SUPERINTENDENCIA DE ORDENAMIENTO TERRITORIAL, USO Y GESTIÓN DEL SUELO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

(EGSI V3)

Comité de Seguridad de la Información de la SOT

CONTENIDO

1. ANTECEDENTES **4**

2. DECLARACIÓN DE LOS OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN **9**

2.1. OBJETIVO GENERAL 9

2.2. OBJETIVOS ESPECÍFICOS 9

3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN **10**

3.1. DESCRIPCIÓN DE LA POLÍTICA 10

3.2. ALINEACIÓN CON LOS OBJETIVOS ESTRATÉGICOS INSTITUCIONALES. 12

3.3. PRINCIPIOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 13

3.4. ROLES Y RESPONSABILIDADES 14

3.5. ALCANCE Y USUARIOS 22

3.6. CLASIFICACIÓN DE LA INFORMACIÓN 22

3.7. LINEAMIENTOS GENERALES 24

3.7.1. Obligaciones individuales del usuario 25

3.7.2. Manejo documental y seguridad de los activos de información institucional 25

3.7.3. Gestión de usuarios para el acceso a los recursos tecnológicos institucionales 27

3.7.4. Gestión del uso adecuado del correo electrónico 28

3.7.5. Uso adecuado de equipos tecnológicos e informáticos 30

3.7.6. Responsabilidad sobre los activos de información institucional 32

3.7.7. Uso adecuado de la red institucional e internet 32

3.7.8. Gestión de aplicativo de nube institucional de almacenamiento de archivos 34

3.7.9. Gestión y seguridad de contraseñas 34

3.7.10. Gestión de la seguridad física y de instalaciones 35

3.7.11. Control de las vulnerabilidades técnicas 36

3.7.12. Gestión de incidentes de seguridad de la información y continuidad de la operación. 36

3.8. PROTECCIÓN DE DATOS PERSONALES 37

3.8.1. Controles específicos de seguridad 37

4. COMUNICACIÓN DE LA POLÍTICA **38**

5. SANCIONES **38**

6. DEFINICIONES Y ABREVIATURAS **38**

7. DOCUMENTOS DE REFERENCIA **45**

8. FIRMAS DE RESPONSABILIDAD **48**

ÍNDICE DE ILUSTRACIONES

Ilustración 1 . Principios de la seguridad de la Información. 11

ÍNDICE DE TABLAS

Tabla 1 . Alineación con la planificación estratégica institucional. 12
Tabla 2 . Clasificación de la información. 23
Tabla 3 . Abreviaturas 38
Tabla 4 . Términos y definiciones 39

1. Antecedentes

A partir del año 2008, el Ecuador prioriza la recuperación de lo público, orientando sus esfuerzos hacia la garantía de los derechos de la ciudadanía. En este contexto, por primera vez se crean las condiciones necesarias y se reconoce la importancia del ordenamiento territorial como un componente esencial de la planificación, fundamental para el adecuado funcionamiento del Estado. En ese sentido, la Constitución de la República del Ecuador, en su artículo 241, establece que: "La planificación garantizará el ordenamiento territorial y será obligatoria en todos los gobiernos autónomos descentralizados". En concordancia con el mandato constitucional, en el año 2010 se promulgo el Código Orgánico de Organización Territorial (COOTAD), mediante el cual se define la organización político-administrativa del Estado en el territorio, así como el régimen aplicable a los diferentes niveles de gobiernos autónomos descentralizados y los regímenes especiales.

El 05 de julio de 2016, la Asamblea Nacional promulgó la Ley Orgánica de Ordenamiento Territorial, Uso y Gestión del Suelo (en adelante LOOTUGS), con el objetivo de establecer los principios y reglas generales que regulen el ejercicio de las competencias en materia de ordenamiento territorial. Esta ley busca promover un desarrollo equitativo y equilibrado, bajo un enfoque que garantice el ejercicio del derecho a la ciudad, al hábitat seguro y saludable, y a una vivienda adecuada y digna, en armonía con la función social y ambiental de la propiedad.

Posteriormente, en abril de 2019, se expidió el Reglamento a la Ley Orgánica de Ordenamiento Territorial, Uso y Gestión del Suelo, mediante Decreto Ejecutivo N.º 680, cuyo objeto es regular los procedimientos para la formulación, actualización y aplicación de los instrumentos y mecanismos de ordenamiento territorial, planeamiento, uso y gestión del suelo establecidos en dicha Ley.

En este marco, la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo (en adelante la Superintendencia o la SOT) se crea mediante el artículo 95 de la LOOTUGS, con el propósito de ejercer *"la vigilancia y control de los procesos de ordenamiento territorial de todos los niveles de gobierno, y del uso y gestión del suelo, hábitat, asentamientos humanos y desarrollo urbano, que realizan los Gobiernos Autónomos Descentralizados municipales y metropolitanos dentro del marco de sus competencias. La Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo será una entidad técnica de vigilancia y control, con*

capacidad sancionatoria, personería jurídica de derecho público y patrimonio propio, que funcionará de forma desconcentrada e independiente".

Esta Superintendencia es una entidad técnica que vela por el interés de la ciudadanía en relación con el territorio, mediante la vigilancia y control de los procesos de ordenamiento territorial, planeamiento urbanístico, y uso y gestión del suelo, en el marco de la normativa legal vigente y de conformidad con las competencias de cada nivel de gobierno. Su accionar contribuye al desarrollo de territorios resilientes, autónomos, seguros, inclusivos, sustentables, ambientalmente equilibrados, y socialmente justos.

En ejercicio de las competencias que le han sido conferidas, la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo desarrolla diversas acciones y procesos institucionales. Como resultado de este trabajo, se genera información de carácter técnico, jurídico y administrativo, la cual puede presentarse en distintos formatos: impresa o manuscrita en papel, almacenado en medios electrónicos, transmitido mediante el correo institucional u otros canales electrónicos autorizados, proyectada en presentaciones visuales o comunicada verbalmente en conversaciones y reuniones mantenidas por servidores, trabajadores y funcionarios de la Institución.

Ante este escenario, se evidencia la necesidad urgente de establecer una política institucional de seguridad de la información, que garantice la protección, integridad y confidencialidad de los datos que maneja la Superintendencia. La ausencia de lineamientos y controles adecuados incrementa significativamente el riesgo de filtración de datos personales de ciudadanos, servidores y profesionales vinculados a la entidad, lo que podría derivar en sanciones severas, conforme a lo establecido en la Ley Orgánica de Protección de Datos Personales, vigente desde el año 2021.

Adicionalmente, la falta de mecanismos formales de control y prevención facilita la posibilidad de fraudes internos, alteraciones maliciosas de información presupuestaria, contractual o técnica, y otros actos que comprometen la transparencia institucional, abren espacio a prácticas de corrupción y debilitan el cumplimiento de los principios éticos en la gestión pública.

Asimismo, la carencia de una política integral de seguridad incrementa la vulnerabilidad frente a amenazas cibernéticas como ataques de ransomware, accesos no autorizados o pérdida de información crítica, situaciones que podrían provocar la interrupción de servicios esenciales —como plataformas de trámites en línea o sistemas administrativos— generando costos elevados de recuperación, afectaciones operativas y perjuicio directo a la ciudadanía. Cualquier brecha de seguridad que ocurra sin contar con un marco normativo preventivo afecta gravemente la imagen institucional, erosionando la confianza de la ciudadanía y debilitando la legitimidad del sector público en el cumplimiento de sus funciones y responsabilidades.

Frente a estas diversas aristas, la Secretaría Nacional de la Administración Pública, mediante los Acuerdos Ministeriales Nros. 804 y 837, emitidos el 29 de julio y el 19 de agosto de 2011 respectivamente, constituyó la Comisión de Seguridad Informática y Tecnologías de la Información y Comunicación. Este fue el primer órgano técnico encargado de proponer lineamientos orientados a la protección de la infraestructura tecnológica y los datos del Estado, constituyéndose en el antecedente directo y fundamento para el desarrollo posterior del Esquema Gubernamental de Seguridad de la Información (EGSI).

A lo largo del proceso de desarrollo de este esquema, la Secretaría Nacional de la Administración Pública expidió, mediante el Acuerdo Ministerial Nro. 166 (publicado en el Registro Oficial, Suplemento 88, del 25 de septiembre de 2013), el Esquema Gubernamental de Seguridad de la Información (EGSI v1). Este instrumento fue declarado de cumplimiento obligatorio para toda la administración pública central, y estableció la conformación de comités institucionales y la designación de Oficiales de Seguridad de la Información (OSI) en cada entidad, con el objetivo de fortalecer la gobernanza y la protección de los activos de información del Estado.

Ahora bien, en el año 2015 se expide la Ley Orgánica de Telecomunicaciones (Registro Oficial Nro. 439, de 18 de febrero de 2015), mediante la cual se otorga al Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) la rectoría en materia de telecomunicaciones y seguridad de la información. Esta normativa faculta al MINTEL para emitir políticas, directrices y acuerdos vinculantes, entre ellos el Esquema Gubernamental de Seguridad de la Información, fortaleciendo así el marco normativo nacional en protección de datos y ciberseguridad.

Mediante el Acuerdo Ministerial Nro. 025-2019 (Registro Oficial Nro. 228, de 10 de enero de 2020), el Ministerio de Telecomunicaciones y de la Sociedad de la Información emitió el Esquema Gubernamental de Seguridad de la Información versión 2.0. Esta actualización alineó sus controles a las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001 y otorgó un plazo de doce meses a las entidades del sector público para su implementación obligatoria.

En el año 2021 entró en vigencia la Ley Orgánica de Protección de Datos Personales (Registro Oficial Nro. 459, de 26 de mayo de 2021), la cual introduce el principio de seguridad por diseño y por defecto. Esta normativa exige que todos los mecanismos gubernamentales, incluido el EGSI, incorporen medidas técnicas, organizativas y jurídicas específicas que garanticen un tratamiento seguro, legítimo y proporcional de los datos personales, desde su recolección hasta su eliminación.

