un valor cuantitativo a cada valor cualitativo.

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

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.

Tabla 3. VALORACIÓN DEL IMPACTO EN TÉRMINOS DE LA PÉRDIDA DE LA CONFIDENCIALIDAD, Fuente: elaboración propia.

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

Tabla 4. VALORACIÓN DEL IMPACTO EN TÉRMINOS DE LA PÉRDIDA DE LA INTEGRIDAD, Fuente: elaboración propia.

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

Tabla 5. VALORACIÓN DEL IMPACTO EN TÉRMINOS DE LA PÉRDIDA DE LA DISPONIBILIDAD, Fuente: elaboración propia.

Con referencia a las tablas mencionadas, se realiza la valoración de impacto 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	Director(a) de Infraestructura	2	3	1	2,00
A2	Solución para la gestión de servicios de TI (OTRS)	Virtual	Responsable de la Unidad de Gestión Tecnológica	2	3	1	2,00
A3	Portal web institucional	Virtual	Director(a) de comunicación social	2	3	1	2,00
A4	Sistema de registro nacional de identificación (RENI)	Virtual	Director(a) de cedula	3	3	3	3,00
A5	Firewall	Virtual	Director(a) de Infraestructura	3	3	3	3,00
A6	Archivo de procesos disciplinarios	Virtual	Director(a) de Talento Humano	3	3	3	3,00
A7	Centro de datos	Físico y Lógico	Responsable de TI	1	1	3	1,67
A8	Personal de infraestructura	Físico	Responsable de TI	1	1	3	1,67
A9	Personal de desarrollo de sistemas	Físico	Responsable de TI	1	1	3	1,67

Tabla 6. EVALUACIÓN DE LOS ACTIVOS DE INFORMACIÓN (Ejemplo), Fuente: elaboración propia.

* La valoración del impacto de un activo (VA), es el promedio de los valores de los tres principios de 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 del activo	Amenaza
A1	Herramienta de monitoreo ZABBIX	Mal funcionamiento
		Fallo de los enlaces de comunicación
		Fallo en el suministro eléctrico
A2	Solución para la gestión de servicios de TI (OTRS)	Mal funcionamiento
		Pérdida de la información
A3	Portal web institucional	Tratamiento ilícito de datos
		Desfiguración de la página web (Defacement)
		Divulgación de información
		Denegación del servicio
A4	Sistema de registro nacional de identificación (RENI)	Tratamiento no autorizado de datos personales
		Perder conexión con los usuarios
		Ciberataques
		Accesos no autorizados
A5	Firewall	Fallo del equipo
		Fallas en el fluido eléctrico
		Fuga de información
A6	Archivo de procesos disciplinarios	Acceso no autorizado
		Fuga de información
		Alteración de documentos
		Borrado accidental o malicioso
A7	Centro de datos	Entrada no autorizada a las instalaciones
A8	Personal de infraestructura	Falta de personal
A9	Personal de desarrollo de sistemas	Explotación de aplicaciones inseguras desarrolladas por personal sin conocimientos en ciberseguridad

Tabla 7. IDENTIFICACIÓN DE AMENAZAS (Ejemplo), Fuente: elaboración propia.

Identificación de Vulnerabilidades

Se debe identificar las vulnerabilidades que pueden 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
		Fallo en el suministro eléctrico,	Sensibilidad del equipo a los cambios de voltaje
A2	Solución para la gestión de servicios de TI (OTRS)	Mal funcionamiento	Herramienta sin licencia
		Pérdida de la información	Falta de copias de seguridad / copias de seguridad incompletas
A3	Portal web institucional	Tratamiento ilícito de datos	Compartir credenciales de acceso
		Deformación de la página web (Defacement)	Pruebas de software inexistentes o insuficientes
		Divulgación de información.	Almacenamiento de contraseñas sin protección
		Denegación del servicio	Falta de actualización de parches al software base
A4	Sistema de registro nacional de identificación (RENI)	Tratamiento no autorizado de datos personales	Deficiencia en la clasificación de la información
		Perder conexión con los usuarios	La versión del aplicativo no controla varias sesiones activas
		Ciberataques	Falta de monitoreo del aplicativo
		Accesos no autorizados	Compartir credenciales de acceso
A5	Firewall	Fallo del equipo	Falta de mantenimiento
		Fallas en el fluido eléctrico	Sensibilidad del equipo a los cambios de voltaje
		Fuga de información	Cambios en la configuración sin control.
A6	Archivo de procesos disciplinarios	Acceso no autorizado	Roles desactualizados
		Fuga de información	Existen reportes que pueden ser visualizado por varias personas sin restricción
		Alteración de documentos	Almacenamiento de los archivos sin protección
		Borrado accidental o malicioso	Ausencia de registros de auditoría
A7	Centro de datos	Entrada no autorizada a las instalaciones	Protección física insuficiente del edificio
A8	Personal de infraestructura	Falta de personal	Capacidad operativa limitada para la administración, monitoreo y mantenimiento de la infraestructura
A9	Personal de desarrollo de sistemas	Explotación de aplicaciones inseguras desarrolladas por personal sin conocimientos en ciberseguridad.	Escasa conciencia y/o conocimientos de seguridad de la información y desarrollo seguro

Tabla 8. IDENTIFICACIÓN DE VULNERABILIDADES (Ejemplo), Fuente: elaboración propia.

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	VA (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
		Fallo en el suministro eléctrico	Sensibilidad del equipo a los cambios de voltaje	2,00	UPS en funcionamiento
A2	Solución para la gestión de servicios de TI (OTRS)	Mal funcionamiento	Herramienta sin licencia	2,00	Conocimiento del operador
		Pérdida de la información	Falta de copias de seguridad / copias de seguridad incompletas.	2,00	Respallos manuales
A3	Portal web institucional	Tratamiento ilícito de datos	Compartir credenciales de acceso	2,00	Registro de auditoria
		Deformación de la página web (Defacement)	Pruebas de software inexistentes o insuficientes	2,00	No se ha implementado controles
		Divulgación de información.	Almacenamiento de contraseñas sin protección.	2,00	Socialización del cuidado de credenciales
		Denegación del servicio	Falta de actualización de parches al software base	2,00	No se ha implementado controles
A4	Sistema de registro nacional de identificación (RENI)	Tratamiento no autorizado de datos personales	Deficiencia en la clasificación de la información	3,00	No se ha implementado controles
		Perder conexión con los usuarios	La versión del aplicativo no controla varias sesiones activas	3,00	Socialización de funcionalidad
		Ciberataques	Falta de monitoreo del aplicativo	3,00	Actualización de la arquitectura
		Accesos no autorizados	Compartir credenciales de acceso	3,00	Registro de auditoria
A5	Firewall	Fallo del equipo	Falta de mantenimiento	3,00	Soporte contratado
		Fallas en el fluido eléctrico	Sensibilidad del equipo a los cambios de voltaje.	3,00	UPS en funcionamiento
		Fuga de información	Cambios en la configuración sin control.	3,00	No se ha implementado controles
A6	Archivo de procesos disciplinarios	Acceso no autorizado	Roles desactualizados	3,00	Se cuenta con una Política de revisión periódica de permisos
		Fuga de información	Existen reportes que pueden ser visualizado por varias personas sin restricción	3,00	Proyecto de migración a File Server seguro
		Alteración de documentos	Almacenamiento de los archivos sin protección	3,00	Proyecto de migración a File Server seguro
		Borrado accidental o malicioso	Ausencia de registros de auditoría	3,00	Proyecto de migración a File Server seguro
A7	Centro de datos	Entrada no autorizada a las instalaciones	Protección física insuficiente del edificio	1,67	Implementación de proyecto de control de acceso biométrico
A8	Personal de infraestructura	Falta de personal	Capacidad operativa limitada para la administración, monitoreo y mantenimiento de la infraestructura	1,67	Soporte contratado

A9	Personal de desarrollo de sistemas	Explotación de aplicaciones inseguras desarrolladas por personal sin conocimientos en ciberseguridad.	Escasa conciencia y/o conocimientos de seguridad de la información y desarrollo seguro	1,67	Se cuenta con un Plan de Capacitaciones para mejoramiento de Ciber capacidades
----	------------------------------------	---	--	------	--

Tabla 9. IDENTIFICACIÓN DE CONTROLES EXISTENTES (Ejemplo), Fuente: elaboración propia.

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 RIESGO

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 10 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 descuidados	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

Tabla 10. CRITERIOS DE PROBABILIDAD DE OCURRENCIA DE AMENAZAS, Fuente: elaboración propia.

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

Tabla 11. CRITERIOS DE PROBABILIDAD DE OCURRENCIA DE VULNERABILIDADES, Fuente: elaboración propia.

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.

$$Nivel\ de\ riesgo = VA(CID) * Nivel\ de\ amenaza * Nivel\ de\ vulnerabilidad$$

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.

Tabla 12. CRITERIO DE LA EVALUACIÓN DE RIESGOS, Fuente: elaboración propia.

Ejemplo del cálculo de la evaluación de riesgos:

Análisis de Riesgos				Evaluación de Riesgos					
				Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	VA (CID)	Nivel de amenaza	Nivel de vulnerabilidad			
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
		Fallo en el suministro eléctrico.	Sensibilidad del equipo a los cambios de voltaje	2,00	1	1	UPS en funcionamiento	2,00	BAJO
A2	Solución para la gestión de servicios de TI (OTRS)	Mal funcionamiento	Herramienta sin licencia	2,00	2	2	Conocimiento del operador	8,00	MEDIO
		Pérdida de la información	Falta de copias de seguridad / copias de seguridad incompletas.	2,00	2	2	Respaldos manuales	8,00	MEDIO
A3	Portal web institucional	Tratamiento ilícito de datos	Compartir credenciales de acceso	2,00	2	2	Registro de auditoría	8,00	MEDIO
		Deformación de la página web (Defacement)	Pruebas de software inexistentes o insuficientes	2,00	2	2	No se ha implementado controles	8,00	MEDIO
		Divulgación de información.	Almacenamiento de contraseñas sin protección.	2,00	2	2	Socialización del cuidado de credenciales	8,00	MEDIO

		Denegación del servicio	Falta de actualización de parches al software base	2,00	1	2	No se ha implementado controles	4,00	MEDIO
A4	Sistema de registro nacional de identificación (RENI)	Tratamiento no autorizado de datos personales	Deficiencia en la clasificación de la información	3,00	2	2	No se ha implementado controles	12,00	ALTO
		Perder conexión con los usuarios	La versión del aplicativo no controla varias sesiones activas	3,00	2	1	Socialización de funcionalidad	6,00	MEDIO
		Ciberataques	Falta de monitoreo del aplicativo	3,00	2	1	Actualización de la arquitectura	6,00	MEDIO
		Accesos no autorizados	Compartir credenciales de acceso	3,00	2	2	Registro de auditoría	12,00	ALTO
A5	Firewall	Fallo del equipo	Falta de mantenimiento	3,00	2	1	Soporte contratado	6,00	MEDIO
		Fallas en el fluido eléctrico	Sensibilidad del equipo a los cambios de voltaje.	3,00	2	1	UPS en funcionamiento	6,00	MEDIO
		Fuga de información	Cambios en la configuración sin control.	3,00	2	1	No se ha implementado controles	6,00	MEDIO
A6	Archivo de procesos disciplinarios	Acceso no autorizado	Roles desactualizados	3,00	2	1	Se cuenta con una Política de revisión periódica de permisos	6,00	MEDIO
		Fuga de información	Existen reportes que pueden ser visualizado por varias personas sin restricción	3,00	1	1	Proyecto de migración a File Server seguro	3,00	BAJO
		Alteración de documentos	Almacenamiento de los archivos sin protección	3,00	1	1	Proyecto de migración a File Server seguro	3,00	BAJO
		Borrado accidental o malicioso	Ausencia de registros de auditoría	3,00	1	1	Proyecto de migración a File Server seguro	3,00	BAJO
A7	Centro de datos	Entrada no autorizada a las instalaciones	Protección física insuficiente del edificio	1,67	2	1	Implementación de proyecto de control de acceso biométrico	3,34	MEDIO
A8	Personal de infraestructura	Falta de personal	Capacidad operativa limitada para la administración, monitoreo y mantenimiento de la infraestructura	1,67	1	1	Soporte contratado	1,67	BAJO
A9	Personal de desarrollo de sistemas	Explotación de aplicaciones inseguras desarrolladas por personal sin conocimientos en ciberseguridad.	Escasa conciencia y/o conocimientos de seguridad de la información y desarrollo seguro	1,67	2	2	Se cuenta con un Plan de Capacitaciones para mejoramiento de Ciber capacidades	6,68	MEDIO

Tabla 13. CÁLCULO DE LA EVALUACIÓN DE RIESGOS (Ejemplo), Fuente: elaboración propia.

TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El tratamiento de los riesgos es tomar decisiones frente a los diferentes riesgos existentes de acuerdo con la estrategia de la institución. El tratamiento del riesgo implica la selección y la implementación de una o varias opciones para modificar los riesgos.

Se deben seleccionar controles para reducir, aceptar/reterner, evitar o compartir los riesgos y se debe definir un plan de gestión de riesgos (plan de 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:

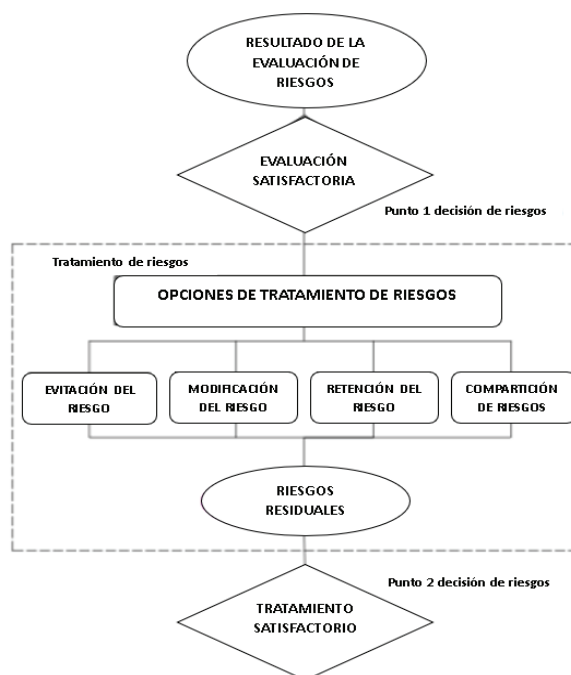


Figura No. 3 ACTIVIDADES PARA EL TRATAMIENTO DE LOS RIESGOS, Fuente: ISO27005

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:

Nro. Activo	Evaluación de Riesgos						Tratamiento de Riesgos								Riesgo residual
	Impacto	Probabilidad		Controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo									
		VA (CID)	Nivel de amenaza				Nivel de vulnerabilidad					Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado		
A1	2,00	2	2	Monitoreo continuo	8,00	MEDIO	MODIFICAR / PREVENCIÓN / 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	
A2	2,00	2	2	Conocimiento del operador	8,00	MEDIO	MODIFICAR / PREVENCIÓN / COMPARTIR	CONTROL PREVENTIVO	Instalar software gratuito	1	1	2,00	BAJO	ACEPTABLE	
	2,00	2	2	Respallos manuales	8,00	MEDIO	MODIFICAR / PREVENCIÓN / COMPARTIR	CONTROL PREVENTIVO	Política de respaldos	1	1	2,00	BAJO	ACEPTABLE	
A3	2,00	2	2	Registro de auditoria	8,00	MEDIO	MODIFICAR / PREVENCIÓN / COMPARTIR	CONTROL PREVENTIVO	Implementar Doble factor de autenticación	1	1	2,00	BAJO	ACEPTABLE	
	2,00	2	2	No se ha implementado controles	8,00	MEDIO	MODIFICAR / PREVENCIÓN / COMPARTIR	CONTROL PREVENTIVO	Endurecimiento de servidores	1	1	2,00	BAJO	ACEPTABLE	
	2,00	2	2	Socialización del cuidado de credenciales	8,00	MEDIO	MODIFICAR / PREVENCIÓN / COMPARTIR	CONTROL PREVENTIVO	Plan de socialización	2	1	4,00	MEDIO	INACEPTABLE	

	2,00	1	2	No se ha implementado controles	4,00	MEDIO	MODIFICAR / PREVENCIÓN / COMPARTIR	CONTROL PREVENTIVO	Endurecimiento de servidores	1	1	2,00	BAJO	ACEPTABLE
A4	3,00	2	2	No se ha implementado controles	12,00	ALTO	MODIFICAR / PREVENCIÓN / COMPARTIR	CONTROL CORRECTIVO	Soporte contratado	1	1	3,00	BAJO	ACEPTABLE
	3,00	2	1	Socialización de funcionalidad	6,00	MEDIO	MODIFICAR / PREVENCIÓN / COMPARTIR	CONTROL PREVENTIVO	Implementar Doble factor de autenticación	1	1	3,00	BAJO	ACEPTABLE
	3,00	2	1	Actualización de la arquitectura	6,00	MEDIO	MODIFICAR / PREVENCIÓN / COMPARTIR	CONTROL CORRECTIVO	Soporte contratado	1	1	3,00	BAJO	ACEPTABLE
	3,00	2	2	Registro de auditoría	12,00	ALTO	MODIFICAR / PREVENCIÓN / COMPARTIR	CONTROL PREVENTIVO	Soporte contratado	1	1	3,00	BAJO	ACEPTABLE
A5	3,00	2	1	Soporte contratado	6,00	MEDIO	MODIFICAR / PREVENCIÓN / COMPARTIR	CONTROL CORRECTIVO	Migrar a una solución FWaaS (firewall como servicio)	1	1	3,00	BAJO	ACEPTABLE
	3,00	2	1	UPS en funcionamiento	6,00	MEDIO	MODIFICAR / PREVENCIÓN / COMPARTIR	CONTROL CORRECTIVO	Migrar a una solución FWaaS (firewall como servicio)	1	1	3,00	BAJO	ACEPTABLE
	3,00	2	1	No se ha implementado controles	6,00	MEDIO	MODIFICAR / PREVENCIÓN / COMPARTIR	CONTROL PREVENTIVO	Implementar una Política de manejo de la configuración	1	1	3,00	BAJO	ACEPTABLE
A6	3,00	2	1	Se cuenta con una Política de revisión periódica de permisos	6,00	MEDIO	MODIFICAR / PREVENCIÓN / COMPARTIR	CONTROL PREVENTIVO	Implementar una solución de DLP (Data Loss Prevention)	1	1	3,00	BAJO	ACEPTABLE
	3,00	1	1	Proyecto de migración a File Server seguro	3,00	BAJO	RETENCIÓN	NO APLICA CONTROL		1	1	3,00	BAJO	ACEPTABLE
	3,00	1	1	Proyecto de migración a File Server seguro	3,00	BAJO	RETENCIÓN	NO APLICA CONTROL		1	1	3,00	BAJO	ACEPTABLE
	3,00	1	1	Proyecto de migración a File Server seguro	3,00	BAJO	RETENCIÓN	NO APLICA CONTROL		1	1	3,00	BAJO	ACEPTABLE
A7	1,67	2	1	Implementación de proyecto de control de acceso biométrico	3,34	MEDIO	MODIFICAR / PREVENCIÓN / COMPARTIR	CONTROL PREVENTIVO	Política de control y monitoreo de acceso al Centro de datos	1	1	1,67	BAJO	ACEPTABLE
A8	1,67	1	1	Soporte contratado	1,67	BAJO	RETENCIÓN	NO APLICA CONTROL		1	1	1,67	BAJO	ACEPTABLE
A9	1,67	2	2	Se cuenta con un Plan de Capacitaciones para mejoramiento de Ciber capacidades	6,68	MEDIO	MODIFICAR / PREVENCIÓN / COMPARTIR	CONTROL PREVENTIVO	Contratar una herramienta de análisis de código estático	1	1	1,67	BAJO	ACEPTABLE

Tabla 13. TRATAMIENTO DE LOS RIESGOS (Ejemplo), Fuente: elaboración propia.

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 y consulta se la debe llevar a cabo durante todas las actividades del proceso de la gestión de riesgos. 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.

INFORMACIÓN 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 riesgo 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.

SEGUIMIENTO Y REVISIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**SEGUIMIENTO Y REVISIÓN DE LOS FACTORES DE RIESGO**

El seguimiento y revisión se lo debe realizar durante todo el proceso de gestión de riesgos.

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 INFORMACIÓN⁶

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).

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

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

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

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

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

REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN

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

- Resultado de la evaluación de los riesgos de la institución.

⁶ Basado en la NTE-INEN-ISO-IEC-27002:2022

- Conjunto de requisitos legales, que debe cumplir la institución.
- Necesidades propias institucionales, 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”.

Estos requisitos se deben considerar para la identificación de los controles que son aplicables (necesarios) en la institución y que posteriormente se registran en el documento Declaración de aplicabilidad – (SoA).

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 tiene 93 controles de seguridad de la información, ciberseguridad y protección de los datos personales, que las instituciones deberán implementar para mitigar los riesgos identificados.

Los controles se encuentran distribuidos en 4 categorías:

- 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 diseñados para la intervención del talento humano como: concientización, acuerdos de confidencialidad, proceso disciplinario, teletrabajo, reporte de eventos de Seguridad de la Información, 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

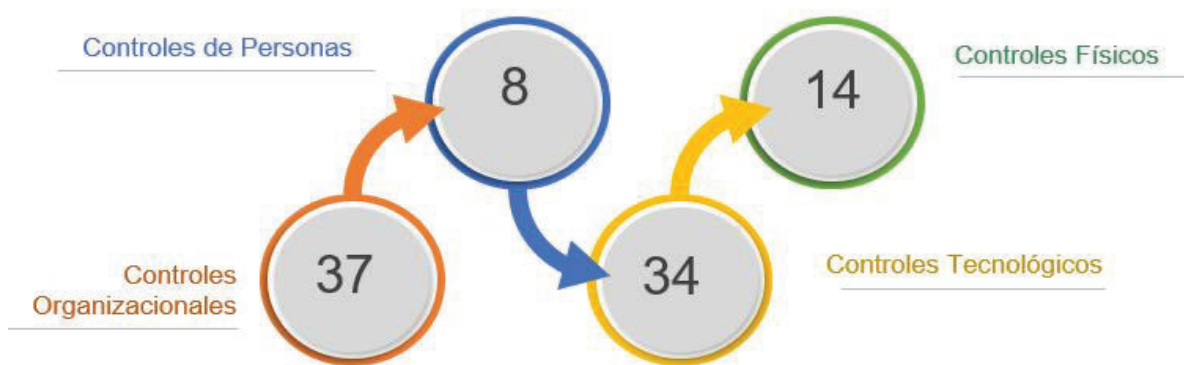


Figura No. 1 ESTRUCTURA DE LOS CONTROLES, Fuente: elaboración propia.

Cada uno de los controles en la presente guía, siguen la siguiente estructura:

- **Número de control:** inicia en uno (1) que hace referencia a la primera categoría, seguido del numeral que hace referencia al control que corresponde en dicha categoría.

Ejemplo: 1.1

- **Nombre del control:** es la descripción del control de seguridad, al cual se le ha incluido el término “documentado e implementado”, que hace referencia a que, los controles deben tener respaldos documentados y deben ser implementados.

Ejemplo: Políticas de seguridad de la información (específicas), documentado e implementado.

- **Detalle del control:** son directrices generales para la implementación del control que las instituciones deben cumplir en el proceso de implementación y/o actualización del EGSi.

Ejemplo: Las instituciones del sector público deben elaborar las políticas específicas, que se deriven de la política de seguridad de la información de alto nivel, las cuales deben ser aprobadas por el comité de seguridad de la información, publicadas, implementadas y socializadas con los funcionarios de la institución y a las partes interesadas relevantes; estas deben ser revisadas a intervalos planificados, al menos una vez al año y cuando ocurran cambios significativos dentro de la institución.

Además, en cada control se hace referencia a la Norma Técnica Ecuatoriana (NTE) INEN ISO/IEC 27002:2023, en la que se especifica las buenas prácticas de manera detallada y completa. Estas deben ser revisadas para la efectiva implementación de los controles.

El orden de la lista de controles de esta guía no implica un orden de prioridad.

