POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Lista de distribución

Proceso	Usuario	Fecha	Entrega	Recibe
Gestión de la Calidad	Responsables de Procesos	09/07/2024	Administrador SGC	Responsable del proceso

Histórico de revisiones

Revisión	Fecha	Descripción de la Modificación	Acta Núm.	Aprobado
0	20/12/2023	Creación del documento	Acta Nro. 03	Comité de Seguridad de la Información
1	09/07/2024	Aprobación del documento	Resolución No.23-CD-SO-04-2024-ISSPOL	Consejo Directivo

Aprobación

ELABORADO	REVISADO	VALIDADO		
Ing. Carlos Fernández **Oficial de Seguridad de la Información**	Ing. Ernesto Rosero **Jefe de Planificación Estratégica y Calidad**	Crnl. Renato González **Director General del ISSPOL**	**Fecha Vigencia:** 09/07/2024	**Versión: 0**

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Instituto de Seguridad Social de la Policía Nacional, en adelante "ISSPOL", forma parte del sistema de seguridad social, y, es un organismo autónomo con finalidad social y sin ánimo de lucro, con personería jurídica, patrimonio propio y domicilio en la ciudad de Quito, cuya misión es "Conceder protección integral al asegurado policial y su familia, con el fin de mejorar la calidad de vida del colectivo policial".

Hablar de seguridad social significa referirnos a los principios de solidaridad, integridad y universalidad; lo que quiere decir que todo ciudadano que habita en el país, debe estar amparado por la mano protectora que brindan los seguros sociales.

El ISSPOL, que se fundamenta en esta doctrina, filosofía y principios antes expuestos, es un órgano provisto de vida y valores, que en su sumatoria se identifican y personalizan por la cultura organizacional, que se convierte en la ventaja competitiva, que permite la diferencia con otras organizaciones que tienen la misma naturaleza de servicio.

1. OBJETIVOS ESTRATÉGICOS DE LA ORGANIZACIÓN

Para el período 2021-2025, el ISSPOL ha definido los siguientes Objetivos Estratégicos Institucionales (OEI):

- OEI 1: Garantizar al policía y su familia protección integral frente a los riesgos asistenciales y económicos.
- OEI 2: Atender las necesidades fundamentales para lograr el bienestar individual y un mejor nivel de vida para todos los miembros del colectivo policial.
- OEI 3: Brindar asistencia y protección a los más necesitados y no asalariados de la mutualidad de la Policía Nacional.
- OEI 4: Fortalecer las capacidades Institucionales.

Según lo señalado, la información que se genera y gestiona constituye un activo estratégico clave para garantizar la prestación de los servicios a los asegurados del ISSPOL. En este contexto, la **"Política de Seguridad de la Información"**, en adelante "Política" busca proteger: la información durante su ciclo de vida (creación, difusión, modificación, almacenamiento, preservación y eliminación), los medios que permiten dicho ciclo y los usuarios que acceden a la información y/o manipulan.

Esto se hace para salvaguardar la confidencialidad, integridad y disponibilidad de la información propia de la Institución.

2. DECLARACIÓN DE INTENCIÓN DE LA DIRECCIÓN GENERAL

Dado que la información de los asegurados que maneja el ISSPOL es sensible, el Instituto está obligado a proporcionar todos los medios y recursos necesarios para proteger la información que maneja, las tecnologías utilizadas para su procesamiento e implementar controles que ayuden a reducir o mitigar las amenazas internas o externas.

En ese contexto, el ISSPOL a través de esta Política de alto nivel, se compromete a asegurar la confidencialidad de los datos, mantener la integridad, la disponibilidad, legalidad y confiabilidad de la información, promoviendo una gestión de riesgos efectiva, garantizando la continuidad de los sistemas de información, fomentando una cultura y visión de seguridad de la información que contribuya al logro de los objetivos estratégicos e institucionales.

3. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

- Fomentar una cultura orientada a la seguridad de la información en el ISSPOL.
- Comprometer a todas las Autoridades, Directores/Jefes de Gestión y servidores del ISSPOL en la difusión, consolidación y cumplimiento de esta Política.
- Implementar medidas de seguridad, teniendo en cuenta los recursos disponibles y partidas presupuestarias
- Actualizar las políticas, procedimientos, directrices y controles de seguridad de la información para garantizar que sean efectivos y eficientes.
- Promover la práctica de asegurar la continuidad de las funciones del ISSPOL, tal como se define en esta Política

4. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información, en adelante "CSI", es responsable de impulsar, velar y responder por la seguridad de la información de la organización.

Entre otras funciones, asume la responsabilidad de coordinar la implementación de un "Sistema de Gestión de Seguridad de la Información", en adelante "SGSI", su mejora continua, colaborando muy estrechamente con el "Oficial de Seguridad de la Información", en adelante "Oficial".