En esa misma línea, se promulgó la Ley Orgánica para la Transformación Digital y Audiovisual (Registro Oficial Nro. 245, de 7 de febrero de 2023), mediante la cual se crea el Marco de Seguridad Digital del Estado. Esta normativa reafirma la obligatoriedad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en las entidades públicas y dispone que el MINTEL actualice el Esquema Gubernamental de Seguridad de la Información conforme a la agenda de gobierno digital. Por su parte, el Reglamento General a dicha ley (Registro Oficial Nro. 813, Segundo Suplemento del Registro Oficial Nro. 350, de 11 de julio de 2023) detalla los procedimientos y plazos para su aplicación, ratificando que todas las entidades del sector público deben adoptar el EGSI como parte de su gestión de riesgos digitales.

La última actualización de este esquema se realizó mediante el Acuerdo Ministerial MINTEL-MINTEL-2024-0003 (Registro Oficial Nro. 08, de 8 de febrero de 2024), a través del cual se derogó la versión 2.0 y se expidió el EGSI v3.0. Esta nueva versión amplía los controles a 108 hitos, integra la Política de Seguridad Digital del Estado y establece un nuevo plazo de 12 meses para su implementación obligatoria en todas las entidades del sector público, así como en los concesionarios de servicios estatales.

Ante este desarrollo del esquema, la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo requiere la creación de una Política de Seguridad de la Información que responda a la necesidad de proteger los activos informativos de la institución en un contexto donde la información se genera, almacena y transmite en múltiples formatos y plataformas.

Desde la emisión de normativas y esquemas como el Esquema Gubernamental de Seguridad de la Información, hasta la incorporación de estándares internacionales y leyes nacionales como la Ley Orgánica de Protección de Datos Personales, se ha evidenciado que la seguridad de la información es un pilar fundamental para garantizar la continuidad operativa, la transparencia y la confianza ciudadana. Esta política se fundamenta en la consolidación de un marco normativo robusto que se adapta a la evolución tecnológica y a las demandas del entorno digital.

La importancia de contar con una política formal y actualizada radica en que esta establece los lineamientos claros y el compromiso institucional necesario para preservar la confidencialidad, integridad y disponibilidad de la información. A través de ella, se definen las responsabilidades de las autoridades y servidores, y se promueve una cultura organizacional orientada a la prevención de incidentes de seguridad, la gestión eficiente de riesgos y la protección contra amenazas internas y externas. Sin una política vigente, la institución queda expuesta a vulnerabilidades que pueden comprometer datos sensibles, afectar la prestación de servicios y dañar la reputación institucional.

Los riesgos asociados a la ausencia o desactualización de una política de seguridad son múltiples y severos. Sin controles adecuados, se incrementan las posibilidades de filtraciones de datos personales y administrativos, fraudes internos, alteraciones maliciosas de información y ataques cibernéticos, como ransomware, que pueden paralizar operaciones críticas. Además, la falta de alineación con normativas vigentes puede acarrear sanciones legales y la pérdida de financiamiento externo. Por tanto, mantener la política actualizada es vital para enfrentar estos desafíos y garantizar un marco preventivo efectivo que proteja los intereses de la entidad y sus usuarios.

Para finalizar, el propósito de esta Política de Seguridad de la Información es definir de manera clara las reglas básicas que orientarán la gestión de la seguridad de la información en la institución. Este documento de alto nivel debe normar los aspectos más relevantes y perdurables en el tiempo, asegurando una gestión sostenida y coherente en la protección de la información. Así, esta política representa el compromiso institucional para prevenir, detectar y mitigar riesgos, garantizando la continuidad, confiabilidad y legalidad en el manejo de los datos, en beneficio del servicio público y la confianza ciudadana.

2. Declaración de los objetivos de seguridad de la información

2.1. Objetivo general

Establecer lineamientos y directrices que garanticen la protección integral de los activos de información institucional, asegurando su confidencialidad, integridad, disponibilidad y trazabilidad frente a amenazas y riesgos potenciales, promoviendo una cultura organizacional orientada a la gestión responsable y segura de la información.

2.2. Objetivos específicos

Objetivo específico 1: Fortalecer la construcción de una cultura organizacional con base en la seguridad de la información, de manera que se convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos institucionales.

Objetivo específico 2: Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos no deseados contando como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos, alineado con los controles obligatorios del EGSI V3.

Objetivo específico 3: Garantizar la adecuada administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Institución.

Objetivo específico 4: Implementar mecanismos que garanticen la protección de datos personales y sensibles en los sistemas que gestionen información ciudadana.

3. Política de Seguridad de la Información

La SOT se compromete a implementar un Sistema de Gestión de Seguridad de la Información cumpliendo con los principios de confidencialidad, integridad y disponibilidad de los activos de información, promoviendo una gestión eficaz de riegos y generando una cultura de seguridad, que contribuya al logro de los objetivos institucionales en concordancia con la misión y visión de esta.

3.1. Descripción de la Política

Para la implementación efectiva del EGSI, conforme a los lineamientos establecidos en la norma internacional ISO/IEC 27001 y lo dispuesto en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, es indispensable contar con una Política de Seguridad de la Información que guíe el accionar institucional en materia de protección de activos informáticos.

Esta política establece el marco de referencia para la gestión de la seguridad de la información en la institución, asegurando que se mantenga la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional, tanto en su forma física como digital. Su propósito es prevenir, detectar, responder y recuperarse frente a incidentes de seguridad, minimizando los riesgos y garantizando la continuidad de los servicios públicos.

Asimismo, la política promueve la implementación de controles adecuados en función de las amenazas existentes, fomenta una cultura organizacional basada en la protección de la información, y fortalece la confianza de la ciudadanía y de los actores institucionales en el cumplimiento de las obligaciones legales y regulatorias.

En este contexto, la Política de Seguridad de la Información no solo es un documento de referencia, sino una herramienta estratégica que permite alinear los objetivos institucionales con las mejores prácticas de gobernanza digital, resiliencia operativa y transparencia administrativa.

Ilustración 1. Principios de la seguridad de la Información.

Fuente: https://infosegur.wordpress.com/tag/disponibilidad/

La información es, sin duda, uno de los activos más importantes y valiosos para la SOT, ya que contiene datos críticos y sensibles relacionados con sus actuaciones, procesos, usuarios, proveedores y la ciudadanía en general. Toda la información generada se debe ser protegida, garantizando en todo momento su confidencialidad, integridad y disponibilidad.

Para lograr cumplir con este objetivo, es fundamental desarrollar e implementar una política de seguridad de la información en la SOT. Esta política permitirá definir el propósito, dirección, principios y reglas básicas que orientarán las acciones necesarias para proteger adecuadamente los activos de información —tanto físicos como digitales— frente a los diversos riesgos a los que están expuestos, tales como pérdida, robo, alteración, daño, destrucción, eliminación o accesos no autorizados, incluidos los ataques cibernéticos.

Está política se concibe como el conjunto de mecanismos y directrices que deben seguir para proteger y garantizar confidencialidad, integridad y disponibilidad de la información de la SOT. Para garantizar la seguridad de la información, tanto física como digital, en la SOT, es fundamental definir claramente los responsables y recursos necesarios. Asimismo, se debe identificar, evaluar y gestionar los riesgos que amenazan los activos de información institucionales, prestando especial atención a aquellos procesos y funciones donde exista una

mayor probabilidad de que dichos riesgos se materialicen. A partir de este análisis, se deben establecer controles y medidas de seguridad adecuadas que protejan eficazmente los activos de información.

Es esencial definir directrices claras para la gestión y almacenamiento de la información, con el fin de asegurar su integridad, confidencialidad y disponibilidad. La implementación de estas medidas debe ir acompañada de un seguimiento continuo que permita verificar su efectividad y realizar ajustes cuando sea necesario. Todo este esfuerzo fortalece la capacidad de la institución para resistir y recuperarse ante incidentes de seguridad, mejorando así su resiliencia. Finalmente, es clave fomentar una cultura de seguridad en toda la institución, promoviendo la conciencia y el compromiso de todos los miembros con la protección de la información.

3.2. Alineación con los objetivos estratégicos institucionales.

Mediante la Resolución No. SOT-DS-2022-010, de fecha 11 de julio de 2022, la Máxima Autoridad aprobó el Plan Estratégico Institucional 2022-2025 (PEI) de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo. En dicha planificación estratégica se establecieron los objetivos estratégicos institucionales.

Tabla 1. Alineación con la planificación estratégica institucional.

OBJETIVO ESTRATÉGICO INSTITUCIONAL	**ESTRATEGIA**
OE2. Incrementar la disponibilidad de información e interoperatividad de los sistemas de información de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo.	**E2.1.** Fortalecer los procesos de registro y recopilación de información de los entes controlados para la toma de decisiones y un efectivo proceso de vigilancia y control. **E2.2.** Fortalecer el equipamiento tecnológico del Centro de Datos institucional en almacenamiento y procesamiento de la información. **E2.4.** Desarrollar mecanismos que garanticen la seguridad y disponibilidad de la información interna y externa. **E2.5.** Gestionar la cooperación interinstitucional que garanticen el acceso a la información.
OE5. Fortalecer las capacidades Institucionales.	**E5.5.** Fortalecer las capacidades técnicas y administrativas del personal de la SOT. **E5.6.** Fortalecer una gestión documental y archivística para resguardar y garantizar la disponibilidad de la documentación en la SOT. **E5.7.** Fortalecer la infraestructura y el equipamiento tecnológico e informático.

Fuente: PEI 2022 – 2025
Elaboración: CSISOT, 2025

3.3. Principios de la Política de Seguridad de la Información

La gestión de la seguridad de la información en la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo (SOT) se rige por los siguientes principios fundamentales, estipulados en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, los cuales orientan todas las acciones, controles y decisiones relacionados con la protección de los activos de información institucional. Asimismo, se complementa con principios adicionales que la institución ha considerado necesarios para fortalecer su marco de seguridad y garantizar una gestión integral y efectiva:

Confidencialidad: La información será accesible únicamente a las personas autorizadas, protegiendo su acceso contra divulgación, visualización, transferencia o uso indebido no autorizado.

Integridad: La información debe permanecer exacta, consistente, completa y veraz a lo largo de su ciclo de vida, evitando su modificación no autorizada, alteración, destrucción o corrupción de datos.

Disponibilidad: La información debe ser accesible y utilizable por los usuarios autorizados cuando sea requerida para el cumplimiento de los fines institucionales.

