POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DEFENSORÍA DEL PUEBLO

Tabla de contenido

1. Antecedentes

El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), a través de su acuerdo ministerial Nro. MINTEL-MINTEL-2024-0003 de fecha 08 de febrero de 2024, resolvió expedir el Esquema Gubernamental de Seguridad de la Información (EGSI), como mecanismo para implementar el Sistema de Gestión de Seguridad de la Información en el sector público.

El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), en el artículo 2 de dicho acuerdo expresa: "*Artículo 2.- El EGSI es de implementación obligatoria en las entidades, organismos e instituciones del sector público, de conformidad con lo establecido en el artículo 225 de la Constitución de la República del Ecuador y los artículos 7 literal o), y 20 de la Ley Orgánica para la Transformación Digital y Audiovisual; y, además, es de implementación obligatoria para terceros que presten servicios públicos mediante concesión, u otras figuras legalmente reconocidas, quienes podrán incorporar medidas adicionales de seguridad de la información".*

El Esquema Gubernamental de Seguridad de la Información (EGSI) busca preservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y la selección de controles para el tratamiento de dichos riesgos.

Bajo este precepto es necesario que todas las personas servidoras y trabajadoras que conforman la Institución Nacional de Derechos Humanos tengan pleno conocimiento sobre la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), considerando su importancia en la protección de los activos de información que maneja la Defensoría del Pueblo del Ecuador, lo que permitirá brindar una mejor atención a la ciudadanía, elevando el nivel de confianza de los usuarios tanto internos como externos.

Por lo tanto, es fundamental la generación e implementación de la Política de Seguridad de la Información en la Defensoría del Pueblo del Ecuador, para poder asumir los compromisos normativos, emitir lineamientos y gestionar acciones encaminadas a resguardar y salvaguardar la información generada por cada uno de los procesos y procedimientos que lleva a cabo la institución.

La Política de Seguridad de la Información contemplará un conjunto de medidas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información, que constituyen los tres componentes básicos del "EGSI" resguardando la información, los equipos y servicios tecnológicos que sirven de soporte a los procesos institucionales, minimizando el creciente número de amenazas tecnológicas, lo cual requiere de un esfuerzo constante para adaptarse y gestionar los riesgos introducidos por éstas, así como el compromiso de las autoridades institucionales para el cumplimiento de la política de alto nivel.

2. Objetivo de la Política

El objetivo de la Política de alto nivel es establecer los lineamientos y medidas necesarias que permitan a la Defensoría del Pueblo de Ecuador (DPE) garantizar la protección de sus activos de información, así como sus recursos tecnológicos relacionados a su gestión y consumo, previniendo la materialización de riesgos que puedan afectar su confidencialidad, integridad y disponibilidad.

3. Política de Seguridad de la Información

3.1. Descripción de la Política

La máxima autoridad y el Comité de Seguridad de la Información de la Defensoría del Pueblo, entendiendo la importancia de una adecuada gestión de la información, se han comprometido con la implementación de un sistema de gestión de seguridad de la información basado en buenas prácticas, buscando establecer un marco de confianza en el ejercicio de sus deberes con los ciudadanos, implementando controles adecuados para garantizar la seguridad de la información, todo enmarcado en el estricto cumplimiento de la legislación vigente y en concordancia con la misión y visión de la institución.

Para la Defensoría del Pueblo, la protección de la información busca la disminución del impacto generado sobre sus activos y por los riesgos identificados de manera sistemática, con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo expuesto, esta política será aplicada en la Institución, sus funcionarios, terceros, proveedores y la ciudadanía en general.

3.2. Lineamientos de la Política

3.2.1 Gestión de Activos

La gestión de activos estará determinada por los siguientes aspectos mínimos:

Identificación de Activos: La Defensoría del Pueblo del Ecuador a través del Comité de Seguridad de la Información y la/s unidad/es poseedoras de los activos de información, realizarán la identificación y recopilación de los documentos relacionados con el objetivo y alcance definido en el proyecto.