Es por eso, que mediante Resolución No.177-CD-SE-27-2022-ISSPOL de 10 de agosto de 2022, los miembros del Consejo Directivo aprueban el "REGLAMENTO PARA EL FUNCIONAMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN"; dicho instrumento jurídico, establece en el "Art.2 Ámbito", la conformación del "COMITÉ DE SEGURIDAD DE LA INFORMACIÓN", integrado por los representantes de las Unidades Organizativas, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

Conformación del Comité de Seguridad de la Información	
Área/Dirección/Gestión	***Representante***
Dirección Administrativa	*Director Administrativo – **(Presidente)***
Dirección de Prestaciones	*Director de Prestaciones*
Dirección de Servicios Sociales	*Director de Servicios Sociales*
Dirección de Riesgos	*Director de Riesgos*
Jefatura de Comunicación Social	*Jefe de Comunicación Social*
Jefatura de Talento Humano	*Jefe de Talento Humano*
Jefatura de Planificación Estratégica y Calidad	*Jefe de Planificación Estratégica y Calidad*
Jefatura de Tecnologías de Información y Comunicación	*Jefe de Tecnologías de Información y Comunicación – **(Secretario)***
Asesoría Jurídica	*Asesor Jurídico*

*"El **Oficial de Seguridad de la Información** asistirá al comité, con voz, pero sin voto. La participación en las reuniones de cualquier otro funcionario de la Institución que no pertenezca al Comité deberá contar con el visto bueno de su Presidente".*

5. ROLES Y RESPONSABILIDADES

Se han identificado las siguientes atribuciones y responsabilidades conforme lo establecido en el "Estatuto Orgánico de Gestión Organizacional por Procesos" y "Reglamento de funcionamiento del Comité de Seguridad de la Información"; además se incluyen otras responsabilidades específicas para lograr los objetivos de esta Política:

Roles	Responsabilidades
Dirección General:	*"f) Presentar para la aprobación del Consejo Superior los estados financieros auditados, presupuestos, planes de inversión, informes de labores y programas de actividades del ISSPOL ejecución de planes,*

	programas y proyectos conforme la planificación de actividades del ISSPOL". *"h) Proponer al Consejo Directivo políticas y planes para un mejor desarrollo de la seguridad social policial".* **Otras específicas:** • Aprobar el Plan de Comunicación y Sensibilización en Seguridad de Información. • Aprobar el Plan de Gestión de Riesgos de Seguridad de la Información.
Comité de Seguridad de la Información (CSI)	*"a) Gestionar la aprobación de la política y normas institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la Institución".* *"o) El Comité de Seguridad de la Información designará al interior de su institución a un funcionario como Oficial de Seguridad de la Información (OSI)".* *"e) Promover la difusión de la seguridad de la información dentro de la institución".* *Además de las que están definidas en el Reglamento del CSI* **Otras específicas:** • Gestionar ante la Dirección General, la aprobación de políticas (lineamientos), procedimientos, directrices y controles para la gestión de seguridad de la información y del SGSI propuestos por el Oficial. • Informar los riesgos de seguridad de la información a la Dirección General, para su consolidación en la matriz de riesgos y su

	seguimiento; y, evaluar, dirigir, monitorear y supervisar la gestión de seguridad de la información y del SGSI. • Coordinar con el Comité de Gestión de la Calidad y Desarrollo Institucional y Comité Gerencial de Sistemas de la Institución, para mantener un alineamiento y estrategias comunes de gestión. • Requerir la revisión de la Política. • Ejecutar las acciones que estén a su alcance para garantizar la continuidad operativa.
Directores y Jefes:	• Supervisar el cumplimiento de las políticas, normativas y procedimientos. • Generar las acciones coordinadas para proteger la información dentro de sus competencias de acuerdo con las políticas, procesos y procedimientos establecidas por la Institución. • Emplear un fuerte liderazgo y compromiso para asegurar el mejoramiento de los procesos en relación con la seguridad de la información.
Oficial de Seguridad de la Información (OSI):	*"**b)** Generar propuestas para la elaboración de la documentación esencial del Sistema de Gestión de Seguridad de la Información".* *"**c)** Asesorar a los funcionarios en la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas".* *"**d)** Elaborar el Plan de concienciación en Seguridad de la Información basado en el Sistema de Gestión de Seguridad de la Información (SGSI)".* *Además de las que están definidas en el Reglamento del CSI* **Otras específicas:**

	• Elaborar, implementar, mantener, actualizar las políticas, procesos, procedimientos, metodologías, planes y controles concernientes a la gestión de seguridad de la información en coordinación con las Gestiones/Direcciones, su mejora continua; y, una vez aprobados, difundirlos al personal que corresponde. • Coordinar y monitorear la implementación efectiva de los controles de seguridad de la información definidos en el plan de gestión de riesgos con los responsables de los procesos de negocio. • Garantizar que los servicios prestados por personas naturales o jurídicas cumplan con las políticas de seguridad de la información establecidas. • Coordinar con las Unidades Organizativas (Gestiones/Direcciones) de la Institución para apoyar y cumplir los objetivos que en Seguridad de la Información han sido planteados. • Participar en evaluaciones de amenazas a la seguridad de la información y proponer medidas de mitigación • Realizar el control de su implementación, velando por su correcta aplicación. • Establecer contactos con Oficiales de Seguridad de la Información de otras instituciones públicas y especialistas externos, que le permitan estar al tanto de las tendencias, normas, métodos de seguridad pertinentes, intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad. • Tomar contacto con Instituciones/Organismos especializados en temas relativos a la seguridad de la información: • Intercambiar información confidencial para fines de asesoramiento o de transmisión de experiencias, siempre y cuando se suscriba un "Acuerdo de confidencialidad y no divulgación de información" con