Trazabilidad (responsabilidad y auditabilidad): El registro y seguimiento de los accesos, transacciones y modificaciones realizadas sobre los activos de información, permitiendo su posterior revisión, auditoría y control.

Legalidad: Todo tratamiento de información debe cumplir los parámetros establecidos en el marco legal vigente.

Seguridad por diseño y por defecto

Incorporar la seguridad desde la fase inicial de cualquier proceso, sistema, infraestructura o desarrollo de servicios, garantizando que los controles de seguridad estén presentes desde el diseño y a lo largo de su ciclo de vida, mediante evaluación previa de riesgos, definición temprana de medidas de mitigación y la evaluación continua de vulnerabilidades.

Mejora continua

Establecer un proceso permanente de evaluación, monitoreo, aprendizaje y mejora de los controles de seguridad, que se adapte a los cambios tecnológicos, organizacionales y normativos, a través de evaluaciones periódicas de riesgos y la actualización constante de de políticas, normas y procedimientos.

3.4. Roles y Responsabilidades

Con el fin de garantizar el cumplimiento de los objetivos de la Política de Seguridad de la Información, se establecen los roles y responsabilidades con base en los lineamientos dispuestos en la Resolución SOT-DS-2024-012 de 08 de julio de 2024.

3.4.1 Superintendente de Ordenamiento Territorial, Uso y Gestión del Suelo

Responsable de aprobar la política interna y sus futuras modificaciones con la asesoría del Comité de Seguridad de la Información de la SOT.

3.4.2 Comité de Seguridad de la Información (CSI)

El Comité de la Seguridad de la Información de la SOT, es un cuerpo integrado por servidores de esta entidad, cuyo objetivo busca garantizar y facilitar la implementación de las iniciativas de seguridad de la información en la institución. Se constituyó mediante Resolución SOT-DS-2024-012, de 08 de junio de 2024. El CSISOT cumple un conjunto de responsabilidades clave orientadas a proteger los activos de información institucionales y fortalecer la gestión de la seguridad. Entre sus principales funciones se encuentran:

- Establecer los objetivos de la seguridad de la información, alineados a los objetivos institucionales.
- Gestionar la implementación, control y seguimiento de las iniciativas relacionadas a la seguridad de la información.
- Gestionar la aprobación de la política de seguridad de la información institucional, por parte de la máxima autoridad de la Institución.
- Aprobar las políticas específicas internas de seguridad de la información, que deberán ser puestas en conocimiento de la máxima autoridad.
- Realizar el seguimiento del comportamiento de los riesgos que afectan a los activos y recursos de información frente a las amenazas identificadas.

- Conocer y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto de acuerdo con la categorización interna de incidentes.
- Coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios, con base al Esquema Gubernamental de Seguridad de la Información.
- Promover la difusión de la seguridad de la información dentro de la institución.
- 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.
- Reunirse ordinariamente de forma bimestral y extraordinariamente en cualquier momento previa convocatoria.
- Informar semestralmente a la máxima autoridad sobre los avances de la implementación y mejora continua del Esquema Gubernamental de Seguridad de la Información.
- Las demás que se establezcan en la normativa vigente

El CSI de la SOT, está conformado por los siguientes integrantes:

- Coordinador/a General de Planificación y Gestión Estratégica
- Director de Administración del Talento Humano.
- Director/a Administrativo.
- Director/a de Comunicación Social.
- Coordinador/a General de Tecnologías de la Información y la Comunicación.
- Coordinador General de Asesoría Jurídica.
- Delegado de Protección de Datos Personales

El Comité de Seguridad de la Información será presidido por el responsable de la Coordinación General de Planificación y Gestión Estratégica, mientras que el responsable de la Dirección de Administración de Talento Humano ejercerá la Secretaría. El Oficial de Seguridad de la Información participará en las sesiones con voz, pero sin voto, y los representantes de los procesos Agregadores de Valor asistirán únicamente cuando se aborden temas relacionados con su gestión, también con voz, pero sin voto.

3.4.3 Presidencia del Comité de Seguridad de la Información.

De conformidad con lo dispuesto en el Acuerdo No. MINTEL-MINTEL-2024-0003 y en la Resolución SOT-DS-2024-012, de 08 de junio de 2024, la Presidencia del Comité de Seguridad de la Información asume un rol estratégico en la conducción, coordinación y supervisión de las políticas, lineamientos y acciones orientadas a garantizar la protección de la información institucional. En este marco, se detallan las responsabilidades que le competen, en observancia de la normativa vigente y en coherencia con los objetivos institucionales de seguridad y gestión de la información:

- Ejercer la representación oficial del Comité.
- Conducir y presidir las sesiones ordinarias y extraordinarias del Comité.
- Velar por el cumplimiento de las responsabilidades del Comité.
- Convocar, directamente o a través de Secretaría del Comité, a las sesiones ordinarias o extraordinarias.
- Suscribir los documentos que sean emitidos por el Comité.
- Suscribir con el Secretario del Comité, las actas de las sesiones y resoluciones.
- Informar a la máxima autoridad lo tratado en las sesiones del Comité y remitir el Acta de sesión correspondiente.
- Someter a decisión y aprobar con los miembros del Comité las políticas y demás normas, en el ámbito de las responsabilidades de este.
- Las demás conferidas por la normativa vigente.

3.4.4 Secretaría del Comité de Seguridad de la Información.

La Secretaría del Comité de Seguridad de la Información tiene a su cargo la gestión administrativa y técnica necesaria para el adecuado funcionamiento del Comité, lo que incluye el registro y custodia de la documentación generada, el seguimiento de los acuerdos adoptados y la comunicación efectiva entre los miembros, contribuyendo así al fortalecimiento de la seguridad de la información institucional, de conformidad con lo establecido en el Acuerdo No. MINTEL-MINTEL-2024-0003 y en la Resolución SOT-DS-2024-012, de 08 de junio de 2024, a continuación se detallan sus responsabilidades:

- Elaborar, por disposición del Presidente del Comité, las convocatorias a las sesiones ordinarias o extraordinarias e incluir los documentos de los temas por tratarse, en los casos que corresponda.
- Consolidar la información remitida por las unidades administrativas para ser presentada en las sesiones.

- Constatar el quórum necesario para la instalación de las sesiones y mantener un registro de los asistentes.
- Dar lectura al orden del día respectivo, así como al acta aprobada de la sesión anterior.
- Participar en las sesiones con voz y voto.
- Asesorar al Comité, dentro del ámbito de sus competencias.
- Llevar el registro de todas las actas de sesión a las que haya sido convocado el Comité de Seguridad de la Información.
- Llevar un registro de las decisiones que se adopten.
- Dar fe de las decisiones y actuaciones que se tomen, con la expresión del número de votos consignados.
- Prestar la colaboración necesaria a los miembros del Comité o sus delegados para el cumplimiento de las responsabilidades asignadas en esta Resolución y normativa vigente.
- Recibir las propuestas de los miembros del Comité para la elaboración del orden del día de las sesiones, y ponerlas a consideración del Presidente.
- Mantener y custodiar los expedientes generados por el Comité que contendrán las actas de las sesiones debidamente codificadas, convocatorias, listas de asistencia, informes y otros documentos relacionados con la gestión del Comité.
- Notificar, para su gestión y cumplimiento, los acuerdos, decisiones y resoluciones adoptadas por el Comité a las unidades administrativas correspondientes.
- Las demás asignadas por el Presidente del Comité o que le sean conferidas por la normativa vigente

3.4.5 Oficial de Seguridad de la Información

El Oficial de Seguridad de la Información desempeña un rol clave en la protección y gestión de los activos de información de la institución, asegurando la implementación efectiva de las políticas, procedimientos y controles establecidos. De acuerdo con lo dispuesto en el Acuerdo No. MINTEL-MINTEL-2024-0003, a continuación se detallan las responsabilidades específicas que le competen, orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información institucional:

- Identificar y conocer la estructura organizacional de la institución.
- Identificar las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI.

- Coordinar la implementación y actualización del Esquema Gubernamental de Seguridad de la Información EGSI en su institución.
- Coordinar con las áreas respectivas las propuestas para la elaboración de la documentación esencial del Esquema Gubernamental de Seguridad de la Información (EGSI).
- Elaborar, asesorar y coordinar con los funcionarios, la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas.
- 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.
- Fomentar la cultura de seguridad de la información en la institución, en coordinación con las áreas respectivas.
- 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.
- 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.
- Elaborar el procedimiento o plan de respuesta para el manejo de los incidentes de seguridad de la información presentados al interior de la institución.
- 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.
- 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.
- Mantener toda la documentación generada durante la implementación, seguimiento y mejora continua del EGSI, debidamente organizada y consolidada, tanto políticas, controles, registros y otros.
- Coordinar con las diferentes áreas que forman parte de la implementación del Esquema Gubernamental de Seguridad de la Información, la verificación, monitoreo y el control del cumplimiento de las normas, procedimientos políticas y controles de seguridad institucionales establecidos de acuerdo a las responsabilidades de cada área.

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

3.4.6 Delegado de Protección de Datos Personales

El Delegado de Protección de Datos Personales tiene la responsabilidad de supervisar y garantizar el cumplimiento de la normativa vigente en materia de protección de datos, velando por la adecuada gestión, tratamiento y resguardo de la información personal manejada por la institución. A continuación se detallan sus responsabilidades, en concordancia con lo establecido en la Ley Orgánica de Protección de Datos Personales:

- Informar y asesorar al Responsable y a los Encargados del Tratamiento de Datos Personales sobre las obligaciones legales y regulatorias emitidas por la Autoridad de Protección de Datos Personales.
    - Supervisar el cumplimiento de la normativa en materia de protección de datos dentro de todos los procesos, sistemas y actividades institucionales de la SOT.
    - Asesorar en el análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, y supervisar su aplicación;
    - Cooperar con la Autoridad de Protección de Datos Personales y actuar como canal de comunicación oficial ante requerimientos, inspecciones o auditorías, con relación a las cuestiones referentes al tratamiento de datos personales
    - Promover una cultura organizacional de privacidad y protección de datos, mediante acciones de sensibilización, formación y mejora continua.