ÍNDICE

1. CONTROLES ORGANIZACIONALES.....	
1.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN (ESPECÍFICAS), DOCUMENTADO E IMPLEMENTADO	
1.2. ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN, DOCUMENTADO E IMPLEMENTADO.	
1.3. SEPARACIÓN DE FUNCIONES, DOCUMENTADO E IMPLEMENTADO	
LAS INSTITUCIONES DEL SECTOR PÚBLICO DEBEN IDENTIFICAR Y SEPARAR LAS FUNCIONES ESPECIALMENTE DE SUS PROCESOS CRÍTICOS QUE PUEDAN GENERAR CONFLICTOS DE INTERÉS, CON EL FIN DE PREVENIR QUE UNA PERSONA PUEDA ACCEDER, MODIFICAR O USAR ACTIVOS SIN AUTORIZACIÓN O SIN QUE ESTO SEA DETECTADO.	
1.4. RESPONSABILIDADES DE LA DIRECCIÓN, DOCUMENTADO E IMPLEMENTADO	
1.5. CONTACTO CON LAS AUTORIDADES, DOCUMENTADO E IMPLEMENTADO	
1.6. CONTACTO CON GRUPOS DE INTERÉS ESPECIAL, DOCUMENTADO E IMPLEMENTADO	
1.7. INTELIGENCIA DE AMENAZAS, DOCUMENTADO E IMPLEMENTADO	
1.8. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS, DOCUMENTADO E IMPLEMENTADO	
1.9. INVENTARIO DE INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS, DOCUMENTADO E IMPLEMENTADO	
1.10. USO ACEPTABLE DE LA INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS, DOCUMENTADO E IMPLEMENTADO	
1.11. DEVOLUCIÓN DE ACTIVOS, DOCUMENTADO E IMPLEMENTADO.....	
1.12. CLASIFICACIÓN DE LA INFORMACIÓN, DOCUMENTADO E IMPLEMENTADO	
1.13. ETIQUETADO DE LA INFORMACIÓN, DOCUMENTADO E IMPLEMENTADO	
1.14. TRANSFERENCIA DE INFORMACIÓN, DOCUMENTADO E IMPLEMENTADO	
1.15. CONTROL DE ACCESO, DOCUMENTADO E IMPLEMENTADO	
1.16. GESTIÓN DE IDENTIDAD, DOCUMENTADO E IMPLEMENTADO	
1.17. INFORMACIÓN DE AUTENTICACIÓN, DOCUMENTADO E IMPLEMENTADO	
1.18. DERECHOS DE ACCESO, DOCUMENTADO E IMPLEMENTADO	
1.19. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON PROVEEDORES, DOCUMENTADO E IMPLEMENTADO	
1.20. ABORDAR LA SEGURIDAD DE LA INFORMACIÓN EN LOS ACUERDOS CON PROVEEDORES, DOCUMENTADO E IMPLEMENTADO	
1.21. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA CADENA DE SUMINISTRO DE LAS TIC, DOCUMENTADO E IMPLEMENTADO	
1.22. MONITOREO, REVISIÓN Y GESTIÓN DE CAMBIOS DE SERVICIOS DE PROVEEDORES, DOCUMENTADO E IMPLEMENTADO	
1.23. SEGURIDAD DE LA INFORMACIÓN PARA EL USO DE SERVICIOS EN LA NUBE, DOCUMENTADO E IMPLEMENTADO	
1.24. PLANIFICACIÓN Y PREPARACIÓN DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, DOCUMENTADO E IMPLEMENTADO	
1.25. EVALUACIÓN Y DECISIÓN SOBRE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN, DOCUMENTADO E IMPLEMENTADO	
1.26. RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, DOCUMENTADO E IMPLEMENTADO	
1.27. APRENDIENDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, DOCUMENTADO E IMPLEMENTADO	
1.28. RECOPIACIÓN DE EVIDENCIAS, DOCUMENTADO E IMPLEMENTADO	
1.29. SEGURIDAD DE LA INFORMACIÓN DURANTE LA INTERRUPCIÓN, DOCUMENTADO E IMPLEMENTADO	
1.30. PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO, DOCUMENTADO E IMPLEMENTADO	

1.31. REQUISITOS LEGALES, ESTATUTARIOS, REGLAMENTARIOS Y CONTRACTUALES, DOCUMENTADO E IMPLEMENTADO	
1.32. DERECHOS DE PROPIEDAD INTELECTUAL, DOCUMENTADO E IMPLEMENTADO	
1.33. PROTECCIÓN DE REGISTROS, DOCUMENTADO E IMPLEMENTADO	
1.34. PROTECCIÓN DE DATOS PERSONALES	
1.35. REVISIÓN INDEPENDIENTE DE SEGURIDAD DE LA INFORMACIÓN, DOCUMENTADO E IMPLEMENTADO	
1.36. CUMPLIMIENTO DE POLÍTICAS, REGLAS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN, DOCUMENTADO E IMPLEMENTADO	
1.37. PROCEDIMIENTOS OPERATIVOS, DOCUMENTADOS E IMPLEMENTADOS	
LAS INSTITUCIONES DEL SECTOR PÚBLICO DEBEN TENER CLARO QUE LA EXTENSIÓN DE LOS PROCEDIMIENTOS DEBE SER APROPIADA AL TAMAÑO Y COMPLEJIDAD DE LA INSTITUCIÓN; ES DECIR, NO SE DEBEN APLICAR PROCEDIMIENTOS MUY DETALLADOS O COMPLICADOS EN UNA INSTITUCIÓN PEQUEÑA, NI PROCEDIMIENTOS MUY SIMPLES EN UNA INSTITUCIÓN GRANDE Y COMPLEJA. ESTO CON EL PROPÓSITO DE QUE LA INSTITUCIÓN ASEGURE QUE HAYA SUFICIENTE DOCUMENTACIÓN DISPONIBLE PARA ABORDAR LAS ACTIVIDADES REPRESENTATIVAS EN EL ENTORNO DE TRABAJO DIARIO.	

2. CONTROL DE PERSONAS, DOCUMENTADO E IMPLEMENTADO

2.1. SELECCIÓN	
2.2. TÉRMINOS Y CONDICIONES DE EMPLEO, DOCUMENTADO E IMPLEMENTADO	
2.3. CONCIENCIACIÓN, EDUCACIÓN Y FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN, DOCUMENTADO E IMPLEMENTADO	
2.4. PROCESO DISCIPLINARIO, DOCUMENTADO E IMPLEMENTADO	
2.5. RESPONSABILIDADES DESPUÉS DE LA TERMINACIÓN O CAMBIO DE EMPLEO, DOCUMENTADO E IMPLEMENTADO	
2.6. ACUERDOS DE CONFIDENCIALIDAD O NO DIVULGACIÓN, DOCUMENTADO E IMPLEMENTADO	
2.7. TRABAJO REMOTO, DOCUMENTADO E IMPLEMENTADO	
2.8. INFORME DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN, DOCUMENTADO E IMPLEMENTADO	

3. CONTROLES FÍSICOS

3.1. PERÍMETROS DE SEGURIDAD FÍSICA, DOCUMENTADO E IMPLEMENTADO	
3.2. ENTRADA FÍSICA, DOCUMENTADO E IMPLEMENTADO	
3.3. SEGURIDAD DE OFICINAS, DESPACHOS E INSTALACIONES, DOCUMENTADO E IMPLEMENTADO	
3.4. MONITOREO DE SEGURIDAD FÍSICA, DOCUMENTADO E IMPLEMENTADO	
3.5. PROTECCIÓN CONTRA LAS AMENAZAS EXTERNAS Y AMBIENTALES, DOCUMENTADO E IMPLEMENTADO	
3.6. TRABAJO EN ÁREAS SEGURAS, DOCUMENTADO E IMPLEMENTADO	
3.7. PUESTO DE TRABAJO DESPEJADO Y PANTALLA LIMPIA, DOCUMENTADO E IMPLEMENTADO	
3.8. UBICACIÓN Y PROTECCIÓN DE EQUIPOS, DOCUMENTADO E IMPLEMENTADO	
3.9. SEGURIDAD DE LOS ACTIVOS FUERA DE LAS INSTALACIONES, DOCUMENTADO E IMPLEMENTADO	
3.10. MEDIOS DE ALMACENAMIENTO, DOCUMENTADO E IMPLEMENTADO	
3.11. SERVICIOS DE SOPORTE, DOCUMENTADO E IMPLEMENTADO	
3.12. SEGURIDAD DEL CABLEADO, DOCUMENTADO E IMPLEMENTADO	
3.13. MANTENIMIENTO DE EQUIPO, DOCUMENTADO E IMPLEMENTADO	
3.14. ELIMINACIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS, DOCUMENTADO E	

IMPLEMENTADO.....

4. CONTROLES TECNOLÓGICOS

- 4.1. DISPOSITIVOS FINALES DE USUARIO, DOCUMENTADO E IMPLEMENTADO.....
- 4.2. DERECHOS DE ACCESO PRIVILEGIADO, DOCUMENTADO E IMPLEMENTADO
- 4.3. RESTRICCIÓN DE ACCESO A LA INFORMACIÓN, DOCUMENTADO E IMPLEMENTADO ..
- 4.4. ACCESO AL CÓDIGO FUENTE, DOCUMENTADO E IMPLEMENTADO
- 4.5. AUTENTICACIÓN SEGURA, DOCUMENTADO E IMPLEMENTADO
- 4.6. GESTIÓN DE LA CAPACIDAD, DOCUMENTADO E IMPLEMENTADO
- 4.7. PROTECCIÓN CONTRA MALWARE, DOCUMENTADO E IMPLEMENTADO.....
- 4.8. GESTIÓN DE VULNERABILIDADES TÉCNICAS, DOCUMENTADO E IMPLEMENTADO
- 4.9. GESTIÓN DE LA CONFIGURACIÓN, DOCUMENTADO E IMPLEMENTADO
- 4.10. ELIMINACIÓN DE INFORMACIÓN, DOCUMENTADO E IMPLEMENTADO
- 4.11. ENMASCARAMIENTO DE DATOS, DOCUMENTADO E IMPLEMENTADO.....
- 4.12. PREVENCIÓN DE FUGA DE DATOS, DOCUMENTADO E IMPLEMENTADO
- 4.13. COPIA DE SEGURIDAD DE LA INFORMACIÓN, DOCUMENTADO E IMPLEMENTADO ..
- 4.14. REDUNDANCIA DE LAS INSTALACIONES DE TRATAMIENTO DE INFORMACIÓN,
DOCUMENTADO E IMPLEMENTADO
- 4.15. REGISTRO DE EVENTOS, DOCUMENTADO E IMPLEMENTADO
- 4.16. ACTIVIDADES DE MONITOREO, DOCUMENTADO E IMPLEMENTADO
- 4.17. SINCRONIZACIÓN DEL RELOJ, DOCUMENTADO E IMPLEMENTADO
- 4.18. USO DE PROGRAMAS DE UTILIDAD PRIVILEGIADOS, DOCUMENTADO E
IMPLEMENTADO.....
- 4.19. INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS, DOCUMENTADO E
IMPLEMENTADO.....
- 4.20. SEGURIDAD DE REDES, DOCUMENTADO E IMPLEMENTADO.....
- 4.21. SEGURIDAD DE LOS SERVICIOS DE RED, DOCUMENTADO E IMPLEMENTADO
- 4.22. SEPARACIÓN EN LAS REDES, DOCUMENTADO E IMPLEMENTADO
- 4.23. FILTRADO WEB, DOCUMENTADO E IMPLEMENTADO
- 4.24. USO DE CRIPTOGRAFÍA, DOCUMENTADO E IMPLEMENTADO
- 4.25. CICLO DE VIDA DE DESARROLLO SEGURO, DOCUMENTADO E IMPLEMENTADO ..
- 4.26. REQUISITOS DE SEGURIDAD DE LA APLICACIÓN, DOCUMENTADO E
IMPLEMENTADO.....
- 4.27. ARQUITECTURA DEL SISTEMA SEGURO Y PRINCIPIOS DE INGENIERÍA,
DOCUMENTADO E IMPLEMENTADO
- 4.28. CODIFICACIÓN SEGURA, DOCUMENTADO E IMPLEMENTADO
- 4.29. PRUEBAS DE SEGURIDAD Y ACEPTACIÓN EN EL DESARROLLO, DOCUMENTADO E
IMPLEMENTADO.....
- 4.30. DESARROLLO SUBCONTRATADO, DOCUMENTADO E IMPLEMENTADO
- 4.31. SEPARACIÓN DE LOS ENTORNOS DE DESARROLLO, PRUEBAS Y PRODUCCIÓN,
DOCUMENTADO E IMPLEMENTADO
- 4.32. GESTIÓN DE CAMBIOS, DOCUMENTADO E IMPLEMENTADO
- 4.33. INFORMACIÓN DE PRUEBA, DOCUMENTADO E IMPLEMENTADO
- 4.34. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN DURANTE LAS PRUEBAS DE
AUDITORÍA, DOCUMENTADO E IMPLEMENTADO

GLOSARIO DE TÉRMINOS

TÉRMINOS ABREVIADOS

FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN ¡ERROR! MARCADOR NO DEFINIDO.

CONTROLES ORGANIZACIONALES

1.1. Políticas de seguridad de la información (específicas), documentado e implementado

Las instituciones del sector público deben elaborar las políticas específicas, que se deriven de la política de seguridad de la información de alto nivel, las cuales deben ser aprobadas por el comité de seguridad de la información, publicadas, implementadas y socializadas con los funcionarios de la institución y a las partes interesadas relevantes; estas deben ser revisadas a intervalos planificados, al menos una vez al año y cuando ocurran cambios significativos dentro de la institución.

Las políticas específicas se enfocan en áreas o temas particulares, y deben estar alineadas con el contexto organizacional, los riesgos identificados y los requisitos legales y regulatorios aplicables en la institución, ejemplo de políticas específicas: Uso aceptable de la información y otros activos asociados, clasificación de la información, control de acceso, y protección de los datos personales, entre otros.