	aquellas Instituciones/Organizaciones especializadas en temas relativos a la seguridad de la información/informática.
Asesoría Jurídica:	*"3. Asesoría interna del ISSPOL"* **Otras específicas:** • Asesorar en el cumplimiento de las normas del ordenamiento jurídico vigente, nacionales e internas aplicables en operaciones, actos y contratos, emitiendo los criterios jurídicos que fueran necesarios y en el cumplimiento de las directrices y políticas, que estén relacionadas con la Seguridad de la Información. • Revisar y actualizar los acuerdos de confidencialidad y protección de datos personales para asegurarse de que cumplan con las leyes y regulaciones aplicables. Observando los requisitos que deben ser parte del mismo, considerando la no divulgación de la información de acuerdo a la necesidad del ISSPOL. • Asesorar al Instituto sobre las políticas y prácticas adecuadas para proteger la información personal de los servidores y asegurados, incluyendo la implementación de medidas técnicas y organizativas apropiadas. • Coordinar con las Direcciones/Gestiones y el Oficial de Seguridad de la Información, para garantizar la implementación efectiva de la Política de Protección de Datos personales.
Gestión de Planificación Estratégica y Calidad:	*"j) Proponer políticas de Seguridad de la Información para aplicación transversal en el ISSPOL".* *"k) Elaborar, coordinar y ejecutar el Plan de concienciación en Seguridad de la Información".* *"o) Informar al Comité de Seguridad de la Información, el avance de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), ¿así como las alertas que impidan su implementación".*

	*"**p)** Verificar el cumplimiento de las normas, procedimientos y controles de seguridad institucionales establecidos".*
Gestión de Comunicación Social:	*"**a)** Proponer estrategias comunicacionales, publicitarias y de relaciones públicas en el corto, mediano y largo plazo para informar, y difundir las decisiones, directrices, acciones y actividades institucionales".* *"**b)** Elaborar y ejecutar los planes, programas y proyectos de comunicación, imagen institucional y relaciones públicas validados por la Máxima Autoridad y realizar su evaluación".* **Otras específicas:** • Efectuar la difusión de las Políticas de Seguridad de la Información a todo los servidores y terceros que presten servicios en la Institución y a las entidades externas relevantes. • Emplear los medios disponibles (intranet, boletín, correo electrónico, página web, etc.), para la difusión, concientización, sensibilización y capacitación en temas relacionados con la seguridad de la información.
Gestión Administrativa:	*"**a)** Supervisar el cumplimiento de las políticas emanadas por la máxima autoridad de conformidad con lo dispuesto en las leyes, normas y reglamentos pertinentes".*
Gestión de Talento Humano:	*"Reglamento interno de administración de talento humano"* **Otras específicas:** • Asegurarse de que se implementen políticas y procedimientos adecuados para el manejo de la información personal de los servidores y candidatos, incluyendo el cumplimiento con las leyes y regulaciones aplicables.

	• Informar a todos los servidores vinculados a la Institución la obligación de cumplir con la Política de Seguridad de la Información y todos los estándares, procesos, procedimientos, prácticas y lineamientos del SGSI de la Institución y otras normas, procedimientos y prácticas internas. • Controlar que los acuerdos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todos los servidores de la Institución sin excepción. • Gestionar la custodia de los acuerdos firmados, en los expedientes, físicos o electrónicos, de cada servidor. • Controlar que la firma de los acuerdos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionarios a la Institución, sin excepción. • Implementar medidas de seguridad de recursos humanos, como verificaciones de antecedentes y evaluaciones de riesgos, para garantizar que los empleados tengan la confianza y credibilidad necesarias para proteger la información confidencial. • Entregar obligatoriamente copia de esta política (formato digital) al ingreso de un servidor a la Institución.
	"a) Planear, organizar, dirigir y controlar, el funcionamiento del Área de Sistemas". *"c) Coordinar las actividades técnicas con los responsables de la administración de Infraestructura y BDD, Desarrollo de Software y Soporte Técnico".* *"e) Determinar y actualizar normas y procedimientos del buen uso de HARWARD Y SOFTWARE".* **Otras específicas:**

Gestión de Tecnologías de la Información:	• Implementar y mantener sistemas de autenticación y autorización para garantizar que los usuarios tengan el acceso adecuado a la información confidencial. • Mantener actualizadas las políticas y procedimientos de seguridad de la información para asegurarse de que se ajusten a las necesidades y requisitos de la Institución. • Coordinar con otras Direcciones/Gestiones, como Talento Humano y Legal, para garantizar que se tomen medidas adecuadas para proteger la información confidencial. • Controlar la existencia de documentación física y/o electrónica actualizada relacionada con los procedimientos de comunicaciones, operaciones y sistemas • Cumplir con los procedimientos relativos a los dominios de control de acceso, adquisición, desarrollo y mantenimiento de los sistemas de información y gestión de las comunicaciones y operaciones. • Gestionar los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Institución. • Gestionar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases. • Proponer mejoras en función de nuevas tecnologías que ayuden al objeto de la Política. • Gestionar la aceptación, entendimiento y firma de acuerdos de confidencialidad y de no divulgación de información por parte de terceros (ej., contratistas, proveedores, pasantes, entre otros) que deban realizar labores dentro de la institución sea por medios lógicos o físicos y que involucren el manejo de seguridad de información.

	• Establecer, mantener y dar a conocer las políticas y procedimientos de los servicios de tecnología, el uso de los servicios tecnológicos en toda la Institución, de acuerdo con las mejores prácticas y lineamientos institucionales y normativa vigente, para ello será responsable de: - Mantener la custodia de la información que reposa en los diferentes sistemas, bases de datos y aplicativos de la Institución. - Informar de los eventos que están en contra de la seguridad de la información e infraestructura tecnológica de la Institución al Comité de Seguridad de la Información, a las diferentes Direcciones/Gestiones de la Institución - Designar al responsable de Seguridad Informática y sus atribuciones/responsabilidades. • Llevar el inventario del hardware, software, redes y demás aplicativos informáticos instalados en la Institución. • Realizar otras acciones vinculadas a su naturaleza en la gestión de seguridad de la información.
Gestión de Cumplimiento	• Monitorear y hacer cumplir las políticas y procedimientos de seguridad de la información en toda la Institución.
Gestión Documental y Archivo	• Clasificar la información de acuerdo con el grado de sensibilidad y criticidad. • Documentar, mantener actualizada, custodiada, y preservar la misma, aplicando las medidas de seguridad que establecen los instructivos institucionales y la Norma Técnica de Gestión Documental y Archivo. • Otorgar los permisos de acceso a la información de acuerdo con sus funciones y competencias.