- Coordinar la atención oportuna y técnica de las solicitudes de ejercicio de derechos por parte de los titulares, así como la gestión de incidentes de seguridad relacionados con datos personales.
- Mantener y actualizar el registro institucional de actividades de tratamiento de datos personales, incluyendo la documentación relacionada con análisis de riesgos, evaluaciones de impacto y actualizaciones normativas.
- Las demás que llegase a establecer la Autoridad de Protección de Datos Personales con ocasión de las categorías especiales de datos personales.

3.4.7 Coordinación General de Tecnologías de la Información y Comunicación (o quien hiciera sus veces)

La Coordinación General de Tecnologías de la Información y Comunicación ejerce funciones estratégicas relacionadas con la, gestión y supervisión de los recursos y servicios tecnológicos de la institución, asegurando su adecuado funcionamiento. Esta función se desempeña en cumplimiento de lo dispuesto en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, así como de la normativa técnica y legal vigente aplicable al entorno digital. A continuación se detallan sus responsabilidades específicas.

- Implementar, mantener y mejorar continuamente los mecanismos tecnológicos de protección, monitoreo, respaldo y recuperación de la información institucional que se gestione exclusivamente mediante medios digitales o electrónicos.
- Velar por la aplicación efectiva de los controles de seguridad tecnológica definidos en el Esquema Gubernamental de Seguridad de la Información, con responsabilidad exclusiva sobre los activos de información en formato digital o electrónico.
- Coordinar con el Oficial de Seguridad de la Información y el Comité de Seguridad de la Información la implementación de controles específicos de seguridad para los sistemas informáticos, servicios en línea, plataformas digitales y demás tecnologías de la información utilizadas por la institución.
- Definir y mantener los mecanismos de respaldo, recuperación y continuidad operativa de los activos de información digital, garantizando su disponibilidad frente a incidentes tecnológicos o de seguridad.
- Ejecutar medidas preventivas y correctivas sobre la infraestructura tecnológica institucional ante incidentes que afecten la confidencialidad, integridad o disponibilidad de la información digital, incluyendo accesos no autorizados, fallas técnicas o ciberataques.

- Brindar asistencia técnica y acompañamiento a las unidades administrativas en el uso seguro de los sistemas y plataformas digitales, fomentando buenas prácticas de seguridad de la información como la gestión de credenciales, actualizaciones de software y cumplimiento de políticas institucionales aplicables al entorno digital.

3.4.8 Coordinación General Administrativa Financiera (o quien hiciera sus veces).

La Coordinación General Administrativa Financiera tiene a su cargo la organización y supervisión de los recursos administrativos de la institución, asegurando el cumplimiento eficiente de los procesos internos. Esta función se ejerce en atención a la normativa aplicable y a las necesidades institucionales. A continuación se describen sus responsabilidades.

- Gestionar los activos de información físicos institucionales, tales como documentos impresos, archivos físicos, medios ópticos o magnéticos, mobiliario, equipos de cómputo, impresoras y demás equipos periféricos que contengan, transporten o generen información institucional.
- Controlar las condiciones físicas de almacenamiento, conservación, traslado y disposición final de los activos de información físicos, a fin de evitar su pérdida, sustracción, deterioro o acceso no autorizado.
- Administrar el inventario, mantenimiento, asignación, traslado y retiro de equipos que puedan contener información institucional en formato físico, conforme a las políticas de seguridad de la información.
- Implementar controles para restringir el acceso a espacios donde se almacenen activos de información físicos, tales como bodegas, oficinas, archivos centrales áreas de gestión documental y otros relacionados.
- Coordinar con la Dirección de Gestión Documental y Archivo (o quien hiciera sus veces) los procedimientos de archivo, custodia y disposición de documentos físicos, conforme a las normas de seguridad de la información establecidas en la institución.
- Promover la política de seguridad de la información en el ámbito de su competencia, mediante procesos de socialización y capacitación interna orientados al manejo seguro de los activos de información físicos.
- Custodiar los bienes institucionales que contengan o hayan contenido información (por ejemplo, equipos de cómputo), cuando estos sean dados de baja, trasladados o retirados de la institución, garantizando que la información almacenada sea entregada o transferida de forma segura a la unidad generadora correspondiente.

- Aplicar buenas prácticas de seguridad en el manejo de activos de información físicos, como el uso de archivadores bajo llave, la eliminación segura de documentos confidenciales y la gestión adecuada de medios físicos portátiles.

3.5. Alcance y usuarios

La Política de Seguridad de la Información es de cumplimiento obligatorio y constituye responsabilidad para toda persona que, bajo cualquier modalidad de relación laboral, contractual, académica o de cooperación o prestación de servicios, desempeñe actividades o funciones en la SOT, conforme las directrices y alcance establecido en este documento y en el Esquema de Seguridad de la Información.

El personal antedicho deberá aplicar medidas de protección necesarias para resguardar la información, con el fin de minimizar el riesgo de difusión, acceso y uso no autorizado, evitando impactos negativos en la imagen y gestión institucional.

La presente política es aplicable a todo activo de información, ya sea impreso, almacenado electrónicamente o trasmitido mediante correo u otros medios electrónicos o físicos, que la institución posea actualmente o adquiera en el futuro.

La ausencia de una mención explícita en el presente documento, no exime e la obligación de proteger todos los activos de información.

3.6. Clasificación de la información

Con el fin de garantizar la adecuada protección de los activos de información institucional y conforme a las definiciones que establece la Ley Orgánica de Transparencia y Acceso a la Información Pública (2023), se busca asegurar que toda la información generada, administrada o custodiada por la institución sea gestionada de manera responsable, considerando su sensibilidad, criticidad y el impacto que podría ocasionar su divulgación no autorizada; en este contexto, toda información institucional será clasificada de acuerdo con la siguiente caracterización tomando en cuenta los mismos criterios de sensibilidad, criticidad e impacto.

Tabla 2. Clasificación de la información.

Nivel de Clasificación	Definición
Información reservada	Información o documentación, final o preparatoria, haya sido o no generada por el sujeto obligado, que requiere de forma excepcional limitación en su conocimiento y distribución, de acuerdo con los criterios expresamente establecidos en la ley, y siempre que no sea posible su publicidad bajo un procedimiento de disociación, por existir un riesgo claro, probable y específico de daño a intereses públicos conforme a los requisitos contemplados en esta Ley. No existirá reserva de información en los casos expresamente establecidos en la Constitución de la República del Ecuador y la ley.
Información pública	Todo tipo de dato en documentos de cualquier formato, final o preparatoria haya sido o no generada por el sujeto obligado, que se encuentre en poder de los sujetos obligados por esta Ley, contenidos, creados u obtenidos por ellos, que se encuentren bajo su responsabilidad y custodio o que se hayan producido con recursos del Estado.
Información confidencial	Información o documentación, en cualquier formato, final o preparatoria, haya sido o no generada por el sujeto obligado, derivada de los derechos personalísimos y fundamentales, y requiere expresa autorización de su titular para su divulgación, que contiene datos que, al revelarse, pudiesen dañar los siguientes intereses privados: a) El derecho a la privacidad, incluyendo privacidad relacionada a la vida, la salud o la seguridad, así como el derecho al honor y la propia imagen; b) Los datos personales cuya difusión requiera el consentimiento de sus titulares y deberán ser tratados según lo dispuesto en la Ley Orgánica de Protección de Datos Personales; c) Los intereses comerciales y económicos legítimos; y, d) Las patentes, derechos de autor y secretos comerciales.

3.7. Lineamientos generales

Los lineamientos establecidos en el presente documento son de **cumplimiento obligatorio** para todas las servidoras y servidores de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo, así como para todas aquellas personas que, bajo cualquier modalidad, presten servicios en la institución, incluyendo contratos civiles, prácticas preprofesionales o pasantías.

En este sentido, su aplicación es permanente en todo momento en concordancia con la normativa legal, reglamentaria y las resoluciones vigentes. En caso de producirse modificaciones en el marco normativo aplicable, prevalecerán las disposiciones actualizadas sobre lo establecido en el presente documento.

Los registros, tanto físicos como electrónicos deberán almacenarse en zonas seguras con controles de acceso que garanticen su integridad, disponibilidad y confidencialidad, restringiendo el acceso únicamente a personal autorizado. Al cesar sus funciones, las y los servidores deberán entregar la totalidad de la documentación, expedientes, claves de acceso, registros, dispositivos electrónicos y cualquier otro recurso bajo su custodia.

De igual forma, es obligatorio reportar de manera inmediata a la Coordinación de Tecnologías de la Información y Comunicación, a través de la mesa de servicios tecnológicos (soporte@sot.gob.ec), cualquier actividad sospechosa que pueda comprometer la seguridad de la información institucional, incluyendo incidentes cibernéticos, malware o intentos de acceso no autorizado.

En cuanto al almacenamiento de la información digital institucional, el medio oficial dispuesto es la nube de archivos institucional (NextcloudSOT).

Finalmente, se prohíbe al personal de la SOT realizar acciones que vulneren los principios de protección, integridad confidencialidad y disponibilidad de los activos de información institucionales.

3.7.1. Obligaciones individuales del usuario

a. El uso de los recursos institucionales (computadores, portátiles, dispositivos móviles, plataformas digitales, servicios de internet, correo institucional, entre otros) estará destinado exclusivamente al cumplimiento de actividades propias de la institución.

b. Queda estrictamente prohibido almacenar, visualizar o exponer contraseñas, datos personales o claves de acceso en lugares visibles, tales como escritorios, pantallas o dispositivos.

c. Toda documentación impresa deberá mantenerse debidamente archivada y resguardada, conforme los procedimientos institucionales.

d. El personal de la SOT deberá retirar de manera inmediata cualquier documento físico impreso en los equipos de impresión institucional, evitando su exposición o pérdida.

e. El acceso a información no autorizada, no asignada o sin el debido permiso expreso, está prohibido para todo el personal de la SOT.

f. El uso de internet y de los recursos tecnológicos institucionales deberá realizarse de manera ética, profesional y conforme a la normativa.

g. El personal de la SOT deberá reportar de manera inmediata a la Coordinación General de Tecnologías de la Información y Comunicación, o quien haga sus veces, cualquier actividad sospechosa que pueda comprometer la seguridad de la información digital institucional, tales como accesos no autorizados a sistemas, ataques cibernéticos, presencia de software malicioso o vulneraciones a redes o plataformas tecnológicas.

h. Los incidentes relacionados con activos de información físicos deberán ser comunicarse a la unidad responsable de su custodia o al área administrativa competente, de conformidad con los procedimientos internos establecidos.