La mejora continua del control se puede lograr integrando este conjunto de políticas específicas dentro de la política de seguridad de la información macro o de alto nivel, lo que se denomina Manual de Políticas de Seguridad de la Información, integrándolas al sistema de gestión de seguridad de la información, lo cual constituye un instrumento completo y organizado que da las pautas o directrices para gestionar la seguridad de la información en la institución.

La NTE INEN ISO/IEC 27002:2023, 5.1 proporciona más orientación sobre las directrices para las políticas de seguridad de la información.

1.2. Roles y Responsabilidades de Seguridad de la Información, documentado e implementado.

Las instituciones del sector público deben asignar y documentar los roles y responsabilidades de los actores claves que conforman la estructura organizacional de seguridad de la información (Máxima autoridad, Comité de seguridad de la información, Oficial de Seguridad de la Información), incluyendo las del personal y partes interesadas, acorde a lo establecido en el acuerdo ministerial con la que se expide este documento y a las políticas de seguridad de la información de cada institución.

A continuación se enuncia los roles y responsabilidades de seguridad de la información que las instituciones deben cumplir:

- Máxima autoridad: se detallan en el Artículo 5
- Comité de Seguridad de la Información: se detallan en el Artículo 7
- Oficial de Seguridad de la Información: se detallan en el Artículo 9
- Funcionarios y partes interesadas: se establecerán acorde a las propias necesidades institucionales, las cuales deben ser socializadas y cumplidas con lo establecido en las políticas.

La NTE INEN ISO/IEC 27002:2023, 5.2 proporciona más orientación sobre las directrices para el establecimiento de roles y responsabilidades.

1.3. Separación de Funciones, documentado e implementado

Las instituciones del sector público deben identificar y separar las funciones especialmente de sus procesos críticos que puedan generar conflictos de interés, con el fin de prevenir que una persona pueda acceder, modificar o usar activos sin autorización o sin que esto sea detectado.

En el caso de instituciones en donde los recursos son limitados y resulte difícil la separación de funciones, y una persona puede tener múltiples responsabilidades; considerar el registro de las actividades esenciales y la revisión periódica por personas independientes (ej. comité de seguridad de la información).

La NTE INEN ISO/IEC 27002:2023, 5.3, proporciona más orientación sobre las medidas que se deben tomar en cuenta para la separación de funciones.

1.4. Responsabilidades de la dirección, documentado e implementado

La dirección en la implementación del EGSI es representada por: la máxima autoridad, comité de seguridad de la información, y todo el Nivel jerárquico superior, quienes deben demostrar su compromiso con la seguridad de la información.

La máxima autoridad deberá:

- Conformar la estructura de seguridad de la información institucional (actores y responsabilidades para la seguridad de la información).
- Designar formalmente al Oficial de Seguridad de la Información y a los miembros del comité de seguridad de la información.
- Disponer el cumplimiento de la implementación y mejora continua del EGSI, mediante la difusión, capacitación, formación y sensibilización del contenido de este documento.
- Aprobar la política de seguridad de la información de alto nivel.
- Asignar recursos antes, durante y después de la implementación del EGSI.
- Tomar conocimiento de los riesgos y disponer su monitoreo y gestión.

El Comité de Seguridad de la Información deberá:

- Cumplir con las responsabilidades mencionadas en el Artículo 9 del Acuerdo Ministerial con el que se expide este documento.

Los funcionarios del Nivel Jerárquico superior deben:

- Asegurar el cumplimiento de las normas legales dentro de sus competencias.
- Cumplir con las responsabilidades designadas a su área.
- Cumplir con lo solicitado por el comité de seguridad de la información a través del Oficial de Seguridad de la Información.
- Implementar los controles de seguridad correspondientes a su área.
- Otras responsabilidades inmersas en los controles de seguridad.

La NTE INEN ISO/IEC 27002:2023, 5.4, proporciona más orientación sobre las responsabilidades de la dirección.

1.5. Contacto con las autoridades, documentado e implementado

Las instituciones del sector público deben establecer un procedimiento para identificar y establecer los enlaces necesarios con entidades relevantes (por ejemplo: CSIRT del Ecuador, CSIRT sectoriales, fiscalía, policía, Superintendencia de Protección de Datos Personales, servicios de emergencia, proveedores de energía eléctrica, proveedores de bienes o servicios de telecomunicaciones o de acceso a Internet, entre otros), para

informar o reportar incidentes derivados del incumplimiento de la política de seguridad, cumplimiento de requisitos legales, colaboración ante situaciones críticas, entre otros.

La NTE INEN ISO/IEC 27002:2023, 5.5, proporciona más orientación sobre las consideraciones del control.

1.6. Contacto con grupos de interés especial, documentado e implementado

Las instituciones del sector público deben establecer contactos pertinentes con instituciones, asociaciones profesionales, foros y organismos internacionales en materia de seguridad de la información y ciberseguridad, con el fin de fortalecer las habilidades y capacidades del OSI y el equipo relacionado con actividades de seguridad de la información.

La NTE INEN ISO/IEC 27002:2023, 5.6, proporciona más orientación sobre las consideraciones del control.

1.7. Inteligencia de amenazas, documentado e implementado

Las instituciones del sector público deben elaborar un proceso formal, para analizar y recopilar la información de las amenazas de seguridad, con el fin de producir inteligencia de amenazas que permitan tomar decisiones sobre riesgos que aún no se han materializado, pero es probable que ocurran.

Para la implementación del control se recomienda conformar un equipo con personal interno que realice dicho análisis, caso contrario podrán externalizar este servicio.

Para el caso de instituciones que cuenten con recursos limitados podrían obtener la información de fuentes externas.

La NTE INEN ISO/IEC 27002:2023, 5.7, proporciona más orientación sobre las recomendaciones de implementación del control.

1.8. Seguridad de la información en la Gestión de proyectos, documentado e implementado

Las instituciones del sector público deben contemplar la seguridad de la información dentro de la gestión de todo tipo de proyecto, integrando prácticas, definición de políticas y controles, gestión de riesgos y consideraciones o requisitos específicas, desde la fase inicial hasta la culminación del proyecto, con el fin de garantizar la confidencialidad, integridad y disponibilidad de los datos, activos involucrados y el cumplimiento de los estándares de seguridad y normativa establecidos por la institución.

La NTE INEN ISO/IEC 27002:2023, 5.8, proporciona más orientación sobre la lista de temas específicos a considerar para implementar el control.

1.9. Inventario de información y otros activos asociados, documentado e implementado

Las instituciones del sector público deben identificar, documentar y mantener actualizado el inventario de activos de información y otros activos asociados (hardware, software, máquinas virtuales, instalaciones, personal, otros), el mismo que deberá estar clasificado de acuerdo con su valor e impacto y asegurando la identificación de los propietarios de dichos activos.

Considerar la siguiente información al momento de realizar el inventario: proceso macro, subproceso al que pertenece el activo, tipo de activo, descripción del activo, propietario, ubicación. Otros: fabricante, código de serie, modelo, fecha de adquisición, clasificación, etiquetado (cuando corresponda).

Inventario:

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.

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, cámara web, etc.
- Periféricos de salida: monitor, proyector, audífonos, parlantes, impresoras, etc.
- Periféricos y dispositivos de almacenamiento: sistema de almacenamiento (NAS, SAN), 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.

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, video conferencia, servidor (proxy, de archivos, de correo electrónico, de impresiones, de mensajería instantánea, de aplicaciones, de base de datos), etc.
- Aplicativos informáticos de la institución.

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/prevencción de intrusos (IDS/IPS), firewall de aplicaciones web, balanceadoras de carga, switch de contenido, etc.

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, 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.

1.10. Uso aceptable de la información y otros activos asociados, documentado e implementado

Las instituciones del sector público deben establecer, documentar y socializar la política de uso aceptable para el manejo de la información y otros activos asociados, 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 las instituciones.

Al menos deberían considerarse reglamentar el uso de los siguientes activos:

- Correo electrónico institucional
- Acceso y uso de la Internet y sus aplicaciones/servicios:

Correo electrónico institucional:

Servicio que 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.
- 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 personal (Gmail, Yahoo, Hotmail, entre otros), sitios de almacenamiento (WeTransfer, Google Drive, OneDrive, Dropbox, entre otros); gratuitos y de libre uso.

Acceso y uso de la Internet y sus aplicaciones/servicios:

- El Oficial de Seguridad de la Información en coordinación con el área tecnológica, se 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.

Para activos externos como el caso de almacenamiento en la nube pública, se debería mantener al menos acuerdos con los proveedores (Niveles de servicio, de confidencialidad, otros).

La NTE INEN ISO/IEC 27002:2023, 5.10, proporciona una orientación amplia que se debe considerar para implementar el control.

1.11. Devolución de activos, documentado e implementado

Las instituciones del sector público garantizaran que previo a la desvinculación o cambio de los funcionarios, todos los activos de información (equipos informáticos, documentos físicos, acceso a sistemas, otros), de la institución que estén a su cargo sean devueltos o sean dados de baja de manera segura al finalizar su uso, lo cual deberá estar documentado y los responsables del proceso deben asegurarse del cumplimiento de los lineamientos establecidos.

La NTE INEN ISO/IEC 27002:2023, 5.11, proporciona más orientación de que se debe considerar para implementar el control.

1.12. Clasificación de la información, documentado e implementado

Las instituciones del sector público deben establecer una política para la clasificación de la información, en la que se determine niveles de clasificación acorde a su valor y criticidad y siguiendo el conjunto de normativas legales vigentes como:

- Ley Orgánica de Transparencia y Acceso a la Información Pública – LOTAIP.
- Regla Técnica de gestión documental y archivo para la clasificación de documentos.
- Ley Orgánica de Protección de Datos Personales – LOPDP.
- Ley de Seguridad Pública y del Estado, para instituciones que formen parte del sistema de seguridad pública y del Estado y del sistema nacional de inteligencia, la información se clasifica también en: Reservada, Secreta, Secretísima.
- Otras relacionadas.

La clasificación de la información debe basarse en las necesidades de seguridad de la información de cada institución.

La norma NTE INEN ISO/IEC 27002:2023, 5.12, proporciona orientación sobre más consideraciones a tomar en cuenta para la clasificación de información.

1.13. Etiquetado de la información, documentado e implementado

Las instituciones del sector público, una vez identificado y clasificado la información deberá establecer y documentar procedimientos que aseguren que la información sea etiquetada de acuerdo con la clasificación definida por la institución, facilitando así su manejo seguro.

Además, se debe proporcionar capacitación y concienciación a todos los funcionarios y otras partes interesadas sobre la importancia del etiquetado de la información y cómo deben manejar la información de acuerdo con los niveles de clasificación establecidos.

La NTE INEN ISO/IEC 27002:2023, 5.13, proporciona orientación de recomendaciones para etiquetar la información.

1.14. Transferencia de información, documentado e implementado

Las instituciones del sector público deben documentar políticas y procedimientos robustos que permitan asegurar la transferencia de información interna y externa (aplicaciones de mensajería instantánea, redes sociales, otros), para esto utilizar acuerdos de transferencia de información.

La NTE INEN ISO/IEC 27002:2023, 5.14, proporciona más orientación acerca de los controles que permitan asegurar la transferencia de la información institucional.

1.15. Control de acceso, documentado e implementado

Las instituciones del sector público elaborarán, implementarán y socializarán una 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 que permitan supervisar las actividades de los usuarios y detectar posibles comportamientos anómalos. El enfoque principal es el control general del acceso a sistemas y datos, es decir, “quien accede a que”.

La NTE INEN ISO/IEC 27002:2023, 5.15, proporciona más orientación acerca de las reglas basadas en el principio de mínimo privilegio para el control de acceso.

1.16. Gestión de identidad, documentado e implementado

Las instituciones del sector público elaborarán, implementarán y socializarán un procedimiento para gestionar el ciclo de vida de las identidades digitales para que estas sean únicas, y se vinculen a una sola persona con el fin de mantener un registro de las acciones realizadas. El enfoque principal del control es la administración del ciclo de vida de las identidades, es decir, creación, modificación y desactivación de identidades digitales.

La NTE INEN ISO/IEC 27002:2023, 5.16, proporciona más orientación para mantener un adecuado nivel de confianza bajo un esquema de gestión de los riesgos identificados.

1.17. Información de autenticación, documentado e implementado

Las instituciones del sector público establecerán políticas específicas y claras para la gestión de la información de autenticación como la asignación de credenciales, requisitos de contraseñas seguras y su responsabilidad de uso. El enfoque principal es la protección de los datos de autenticación, es decir; contraseñas, PINs, claves secretas, otras.

La NTE INEN ISO/IEC 27002:2023, 5.17, proporciona más orientación acerca del manejo y la gestión adecuada de la información de autenticación.

1.18. Derechos de acceso, documentado e implementado

Las instituciones del sector público establecerán procedimientos específicos para otorgar, modificar y revocar derechos de acceso a sistemas de información y servicios (de preferencia basado en roles y con el principio del menor privilegio). El enfoque principal del control es la asignación y control de los permisos sobre activos; es decir, que privilegios o roles tiene cada identidad.