Clasificación de Activos: La Defensoría del Pueblo del Ecuador a través del Comité de Seguridad de la Información y la/s unidad/es poseedoras de los activos de información, realizará la clasificación de dichos activos, quienes deben realizar dicha clasificación de acuerdo con la criticidad, sensibilidad y reserva de esta, para lo cual considerarán la normativa vigente que los apalanque.

Etiquetado de la Información: La Defensoría del Pueblo y la/s unidad/es poseedoras de los activos de información determinarán junto con la Dirección Administrativa, Dirección de Gestión Documental y Dirección de Tecnologías de la Información y comunicaciones el mecanismo, responsable y obligatoriedad para el etiquetado o rotulación de Activos.

Devolución de los Activos: La Defensoría del Pueblo del Ecuador a través de la Dirección de Administración de Talento Humano, determinará el mecanismo y responsable del cumplimiento, mediante el cual se genera obligatoriedad para que los/as servidores/as, realicen la entrega de activos físicos y de la información una vez finalizado su relación con la Institución, para lo cual coordinaran con las diferentes unidades que participen en el proceso.

Gestión de medios removibles: Se ejecutará conforme se determinada en la Política general de uso de equipos y sistemas informáticos.

Disposición de los activos: La Defensoría del Pueblo del Ecuador a través de la Dirección Administrativa y la Dirección de Tecnologías de la Información y Comunicaciones, determinarán la obligatoriedad para la construcción y cumplimiento de un procedimiento mediante el cual se realice de forma segura y correcta la eliminación, retiro, traslado o re uso cuando ya no se requieran los activos. Esta política determinará la toma de respaldos de los activos, evitando así el acceso o borrado no autorizado de la información; la política debe identificar al responsable de emitir las correspondientes autorizaciones, lo cual aplicará tanto para medios removibles como activos de procesamiento y/o almacenamiento de información.

Dispositivos móviles: Se ejecutará conforme se determinada en la Política General de Uso de Equipos y Sistemas Informáticos.

3.2.2 Manejo de la Información:

La información institucional debe contar con medidas de protección física que eviten el acceso y/o utilización indebida por personal no autorizado.

La información que sea administrada, recibida o gestionada por el usuario interno o externo, catalogada como sensible no puede ser copiada, transferida, difundida, publicitada o cedida por ningún medio físico o electrónico, salvo disposición y/o requerimiento para los fines legales conforme lo determine la ley.

La información que se gestione en el correo electrónico institucional se sujetará a la Política de uso de cuentas de correo institucional de la Dirección de Tecnologías de la Información y comunicaciones.

La inclusión de nuevos servicios para el procesamiento de la información deberá ser autorizada por el poseedor de la información involucrada y avalada por la Dirección de Tecnologías de Información y Comunicaciones.

Los equipos tecnológicos que contengan la información generada por las personas servidoras y/o trabajadoras de la institución se sujetarán a la política general de uso de equipos y sistemas informáticos.

El uso de Internet debe estar orientado a las actividades institucionales como apoyo en la gestión y la realización de las labores asignadas a cada usuario; por lo tanto, queda restringido el acceso a otro tipo de contenidos y se sujetará a la Política de uso del servicio de internet.

3.2.3 Talento Humano a cargo de la Información:

Las personas servidoras y/o trabajadoras deberán mantener su estación de trabajo y su equipo de computación organizado, observando los siguientes aspectos:

a) Guardar todos los archivos institucionales dentro de carpetas organizadas en la carpeta de documentos, evitando almacenarlos en el escritorio (carpetas digitales).
b) Bloquear la pantalla del computador al ausentarse de su puesto de trabajo.
c) Retirar de las impresoras la documentación de forma inmediata luego de su impresión.
d) Evitar mantener información sensible (contraseñas, información personal, documentación legal, pedidos de información, etc.) en los escritorios y/o pantallas de los equipos de computación.
e) Retirar los dispositivos de almacenamiento removibles, (memoria USB, cd, discos duros externos, etc.), una vez finalizado su uso.
f) El espacio físico o área de trabajo asignado a cada servidora y/o trabajadora debe estar libre de documentación, expedientes, u objetos que dificulten sus funciones y pongan en riesgo la seguridad de la información contenida.
g) Es responsabilidad de cada persona servidora y/o trabajadora la debida custodia de la información a la que tenga acceso para el cumplimiento de sus funciones.