3.7.2. Manejo documental y seguridad de los activos de información institucional

a. Todos los documentos generados o recibidos por las unidades administrativas de la SOT, en el ejercicio de sus funciones, deberán ser registrados e ingresados en el sistema de gestión documental institucional (físico y digital). Se exceptúa únicamente la información calificada como confidencial, para la cual la unidad institucional responsable de la gestión documental deberá generar mecanismos para su registro y tratamiento.

b. La unidad institucional responsable de la gestión documental a nivel central será la encargada de definir los permisos de acceso dentro del sistema de gestión documental institucional.

c. Se asegura el acceso a la información generada por la institución que no haya sido calificada como reservada o confidencial, en observancia de los principios de transparencia activa y pasiva establecidos en la Ley Orgánica de Transparencia y Acceso a la Información Pública, garantizando así, el derecho de los usuarios o de la ciudadanía en general.

d. El almacenamiento de los activos de información, tanto en soporte físico como digital, deberá realizarse en condiciones seguras, cumpliendo estándares físicos, ambientales y tecnológicos adecuados.

e. Cada unidad administrativa de la SOT será responsable de mantener ordenado y depurado tanto su archivo físico y digital, conforme su origen y contenido, garantizando la integridad, confidencialidad y disponibilidad de los activos de información institucional.

f. Para el traspaso y préstamo de documentación, la unidad responsable de la gestión documental emitirá los procedimientos, lineamientos, formatos respectivos y demás disposiciones necesarias.

g. Queda prohibido el traslado de archivos físicos fuera de las instalaciones de la SOT, tanto en matriz como en el nivel desconcentrado, salvo en los casos de traslados y/o préstamos documentales debidamente autorizados conforme lo establecido en el literal anterior.

h. La documentación mediante servicios de mensajería, transporte y entrega de correspondencia a nivel nacional deberá gestionarse conforme los procedimientos, lineamientos y formatos emitidos por la unidad responsable de la gestión documental, o quien haga sus veces. Los contratos suscritos con terceros por estos servicios deberán incluir cláusulas de responsabilidad y confidencialidad para el manejo y transporte de la documentación.

i. Al término de la relación laboral del personal de la SOT, la unidad administrativa titular de la información será responsable de recibir la documentación institucional a cargo del servidor saliente, manteniéndola bajo su custodia. Asimismo, El área dueña de la información debe verificar la devolución de los activos institucionales, incluyendo tanto la información física como digital, según la norma pertinente.

j. La unidad responsable de la gestión documental, o quien haga sus veces, emitirá el protocolo que regule el procedimiento de devolución y verificación del estado e integridad de la documentación.

k. La eliminación de la documentación que conforman los activos de información pública institucional se realizará conforme a los criterios de valoración documental y previa autorización de la autoridad competente.

l. Para la eliminación y/o borrado seguro de medios digitales institucionales que contengan documentos oficiales, en especial aquellos con datos personales o información clasificada como reservada o confidencial, se realizará conforme la normativa vigente en la materia, mediante mecanismos de destrucción certificada o sobreescritura criptográfica.

m. Está prohibido almacenar o compartir documentos que contengan datos personales sin medidas de seguridad adecuadas, ni el consentimiento correspondiente.

n. Los datos y registros de información física y digital considerados críticos deberán protegerse contra pérdida, destrucción o alteración. En determinados casos, será necesario almacenarlos mediante métodos más seguros, así como realizar respaldos periódicos de la información derivada de las actividades fundamentales de la institución.

o. Para todos los aspectos relacionados con la gestión documental que no se encuentren expresamente señalados en el presente instrumento, se aplicará lo dispuesto en las políticas, manuales, instructivos y normas técnicas institucionales emitidas por la unidad responsable de la gestión documental, o por quien haga sus veces.

3.7.3. Gestión de usuarios para el acceso a los recursos tecnológicos institucionales

a. La gestión de usuarios para el acceso a los recursos tecnológicos institucionales será responsabilidad exclusiva de la Coordinación General de Tecnologías de la Información y Comunicación, o quien haga sus veces. Esta se realizará únicamente a partir de una solicitud expresa emitida por la Dirección de Administración de Talento Humano a través de la mesa de servicios de tecnología.

   La solicitud deberá incluir, sin excepción, la documentación que acredite el cumplimiento de los principios y deberes establecidos en la normativa vigente en materia de protección de datos personales. En particular, deberá adjuntarse:

   - El Acuerdo de Confidencialidad debidamente firmado por el personal de la SOT.
   - El Acuerdo de Uso de Recursos Tecnológicos y Manejo de Información Personal, conforme a lo dispuesto en la Ley Orgánica de Protección de Datos Personales y la política institucional.

   La CGTIC no procederá con la creación, habilitación o asignación de credenciales de usuario si no se han presentado, de manera completa y verificable los documentos antes señalados.

b. En la solicitud de creación de usuario, la Dirección de Administración de Talento Humano, deberá especificar los servicios a los que el usuario tendrá acceso, los cuales podrán incluir:

   – Acceso a la red institucional

- Acceso a equipos informáticos o estaciones de trabajo de TI
- Acceso a internet
- Acceso a correo institucional
- Acceso a sistema de gestión documental institucional
- Acceso a sistema de almacenamiento en nube Nextcloud

c. Para el acceso a aplicaciones, módulos o sistemas institucionales, la solicitud deberá ser presentada por el responsable del proceso mediante el sistema de gestión documental institucional dirigida a la CGTIC. Esta solicitud deberá contener: el nombre del usuario, los permisos requeridos, el sistema o módulo específico y la justificación del acceso solicitado. La CGTIC validará esta información y procederá únicamente si se cumplen los requisitos de documentación establecidos en esta política.

d. En caso de cambios en la denominación del cargo del usuario, o si se generan circunstancias que hagan innecesario o inadecuado su acceso a sistemas, módulos o aplicaciones previamente autorizados, el responsable del proceso deberá notificar de manera inmediata la baja de permisos o accesos. Esta notificación se realizará a través de correo electrónico dirigido a la mesa de servicios de tecnología, indicando con claridad: el nombre del usuario, el sistema afectado y el motivo de la desvinculación o modificación.

e. En caso de salida definitiva del usuario, la Dirección de Administración de Talento Humano será la única unidad autorizada para solicitar a la CGTIC la baja del usuario institucional en todos los sistemas y servicios de la SOT. Esta solicitud deberá remitirse a la mesa de servicios de tecnología, indicando expresamente el nombre completo del usuario y la fecha en la que deberá efectuarse la desactivación de sus credenciales institucionales.

3.7.4. Gestión del uso adecuado del correo electrónico

a. El servicio y las cuentas de correo electrónico institucional bajo el dominio “@sot.gob.ec” son propiedad de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo. El personal de la SOT deberá utilizarlas de manera adecuada y responsable, conforme las siguientes disposiciones:
   - El uso de la cuenta del correo electrónico institucional es responsabilidad exclusiva del personal de la SOT.
   - Los mensajes de correo electrónico enviados y recibidos que tengan valor documental para la SOT archivarse de acuerdo la Ley del Sistema Nacional de Archivos.

b. El correo electrónico institucional deberá emplearse únicamente para el ejercicio de funciones y/o la elaboración de productos asignados al personal de la SOT. Queda prohibido su uso con fines distintos a los institucionales. El titular de la cuenta será responsable tanto del contenido de los mensajes enviados como de los documentos o archivos adjuntos remitidos.

c. Está estrictamente prohibido enviar mediante correo electrónico institucional información o archivos clasificados como reservados o confidenciales.

d. Queda prohibido utilizar el correo electrónico institucional para actividades de carácter personal, político, comercial, de entretenimiento u otras ajenas al quehacer institucional. Asimismo, no podrá emplearse para el envío de correos masivos no autorizados, el registro en servicios personales o la transmisión de mensajes vulgares, obscenos o inapropiados. El incumplimiento será sancionado conforme la normativa correspondiente.

e. El personal de la SOT no deberá responder correos, abrir enlaces de origen dudoso, ni proporcionar contraseñas por este medio, incluso cuando la solicitud parezca provenir de una dirección autorizada. En caso de que la cuenta se vea comprometida o exista riesgo de seguridad, el usuario deberá informar de inmediato a la CGTIC mediante la mesa de servicios de tecnología.

f. Es responsabilidad del personal de la SOT eliminar los mensajes de origen desconocido y asumir las consecuencias derivadas de la apertura de archivos adjuntos no verificados.

g. El Comité de Seguridad de la Información de la SOT evaluará todo incidente o señal de posible uso indebido de las cuentas de correo institucionales. Únicamente cuando el análisis técnico y contextual lo justifique, el Comité autorizará la revisión y control de las cuentas de correo electrónico asignadas. Los resultados serán comunicados de manera formal e inmediatamente a la máxima autoridad para las acciones que correspondan.

h. Está expresamente prohibido el uso de servicios de correo electrónico externos (como Gmail, Outlook, Yahoo, entre otros) para el envío o recepción de información institucional. Toda comunicación oficial deberá realizarse exclusivamente a través de cuentas de correo electrónico bajo el dominio institucional "@sot.gob.ec". La Coordinación General de Tecnologías de la Información y Comunicación implementará el bloqueo técnico de accesos a correos externos desde la red institucional.

   En caso de requerirse el uso de dominios diferentes al institucional, deberá solicitar autorización al Comité de Seguridad de la Información, mediante documento ingresado en el sistema de gestión documental institucional, motivando la necesidad y asumiendo la responsabilidad que conlleva dicha autorización.

i. Las cuentas de correo electrónico genéricas (ej. info@, contacto@, soporte@) podrán crearse únicamente cuando exista una necesidad institucional debidamente justificada. La solicitud deberá ser presentada por la autoridad responsable del área requirente, para aprobación de la Coordinación General de Tecnologías de la Información y Comunicación, la cual informará al Comité de Seguridad de la Información.

j. Toda cuenta genérica deberá estar vinculada a un servidor, funcionario o trabajador con nombramiento o contrato vigente, quien será designado como custodio responsable de su uso, acceso, trazabilidad y seguridad. La entrega de usuarios y contraseñas de estas cuentas se efectuará exclusivamente a dicha persona, quien asumirá plena responsabilidad sobre su uso y deberá cumplir las políticas institucionales de seguridad de la información.

k. El reenvío de correos institucionales a cuentas personales está prohibido. Solo se exceptúan las respuestas necesarias a destinatarios externos.