La NTE INEN ISO/IEC 27002:2023, 5.18, proporciona más orientación acerca de los mecanismos adecuados para proporcionar derechos de acceso.

1.19. Seguridad de la información en las relaciones con proveedores, documentado e implementado

Las instituciones del sector público deben identificar y evaluar los riesgos asociados a cada relación laboral con los proveedores, así como también documentar políticas y/o procedimientos relacionados.

La NTE INEN ISO/IEC 27002:2023, 5.19, proporciona más orientación acerca de las medidas de seguridad con proveedores, considerar también los principios mencionados en las normas de control interno de la Contraloría General del Estado, Ley Orgánica de Protección de Datos Personales con su reglamento y demás normativa relacionada.

1.20. Abordar la seguridad de la información en los acuerdos con proveedores, documentado e implementado

Las instituciones del sector público establecerán los requisitos de seguridad de la información necesarios que deben ser establecidos, registrados y consensuados en los acuerdos con los proveedores (contratos, acuerdos de niveles de servicios, otros), adaptándose al tipo de relación que se establezca.

La NTE INEN ISO/IEC 27002:2023, 5.20, proporciona más orientación acerca de los mecanismos adecuados para abordar la seguridad de la información en los acuerdos con los proveedores.

1.21. Gestión de seguridad de la información en la cadena de suministro de las TIC, documentado e implementado

Las instituciones del sector público establecerán y documentarán procesos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC (Ejemplos: fabricantes de hardware y software, servicios de infraestructura y nube, integradores de sistemas y otros terceros que no mantienen relación directa con la institución).

La NTE INEN ISO/IEC 27002:2023, 5.21, proporciona más orientación acerca de la identificación y requisitos de seguridad de la información en las cadenas de suministro.

1.22. Monitoreo, revisión y gestión de cambios de servicios de proveedores, documentado e implementado

Las instituciones del sector público realizarán un monitoreo continuo de los servicios de los proveedores y sus cambios con el objetivo de mantener un entorno seguro y confiable para la información de la institución; para lo cual deben implementar procedimientos para supervisar la prestación del servicio y revisar los informes elaborados por los proveedores.

La NTE INEN ISO/IEC 27002:2023, 5.22, proporciona más orientación acerca de la identificación y requisitos de seguridad de la información en las cadenas de suministro.

1.23. Seguridad de la información para el uso de servicios en la nube, documentado e implementado

Las instituciones del sector público deben documentar e implementar una política que considere lineamientos específicos para el contrato y uso de los servicios en la nube (monitoreo uso de servicios, manejo de incidentes, cambios, capacidades, controles de seguridad). Considerar lo establecido en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2023-0015 y sus actualizaciones.

La NTE INEN ISO/IEC 27002:2023, 5.23, proporciona más orientación acerca de los aspectos de seguridad de la información a considerar para el uso de los servicios de la nube.

1.24. Planificación y preparación de la gestión de incidentes de seguridad de la información, documentado e implementado

Las instituciones del sector público deben implementar y documentar políticas, procedimientos y planes para la Gestión de Incidentes en el cual consten los roles y responsabilidades, notificaciones y comunicación, así como un programa de pruebas y revisión.

Este control hace referencia a las acciones que una institución debe tomar, antes de que ocurra un incidente; con el objetivo de estar preparados para brindar una respuesta a incidentes de seguridad de la información.

La NTE INEN ISO/IEC 27002:2023, sección 5.24, describe los procedimientos que deben implementarse para gestionar y recuperarse de fallos del sistema, errores, brechas de seguridad; incluyendo medidas de contingencia y actividades de auditoría que las instituciones deben considerar.

1.25. Evaluación y decisión sobre eventos de seguridad de la información, documentado e implementado

Las instituciones del sector público deben establecer y documentar un procedimiento para identificar, analizar, clasificar, evaluar y responder a eventos de seguridad de la

información; pues este control permite analizar eventos de seguridad, clasificarlos y decidir si es un incidente o no.

La NTE INEN ISO/IEC 27002:2023, 5.25, proporciona más orientación acerca de la evaluación y decisión sobre eventos de seguridad de la información.

1.26. Respuesta a incidentes de seguridad de la información, documentado e implementado

Las instituciones del sector público deben establecer como punto de contacto al Oficial de Seguridad de la Información y una línea de reporte clara para responder ante los incidentes, las actividades deben estar debidamente documentadas en los procedimientos; considerar que, los registros de incidentes deben demostrar que se ejerce un control de gestión adecuado.

Este control establece como actuar ante incidentes reales, de manera conjunta con el control 1.25 y 1.26 son parte del ciclo completo de gestión de incidentes.

La NTE-INEN ISO/IEC 27002:2023, sección 5.26, proporciona una lista de acciones que se deben llevar a cabo en las instituciones, para gestionar adecuadamente los incidentes de seguridad de la información.

1.27. Aprendiendo de los incidentes de seguridad de la información, documentado e implementado

Las instituciones del sector público deben establecer un proceso que contemple una bitácora para el aprendizaje de los incidentes, con el fin de evitar que se repitan en el futuro y en el caso de que no se puedan evitar, se logre abordar con mayor eficacia. Es importante tener presente que este proceso ayuda a identificar dónde los controles no funcionaron según lo previsto y dónde se requieren mejoras.

La NTE INEN ISO/IEC 27002:2023, sección 5.27, proporciona buenas prácticas que se deben considerar para este proceso.

1.28. Recopilación de evidencias, documentado e implementado

Las instituciones del sector público deben asegurar que cuando se requiera recopilar evidencia digital en respuesta a un incidente de seguridad o para cualquier investigación con fines legales, estas deben mantener la cadena de custodia para que ninguna persona pueda modificar o destruirla; para esto, dicho proceso debe estar documentado.

La NTE INEN ISO/IEC 27002:2023, sección 5.28, describe los factores que deben tenerse en cuenta al elaborar los procedimientos para la recopilación de pruebas.

La NTE INEN ISO/IEC 27037:2019 proporciona definiciones y directrices para la identificación, recopilación, adquisición y preservación de evidencia digital, que se deberían considerar.

1.29. Seguridad de la información durante la interrupción, documentado e implementado

Las instituciones del sector público deben incluir la seguridad de la información como parte de sus Planes de Continuidad de Negocio, Recuperación de Desastres u otros, con el propósito de mantener la seguridad en un nivel adecuado durante interrupciones de cualquier tipo, para una rápida recuperación y la mitigación de los riesgos.

La NTE INEN ISO/IEC 27002:2023, sección 5.29, describe buenas prácticas para mantener o restaurar la seguridad de la información luego de una interrupción que las instituciones deberían considerarlas.

1.30. Preparación de las TIC para la continuidad del negocio, documentado e implementado

Las instituciones del sector público deben garantizar que se ejecuten pruebas al menos de los sistemas críticos y los modos de falla probables, los hallazgos se deben utilizar para mejorar la eficacia; para esto, se deberá mantener los registros de las pruebas de continuidad de las TIC.

La NTE INEN ISO/IEC 27002:2023, sección 5.30, enumera los aspectos que deben tenerse en cuenta para la preparación de las TIC para la continuidad del negocio. Existe diferentes estándares en el campo de la continuidad del negocio que las instituciones del sector público deben considerarlos para el diseño e implementación de procesos estructurados.

1.31. Requisitos legales, estatutarios, reglamentarios y contractuales, documentado e implementado

Las instituciones del sector público deben identificar, documentar y cumplir con todos los requisitos legales, reglamentarios y contractuales aplicables; además, para la actualización de estos requisitos y la identificación de los controles implementados el área jurídica y el OSI trabajarán en conjunto.

Considerar entre otras, la siguiente normativa:

- 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.

La NTE INEN ISO/IEC 27002:2023, sección 5.31, enumera los aspectos que deben tenerse en cuenta al crear políticas y procedimientos relacionados.

1.32. Derechos de propiedad intelectual, documentado e implementado

Las instituciones del sector público deben establecer directrices para que se respeten y protejan adecuadamente los derechos de propiedad intelectual en el contexto de la seguridad de la información, pues existe un grave riesgo de que se emprendan acciones legales contra la institución y/o sus funcionarios, en caso de una infracción.

La NTE INEN ISO/IEC 27002:2023, 5.32 proporciona directrices sobre la protección de los derechos de autor que las instituciones deben considerar.

1.33. Protección de registros, documentado e implementado

Las instituciones del sector público deben mantener un inventario de los registros esenciales, como: registros contables, registros de bases de datos, registros de transacciones, registros de auditoría y procedimientos operativos, que se requiere conservar y que deben protegerse contra pérdidas y violaciones de la confidencialidad

e integridad; de acuerdo con los plazos establecidos en la normativa legal vigente que corresponda a las actividades de la institución.

La NTE INEN ISO/IEC 27002:2023, sección 5.33, proporciona más orientación sobre la protección de los registros institucionales.

1.34. Protección de datos personales

Las instituciones del sector público deben cumplir con las obligaciones establecidas en la Ley Orgánica de Protección de Datos Personales (LOPD), su reglamento, y toda la normativa secundaria emitida por la Superintendencia de Protección de Datos Personales. Considerando que la seguridad de la información es un componente esencial para la protección de datos personales, la implementación del EGSI es útil, pero no es suficiente. No obstante, una implementación eficaz y eficiente del EGSI contribuye significativamente a la conformidad en protección de datos personales.

Consecuentemente, las instituciones públicas deberán integrar el EGSI con los principios establecidos en la guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales de la Superintendencia de Protección de Datos Personales, los cuales son resumidos a continuación:

a) Gestión de riesgos para la protección de derechos y libertades. El EGSI está enfocado a la gestión de riesgos de seguridad de la información. Por ello, es necesario realizar una gestión de riesgos para la protección de derechos y libertades que estime el impacto que pueden sufrir los titulares de los datos personales, en caso de que un riesgo se materialice. Esto incluye a riesgos primordialmente jurídicos, y riesgos de seguridad de datos personales. La gestión de riesgos para la protección de derechos y libertades es fundamental para poder realizar la evaluación de impacto del tratamiento de datos personales.

b) Integración de la gestión de riesgos para la protección de derechos y libertades con la gestión riesgos de seguridad de la información. La seguridad de la información y la protección de datos personales son interdependientes. La gestión de riesgos de seguridad de la información tiene como finalidad proteger los activos de la institución. La gestión de riesgos para la protección de derechos y libertades tiene como finalidad proteger los derechos y libertades de los titulares de los datos. No obstante, un mismo riesgo de seguridad de la información que impacta en los activos de la institución, también puede vulnerar los derechos y libertades de los titulares de los datos. Es fundamental integrar ambas gestiones de riesgos a partir de métricas y modelos interdependientes.

c) Rol de los estándares de mejores prácticas. El EGSI equivale a un estándar de mejores prácticas de seguridad de la información, para las instituciones públicas del Ecuador. El EGSI toma como referencia la NTE INEN ISO/IEC 27001:2022, para la implementación de sistemas de gestión de seguridad de la información. No obstante, hay que complementarlo con otros estándares de mejores prácticas en el ámbito de la implementación de sistemas de gestión de protección de datos personales, tales como la NTE INEN ISO/IEC 27701:2021, y las guías de seguridad en el tratamiento de datos personales emitidas por la Superintendencia de Protección de Datos Personales.

d) Justificación de todos los racionales. Es fundamental desarrollar métricas que justifiquen los valores ingresados en la etapa de evaluación de riesgos del EGSI. Los racionales utilizados en la gestión de riesgos de seguridad de la información obtenidos en el EGSI, pueden ser también útiles para realizar una gestión de riesgos para la protección de derechos y libertades, pues un riesgo contra los activos de la institución puede ser también un riesgo para los derechos y libertades de los titulares de datos

personales.

e) Conformidad en riesgos. Para conformarse a la Ley Orgánica de Protección de Datos Personales es necesario aplicar el principio de conformidad en riesgos. Esto quiere decir que la finalidad de una gestión de riesgos es reducir la incertidumbre para tomar decisiones informadas en la protección de los derechos y libertades de los titulares de datos personales. Para que la gestión de riesgos de seguridad de la información sea útil en la conformidad a la LOPDP, la implementación del EGSI debe seguir el mismo principio de protección en la práctica, priorizando la objetividad en los datos, métricas, y modelos utilizados en la gestión de riesgos.

f) Auditorías. Consiste en realizar auditorías jurídicas, organizacionales y técnicas, para la protección de los derechos y libertades de los titulares de los datos. La finalidad es el 'ser' y no sólo el 'deber ser' para todas las obligaciones establecidas en la LOPDP, su reglamento y la normativa emitida por la Superintendencia de Protección de Datos Personales. Estas auditorías o evaluaciones pueden ser internas o externas de acuerdo a lo establecido en el EGSI, y otros estándares de mejores prácticas en gestión de la protección de datos personales como la NTE INEN ISO/IEC 27701:2021. Especial consideración debe darse a las auditorías o evaluaciones técnicas, considerando que los riesgos de seguridad de datos usualmente no son visibles. Es fundamental identificar los riesgos de terceros provenientes de las dependencias del software, y de la interacción con interfaces de programación de aplicaciones.

g) Vulneraciones de la seguridad de datos personales. Las dimensiones de la seguridad de datos personales son las mismas que las de la seguridad de la información, es decir: confidencialidad, integridad y disponibilidad. Esto quiere decir, que una implementación eficaz y eficiente del EGSI, y sobre todo, una gestión de riesgos de seguridad de la información que cumpla con estos principios, es útil para la conformidad a la LOPDP. No obstante, la evaluación de impacto del tratamiento de datos personales debe enfocar estos principios desde la perspectiva del impacto que pueden sufrir los titulares de datos personales.