Es responsabilidad de las personas servidoras y/o trabajadoras proteger sus claves de acceso de cualquier índole, para lo cual deben generar contraseñas seguras y de difícil suposición, considerando lo siguiente:

a) Las claves y contraseñas son personales e intransferibles, es responsabilidad exclusiva de cada persona servidora y trabajadora su conservación.
b) En caso de que el usuario principal se ausente temporalmente de la Institución, se deberá asignar una cuenta de usuario independiente al servidor que quede a cargo de las aplicaciones que éste administre, cuando lo amerite.
c) Se sugiere que las claves y contraseñas sean cambiadas cada tres meses.
d) El usuario ante la sospecha de que una de sus cuentas o sus contraseñas haya sido vulneradas, deberá comunicar de inmediato al Oficial de Seguridad de la Información (OSI) y cambiar las contraseñas de todas sus cuentas, con el soporte de la Dirección de Tecnologías de Información y Comunicaciones.
e) Cuando una persona servidor y/o trabajadora, abandone la Institución de manera permanente, su usuario y clave serán deshabilitados inmediatamente por la Dirección de Tecnologías de Información y Comunicaciones una vez que se reciba la respectiva notificación por parte de la Dirección de Administración de Talento Humano.

Para mantener la privacidad de la información, todas las personas servidoras y trabajadoras deberán conocer las restricciones con relación al manejo de datos e información respecto a la cual tengan responsabilidad con motivo del ejercicio de sus funciones. La Institución debe contar con un "*Acuerdo de Confidencialidad*", el cual deberá ser suscrito por todo el personal de la Institución sin excepción. Este documento reposará en el expediente personal de cada servidor, cuya custodia es responsabilidad de la Dirección de Administración del Talento Humano.

Al cesar la relación laboral la persona servidora y/o trabajadora se encuentra obligada a entregar toda la documentación a su cargo, tanto física como digital a su inmediato superior, lo que deberá ser verificado por la Dirección de Administración de Talento Humano en el trámite de liquidación.

3.2.4 Seguridad de la Información en Teletrabajo:

Se deberá controlar el acceso remoto a la red de la Defensoría del Pueblo, a través de la Dirección de Tecnologías de la Información y Comunicaciones, en modalidad de trabajo a distancia, esto es, desde fuera de las instalaciones propias.

Los servicios de conexión en dicha modalidad estarán destinados exclusivamente a personal de la Defensoría del Pueblo, su uso por parte de cualquier otro tipo de colaborador requerirá de la comunicación respectiva al Oficial de seguridad de la información, previa autorización de la Dirección de Administración de Talento Humano, con el debido soporte de la Dirección de Tecnologías de la Información y Comunicaciones.

El equipo utilizado para la conexión en la modalidad de teletrabajo podrá ser propiedad de la persona servidora o trabajadora o proporcionado por la Defensoría del Pueblo. En cualquier caso, es obligatorio que el equipo cumpla con los siguientes requerimientos de seguridad:

a) Capacidad de realizar una conexión a través de una VPN.
b) Disponer de un sistema operativo actualizado con los últimos parches y actualizaciones de seguridad.
c) Software antivirus instalado.
d) Software de firewall/cortafuegos personal instalado.