Gestión de activos fijos	• Inventariar los activos de Hardware, donde consten equipos móviles, fijos, periféricos de salida, periféricos de entrada, dispositivos, sistemas ente otros vinculados a las acciones que ejecuta la Institución y que permitan dar continuidad al negocio. • Inventariar los activos de Software, Redes y demás aplicativos informáticos de la Institución. • Identificar los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información
Servidores civiles y policiales	• Responsables de cumplir con las políticas, lineamientos, procesos, procedimientos del SGSI y aplicarlas en sus actividades laborales dentro y fuera de la Institución. • Reportar de manera oportuna y adecuada los incidentes y vulnerabilidades de seguridad al Oficial de Seguridad de la Información y Gestión de Tecnologías de la Información a través de los correos electrónicos. o seguridadinformacion@isspol.org.ec o soportetic@isspol.org.ec

6. MARCO NORMATIVO

La Política de Seguridad de la Información se fundamenta en leyes y normativas como la Constitución de la República del Ecuador, la Ley Orgánica de Transparencia y Acceso a la Información Pública, la Ley de Seguridad Social de la Policía Nacional, la Ley Orgánica de Telecomunicaciones, la Ley Orgánica de Protección de Datos Personales, Código Integral Penal, Normas de Control Interno de la Contraloría General del Estado (CGE), Acuerdo Ministerial No. 025-2019 relacionado con "Esquema Gubernamental de Seguridad de la Información (EGSI v2.0)", Norma Técnica Ecuatoriana NTE INEN ISO/IEC 27001:2014, Código de Ética y Reglamento para el funcionamiento del Comité de Seguridad de la Información del ISSPOL . Estas leyes establecen los requisitos mínimos para la protección de la información.

7. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

7.1. Descripción general

La política de seguridad de la información del ISSPOL se basa en un análisis de riesgos para concienciar a las autoridades y servidores sobre la importancia de la información que manejan. Su implementación requiere un alto nivel de compromiso institucional y se basa en normativas y buenas prácticas que establecen lineamientos para mejorar la seguridad de la información y especificar el mal uso y sus consecuencias.

La política se enmarca en una normativa que incluye a la Superintendencia de Bancos, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (Esquema Gubernamental de Seguridad de la Información, EGSI v2.0), la Contraloría General de Estado (Normas de Control Interno 410-10 Seguridad de tecnología de información) y las buenas prácticas definidas en el estándar ISO 27001.

ISSPOL se compromete a implementar, mantener y mejorar un SGSI para proteger la información y los recursos utilizados, permitiendo que los activos críticos alcancen un nivel de seguridad suficiente y se adapten a los cambios en el riesgo, el entorno y la tecnología.

7.2. Objetivo general

Establecer lineamientos, normas y procedimientos claros para proteger de manera integral los activos de información de la institución, garantizando su confidencialidad, integridad y disponibilidad, previniendo y gestionando eficazmente los riesgos de seguridad, promoviendo el uso responsable de la información, asegurando el cumplimiento de las normativas y regulaciones aplicables, y comprometiéndose con la mejora continua de los procesos y controles de seguridad a fin de adaptarse a los cambios y nuevas amenazas, todo ello con el propósito de preservar el valor y utilidad de la información para la Institución.

7.3. Objetivos específicos

- Identificar los activos de información crítica del ISSPOL y definir medidas de protección adecuadas para cada uno de ellos.

- Establecer políticas específicas que aseguren que los lineamientos y procedimientos de gestión de seguridad de la información sean consistentes con los controles de seguridad necesarios para prevenir, controlar y reducir los riesgos de seguridad de la información, garantizando así la continuidad del negocio.
- Asegurar el cumplimiento de las normas internas de seguridad de la información, así como las normas gubernamentales, los requisitos normativos y las directivas de los organismos de control, con el fin de proteger los activos de información.
- Integrar en la cultura organizacional un plan formal de difusión, capacitación y concientización sobre la seguridad de la información que sea preventiva y proactiva ante eventos que puedan poner en riesgo la continuidad del negocio, con el objetivo de disminuir las vulnerabilidades relacionadas con el recurso humano.

7.4. AMBITO DE APLICACIÓN

Es de aplicación obligatoria para todos los servidores civiles, policiales y terceros, que tengan acceso a la información del ISSPOL (física o digital) en todas las etapas de su ciclo de vida, así como, a los recursos y a la totalidad de los procesos y servicios, independientemente de su cargo y función, por lo tanto, todos los servidores deben conocer y adherirse a esta política.

Por las razones anteriores, la información generada y gestionada por el ISSPOL es un medio esencial para asegurar la continuidad del negocio, y la seguridad de la información como una herramienta para gestionar su integridad, disponibilidad y confidencialidad.

Así mismo, se aplica a todo el Sistema Gestión de Seguridad de la Información (SGSI) en concordancia con la definición del documento del Alcance del SGSI.