3.7.5. Uso adecuado de equipos tecnológicos e informáticos

a. El acceso remoto estará restringido y deberá hacerse a través de conexiones de Red Privada Virtual (VPN) con doble autenticación.

b. Queda prohibido conectar los equipos informáticos institucionales a redes no autorizadas. Solo se permitirá el uso de redes institucionales proporcionadas por la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo. La CGTIC, o quien haga sus veces, implementará el bloqueo técnico de acceso a redes externas desde los dispositivos oficiales. En caso de requerirse conexión a otras redes, el personal de la SOT deberá solicitarlo mediante la mesa de servicios de tecnología a la Coordinación General de Tecnologías de la Información y Comunicación indicando la justificación correspondiente.

c. Ningún miembro del personal de la SOT podrá instalar, desinstalar o modificar software en los equipos informáticos asignados. La configuración de los equipos, así como la instalación de software, aplicaciones o dispositivos será responsabilidad exclusiva de CGTIC. En caso de requerirse software adicional, la solicitud debe presentarse mediante la mesa de servicios de tecnología. De igual manera, todo software instalado deberá contar con la respectiva licencia de uso.

d. Se prohíbe la manipulación técnica de los equipos informáticos y tecnológicos por personal no autorizados.

e. El personal de la SOT que disponga de un equipo institucional (computador de escritorio o portátil), deberá cumplir las siguientes normas:

- Bloquear o cerrar sesión del computador siempre que se ausente de su puesto de trabajo, a fin de evitar accesos no autorizados.
- Almacenar únicamente información institucional generada en el ejercicio de sus funciones dentro de la SOT.
- Permitir el acceso a los equipos en casos de evaluaciones internas.

f. La máxima autoridad o el Comité de Seguridad de la Información de la SOT podrán disponer el monitoreo del uso de los equipos tecnológicos e informáticos institucionales en caso de incidentes de seguridad de la información.

g. Queda prohibido trasladar equipos tecnológicos e informáticos fuera de las instalaciones de la SOT, tanto en matriz como a nivel desconcentrado, sin autorización previa de la Dirección Administrativa. En los casos de traslado autorizado, el personal de la SOT será responsable del uso y asumirá los riesgos de seguridad de la información derivados de la conexión a redes externas o fuera del control institucional.

h. En el caso de pérdida, robo o hurto de los equipos institucionales se deberá notificar de manera inmediata a la Coordinación General de Tecnologías de la Información y Comunicación para el bloqueo del usuario y a la Dirección Administrativa para las acciones correspondientes.

i. Se prohíbe el uso de dispositivos de almacenamiento externo a través de puertos USB (como memorias externas, discos duros portátiles u otros medios removibles) en los equipos institucionales. La CGTIC procederá al bloqueo técnico de dichos en todos los dispositivos institucionales. Cualquier solicitud de habilitación temporal de estos puertos deberá contar con autorización expresa de la CGTIC en conjunto con el Oficial de Seguridad de la Información, quienes informarán al Comité de Seguridad de la Información de la SOT.

j. La CGTIC será responsable de realizar el respaldo diario de los archivos generados y almacenados en la nube de información institucional. Dicho respaldo estará sujeto a la capacidad disponible en el hardware de almacenamiento con el que cuente la institución, por lo que la conservación de la información se encuentra limitada al espacio disponible.

k. Antes de la baja de equipos institucionales, el personal de la SOT deberá eliminar todos los datos confidenciales, previa coordinación con la unidad responsable de la información, asegurando el respectivo respaldo.

l. Todo el personal de la SOT deberá cumplir con los requisitos institucionales relativos a la protección y cuidado de los equipos tecnológicos e informáticos o bajo su responsabilidad, independientemente del nivel de sensibilidad de la información que contengan.

m. El uso indebido, intencional negligente o con fines no permitidos o negligentes de los equipos tecnológicos e informáticos institucionales será causal de sanción conforme a la normativa correspondiente.

3.7.6. Responsabilidad sobre los activos de información institucional

a. Toda información generada, recibida o gestionada dentro de la SOT, ya sea en formato físico o digital, constituye propiedad institucional.
b. El personal de la SOT es responsable de la protección y custodia de los activos de información institucional, independientemente del medio, sistema o plataforma en el que se almacenen o procesen (sistemas administrativos, aplicativos informáticos, servicios tecnológicos, bases de datos, reportes, archivos temporales o permanentes, entre otros).
c. Al finalizar sus funciones o contratos, los servidores y contratistas están obligados a devolver todos los documentos, dispositivos, claves, registros y activos de información asignados durante el ejercicio de sus funciones.
d. Es obligación del personal de la SOT almacenar los activos de información digital que se generen en el ejercicio de sus funciones en la nube de archivos institucional (NextcloudSOT) y/o en el sistema de gestión documental, según corresponda.
e. En caso de desvinculación de un servidor, su superior jerárquico podrá solicitar la apertura de los equipos tecnológicos asignados al exservidor, así como el acceso a su espacio de almacenamiento en la nube de archivos institucional y a un respaldo de su correo electrónico. Respecto a los equipos informáticos, la CGTIC consultará al área correspondiente si requiere acceso al equipo para efectuar un respaldo de la información.

   El propósito de esta acción es revisar, organizar y resguardar la información que, por su naturaleza, resulte necesaria para garantizar la continuidad de los procesos institucionales. Este procedimiento deberá ejecutarse con rigor, asegurando la integridad y confidencialidad de los datos. La información recuperada se almacenará exclusivamente en la carpeta correspondiente al grupo del área generadora de la información, dentro de la plataforma Nextcloud, a fin de garantizar su disponibilidad para los responsables legítimos y asegurar la trazabilidad del proceso.

3.7.7. Uso adecuado de la red institucional e internet

a. El acceso a contenidos de internet que incluyan violencia, racismo, material sexual, juegos en línea, plataformas de streaming, compras en línea o descargas de música y/o videos queda restringido para todo el personal de la SOT.

b. En caso de que una página restringida sea necesaria para el cumplimiento de las funciones institucionales, el personal de la SOT deberá solicitar acceso a la Coordinación General de Tecnologías de la Información y Comunicación, adjuntando la respectiva justificación.

c. La CGTIC diseñará, propondrá y ejecutará perfiles de navegación diferenciados, con base en criterios de seguridad de la información, proporcionalidad técnica y efectividad en el desempeño de funciones institucionales. La aprobación de dichos perfiles corresponderá al Comité de Seguridad de la Información, como parte de las medidas destinadas a garantizar el uso adecuado y seguro de los recursos tecnológicos institucionales.

d. El uso de servicios de mensajería web tales como WhatsApp Web, Telegram Web, Facebook Messenger u otros similares queda prohibido. La única plataforma autorizada para mensajería web dentro en la institución es **nextcloud.sot.gob.ec**.

   Podrán otorgarse permisos adicionales de manera controlada y temporal, sin exceder el último día del año en curso. La solicitud deberá presentarse mediante el formulario de accesos especiales y ser gestionada por el jefe inmediato de quien requiera el permiso especial. Toda habilitación temporal requerirá autorización expresa de la Coordinación General de Tecnologías de la Información y Comunicación y del Oficial de Seguridad de la Información, quienes informarán al Comité de Seguridad de la Información de la SOT.

e. La CGTIG implementará los mecanismos de bloqueo técnico necesarios para impedir el acceso a servicios no autorizados desde la red institucional, en cumplimiento de las políticas de seguridad de la información vigentes.

f. Únicamente podrán conectarse a la red institucional los equipos pertenecientes a la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo. El acceso a equipos externos podrá habilitarse de forma controlada y temporal, sin superar el último día del año en curso, mediante la presentación del formulario de accesos especiales, gestionado por el jefe inmediato del solicitante. Toda habilitación temporal deberá contar con autorización expresa de la CGTIC y del OSI, quienes pondrán en conocimiento al Comité de Seguridad de la Información de la SOT.

g. Todos los equipos institucionales deberán contar obligatoriamente con el software antivirus provisto por la institución, instalado, activo y actualizado como condición para acceder a la red. En el caso de los equipos externos, será obligatorio disponer de un antivirus instalado, activado y actualizado.

h. La SOT garantizará la protección de la información y de los recursos de procesamiento mediante la implementación de controles de seguridad, tales como antivirus, cortafuegos,

control de contenidos y navegación, así como mecanismos de protección para el correo electrónico entrante y saliente.

3.7.8. Gestión de aplicativo de nube institucional de almacenamiento de archivos

a. La Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo establece como única plataforma autorizada para el almacenamiento, gestión y compartición de archivos el aplicativo Nextcloud, disponible exclusivamente en el dominio nextcloud.sot.gob.ec.
b. El uso de nubes externas (OneDrive, Google Drive, Dropbox, Mega, WeTransfer u otras) está estrictamente prohibido para todos los perfiles. Sólo se podrán habilitar accesos excepcionales de forma controlada y temporal, sin exceder el último día del año en curso, mediante el formulario de accesos especiales. La solicitud deberá ser presentada por el jefe inmediato del funcionario que requiera el permiso y contar con autorización expresa de la CGTIC y el OSI, quienes informarán al Comité de Seguridad de la Información de la SOT.

   El uso de la plataforma deberá enmarcarse en los principios de confidencialidad, integridad, disponibilidad y trazabilidad de la información.
c. En caso de compartición externa de archivos o carpetas mediante enlaces públicos generados desde la plataforma Nextcloud, la responsabilidad por el uso indebido o divulgación de la información recaerá directamente en el usuario que generó el enlace.
d. Se exhorta a que en todo enlace externo sea configurado con fecha de expiración y contraseña de acceso.
e. La GTIC podrá evaluar periódicamente el uso de Nextcloud, revisar los permisos de compartición y aplicar restricciones de acceso en caso de detectar riesgos o usos inadecuados.