La ejecución de actividades en la modalidad de teletrabajo desde un equipo propio del personal requerirá de todas las medidas de seguridad oportunas, con el objetivo de que el trabajo remoto no suponga una amenaza para la seguridad de la información de la Defensoría del Pueblo; además, se podrán establecer medidas de seguridad adicionales a las existentes para asegurar de una manera más fiable la conexión segura en remoto.

3.2.5 Control de Acceso:

El personal de la Institución debe portar de manera visible el carné de identificación institucional para ser reconocido como persona servidora o trabajadora y pueda circular por las instalaciones.

El cuidado del carné de identificación institucional es responsabilidad de cada servidor y por lo tanto será responsable en caso de pérdida del mismo, dicho lineamiento se sujetará a lo establecido en el reglamento de talento humano de la Defensoría del Pueblo.

La Dirección Administrativa debe gestionar la seguridad física en la Institución, previniendo accesos no autorizados, evitando daños en las instalaciones y resguardando los equipos en su diferente índole, ubicándolos en áreas protegidas con controles de acceso adecuados, para lo cual tomará en cuenta lo siguiente:

a) Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipo informático y de las instalaciones en las cuales se almacena la información de la Institución.
b) Proteger el ingreso a las áreas restringidas, con controles de acceso para personal no autorizado.
c) Proteger la infraestructura donde se encuentran los activos de información identificados en la institución mediante la implementación de controles.
d) Mantener los equipos tecnológicos en un área físicamente segura y tomar las medidas para reducir el riesgo de robo o pérdida.
e) Generar una cultura en el personal para no ingerir alimentos ni bebidas en las cercanías de las áreas de procesamiento de información.

La gestión de la seguridad del centro de datos en la Institución debe prevenir los accesos no autorizados, resguardando los equipos servidores y de almacenamiento en un área protegida y adecuada para el efecto, siguiendo normas técnicas como:

a) Control ambiental para mantener el correcto funcionamiento de los equipos en los cuales se almacena la información de la Institución.
b) Disponer de energía regulada y UPS que proteja los equipos contra cortes de energía y permita apagarlos correctamente.
c) Proteger el ingreso al área, con controles de acceso solo para personal de la Dirección de Tecnologías de Información y Comunicaciones.
d) Proteger la infraestructura donde se encuentran los activos de información identificados en la institución mediante la implementación de controles.
e) No ingresar al área con alimentos, bebidas o elementos que puedan afectar al normal funcionamiento de las áreas de procesamiento de información.

Los prestadores de servicios externos y contratistas que se relacionen con el acceso, procesamiento, comunicación, gestión de información o los sistemas de información de la Defensoría del Pueblo, deben cumplir todos los requisitos de seguridad pertinentes y deben incluir en sus contratos una cláusula de acuerdo de confidencialidad, conforme la normativa lo permita.

En ningún caso y sin excepción, se otorgará a terceros accesos a la información de la Institución, instalaciones de procesamiento de datos u otras áreas críticas, sin que se hayan implementado los controles pertinentes y se hayan firmado los acuerdos de confidencialidad o contratos en los cuales se establezcan las condiciones para el acceso.

3.3. Declaración de los objetivos de seguridad de la información

Los objetivos de seguridad de la información, contenidos en el presente documento se ajustan al Plan Estratégico Institucional de la Defensoría del Pueblo, alineados a los objetivos y estrategias definidas para alcanzarlos, detallándose a continuación:

- Garantizar que la información generada en la Defensoría del Pueblo, no se revele a personas, entidades, procesos o terceros que no lo requieran conforme lo establezca la normativa legal vigente, fortaleciendo las capacidades institucionales en el tratamiento, almacenamiento y en los pedidos de información.

- Garantizar que la ciudadanía, usuarios internos y externos, entidades y otros interesados puedan acceder y utilizar la información generada por la Defensoría del Pueblo cuando lo requieran, de una manera segura, incrementando el reconocimiento a nivel nacional e internacional de la institución, con información verás, actualizada y confiable.