7.5. LINEAMIENTOS

Para el cumplimiento de la Política se establecieron los siguientes lineamientos:

a. Asegurar la confidencialidad, integridad y disponibilidad de la información relacionada con los procesos de cumplimiento, prevención de sobornos y protección de datos personales, mediante la implementación de medidas técnicas y organizativas apropiadas.
b. Implementar programas de capacitación y concientización en materia de seguridad de la información, enfocados en la prevención del soborno, el cumplimiento normativo y la protección de datos personales, dirigidos a todo el personal de la institución.

c. Realizar evaluaciones periódicas del desempeño de la política de seguridad de la información, con el fin de identificar oportunidades de mejora y asegurar su efectividad en la prevención del soborno, el cumplimiento normativo y la protección de datos personales. Además, se debe garantizar el cumplimiento de las leyes y regulaciones aplicables en materia de protección de datos personales.
d. Utilizar la información sensible de ISSPOL de manera ética y responsable, y únicamente para fines propios de la institución.
e. Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
f. Previo a la entrega de información entre las diferentes instituciones públicas, privadas o entes gubernamentales de control, las unidades organizativas (responsables de proveer la información solicitada) deberán considerar los siguientes criterios:
   - Autorización de la máxima autoridad o su delegado.
   - Tipo de información solicitada.
   - Protección de activos de información.
   - Protección de datos en base a la Constitución, Ley Orgánica de Protección de Datos Personales, LOTAIP y demás Leyes nacionales aplicables a los planes, programas y proyectos de la Institución, particularmente datos personales de ciudadanos y/o financieros.
   - Convenios para gestión o intercambio de información, incidentes de la seguridad de la información y violaciones de la seguridad.
   - Cumplimiento de Políticas de control de accesos.
   - Entendimiento adecuado en los acuerdos de confidencialidad de la información entre la Institución y el solicitante con el objeto de cumplir los requisitos de la seguridad de la Institución.
   - Previo a la suscripción de cualquier convenio comercial, las unidades organizativas (responsables de proveer la información solicitada) deberán acatar lo establecido en la "Política de Protección de Datos Personales".
g. Mantener la confidencialidad, integridad y disponibilidad de la información relacionada con el ISSPOL, por los todos los servidores civiles, policiales y terceros, que traten con información sensible deben mediante la suscripción del "ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN" (Anexo 2); este acuerdo estará bajo la administración de la Gestión de Talento Humano y será de conocimiento del Delegado de Protección de Datos Personales/Oficial de Seguridad de la Información o quien haga sus veces.

h. Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos designados para el cumplimiento de sus funciones. No está permitida la conexión de equipos de cómputo y de comunicaciones ajenas a la Institución, a la red Institucional ni el uso de dispositivos de acceso externo a internet o de difusión de señales de red que no hayan sido previamente autorizadas por la Gestión de Tecnologías de Información.
i. Monitorear los acuerdos de confidencialidad con el fin de asegurar su cumplimiento.
j. Velar por la aplicación de la normativa relacionada a las normas técnicas ecuatorianas NTE INEN-ISO/IEC 27001 conforme al ámbito de la Institución.
k. Establecer los medios necesarios para garantizar la continuidad del negocio y operación de la información, con la capacidad instalada tanto a nivel de planta central como a nivel de las coordinaciones zonales.
l. Utilizar software licenciado obtenido por la institución. Se prohíbe la instalación o el uso de software no institucional sin la aprobación de la Gestión de Tecnologías de Información.
m. Designar a los custodios y responsables de la información de cada una de las unidades organizativas donde se genera la misma.
n. El uso de activos de información de ISSPOL por los servidores civiles y policiales y terceros, deberá estar de acuerdo tácitamente con el cumplimiento de la Política y directrices de seguridad de la información de ISSPOL.
o. ISSPOL se reserva el derecho de revocar los privilegios en cualquier momento sobre los recursos utilizados para acceder y procesar la información del usuario en los casos en que se crea que afecta la seguridad de la información.
p. Los sistemas y servicios tecnológicos solo se pueden usar para fines autorizados y legales, se prohíbe la transmisión, transferencia o almacenamiento de cualquier información en violación de cualquier ley o reglamento, incluidos materiales protegidos por derechos de propiedad intelectual, pornográficos, obscenidad, difamación que tengan un impacto negativo en la productividad y el trabajo de la institución o sean una amenaza legal o estén relacionados con ISSPOL y otras prohibiciones sobre el uso de estos servicios en los documentos vigentes.
q. Se desarrollará periódicamente (no más de un año) un Plan Director de Seguridad de la Información, cuyo alcance se articulará con los requerimientos y necesidades institucionales (internas y externas) en materia de seguridad de la información. El plan será revisado por el Comité y puesto en consideración ante la Dirección General para su aprobación.
r. Informar de manera inmediata a la Gestión de TI /Oficial de Seguridad de la Información, sobre la existencia de un potencial incidente de seguridad de la información/informática que afecte los activos de información críticos de la Institución. Para dar respuesta y mitigar un incidente de seguridad de la información, se debe seguir el "PGC-07 Procedimiento de Gestión de incidentes

de seguridad de información". (Disponible en la intranet / Pestaña Sistema de Gestión de Calidad)

s. Para cualquier requerimiento de usuario o incidente que cause una interrupción en los servicios que brinda la Gestión de Tecnologías de Información, esta debe reportarse a través del servicio técnico de Mesa Ayuda "PTI-13 Gestión requerimientos incidentes mesa ayuda P". (Disponible en la intranet / Pestaña Sistema de Gestión de Calidad)

t. Establecer la responsabilidad, y sanciones a los servidores civiles y policiales y terceros o cualquier persona que tenga relación con el ISSPOL, en los casos que correspondan y que tengan relación con:
   - Reportar las violaciones a la seguridad.
   - Preservar la confidencialidad, integridad y disponibilidad de la información en cumplimiento de esta Política.
   - Cumplir las políticas y procedimientos inherentes al Sistema de Gestión de la Seguridad de la Información.