3.7.9. Gestión y seguridad de contraseñas

a. Todas las contraseñas asociadas a cuentas de usuario final son estrictamente personales e intransferibles, por lo que no deberán compartirse en ninguna circunstancia ni a través de ningún medio.
b. Las contraseñas creadas por el personal de la SOT para acceder a los distintos sistemas informáticos son de administración y gestión exclusiva de cada usuario, quien asume plena responsabilidad sobre su uso y custodia.
c. Para garantizar la seguridad de las cuentas de usuario final, las contraseñas deberán cumplir con los siguientes requisitos mínimos:

- Tener una longitud mínima de nueve (9) caracteres.
- Incluir letras mayúsculas y minúsculas.
- Incorporar números y al menos un carácter especial (ejemplo: “,#,*,.,?)

d. Las contraseñas deberán actualizarse obligatoriamente cada treinta (30) días.

e. Las contraseñas correspondientes a cuentas especiales de administración de infraestructura serán de uso exclusivo y responsabilidad de la CGTIC.

f. En caso de sospecha de compromiso, exposición o vulneración de la contraseña, el personal de la SOT deberá proceder de inmediato al cambio de esta, o en su defecto, solicitar el restablecimiento forzado.

g. Las contraseñas de las cuentas institucionales en redes sociales deberán ser modificadas cada vez que se produzca la desvinculación de un servidor de la Dirección de Comunicación Social.

3.7.10. Gestión de la seguridad física y de instalaciones

a. El Comité de Seguridad de la Información de la SOT, en coordinación con los responsables de las unidades administrativas, clasificarán las instalaciones en zonas de acceso público, controlado y/o restringido, asegurando que dicha clasificación quede debidamente documentada.

b. Se prohíbe el ingreso del personal de la SOT a las instalaciones de la institución, tanto a nivel central como desconcentrado, fuera del horario laboral establecido, fines de semana y feriados. Cuando sea necesario acceder a las instalaciones fuera de estos horarios, se debe solicitar autorización mediante el sistema de gestión documental institucional, dirigida a la Coordinación General Administrativa Financiera, la cual llevará un registro de todas las autorizaciones emitidas, disponible para revisión en cualquier momento. El personal de la SOT que ingrese será responsable de los riesgos relacionados con la seguridad de la información.

c. La CGAF será la responsable de emitir las directrices para la custodia de la infraestructura donde se encuentran los activos de información, mientras que cada unidad administrativa será responsable de la implementación de estos controles.

d. El personal de la SOT deberá mantener los equipos tecnológicos en condiciones de seguridad adecuadas, con el fin de minimizar los riesgos de robo o pérdida.

3.7.11. Control de las vulnerabilidades técnicas

a. Verificar que los sistemas operativos y sistemas de procesamiento de información estén actualizados con las últimas versiones compatibles con los aplicativos utilizados por la SOT, aplicando los parches de seguridad correspondientes a cada sistema operativo.

b. La CGTIC deberá realizar validaciones periódicas de los siguientes controles:

- Revisar periódicamente las reglas de acceso en los equipos de seguridad perimetral.
- Generar informes periódicos sobre usuarios y perfiles de acceso a la infraestructura tecnológica.
- Proponer actualizaciones a los controles existentes, según los requerimientos o necesidades identificadas.

3.7.12. Gestión de incidentes de seguridad de la información y continuidad de la operación.

a. La Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo (SOT) garantizará la existencia de mecanismos adecuados para la gestión de incidentes de seguridad de la información, con el objetivo de preservar la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información institucionales. Para ello, se establecen dos canales diferenciados de notificación y atención de incidentes:

- *Canal digital:* Todo incidente relacionado con activos de información digitales deberá ser notificado y gestionado a través de la mesa de servicios tecnológicos de la Coordinación General de Tecnologías de la Información y Comunicación, que será responsable de su recepción, análisis, respuesta y documentación.
- *Canal físico:* Los incidentes relacionados con documentos físicos -como extravíos, mal uso o deterioro de archivos en medios impresos, ópticos u otros- serán gestionados por la Dirección de Gestión Documental y Archivo, o quien haga sus veces, conforme a los procedimientos establecidos para la custodia, recuperación y resguardo de documentos físicos institucionales.

En ambos casos, los responsables deberán comunicar al Oficial de Seguridad de la Información y al Comité de Seguridad de la Información de la SOT.

b. La SOT fomentará la notificación de incidentes relacionados con la seguridad de la información, plataformas tecnológicas o sistemas informáticos, asignando las responsabilidades correspondientes para su tratamiento. Los incidentes reportados deberán ser investigados y gestionados.

Todo incidente de seguridad que involucre datos personales deberá ser tratado bajo el protocolo de gestión de incidentes de seguridad de la información, notificando al Delegado de Protección de Datos Personales, quien a su vez comunicará al Comité de Seguridad de la Información de la SOT.

c. La SOT garantizará una respuesta oportuna y eficaz ante cualquier afectación a los activos de información institucionales, aplicando el Plan de tratamiento de riesgos y el Plan de continuidad con el fin de mitigar los riesgos asociados y asegurar la continuidad operativa de la Institución.

3.8. Protección de datos personales[1]

La Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo, en observancia de la Ley Orgánica de Protección de Datos Personales (LOPDP) y su Reglamento, establece las siguientes directrices, reconociendo a la seguridad de la información como un componente transversal y habilitador para garantizar la protección de los datos personales institucionales, particularmente en lo referente a los principios de confidencialidad, integridad y disponibilidad.

3.8.1. *Controles específicos de seguridad*

La SOT implementará controles específicos en materia de seguridad de la información aplicables al tratamiento de datos personales:

a. La clasificación de la información deberá contemplar expresamente la categoría de información confidencial para los datos personales.
b. Todo tratamiento de datos personales deberá contar con el correspondiente consentimiento informado, debidamente registrado, salvo en los casos de excepción previstos en la LOPDP.
c. Se establecerán mecanismos de control de acceso lógico (digital) y físico diferenciados para los activos de información que contengan datos personales.
d. Todo acceso a bases de datos de carácter personal será registrado mediante trazabilidad (logs de acceso), administrados por el área de tecnologías de la información y disponible para fines de control.

[1] Este acápite no sustituye ni modifica la Política General de Protección de Datos Personales de la SOT, la cual mantiene su plena vigencia y se integra como documento normativo complementario de esta política.

e. Se aplicarán controles de cifrado de datos, tanto en tránsito como en almacenamiento, especialmente para el caso de datos sensibles.
f. Se realizarán periódicamente Evaluaciones de Impacto a la Protección de Datos personales (EIPD), coordinadas por el Delegado de Protección de Datos Personales en conjunto con el Oficial de Seguridad de la Información.
g. Los contratos y convenios con terceros que impliquen acceso a datos personales deberán incluir cláusulas específicas de seguridad de la información y confidencialidad, conforme al principio de corresponsabilidad establecido en la LOPDP.

4. Comunicación de la Política

La Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo socializará la Política de Seguridad de la Información a todo su personal, mediante la aplicación de las estrategias y lineamientos establecidos en el Plan de Comunicación y Sensibilización, con el propósito de fortalecer la cultura instituciona en materia de seguridad de la información, protección de los activos de información y cumplimiento de las disposiciones legales correspondientes.

5. Sanciones

Toda violación a la presente Política de Seguridad de la Información será objeto de las acciones disciplinarias que correspondan, conforme a los procedimientos establecidos y la normativa interna de la SOT, sin perjuicio de las responsabilidades administrativas, civiles o penales que pudieran derivarse.

6. Definiciones y abreviaturas

Se describen a continuación los términos y abreviaturas utilizadas a lo largo del documento, con el objetivo de asegurar una comprensión uniforme y precisa de los conceptos empleados por todo el personal de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo.

Tabla 3. Abreviaturas

Abreviatura	Definición
CSISOT	Comité de Seguridad de la Información de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo
CGAF	Coordinación General Administrativa Financiera
CGAJ	Coordinación General de Asesoría Jurídica

CGPG	Coordinación General de Planificación y Gestión Estratégica
CGTIC	Coordinación General de Tecnologías de la Información y Comunicación
COOTAD	Código Orgánico de Organización Territorial, Autonomía y Descentralización
DATH	Dirección de Administración de Talento Humano
DPDP	Delegado de Protección de Datos Personales
EGSI	Esquema Gubernamental de Seguridad de la Información
EIPD	Evaluaciones de Impacto a la Protección de Datos personales
LOOTUGS	Ley Orgánica de Ordenamiento Territorial, Uso y Gestión del Suelo
LOPDP	Ley Orgánica de Protección de Datos Personales
LOT	Ley Orgánica de Telecomunicaciones
LOTAIP	Ley Orgánica de Transparencia y Acceso a la Información Pública
LOTDA	Ley Orgánica para la Transformación Digital y Audiovisual
MINTEL	Ministerio de Telecomunicaciones y de la Sociedad de la Información
OSI	Oficial de Seguridad de la Información
PEI	Plan Estratégico Institucional
RLOOTUGS	Reglamento General a la Ley Orgánica de Ordenamiento Territorial, Uso y Gestión del Suelo
RLOTDA	Reglamento General a la Ley Orgánica para la Transformación Digital y Audiovisual
TI	Tecnologías de la Información
SGSI	Sistema de Gestión de Seguridad de la Información
SOT	Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo

Elaboración: CSISOT, 2025

Conforme a lo dispuesto en el Acuerdo Ministerial Nro. MINTEL-MINTEL-20241-0003, publicado en el Tercer Suplemento N°509 del Registro Oficial el 01 de marzo de 2024, se establecen los lineamientos para la implementación del Esquema Gubernamental de Seguridad e la Información. En este contexto, se describen a continuación los términos y definiciones utilizados en la presente Política de Seguridad de la Información, con el fin de garantizar una comprensión uniforme y precisa de los conceptos empleados, facilitando así su correcta aplicación por parte de todo el personal de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo.