- Determinar los riesgos de seguridad de la información a través de la planificación y valoración de los activos y medios en los cuales está contenida, buscando prevenir o reducir los efectos indeseados por su mal uso, lo que incrementa las acciones tendientes a lograr un relacionamiento estratégico con los usuarios internos y externos, donde se incluyen grupos en situación de vulnerabilidad.

- Fortalecer la cultura de seguridad de la información en las personas servidoras y trabajadoras, así como a los usuarios de los servicios de la Defensoría del Pueblo del Ecuador, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, a todo el personal de la institución, lo que permite una construcción de una sociedad informada, igualitaria, inclusiva y sostenible.

3.4. Principios de la Política de Seguridad de la Información

La presente Política responde a las recomendaciones de las mejores prácticas de Seguridad de la Información recogidas en el Estándar Internacional ISO 27001, compartidas por el Ministerio de Telecomunicaciones MINTEL, en el esquema EGSI, así como al cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas que, en el ámbito de Seguridad de la Información, puedan afectar a la Defensoría del Pueblo.

El Sistema de Gestión de Seguridad de la Información tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de la información, por tanto, la Defensoría del Pueblo para su tratamiento ha establecido los siguientes principios:

a) Confidencialidad. - Accesible únicamente a personal autorizado

b) Integridad. - La información debe mantenerse completa y sin modificaciones no autorizadas.

c) Disponibilidad. - La información debe estar disponible cuando se necesite.

Adicionalmente, las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada una de las personas servidoras y trabajadoras, proveedores, o terceros relacionados con la Institución.

El tratamiento de datos personales debe concebirse sobre la base del debido sigilo, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo.

3.5. Protección de Datos Personales en la Defensoría del Pueblo.

Para efectos de esta política, se entiende por datos personales cualquier información que permita identificar o hacer identificable a una persona natural, incluyendo, pero no limitándose a: nombres, números de identificación, domicilios, direcciones de correo electrónico, información financiera y datos de contacto.

Los datos personales sensibles incluyen información relativa a: origen étnico o racial, opiniones políticas, convicciones religiosas, datos biométricos, información de salud, datos sobre la vida u orientación sexual, entre otros.

El tratamiento de datos personales en la Defensoría del Pueblo del Ecuador se regirá conforme a lo dispuesto en la Ley Orgánica de Protección de Datos Personales (LOPDP) y las normativas internas de seguridad de la información.

3.5.1 Principios de Protección de Datos Personales

La Defensoría del Pueblo garantizará que el tratamiento de datos personales se realice bajo los siguientes principios:

- **Licitud y Lealtad:** Los datos personales serán tratados de manera lícita y conforme a la legislación vigente.
- **Finalidad:** Los datos personales solo podrán ser utilizados para el propósito específico para el cual fueron recolectados.
- **Minimización de Datos:** Solo se recolectarán los datos personales estrictamente necesarios para cumplir con la finalidad del tratamiento.
- **Seguridad y Confidencialidad:** Se adoptarán medidas técnicas y organizativas adecuadas para evitar el acceso no autorizado o la divulgación indebida de los datos.
- **Transparencia:** Se garantizará que las personas titulares de los datos personales sean informadas sobre su tratamiento.
- **Responsabilidad Proactiva:** La Defensoría del Pueblo implementará controles adecuados para verificar el cumplimiento de la normativa en protección de datos.

3.5.2 Medidas de Seguridad para la Protección de Datos Personales

Para garantizar la seguridad de los datos personales tratados por la Defensoría del Pueblo, se adoptarán las siguientes medidas:

a) Protección Técnica

- Implementación de cifrado en bases de datos que contengan información personal sensible.
- Restricción del acceso a los datos personales según el principio de necesidad de conocimiento.