Las instituciones del sector público deben nombrar un Delegado(a) de Protección de datos, quien 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; este delegado(a) no podrá ser el Oficial de Seguridad de la Información. El Oficial de Seguridad de la Información entregará los reportes de la gestión de riesgos de seguridad de la información (generados en su gestión) al Delegado(a) de Protección de Datos, como insumo para la evaluación de impacto del tratamiento de datos personales.

Las validaciones y verificaciones del cumplimiento de las obligaciones establecidas por el Delegado(a) de Protección de Datos Personales serán las del Reglamento del Delegado de Protección de Datos Personales.

1.35. Revisión independiente de seguridad de la información, documentado e implementado

Las instituciones del sector público deben revisar periódicamente las actividades de seguridad de la información y sobre todo la implementación del Esquema Gubernamental de Seguridad de la Información. Esta revisión debe ser realizada por un equipo independiente, dentro o fuera de la institución; en una institución pequeña se podría optar por un tercero para la revisión.

La NTE INEN ISO/IEC 27002:2023, sección 5.35, proporciona directrices específicas para la revisión independiente que las instituciones públicas deben considerar.

1.36. Cumplimiento de políticas, reglas y normas de seguridad de la información, documentado e implementado

Las instituciones del sector público deben tener claro que, si se está invirtiendo esfuerzos y recursos en implementar controles de seguridad, se debe validar que los controles están funcionando eficazmente, los funcionarios del nivel jerárquico superior deben revisar el cumplimiento en su área de responsabilidad, las políticas, controles y estándares de seguridad; a través de una revisión formal y/o mediante controles puntuales que pueden ejecutarse en cualquier momento durante el trabajo normal.

La NTE INEN ISO/IEC 27002:2023, sección 5.36, proporciona directrices importantes que las instituciones públicas deben considerar.

1.37. Procedimientos operativos, documentados e implementados

Las instituciones del sector público deben tener claro que la extensión de los procedimientos debe ser apropiada al tamaño y complejidad de la institución; es decir, no se deben aplicar procedimientos muy detallados o complicados en una institución pequeña, ni procedimientos muy simples en una institución grande y compleja. Esto con el propósito de que la institución asegure que haya suficiente documentación disponible para abordar las actividades representativas en el entorno de trabajo diario.

Al menos se deben documentar los siguientes procedimientos:

- Procedimiento en la instalación y configuración de sistemas;
- Procesamiento y manejo de la información tanto automatizada como manual;
- Procedimiento de respaldo y restauración de la información.
- Procedimiento de los servicios de procesamiento de datos, incluyendo la interrelación con otros sistemas;
- Procedimiento para el manejo de errores y otras condiciones excepcionales que pueden surgir durante la ejecución de las tareas incluyendo restricciones en las funcionalidades del sistema.
- Procedimiento de eliminación segura de la información.
- Procedimientos para reinicio y recuperación del sistema en caso de fallas;
- Procedimiento para la obtención de pistas de auditoría y de la información de registro de sistemas;
- Procedimientos de monitoreo de los sistemas

Las instrucciones necesarias que deben incluir los procedimientos operativos se describen en la NTE INEN ISO/IEC 27002:2023, sección 5.37.

2. CONTROL DE PERSONAS, DOCUMENTADO E IMPLEMENTADO**2.1. Selección**

Las instituciones del sector público deben considerar al presente control como esencial para evitar la contratación de personal no idóneo; para esto las comprobaciones de identidad, la revisión de la hoja de vida, la verificación de cualificaciones y la verificación de referencias personales; son varios de los elementos a considerar.

La NTE INEN ISO/IEC 27002:2023, sección 6.1 enumera los elementos que deben considerarse y deberá además alinearse a la normativa legal vigente del órgano regulador del trabajo.

2.2. Términos y condiciones de empleo, documentado e implementado

Las instituciones del sector público deben asegurar que las responsabilidades en materia de seguridad de la información estén claramente definidas en los términos y

condiciones de los contratos y sean comprendidas por los funcionarios, contratistas y terceros desde el inicio de su relación laboral o contractual.

La NTE INEN ISO/IEC 27002:2023, sección 6.2, proporciona directrices importantes que las instituciones públicas deben considerar.

2.3. Concienciación, educación y formación en seguridad de la información, documentado e implementado

Las instituciones del sector público deben asegurar que todos los funcionarios reciban capacitación sobre las políticas y procedimientos pertinentes, incluyendo los requisitos de seguridad, el uso de los productos y paquetes de TI requeridos para su puesto y otros controles. Hay que considerar que, los usuarios sin capacitación pueden tomar medidas incorrectas y cometer errores por desconocimiento en el manejo de la información institucional.

La NTE INEN ISO/IEC 27002:2023, sección 6.3, proporciona directrices importantes que las instituciones públicas deben considerar.

2.4. Proceso disciplinario, documentado e implementado

Las instituciones del sector público deben contar con un proceso disciplinario que incluya aspectos ante la violación de la política de seguridad de la información, este debe estar alineado a la cultura y las prácticas de gestión de la institución. Debe estar documentado y socializado con las partes interesadas, quienes deben conocer su funcionamiento. Se deberá informar el proceso disciplinario a todos los funcionarios desde su ingreso.

La NTE INEN ISO/IEC 27002:2023, sección 6.4, proporciona directrices importantes que las instituciones públicas deben considerar.

2.5. Responsabilidades después de la terminación o cambio de empleo, documentado e implementado

Las instituciones del sector público deben establecer un proceso de desvinculación y/o cambio de empleo que defina aquellas responsabilidades que permanecen vigentes una vez finalizada la relación laboral o por el cambio de un puesto.

La NTE INEN ISO/IEC 27002:2023, 6.5, proporciona más orientación acerca de las responsabilidades y funciones de seguridad de la información que siguen siendo válidos después de la finalización o el cambio de empleo.

2.6. Acuerdos de confidencialidad o no divulgación, documentado e implementado

Las instituciones del sector público para proteger la confidencialidad de su información sensible deben exigir bajo términos legales acuerdos de confidencialidad o no divulgación con el personal de la institución y con las partes interesadas, antes de permitir el acceso a dicha información.

La NTE INEN ISO/IEC 27002:2023, 6.6, proporciona más orientación acerca de los términos y requisitos de los acuerdos de confidencialidad y no divulgación.

2.7. Trabajo remoto, documentado e implementado

Las instituciones del sector público deben documentar y establecer una política específica que contenga controles adecuados que permitan asegurar la información institucional a la que accede, procesa y almacena fuera de las instalaciones de la institución. Para cuando el personal trabaja de forma remota, se debe registrar una lista de usuarios que están autorizados a realizar trabajo remoto, junto con qué tipos de actividades están

autorizadas, en qué ubicaciones, a qué datos se les permite acceder y qué controles deben existir.

La NTE INEN ISO/IEC 27002:2023, 6.7, proporciona más orientación acerca de las reglas y mecanismos que se deben considerar para el trabajo físico remoto.

2.8. Informe de eventos de seguridad de la información, documentado e implementado

Las instituciones del sector público deben documentar e implementar procedimientos formales para la notificación de eventos de seguridad de la información, permitiendo que los funcionarios informen rápidamente cualquier incidente, vulnerabilidad o sospecha de violación de seguridad al Oficial de Seguridad de la Información, aplicando medidas apropiadas de manera oportuna a través de canales seguros.

La NTE INEN ISO/IEC 27002:2023, 6.8, proporciona más orientación acerca de las reglas y mecanismos que se deben considerar para el informe de eventos de seguridad de la información.

3. CONTROLES FÍSICOS

3.1. Perímetros de seguridad física, documentado e implementado

Las instituciones del sector público deben asegurar que las áreas físicas que contienen activos de información estén protegidas mediante perímetros claramente definidos y controlados, con el fin de evitar el acceso no autorizado; es importante considerar la protección interna, así como la protección perimetral, aplicando el concepto de “nunca confiar”, “verificar siempre”.

La guía de implementación en la NTE INEN ISO/IEC 27002:2023, sección 7.1 contiene sugerencias para perímetros de seguridad física, que las instituciones del sector público deben considerar.

3.2. Entrada física, documentado e implementado

Las instituciones públicas deben asegurar que se restrinja el acceso físico donde se encuentren activos de información, garantizando que solo el personal autorizado pueda ingresar a estas áreas. Es importante considerar el establecimiento de puntos de entrada autorizados, sistemas de control de acceso físicos, registro de entrada y salidas, gestión de visitantes, supervisión de entradas, revisión periódica de accesos, otros.

En la NTE INEN ISO/IEC 27002:2023, sección 7.2, se enumeran recomendaciones específicas que se deben tomar en cuenta en las instituciones del sector público.

3.3. Seguridad de oficinas, despachos e instalaciones, documentado e implementado

Las instituciones del sector público deben identificar los controles necesarios para proteger las oficinas, despachos e instalaciones, estos controles deben ser adecuados al valor, la responsabilidad, la importancia de la información y los activos relacionados dentro de dichas áreas.

La NTE INEN ISO/IEC 27002:2023, sección 7.3, incluye una lista de buenas prácticas de seguridad que deben aplicarse para proteger las áreas seguras en las instituciones del sector público.

3.4. Monitoreo de seguridad física, documentado e implementado

Las instituciones del sector público deben establecer un proceso para el monitoreo físico y documentarlo, este proceso debe incluir claramente qué se monitorea, cómo y porqué;

además se debe especificar qué sucede y a quién se notificará en la institución si se activa una alarma. Recordar que, si no hay claridad en este proceso, es posible que los incidentes de seguridad de la información relacionados con el robo o daño de información física no se gestionen correctamente.

La NTE INEN ISO/IEC 27002:2023, sección 7.4, incluye buenas prácticas para el monitoreo e instalación de sistemas de vigilancia, que las instituciones deben considerar.

3.5. Protección contra las amenazas externas y ambientales, documentado e implementado

Las instituciones del sector público, así como cualquier organización, son vulnerables a amenazas que están fuera de su propio control; en ese sentido las instituciones deben realizar una evaluación de riesgos físicos y ambientales específicos que consideren: incendios, inundaciones, terremotos, cortes eléctricos, sabotaje, vandalismo u otros. Se debe documentar los riesgos y clasificarlos según su probabilidad e impacto.

Con este resultado las instituciones del sector público deben implementar controles para proteger los activos de información frente a desastres naturales, accidentes o amenazas provocadas por “personas” que puedan afectar la infraestructura física.

La NTE INEN ISO/IEC 27002:2023, sección 7.5, incluye directrices que las instituciones deben considerar para la localización y la protección de las instalaciones físicas, antes de comenzar operaciones críticas.

3.6. Trabajo en áreas seguras, documentado e implementado

Las instituciones del sector público establecerán políticas y procedimientos que permitan identificar las áreas seguras; implementar medidas de control que aislen y protejan estas áreas del personal y del uso de equipamiento no autorizado. Es importante concientizar a todo el personal institucional de la existencia de estas áreas.

La NTE INEN ISO/IEC 27002:2023, 7.6, proporciona más orientación sobre la implementación de controles efectivos para mantener la seguridad en áreas protegidas.

3.7. Puesto de trabajo despejado y pantalla limpia, documentado e implementado

Las instituciones del sector público elaborarán una política específica de “Puestos de trabajo despejado”; esto es, libre de documentos y dispositivos de almacenamiento extraíbles que puedan contener información sensible y “Pantalla limpia” que hace referencia a no exhibir en el escritorio del computador de trabajo íconos y/o accesos a documentación sensible.

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

La NTE INEN ISO/IEC 27002:2023, 7.7, proporciona más orientación sobre los aspectos adicionales a considerar para las instalaciones de tratamiento de información, como la implementación de auditorías de control.

3.8. Ubicación y protección de equipos, documentado e implementado

Las instituciones del sector público deben establecer e implementar políticas de protección física y ubicación adecuada de los equipos para prevenir amenazas físicas y

ambientales, accesos no autorizados, daños físicos y pérdida de información.

La NTE INEN ISO/IEC 27002:2023, 7.8, proporciona más orientación sobre las directrices adicionales a considerar para proteger los equipos.