u. Incidentes de seguridad de la información categorizados como de gravedad "alta" o "critica", que requieran una evaluación o análisis especializado, podrán ser revisados por personal externo mediante el lanzamiento de un proceso de contratación pública, para esto, el Oficial de Seguridad de la Información presentará un informe ejecutivo al Comité para su aprobación.

v. Para la administración tecnológica en el ámbito de la seguridad de la Información, el/los responsables se apoyarán en herramientas tecnológicas que permitan una adecuada administración, monitoreo y control de los activos de información requeridos para salvaguardar la integridad, confiabilidad y confidencialidad de la información que se produce dentro del ISSPOL

w. Aceptar y reconocer que en cualquier momento y sin previo aviso, la Gestión de Tecnologías de Información puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web y redes sociales propiedad del ISSPOL, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la Institución. Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por petición de las Máximas Autoridades, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales.

x. Todo trabajo realizado por terceros con respecto a temas de seguridad, incidentes de operación o de servicios, estarán sujetos de análisis, revisión y/o verificación por parte del personal que el ISSPOL designe para el efecto.

y. Si los responsables de la Unidades Organizativas omiten informar al Oficial de Seguridad de la Información sobre los incumplimientos de la Política e instrumentos vinculantes se comunicará a la Dirección General.

7.6. Asignación de responsabilidades en Gestión de Seguridad de la Información

ISSPOL, de conformidad con la legislación de seguridad de la información aplicable, establece un compromiso institucional para gestionar y promover una cultura de seguridad de la información mediante la implementación, evaluación, mantenimiento y mejora continua del SGSI a través del estándar internacional ISO/ IEC: 27001.

A continuación, se detallan los procesos de seguridad, indicándose en cada caso el/los responsables/s del cumplimiento de los aspectos de esta Política aplicables a cada caso:

Capitulo	Responsable
Organización de la seguridad de la información: *Establece un marco de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.*	- Dirección Administrativa - Gestión de Tecnologías de la Información - Oficial de Seguridad de la Información
Seguridad relacionada con el personal: *Establece las medidas para la seguridad a abordar en la fase de contratación, durante el empleo y en la fase de término o finalización del empleo.*	- Gestión de Administración de Talento Humano - Oficial de Seguridad de la Información
Gestión de activos: *Identifica los activos de información y define las responsabilidades de protección adecuadas*	- Dirección Administrativa - Oficial de Seguridad de la Información

Control de acceso: *Están orientadas a controlar y monitorizar los accesos (físicos o lógicos) a los medios de información de acuerdo a las políticas definidas por la organización.*	- Dirección Administrativa - Gestión de Tecnologías de la Información - Oficial de Seguridad de la Información
Criptografía: *Las medidas de control para el uso eficaz de la criptografía para proteger la confidencialidad e integridad de la información.*	- Gestión de Tecnologías de la Información - Oficial de Seguridad de la Información
Seguridad física y ambiental: *Se centra en la necesidad de identificar y establecer medidas de control físicas para proteger adecuadamente los activos de información para evitar incidentes que afecten a la integridad física de la información o interferencias no deseadas.*	- Dirección Administrativa - Gestión de Tecnologías de la Información - Oficial de Seguridad de la Información
Seguridad operativa: *Asegura las operaciones correctas y seguras de las instalaciones de procesamiento de información.*	- Gestión de Tecnologías de la Información - Oficial de Seguridad de la Información
Seguridad en las comunicaciones: *Establece los controles adecuados para proteger tanto las comunicaciones externas a la*	- Gestión de Tecnologías de la Información - Oficial de Seguridad de la Información

organización como las que viajan a través de las redes de la propia organización.	
Adquisición desarrollo mantenimiento de sistemas informáticos: *Determina la aplicación de controles para la seguridad de la información al ciclo de vida completo de los sistemas de información, tanto propios como subcontratado.*	- Gestión de Tecnologías de la Información - Oficial de Seguridad de la Información
Relaciones con proveedores: *Establece de modo formal las condiciones para el acceso a los sistemas de información o a los recursos que manejan activos de información, así como él supervisar el cumplimiento de dichas condiciones.*	- Dirección Administrativa - Gestión de Tecnologías de la Información - Oficial de Seguridad de la Información
Gestión de incidentes en la seguridad de la información: *Establece controles para gestionar los incidentes en la seguridad de la información.*	- Todas las Direcciones y Gestiones apoyados con el Oficial de Seguridad de la Información
Gestión en la continuidad del negocio: *Implementa medidas de protección y de recuperación ante posibles desastres de esta naturaleza para minimizar los daños ante un evento o incidentes de seguridad de la información y facilitar el restablecimiento de las operaciones.*	- Dirección Administrativa - Dirección de Riesgos - Gestión de Tecnologías de la Información - Gestión de Administración de Talento Humano - Oficial de Seguridad de la Información

Cumplimiento: *Implementa controles que nos permitan garantizar el cumplimiento con las políticas, normas y legislación aplicable enfocándose principalmente en lo que se refiere a seguridad de la información.*	- Comité de Seguridad de la Información - Oficial de Seguridad de la Información

7.7. Cumplimiento

Esta Política entrará en vigencia a partir de su aprobación por parte del Consejo Directivo, siendo los directores y jefes de cada una de las gestiones, los responsables de informar por escrito a sus subordinados.