- Implementación de mecanismos de auditoría para detectar accesos indebidos a la información.
- Uso de mecanismos de autenticación fuerte para el acceso a sistemas que procesen datos personales.

b) Protección Organizativa

- Creación de procedimientos internos para la recolección, almacenamiento y eliminación segura de datos personales.
- Establecimiento de un protocolo para la notificación y gestión de incidentes de seguridad de la información.
- Capacitación obligatoria a servidores y trabajadores sobre el manejo adecuado de datos personales y medidas de seguridad.

c) Protección Legal

- Garantía de que los convenios o contratos celebrados con terceros incluyan cláusulas de confidencialidad y medidas de seguridad en la gestión de datos personales referente a trámites defensoriales.
- Establecimiento de sanciones internas por el incumplimiento de la normativa de protección de datos, acorde a los reglamentos internos que lo apalanquen.

3.5.3 Derechos de los Titulares de Datos Personales

Las personas cuyos datos sean tratados por la Defensoría del Pueblo tendrán derecho a:

- **Acceder** a sus datos personales para conocer cómo están siendo tratados.
- **Rectificar** datos inexactos o incompletos.
- **Eliminar** sus datos cuando el tratamiento no sea necesario o no cuente con base legal.
- **Oponerse** al tratamiento de sus datos en determinadas circunstancias.
- **Portabilidad** de datos en casos aplicables.

La Defensoría establecerá un mecanismo accesible para que los ciudadanos puedan ejercer estos derechos de manera ágil y efectiva.

3.5.4 Evaluación y Auditoría del Cumplimiento

Para garantizar el cumplimiento de la protección de datos personales:

- El Delegado de Protección de Datos realizará la verificación permanente sobre el cumplimiento de la LOPDP.
- Se establecerán controles internos para verificar que las medidas de seguridad sean aplicadas correctamente.

3.6 Roles y Responsabilidades

La máxima autoridad a través del Comité de Seguridad de la Información (CSI - equipo directivo) es el responsable de asegurar que la seguridad de la información sea gestionada adecuadamente, así como de garantizar y facilitar la implementación de las iniciativas de seguridad de la información en la

institución; y ser el responsable del control y seguimiento en su aplicación.

Cada persona servidora que lidere la unidad (NJS), es responsable de garantizar que los servidores y trabajadores a su cargo protejan la información de acuerdo con las normas establecidas por la institución y que sean inherentes a sus actividades.

El Oficial de Seguridad de la Información (OSI) es el responsable de la implementación y mejora continua del EGSI, así como el de coordinar las acciones del Comité de Seguridad de la Información en relación con la implementación y cumplimiento del Esquema Gubernamental de Seguridad de la Información y garantizará que los informes al respecto estén disponibles en los tiempos previstos para el efecto.

Cada una de las personas servidoras y trabajadoras de la institución tiene la responsabilidad de mantener la seguridad de la información institucional a su cargo.

3.7 Alcance y usuarios

La presente política se aplica al Esquema Gubernamental de Seguridad de la Información "EGSI" de la Defensoría del Pueblo, considerando a todas las personas servidoras y trabajadoras que manejen o administren la información contenida, registrada, transmitida o procesada en la Institución ya sea que se encuentre en medios físicos, electrónicos, en sistemas informáticos, en gestión de procesos internos o que residan en los distintos componentes de la plataforma tecnológica institucional.

Los usuarios de este documento son quienes implementan el EGSI; los miembros del Comité de Seguridad de la Información (CSI), el Oficial de Seguridad de la Información (OSI); las personas servidoras y trabajadoras de la Defensoría del Pueblo del Ecuador y los terceros (proveedores, usuarios externos, instituciones cooperantes, etc.) que en algún momento tengan involucramiento en la gestión de los activos de información de la Institución y que además están obligados a acatarlas.

3.8 Comunicación de la Política

El Comité de Seguridad de la Información, será el encargado de la difusión y notificación de la Política de Seguridad de la Información, para lo cual gestionará con las unidades de Gestión Documental y de Comunicación e Imagen Institucional lo que corresponda acorde a sus atribuciones.