Tabla 4. Términos y definiciones

Término	Definición
A	
Activos de información	Comprende a los sistemas de información, aplicaciones o herramientas de tipo software, bases de datos, equipos computacionales, dispositivos móviles, archivos físicos, documentos electrónicos o cualquier otro activo que por su naturaleza registre, procese, almacene o transmita información.
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.
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)	Es un equipo integrado por los responsables de las áreas de la institución que tiene como objetivo, garantizar y facilitar la implementación de las iniciativas de seguridad de la información en la institución.
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	Políticas, procedimientos, prácticas y 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 la institución 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	
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 la información de ser accesible y utilizable en el momento que sea requerido por una entidad autorizada.
E	
Esquema Gubernamental de Seguridad de la Información	Esquema para preservar la integridad, disponibilidad y confidencialidad de la información.
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.
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 de los incidentes de seguridad de la información.
Gestión de riesgos	Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
I	
Identificación de riesgos	Proceso de encontrar, reconocer y describir riesgos.
Impacto	El costo para la institución de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros (ejem.: pérdida de reputación, implicaciones legales, entre otros).
Incidente de seguridad de la información	Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones de la institución 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.
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. 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.
M	
Malware, software	Software diseñado con malas intenciones que contiene

malicioso	características o capacidades que potencialmente pueden causar daño directamente o indirectamente al usuario y/o al sistema informático del usuario.
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).
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	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	Persona u organización que puede afectar, verse afectada por, o percibirse a sí misma como afectada por una decisión o actividad.
Personal de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo	Para efectos de la presente política, se entenderá por personal de la SOT a toda persona natural que, bajo cualquier modalidad de relación laboral, contractual, académica o de cooperación, presta servicios, desarrolla actividades o cumple funciones en la SOT. Las unidades responsables de procesos deben identificar y clasificar los activos de información bajo su control. Todo servidor institucional es responsable del correcto manejo y custodia de la información bajo su acceso.
Phishing (engaño técnico)	Proceso fraudulento o intento de adquirir información privada o confidencial de manera enmascarada haciéndose pasar por una entidad confiable en una comunicación electrónica.
Plan de continuidad del proceso	Plan orientado a permitir la continuación de las principales funciones de la institución 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 que indica al personal de la institución que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.
Proceso	Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.
Propietario del activo	Puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la institución.

Propietario de la Información	Es el responsable de clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.
Propietario del riesgo	Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.
Proveedor de servicios de internet	Organización que presta servicios de Internet a un usuario y permite a sus clientes acceder a internet.
R	
Registro	Información creada, recibida y mantenida como evidencia y como activo por una institución o persona, en cumplimiento de obligaciones legales y de sus atribuciones.
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.
Seguridad de los Activos de Información	Conforme lo determina el Ministerio de Telecomunicaciones y de la Sociedad de la Información, es proteger, resguardar y asegurar la disponibilidad, confidencialidad e integridad de los activos de información y tecnologías para su procesamiento a efecto de garantizar la continuidad operacional de la Institución.
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)	Recopila información privada o confidencial de un usuario de computador.
Software potencialmente no deseado	Software engañoso, incluyendo el malware y no malicioso, que exhibe las características de software engañoso.
Spam (correo basura)	Abuso de los sistemas de mensajería electrónica para enviar indiscriminadamente mensajes masivos no solicitados.
T	
Tratamiento de riesgos	Proceso de modificar el riesgo, mediante la implementación de controles.

Trazabilidad	Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
Troyano, caballo de Troya	Software malintencionado que aparece para realizar una función deseable.
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.

Fuente: Acuerdo Ministerial Nro. MINTEL-MINTEL-20241-0003
Elaboración: CSISOT, 2025

7. Documentos de referencia

Asamblea Nacional del Ecuador. (2010). *Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD).* Registro Oficial Suplemento 275, 28 de septiembre de 2010. Quito, Ecuador: Asamblea Nacional.

Asamblea Nacional del Ecuador. (2016). *Ley Orgánica de Ordenamiento Territorial, Uso y Gestión del Suelo.* Registro Oficial Suplemento 790 de 5 de julio de 2016. Quito: Asamblea Nacional.

Asamblea Nacional del Ecuador. (2016). *Reglamento a la Ley Orgánica de Ordenamiento Territorial, Uso y Gestión del Suelo*. Registro Oficial Suplemento 790, 5 de julio de 2016. Quito, Ecuador: Asamblea Nacional.

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento 459 de 26 de mayo de 2021. Quito: Asamblea Nacional.

Asamblea Nacional del Ecuador. (2021). *Reglamento a la Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento 488, 27 de julio de 2021. Quito, Ecuador: Asamblea Nacional.

Asamblea Nacional del Ecuador. (2022). *Ley Orgánica para la Transformación Digital y Audiovisual*. Registro Oficial Suplemento 134 de 29 de diciembre de 2022. Quito: Asamblea Nacional.

Asamblea Nacional del Ecuador. (2023). *Ley Orgánica de Transparencia y Acceso a la Información Pública*. Registro Oficial Segundo Suplemento Nº 245, 7 de febrero de 2023. Quito: Asamblea Nacional.

Instituto Ecuatoriano de Normalización. (2021). *NTE INEN-ISO/IEC 27000:2021. Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Fundamentos y vocabulario*. Quito: INEN.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2024). *Acuerdo Ministerial Nro. MINTEL-MINTEL-0003-2024. Expídese el Esquema Gubernamental de Seguridad de la Información (EGSI).* Registro Oficial Tercer Suplemento Nº 509, 1 de marzo de 2024. Quito: MINTEL.

Presidencia de la República del Ecuador. (2024). *Reglamento General a la Ley Orgánica de Transparencia y Acceso a la Información Pública*. Registro Oficial Suplemento Nº 484, 24 de enero de 2024. Quito: Presidencia de la República.

Secretaría Nacional de la Administración Pública – SNAP. (2011). *Acuerdos Ministeriales Nros. 804 y 837 – Constitución de la Comisión de Seguridad Informática y Tecnologías de la Información y Comunicación.* Quito, Ecuador: SNAP.

Secretaría Nacional de la Administración Pública – SNAP. (2013). *Acuerdo Ministerial Nro. 166 – Esquema Gubernamental de Seguridad de la Información (EGSI v1).* Registro Oficial Suplemento 88, 25 de septiembre de 2013. Quito, Ecuador: SNAP.

Secretaría Nacional de la Administración Pública. (2015). *Norma Técnica de Gestión Documental y Archivo (Acuerdo Ministerial N° 1043 de 2 de febrero de 2015).* Registro Oficial Suplemento N° 445. Quito, Ecuador.

Seguridad Informática. (2013, 10 de noviembre). *Disponibilidad*. https://infosegur.wordpress.com/tag/disponibilidad/

Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo . (2022). *Plan Estratégico Institucional 2022-2025.* Quito, Ecuador: SOT.

Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo. (2024). *Resolución No. SOT-DS-2024-008 de 23 de mayo de 2024 – Delegado de Protección de Datos Personales (DPDP).* Quito, Ecuador: SOT.

Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo. (2024). *Resolución No. SOT-DS-2024-009 de 23 de mayo de 2024 – Oficial de Seguridad de la Información (OSI).* Quito, Ecuador: SOT.

Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo. (2024). *Resolución No. SOT-DS-2024-012 de 08 de julio de 2024.* Quito, Ecuador: SOT.

Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo – SOT. (2025). *Resolución No. SOT-DS-2025-004 de 29 de enero de 2025 – Reglamento de Funcionamiento del Comité de Seguridad de la Información de la SOT.* Quito, Ecuador: SOT.

Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo – SOT. (2025). *Resolución No. SOT-DS-2025-020 – Designación del Oficial de Seguridad de la Información (OSI).* Quito, Ecuador: SOT.

8. Firmas de responsabilidad

		Nombre/Cargo	Firma
Aprobado por:	Máxima Autoridad	Pablo Iglesias Paladines **Superintendente de Ordenamiento Territorial, Uso y Gestión del Suelo**	Firmado electrónicamente por: PABLO RAMIRO IGLESIAS PALADINES Validar únicamente con FirmaEC
Revisado por:	Comité de Seguridad de la Información de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo	Samantha Almeida Jara **Coordinadora General de Planificación y Gestión Estratégica**	Firmado electrónicamente por: SAMANTHA AVELINA ALMEIDA JARA Validar únicamente con FirmaEC
		Santiago Saransig Gálvez **Coordinador General de Tecnologías de la Información y Comunicación**	Firmado electrónicamente por: SANTIAGO JAVIER SARANSIG GALVEZ Validar únicamente con FirmaEC
		Diego Narváez Orbe **Coordinador General de Asesoría Jurídica**	Firmado electrónicamente por: DIEGO FABRICIO NARVAEZ ORBE Validar únicamente con FirmaEC
		Grima Tapia Caisaguano **Directora de Comunicación Social**	Firmado electrónicamente por: GRIMA IRENE TAPIA CAISAGUANO Validar únicamente con FirmaEC
		Daniel Coloma Braganza **Director de Administración del Talento Humano**	Firmado electrónicamente por: DANIEL ALEJANDRO COLOMA BRAGANZA Validar únicamente con FirmaEC
		Mario Sebastián Montalvo **Dirección Administrativa**	Firmado electrónicamente por: MARIO SEBASTIAN MONTALVO AGUAYO Validar únicamente con FirmaEC
		Juan Carlos Mayorga **Director de Desarrollo de Software y Base de Datos**	Firmado electrónicamente por: JUAN CARLOS MAYORGA MONTUFAR Validar únicamente con FirmaEC
Elaborado por:	Oficial de Seguridad de la Información	Max Paredes Parada **Director de Planificación Seguimiento y Evaluación**	Firmado electrónicamente por: MAX ABEL PAREDES PARADA Validar únicamente con FirmaEC

Control de versiones del formato referencial

Versión:	1.0
Fecha de la versión:	01-03-2024
Creado por:	Dirección de Infraestructura, Interoperabilidad, Seguridad de la Información y Registro Civil
Aprobado por:	Subsecretaría de Gobierno Electrónico y Registro Civil
Nivel de confidencialidad:	Bajo

Historial de cambios del formato referencial

Versión	**Fecha**	**Detalle del cambio**
1.0	01/03/2024	Emisión inicial del documento

SOT

SUPERINTENDENCIA DE ORDENAMIENTO TERRITORIAL, USO Y GESTIÓN DEL SUELO

www.sot.gob.ec | / SOT_ECUADOR