3.9. Seguridad de los activos fuera de las instalaciones, documentado e implementado

Las instituciones del sector público deben documentar y establecer directrices que eviten la interrupción de las operaciones institucionales por pérdida, daño, robo de dispositivos que por necesidad tengan que operar fuera de las instalaciones y que aseguren que los equipos no queden desprotegidos y/o desatendidos. Se debe controlar dispositivos de propiedad privada utilizados para la institución (Política de traiga su propio dispositivo - BYOD).

La NTE INEN ISO/IEC 27002:2023, 7.9, proporciona más orientación acerca de los controles que precautelan la seguridad de los activos fuera de las instalaciones institucionales.

3.10. Medios de almacenamiento, documentado e implementado

Las instituciones del sector público deben documentar e implementar políticas que protejan la información institucional en medios de almacenamiento y cumplir con el adecuado ciclo de vida de los datos desde su creación hasta su eliminación.

La NTE INEN ISO/IEC 27002:2023, 7.10, proporciona más orientación acerca de la adecuada gestión de los medios de almacenamiento.

3.11. Servicios de soporte, documentado e implementado

Las instituciones del sector público deben garantizar el funcionamiento adecuado y la continuidad de los servicios (electricidad, agua, ventilación refrigeración, telecomunicaciones, diésel, aire acondicionado, generadores de energía, otros), que proveen soporte a las instalaciones de procesamiento (centros de datos, redes, equipos informáticos, otros).

Para garantizar que el servicio de soporte funcione adecuadamente deben mantener actualizados los contactos de emergencia de los servicios de soporte y accesible para los funcionarios; entre otros, considerar:

- Realizar mantenimientos programados,
- Inspecciones rutinarias,
- Implementar controles de acuerdo con la identificación de riesgos.

La NTE INEN ISO/IEC 27002:2023, 7.11, proporciona más orientación de las medidas a considerar para proteger los servicios que dan soporte a las instalaciones de procesamiento.

3.12. Seguridad del cableado, documentado e implementado

Las instituciones del sector público deben establecer medidas para asegurar y proteger los cables (voz, datos, energía) frente accesos no autorizados, daños o destrucción.

Para proteger los cables se puede optar por usar: canaletas, cajas de cableado para proteger el cableado de red como el de alimentación, en cuanto sea posible, identificar y rotular los cables de acuerdo con normas locales o internacionales, realizar inspecciones regulares y mantenimiento del cableado, verificar que el cableado cumpla con los estándares de seguridad y se mantenga en condiciones óptimas.

La NTE INEN ISO/IEC 27002:2023, 7.12, proporciona más orientación de las directrices a considerar para la seguridad del cableado.

3.13. Mantenimiento de equipo, documentado e implementado

Las instituciones del sector público deben elaborar un plan de mantenimientos programados (preventivos y correctivos) para los equipos y dispositivos de procesamiento de datos, para garantizar su correcto funcionamiento.

Para realizar los mantenimientos planificados y emergentes, notificar a los funcionarios y registrar las tareas realizadas.

La NTE INEN ISO/IEC 27002:2023, 7.13, proporciona más orientación de las directrices a considerar para realizar el mantenimiento de equipos.

3.14. Eliminación segura o reutilización de equipos, documentado e implementado

Las instituciones del sector público deben elaborar, implementar y socializar una Política de Borrado Seguro de Información y asegurarse que los medios de almacenamiento que contienen información sensible y/o protegida por derechos de autor, sean eliminados de forma segura antes de volverlos a reutilizar.

El enfoque de este control se centra en los equipos físicos que almacenan o procesan información, como servidores, discos duros, PCs, portátiles, USBs, smartphones, otros.

La NTE INEN ISO/IEC 27002:2023, 7.14, proporciona más orientación de los elementos para eliminar y reutilizar la información de manera segura.

4. CONTROLES TECNOLÓGICOS

4.1. Dispositivos finales de usuario, documentado e implementado

Las instituciones del sector público deben elaborar, implementar y socializar a todos los usuarios una política que incluya directrices sobre cómo configurar dispositivos de usuario final (computadoras, teléfonos móviles, otros) de manera segura y mantenerlos actualizados, manejar y proteger la información como los recursos institucionales que almacenan.

La NTE INEN ISO/IEC 27002:2023, 8.1, proporciona más orientación sobre la implementación de controles efectivos sobre los dispositivos de usuario final.

4.2. Derechos de acceso privilegiado, documentado e implementado

Las instituciones del sector público deben implementar controles para gestionar los accesos privilegiados, es decir; aquellos accesos que permiten realizar acciones sobre los activos de información que no están disponibles para usuarios comunes (bases de datos, sistemas operativos, sistemas de información, consolas, etc.). Estas acciones se atribuyen a roles de administración de los sistemas, quienes pueden modificar configuraciones u operaciones críticas, acceder a información sensible.

Para fines de auditoría por parte de los entes de control, la institución deberá mantener los registros de todos los accesos privilegiados para lo cual se ha de evitar el uso de credenciales genéricas.

La NTE INEN ISO/IEC 27002:2023, 8.2, proporciona más orientación sobre los derechos de acceso privilegiado.

4.3. Restricción de acceso a la información, documentado e implementado

Las instituciones del sector público han de considerar el principio de *menor privilegio*, para la configuración de acceso a los sistemas, tal que la información institucional esté restringida a aquellos usuarios que realmente necesitan conocerla; para el cumplimiento de sus actividades.

La NTE INEN ISO/IEC 27002:2023, 8.3, proporciona más orientación sobre la definición de controles específicos tanto físicos como lógicos para la restricción de acceso a la información.

4.4. Acceso al código fuente, documentado e implementado

Las instituciones del sector público deben restringir la capacidad de visualización, modificación y distribución del código fuente de los sistemas, mediante la implementación de políticas de acceso y mecanismos de control como herramientas de gestión de versiones.

La NTE INEN ISO/IEC 27002:2023, 8.4, proporciona más orientación sobre la administración de los accesos al código fuente de los sistemas institucionales.

4.5. Autenticación segura, documentado e implementado

Las instituciones del sector público deben documentar e implementar una política con directrices claras con procedimientos de autenticación segura que incluya la creación, almacenamiento y gestión de contraseñas.

En función del resultado de la evaluación de riesgos considerar la implementación de controles tecnológicos que permitan múltiples factores de autenticación que combine dos o más de los siguientes factores: “algo que el usuario sabe” (contraseña, PIN), “algo que el usuario tiene” (tarjeta de seguridad, token) y “algo que el usuario es” (biometría).

La NTE INEN ISO/IEC 27002:2023, 8.5, proporciona más orientación sobre los procedimientos y tecnologías de autenticación segura.

4.6. Gestión de la capacidad, documentado e implementado

Las instituciones del sector público deben documentar e implementar un Plan de Capacidades que contemple un monitoreo permanente que permita optimizar y afinar el uso de los recursos tecnológicos (procesamiento, almacenamiento, redes, aplicaciones, otros) y advertir el crecimiento de la demanda, resultado del despliegue de nuevos servicios, cambios tecnológicos, etc.

La NTE INEN ISO/IEC 27002:2023, 8.6, proporciona más orientación sobre los requerimientos y la gestión de la capacidad de los recursos tecnológicos.

4.7. Protección contra malware, documentado e implementado

Las instituciones del sector público deben implementar controles para detectar, prevenir y recuperarse de afectaciones de malware, en combinación con el fortalecimiento adecuado de la cultura de seguridad de la información a los usuarios y la documentación de una política en la que se establezcan directrices claras.

La NTE INEN ISO/IEC 27002:2023, 8.7, proporciona más orientación para establecer medidas de protección contra malware.

4.8. Gestión de vulnerabilidades técnicas, documentado e implementado

Las instituciones del sector público deben realizar las actividades necesarias,

documentadas y planificadas, para obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso; con personal capacitado, y en el caso de instituciones con recursos limitados gestionarlo a través de terceros como: CSIRT Nacional, o CSIRT sectoriales según corresponda.

Identificar y documentar un inventario de los activos de información tipo software con un registro de las vulnerabilidades, en función de su gravedad y potencial impacto, así mismo, se debe establecer una priorización y elaborar un plan para la remediación.

La NTE INEN ISO/IEC 27002:2023, 8.8, proporciona más orientación acerca de la identificación de roles y otros aspectos para la gestión de vulnerabilidades técnicas.

4.9. Gestión de la configuración, documentado e implementado

Las instituciones del sector público deben documentar las configuraciones seguras de los sistemas y activos de información, en función de estándares reconocidos.

Mantener un registro de versiones para que de esta manera no se realicen cambios sin autorización y ejecutar una reversión segura en caso de errores o incidentes sobre los recursos tecnológicos (software, hardware, servicios y redes).

La NTE INEN ISO/IEC 27002:2023, 8.9, proporciona más orientación acerca de la administración y la gestión de la configuración.

4.10. Eliminación de información, documentado e implementado

Las instituciones del sector público deben documentar e implementar un procedimiento para eliminación segura de la información en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento cuando la información recolectada ya no sea necesaria. Es decir, el control se enfoca en la información, su ciclo de vida y eliminación segura, sin importar su soporte (digital o físico).

La NTE INEN ISO/IEC 27002:2023, 8.10, proporciona más orientación acerca de los procedimientos más adecuados para la eliminación de información.

4.11. Enmascaramiento de datos, documentado e implementado

Las instituciones del sector público deben definir los tipos de enmascaramiento, anonimización, seudonimización, cifrado, ofuscación u otros; utilizados en el manejo de la información sensible en sistemas y aplicaciones con el propósito de garantizar que personas no autorizadas puedan acceder a dicha información.

El Oficial de Seguridad de la Información es el encargado de coordinar y supervisar su aplicación dentro del marco de la seguridad de la información.

La NTE INEN ISO/IEC 27002:2023, 8.11, contiene directrices específicas que las instituciones deben considerarlas.

4.12. Prevención de fuga de datos, documentado e implementado

Las instituciones del sector público deben conocer el flujo de la información permitida al interior de la institución como parte de la gestión interna, con el propósito de definir, como deben protegerse y autorizarse.

El Oficial de Seguridad de la Información deberá validar que los funcionarios que tienen acceso a datos considerados sensibles sean conscientes del concepto de fuga de datos; y conozcan qué información deben o no compartir fuera de la institución.

La NTE INEN ISO/IEC 27002:2023, 8.12, contiene medidas específicas adicionales que

apoyan la prevención de fuga de datos y que las instituciones deben considerarlas.

4.13. Copia de seguridad de la información, documentado e implementado

Las instituciones del sector público deben identificar la información necesaria a respaldar, mediante una evaluación de riesgos, para determinar y justificar la frecuencia, periodicidad y el tipo de respaldo. Estas directrices deben documentarse en una Política y/o Procedimiento de RespalDOS y Restauración.

Entre otras acciones, el Oficial de Seguridad de la Información debe confirmar que se implementan los mecanismos adecuados de copia de seguridad y restauración de datos según los resultados de la evaluación de riesgos, al interior de su institución.

En la NTE INEN ISO/IEC 27002:2023, 8.13, se proporcionan recomendaciones fundamentales para la gestión de los respaldos, que las instituciones deben considerarlas.

4.14. Redundancia de las instalaciones de tratamiento de información, documentado e implementado

Las instituciones del sector público deben incluir la redundancia como parte de sus Planes de Continuidad de Negocio, Recuperación de Desastres u otros, para lo cual deben identificar los tiempos de recuperación necesarios tras un fallo y cómo responderían con los sistemas que tienen actualmente; con el propósito de implementar la redundancia necesaria y garantizar la disponibilidad.

La NTE INEN ISO/IEC 27002:2023, 8.14 contiene una lista de consideraciones para ayudar en el diseño de una redundancia adecuada, que las instituciones deben tomar en cuenta.

4.15. Registro de eventos, documentado e implementado

Las instituciones públicas deben determinar el nivel, tipo y frecuencia de la generación de registros y la monitorización requerida, en función de los servicios críticos institucionales, que el Oficial de Seguridad de la Información debe verificar en conjunto con el propietario del activo. Los registros son una herramienta valiosa, pues cubren entre otras, actividades de los administradores, excepciones, eventos del sistema; que en casos específicos permiten detectar que evento condujo a un incidente

La NTE INEN ISO/IEC 27002:2023, 8.15, contiene una lista de consideraciones que se deben tener en cuenta durante el análisis de los registros.

4.16. Actividades de monitoreo, documentado e implementado

Las instituciones del sector público deben identificar qué información, sistemas y servicios que están en riesgo y deben monitorizarse. La implementación de un sistema de monitoreo y la definición de umbrales, a partir del cual las detecciones se convierten en alertas, serán de utilidad para el cumplimiento de este control.

La NTE INEN ISO/IEC 27002:2023, 8.16 proporciona una lista de posibles fuentes de datos y eventos que deben incluirse en el sistema de monitoreo.