Además, al ser un tema técnico y amplio es importante generar un plan comunicacional por fases para que la información tanto de la política institucional como del esquema a implementarse sea comprendida por las personas servidoras y trabajadoras de la institución.

Para lo cual, se propone desarrollar una campaña comunicacional interna en la que consten tres fases:

1. Fase de expectativa / informativa
2. Fase de desarrollo / implementación
3. Fase de refuerzo

La campaña comunicacional interna será difundida por dos canales:

1. Mailyng: correo institucional
2. Espacio físico estratégico (artes impresos)

Se deberá comunicar de manera periódica, al menos una vez al año a todo el personal sobre la política de seguridad de la información por los medios que se consideren oportunos, esta difusión estará a cargo de la Dirección de Comunicación e Imagen Institucional.

3.9 Excepciones y sanciones

La Institución hará responsable a el/la usuario/a de la información, de las consecuencias derivadas por el incumplimiento de la política, lineamientos y normas establecidas en este documento.

Cualquier acción disciplinaria derivada del incumplimiento de ésta (tales como llamadas de atención, sanciones disciplinarias administrativas que estén estipuladas por la Dirección de Administración de Talento Humano), será considerada de acuerdo con los procedimientos establecidos por la Defensoría del Pueblo y en estricto cumplimiento a las políticas y reglamento interno.

El usuario que no cumpla con el uso correcto de la información, materia del presente documento estará sujeto a las sanciones correspondientes. La Institución se reserva el derecho de evaluar periódicamente el cumplimiento de esta política.

3.10 Revisión y actualización de la Política

La presente política de protección será revisada y de ser el caso actualizada periódicamente para adaptarse a cambios normativos o mejoras en la gestión de la seguridad de la información.

4 Glosario de términos

Término	Definición
Política:	Es un conjunto de normas internas que permiten a la Institución definir las reglas claras sobre el uso de los recursos por parte de los servidores/as.
Estándar	Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplirlas políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.
OSI	Oficial de Seguridad de la Información
Activos de información	Cualquier elemento valioso para una organización que debe ser protegido del acceso no autorizado, uso, divulgación, modificación, destrucción o compromiso

Término	Definición
Mejor Práctica	Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.
Procedimientos	Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.
SGSI	Es un Sistema de Gestión de Seguridad de la Información (Information Security Management System, por sus siglas en inglés). Un SGSI es un conjunto de principios o procedimientos que se utilizan para identificar riesgos y definir los pasos de mitigación de riesgos que deben llevarse a cabo.
Confidencialidad:	La información solo tiene que ser accesible o divulgada a aquellos que están autorizados.
Integridad:	La información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros.
Disponibilidad	La información debe estar siempre accesible para aquellos que estén autorizados.
EGSI	(Esquema de Gestión de Seguridad de la Información): Sistema de Gestión de Seguridad de la Información para las Instituciones del Sector Público.

5 Documentos de referencia

- Ley Orgánica para la Transformación Digital y Audiovisual
- Ley Orgánica de Protección de Datos Personales
- Acuerdo Ministerial Nro. MINTEL-MINTEL-0003-2024
- Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)
- Familia de Normas Técnicas ISO/IEC 27000

- Alcance del Esquema Gubernamental de Seguridad de la Información
- Plan estratégico institucional
- Política de seguridad de telefonía IP
- Política de uso de cuentas de correo institucional
- Política de uso de equipos y sistemas informáticos
- Política de uso de servidor de carpetas compartidas
- Política de uso de sistema de soporte a usuarios
- Política de uso del servicio de internet.
- Otros documentos relacionados con la Seguridad de la Información.

Control de versiones del formato referencial

Versión:	2.0
Fecha de la versión:	10-03-2025
Nivel de confidencialidad:	Bajo

Historial de cambios del formato referencial

Versión	Fecha	Detalle de la modificación
1.0	16/12/2024	Versión inicial Aprobada del documento.
2.0	10/03/2025	Versión 2 del documento con aportes LOPDP