Los contratados con posterioridad a la fecha de publicación, deberán recibir una copia digital de este documento y firmar su aceptación.

7.8. Difusión

El Comité será responsable de difundir esta Política y otras políticas específicas, en coordinación con las Gestiones de Talento Humano, Comunicación Social y el Oficial de Seguridad de la Información.

7.9. Sanciones

El incumplimiento de los términos y/o disposiciones de esta Política se considerará un incidente de seguridad de información y estará sujeto a investigación administrativa y medidas disciplinarias en los términos de las leyes vigentes y aplicables.

7.10. Validez y gestión de documentos

- Este documento es válido desde el 09/07/2024.
- El propietario de este documento es el Oficial de Seguridad de la Información, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año o cada vez que el ISSPOL realice cambios relevantes que afecten la adecuada protección de la información, teniendo en cuenta cambios en la misión, objetivos estratégicos, estrategias, productos

estratégicos, infraestructura, personal y/o procedimientos relacionados con la protección de la información.

- Las enmiendas se presentarán al Comité y este a su vez a la Dirección General para que se gestione la aprobación por parte del Consejo Directivo.
- Las políticas específicas podrán ceñirse a la estructura y formato de referencia, descrita en el Anexo 3.

7.11. Evaluación de cumplimiento

Todos Directores, Jefes de Gestión y Unidades Organizativas son responsables de la implementación de las Política de Seguridad de la Información, dentro de sus áreas de responsabilidad, así como del cumplimiento de las políticas específicas, normativas y procedimientos por parte de sus equipos.

ISSPOL debe realizar auditorías internas anuales del sistema de gestión de seguridad de la información para garantizar el cumplimiento de los principios, estándares, políticas y procedimientos de seguridad de la información.

8. Anexos

- Anexo 1 Definiciones
- Anexo 2 Acuerdo de confidencialidad
- Anexo 3 Estructura y formato para políticas específicas

ANEXO 1

DEFINICIONES

Alcance del SGSI: es definir claramente los límites para la implementación del SGSI y cómo los activos de información serán protegidos de riegos/amenazas

Amenaza: todo elemento o acción capaz de atentar contra la seguridad de la información, surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza, que puede ser aprovechada e independientemente de que se comprometa o no la seguridad de un sistema de información

Acuerdo de confidencialidad: es un documento que se firma entre las partes en el cual se comprometen a no divulgar ni compartir información que manejan por motivos de trabajo, o de participación en algún proyecto. Es decir, se comprometen a mantener la confidencialidad de la información a la que tienen acceso

Activo de información: Información de propiedad del ISSPOL, sus medios de almacenamiento y procesamiento, que son considerados críticos para el cumplimiento de los procesos y objetivos de la Institución.

Activos de información: son los recursos que utiliza un SGSI para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección. En el contexto de esta Política, se aplica a los sistemas de información y demás información o equipos, incluyendo documentos en papel, teléfonos móviles, ordenadores portátiles, soportes de almacenamiento de datos, etc.

Comité de Seguridad de la Información (CSI): es el máximo órgano al que compete la Seguridad de la Información en la organización. En este sentido, identifica objetivos y estrategias relacionados con la seguridad de la información y dirige y controla los procesos relacionados con la seguridad.

Entre otras funciones, asume la responsabilidad de coordinar la implementación de un "Sistema de Gestión de Seguridad de la Información (SGSI)", su mejora continua, colaborando muy estrechamente con el "Oficial de Seguridad de la Información (OSI)".

Confidencialidad: Es la propiedad de prevenir la revelación y divulgación intencionada o no intencionada de la información a personas no autorizadas, es decir la información solo tiene que ser accesible o divulgada a aquellos que están autorizados

Control: acciones y mecanismos definidos para prevenir o reducir el impacto de los eventos no deseados que ponen en riesgos los activos de la institución

Controles de seguridad: tienen como objetivo ayudar a gestionar la seguridad de la información en una empresa, así como asegurar la confidencialidad y la integridad de sus datos

Criterios de confidencialidad: El nivel de confidencialidad se determina de acuerdo a los siguientes criterios

- Valor de la información: según los impactos evaluados durante la evaluación de riesgos
- Sensibilidad y grado crítico de la información: según el mayor riesgo calculado para cada elemento de información durante la evaluación de riesgos.
- Obligaciones legales y contractuales: según la Lista de obligaciones legales, normativas y contractuales y de otra índole

Documentación: ésta se encuentra identificada por el procesamiento de información que otorgará datos específicos sobre un tema determinado; de acuerdo con esto puede identificarse como una técnica instrumental y auxiliar, para lograr informar a numerosas personas

Disponibilidad: Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella como usuarios autorizados, ya sean personas, procesos, aplicaciones, es decir la información debe estar siempre accesible para aquellos que estén autorizados

Esquema Gubernamental de Seguridad de la Información (EGSI v2.0): busca preservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos de seguridad de la información y la selección de controles para el tratamiento de los riesgos identificados

Gestión de seguridad: involucra la alineación del Core de negocio (objetivos) y la cultura organizacional con la seguridad de la información en la entidad. La gestión de seguridad es transversal a los procesos de la organización

Implementación: permite expresar la acción de poner en práctica, medidas y métodos, entre otros, para concretar alguna actividad, plan, o misión, en otras alternativas.