4.17. Sincronización del reloj, documentado e implementado

Las instituciones del sector público deben asegurar que la información de salida de los computadores, servidores y los equipos de comunicación, sean completamente consistentes entre todos los dispositivos, al menos dentro del alcance del EGSI.

Una de las acciones que el Oficial de Seguridad de Seguridad de la Información debe

realizar es, verificar que el acceso a la configuración de los relojes del sistema esté restringido para evitar manipulaciones.

En la NTE INEN ISO/IEC 27002:2023, 8.17, se detallan recomendaciones adicionales para asegurar la precisión de los registros de eventos.

4.18. Uso de programas de utilidad privilegiados, documentado e implementado

Las instituciones del sector público deben establecer una restricción estricta en el uso de programas o herramientas que permiten realizar tareas críticas en sistemas, para esto deben controlar quién las usa, controlar cómo se usan, registrar y auditar su utilización.

En la NTE INEN ISO/IEC 27002:2023, 8.18, se detallan recomendaciones para asegurar el uso de las utilidades del sistema.

4.19. Instalación de software en sistemas operativos, documentado e implementado

Las instituciones del sector público deben establecer reglas claras para el control de la instalación de software en sistemas operativos, considerando que una instalación inadecuada puede abrir grandes brechas de seguridad. Consideraciones como las siguientes pudieran ayudar a minimizar el riesgo:

- Inventario del software permitido
- Autorización formal antes de cualquier instalación
- Uso de software legítimo, licenciado o de páginas oficiales
- Desactivación de permisos de instalación a los usuarios finales

La NTE INEN ISO/IEC 27002:2023 8.19, proporciona directrices adicionales que cubren la instalación y el uso del software.

4.20. Seguridad de redes, documentado e implementado

Las instituciones del sector público deben tener conciencia de que la seguridad de red comienza con el establecimiento de una arquitectura de red bien protegida, además se debe contemplar: un diseño seguro, para minimizar la superficie de ataque; el constante monitoreo, para detectar eventos y evitar la materialización de las amenazas; procedimientos documentados, para estar preparados ante incidentes; entre otros.

La NTE INEN ISO/IEC 27002:2023 8.20, proporciona recomendaciones adicionales que las instituciones deben considerar.

4.21. Seguridad de los servicios de red, documentado e implementado

Las instituciones del sector público deben implementar mecanismos de seguridad en los servicios de red, independientemente si se gestionan interna o externamente. Se debe documentar una política con lineamientos claros para definir los requisitos de seguridad para todos los servicios de red, que aborden aspectos como: autorización para el acceso, autenticación de usuarios, uso de red VPN, protección de datos en tránsito, entre otros.

La NTE INEN ISO/IEC 27002:2023, 8.21, proporciona más orientación sobre una lista de reglas y características de seguridad para los servicios de red.

4.22. Separación en las redes, documentado e implementado

Las instituciones del sector público deben segmentar y documentar la gestión de redes, sean físicas (enrutadores, switches, otros) o lógicas (VLANs) con el objetivo de mejorar la seguridad, lo que ayuda a minimizar los riesgos asociados con el acceso no autorizado a

los recursos sensibles.

Para la gestión de las redes, se debe considerar: documentar los diagramas de red, identificar los segmentos de red donde se encuentren los activos críticos de la institución (servicios, usuarios y sistemas de información); considerando el valor y la clasificación de la información, a través de una evaluación de riesgos.

La NTE INEN ISO/IEC 27002:2023, 8.22, proporciona más orientación para implementar la separación en las redes.

4.23. Filtrado web, documentado e implementado

Las instituciones del sector público deben controlar el acceso a sitios web externos, para lo cual deben definir políticas claras de lo que está o no permitido acceder (listas blancas y negras) o usar categorías de contenido para controlar el acceso; con el fin de proteger la operación de la institución de riesgos como pérdida de datos, secuestro y/o robo de credenciales u otros.

Además, se debe comunicar y socializar al personal sobre estas reglas y el uso correcto para acceder a sitios web externos.

La NTE INEN ISO/IEC 27002:2023, 8.23, proporciona buenas prácticas y recomendaciones para el filtrado web.

4.24. Uso de criptografía, documentado e implementado

Las instituciones del sector público deben documentar una política criptográfica, en la que se especifique las directrices, servicios y técnicas a usar para proteger la información acorde a su clasificación, incluir la gestión de claves criptográficas (generación, almacenamiento, distribución y eliminación).

La NTE INEN ISO/IEC 27002:2023, 8.24, proporciona más orientación sobre las responsabilidades relacionadas con el uso de controles criptográficos, que las instituciones deben considerar.

4.25. Ciclo de vida de desarrollo seguro, documentado e implementado

Las instituciones del sector público deben establecer una política en la que se incluya las reglas, metodologías, estándares, utilizadas para el desarrollo seguro de aplicaciones y sistemas durante todo el ciclo de vida, es decir la planificación, implementación y mantenimiento.

La NTE INEN ISO/IEC 27002:2023, 8.25, proporciona más orientación sobre las medidas que se deben tomar en cuenta para incluirlas en la política de desarrollo seguro.

4.26. Requisitos de seguridad de la aplicación, documentado e implementado

Las instituciones del sector público deben exigir que todos los proyectos de desarrollo o adquisición de software incluyan explícitamente requisitos de seguridad acorde a la clasificación de la información que manejan, para lo cual deben realizar una evaluación de riesgos.

La NTE INEN ISO/IEC 27002:2023, 8.26, proporciona más orientación sobre los requisitos que deben aplicarse a la selección y el desarrollo de aplicaciones.

4.27. Arquitectura del sistema seguro y principios de ingeniería, documentado e implementado

Las instituciones del sector público deben integrar principios de seguridad desde las fases iniciales del diseño y desarrollo de sistemas, aplicando un enfoque "Security by Design" y "Security by Default" en todas las etapas del ciclo de vida del sistema. Para lograr este objetivo se debe involucrar al Oficial de Seguridad de la Información y el equipo de seguridad informática, desde el inicio del proyecto.

La NTE INEN ISO/IEC 27002:2023, 8.27, proporciona más orientación sobre los principios y procesos a considerar en la arquitectura del sistema seguro.

4.28. Codificación segura, documentado e implementado

Las instituciones del sector público deben implementar estándares, prácticas y técnicas de codificación segura para desarrollar software, para minimizar la superficie de ataque y la probabilidad de que se introduzcan vulnerabilidades explotables en el código fuente.

La NTE INEN ISO/IEC 27002:2023, 8.28, proporciona más orientación sobre los estándares y procesos de codificación segura que se deben implementar en las instituciones.

4.29. Pruebas de seguridad y aceptación en el desarrollo, documentado e implementado

Las instituciones del sector público deben ejecutar pruebas de seguridad, como: análisis de vulnerabilidades, pruebas de penetración, pruebas automatizadas de código fuente, análisis de métodos formales y revisión manual de código, según corresponda con base al nivel de riesgo y sensibilidad del sistema.

La NTE INEN ISO/IEC 27002:2023, 8.29, proporciona más orientación sobre estos tipos de pruebas que se deben considerar.

4.30. Desarrollo subcontratado, documentado e implementado

Las instituciones del sector público que estén subcontratando el desarrollo a través de terceros deben exigirles que cumplan con los requisitos de seguridad de la información que les permitan asegurar la confidencialidad, integridad y disponibilidad de los activos de información involucrados, a fin de minimizar los riesgos asociados.

Se deberá, supervisar las actividades de desarrollo ejecutadas por los proveedores subcontratados, evaluar continuamente el cumplimiento de los requisitos de seguridad acordados, cumpliendo con las Normas de Control Interno de la Contraloría General del Estado y la legislación vigente que corresponda.

La NTE INEN ISO/IEC 27002:2023, 8.30 proporciona más orientación sobre las recomendaciones que se deben tomar en cuenta al subcontratar el desarrollo de software a terceros.

4.31. Separación de los entornos de desarrollo, pruebas y producción, documentado e implementado

Las instituciones del sector público que realizan desarrollo de software interno o externo deberán tener los siguientes ambientes: desarrollo, pruebas y producción, tal como se indica en las normas internacionales; así como, en las normas de Control Interno de la Contraloría General del Estado. Considerar que estos ambientes pueden ser físicos o virtuales y deben estar documentados, especificando las medidas de seguridad que se tomarán en cuenta en cada entorno.

La NTE INEN ISO/IEC 27002:2023, 8.31 proporciona las recomendaciones que se deben tomar en cuenta para la separación de entornos de desarrollo.

4.32. Gestión de cambios, documentado e implementado

Las instituciones del sector público deben, documentar e implementar un proceso formal para gestionar los cambios de los sistemas de información, instalaciones y servicios, a fin de garantizar la seguridad de la información al realizar estos cambios.

La documentación debe incluir roles y responsabilidades, los riesgos de seguridad asociados a cada cambio, criterios para aprobación del cambio, pruebas, respaldos, entre otros. 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.

La NTE INEN ISO/IEC 27002:2023, 8.32 proporciona más información sobre los procedimientos de control de cambios que deben aplicarse.

4.33. Información de prueba, documentado e implementado

Las instituciones del sector público deben utilizar en la medida de lo posible datos ficticios en los entornos de prueba, sin embargo, si es necesario el uso de datos operativos deben ser anonimizados, controlados y protegidos para evitar violaciones a la confidencialidad de dicha información.

La NTE INEN ISO/IEC 27002:2023, 8.33, proporciona más orientación sobre las consideraciones claves de los datos de prueba.

4.34. Protección de los sistemas de información durante las pruebas de auditoría, documentado e implementado

Las instituciones del sector público durante la ejecución de auditorías independientes (internas o externas) a sus sistemas de información deben establecer medidas que garanticen los principios de la seguridad de la información como la integridad y disponibilidad de la información que se almacena en dichos sistemas de información.

El responsable del área de TI en conjunto con el Oficial de Seguridad deberá evaluar los requisitos de la auditoría, planificar y acordar un cronograma adecuado.

La NTE INEN ISO/IEC 27002:2023, 8,34 proporciona más orientación sobre la realización de auditorías de información.

Correspondencia de controles EGSi v3 - EGSi v2

El propósito de este anexo es proporcionar la correspondencia que existe entre los controles de la nueva versión del EGSi con la versión anterior.

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	Protección de datos personales
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

Tabla 1. Correspondencia de controles EGSi v3 - EGSi v2

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.

Dato personal: Dato que identifica o hace identificable a una persona natural, directa o indirectamente.

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 del sector público para preservar la integridad, disponibilidad y confidencialidad de la información.

Encargado del tratamiento de datos personales. - Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.

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 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 manejo 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 (ejemplo: 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 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 directa 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 Titular de datos personales PII. - Persona natural a la que se refiere la información personal identificable (PII) cuyos datos son objeto de tratamiento (cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no

automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.

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 deben 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

Abreviatura	Definición
BCP	Plan de continuidad del negocio
CSIRT	Centro de Respuesta a Incidentes Informáticos
DRP	Plan de recuperación ante desastres
DLP	Plataforma de prevención de fuga de datos
IAM	Gestión de acceso e identidad
IEC	Comisión Electrotécnica Internacional
INEN	Servicio Ecuatoriano de Normalización
ISO	Organización Internacional de Normalización
TIC	Tecnología de la información y la comunicación
IDS	Sistema de detección de intrusos

IP	Protocolo de internet
TI	Tecnologías de la información
SGSI	Sistema de gestión de seguridad de la información
LOPD	Ley Orgánica de Protección de Datos Personales
MFA	Autenticación Multifactor
NTE	Norma Técnica Ecuatoriana
PIN	Número de identificación personal - Contraseña
PKI	Infraestructura de clave pública
SIEM	Gestión de eventos e información de seguridad
SLA	Service Level Agreement – Acuerdos de nivel de servicio
VPN	Red privada virtual
VLAN	Red de Área Local Virtual

Tabla 2. Términos abreviados



Mgs. Jaqueline Vargas Camacho
DIRECTORA (E)

Quito:
Calle Mañosca 201 y Av. 10 de Agosto
Atención ciudadana
Telf.: 3941-800
Ext.: 3134

www.registroficial.gob.ec

JL/FA

El Pleno de la Corte Constitucional mediante Resolución Administrativa No. 010-AD-CC-2019, resolvió la gratuidad de la publicación virtual del Registro Oficial y sus productos, así como la eliminación de su publicación en sustrato papel, como un derecho de acceso gratuito de la información a la ciudadanía ecuatoriana.

"Al servicio del país desde el 1º de julio de 1895"

El Registro Oficial no se responsabiliza por los errores ortográficos, gramaticales, de fondo y/o de forma que contengan los documentos publicados, dichos documentos remitidos por las diferentes instituciones para su publicación, son transcritos fielmente a sus originales, los mismos que se encuentran archivados y son nuestro respaldo.