Información sensible: es aquella información, así definida por su propietario, cuya revelación, alteración, pérdida o destrucción puede producir daños importantes a la organización propietaria de la misma

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

ISO: en español Organización Internacional de Estandarización, la cual se encarga de conformar y promover un sistema que permite la normalización internacional de una gran cantidad de productos y que además abarca diversas áreas

Información: es un conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente o fenómeno. La información, por lo tanto, procesa y genera el conocimiento humano

Información confidencial o clasificada: Información relativa a materia clasificada como secreta o confidencial, cuya revelación puede causar perjuicio al titular de la información, especialmente si se trata de información que puede afectar a la Institución

Integridad: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas, la información debe permanecer correcta y como el emisor originó sin manipulaciones de terceros

Incidente seguridad de la información: es cualquier evento que tenga el potencial de afectar la preservación de la confidencialidad, integridad, disponibilidad o valor de la información (Ej. Revelación no autorizada o accidental de información clasificada o sensible; Robo o pérdida de información clasificada o sensible; Modificación no autorizada de información clasificada o sensible; Acceso no autorizado a los sistemas de información de la Organización)

Institución: Grupo de personas e instalaciones con una disposición de responsabilidades, autoridades y relaciones

Identificación de activos de información: permite clasificar los activos a los que se les debe brindar mayor protección, pues identifica claramente sus características y rol al interior de un proceso

ISO/IEC 27000: Es un estándar que define el vocabulario estándar empelado en la familia 27000

ISO/IEC 27001: Es un estándar que describe los requisitos a implantar en un Sistema de Gestión de la Seguridad de la Información (SGSI).

ISO/IEC 27002: Es un estándar que proporciona buenas prácticas de seguridad de la información en la que se describen los controles - medidas a tomar.

ISO/IEC 27005: Es un estándar para la gestión de riesgos de seguridad de la información.

ISO 9001:2015: estándar internacional publicado por ISO para establecer de manera efectiva un Sistema de Gestión de la Calidad. Especifica unos requisitos generales para que pueda ser aplicada en cualquier tipo de organización, sin importar el sector, tamaño o tipo

Norma: es una regla que debe ser respetada y que permite ajustar ciertas conductas o actividades

Normas ISO: son un conjunto de normas orientadas a ordenar la gestión de una empresa en sus distintos ámbitos

Oficial de Seguridad de la Información: Responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento del Esquema Gubernamental de Seguridad de la Información (EGSI v2.0) / Sistema de Gestión de Seguridad de la Información (SGSI).

Plan de implementación: conjunto de acciones y actividades que deben llevarse a cabo para poner en funcionamiento e implementar

Plan Director de Seguridad de la Información: El plan consiste en un conjunto de proyectos que se elaboran con el fin de manejar y garantizar la seguridad de la información de la organización, mediante la reducción de los riesgos a los que se encuentran expuestos los sistemas informáticos, hasta conseguir un nivel aceptable

Plan de difusión, capacitación y sensibilización: El plan consiste en un conjunto de lineamientos para difusión, capacitación y sensibilización en materia de seguridad de la información, con el fin de que los servidores civiles, policiales, cumplan con sus responsabilidades de precautelar la seguridad y privacidad de la información dentro y fuera del ISSPOL

Política de Seguridad de la Información: es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información

Proceso: es una secuencia de pasos dispuesta con algún tipo de lógica que se enfoca en lograr algún resultado específico, está compuesto por entradas y 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.

Reglamento del Comité de Seguridad de la Información: documento que tiene como objetivo regular el funcionamiento, responsabilidades, atribuciones y desarrollo de las actividades del Comité de Seguridad de la Información.

Responsable sobre los activos: Cada activo de información tiene designado un propietario en el Inventario de activos. El propietario del activo es el responsable de la confidencialidad, integridad y disponibilidad de la información en el activo en cuestión.

Responsable de Seguridad Informática: Se encargará de definir y documentar controles para la detección y prevención de accesos no autorizados, protección contra software malicioso, garantiza la seguridad de los datos y servicios conectados a las redes de la Institución.

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.

Unidades organizativas: Son las Direcciones, Gestiones y Coordinaciones que pertenecen al ISSPOL.

Usuarios: se refiere a las servidoras/res públicos, servidoras/res policiales directivos/técnico operativo, trabajadores/as, asesores/as, practicantes/pasantes, organismos de control o cualquier persona que, bajo cualquier relación de dependencia con la Institución, hace uso de los sistemas de información para el desarrollo de las actividades que se relacionan con la generación, procesamiento y resguardo de la información.

Sistema de Gestión de Seguridad de la Información (SGSI): es una herramienta de gestión compuesto por un conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados por una organización, con el objetivo de proteger o minimizar los riesgos que atenten con sus activos de información esenciales. El Oficial de Seguridad de la Información será el responsable de su mantenimiento y gestión.

Seguridad: es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

Seguridad de la información: se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan

Seguridad informática: Es un concepto fundamentalmente técnico que se ocupa de las implementaciones técnicas de la protección de la información de la infraestructura TIC. Nos centramos específicamente en aspectos de la seguridad que inciden directamente en los medios informáticos en los que la información se genera, se gestiona, se almacena o se destruye; siempre desde el punto de vista tecnológico de la informática y de la telemática

Sistema de gestión: Es una herramienta que permite controlar, planificar, organizar y automatizar las tareas administrativas de una organización

Sistema integrado de gestión: es un conjunto de elementos y actividades relacionados y coordinados que interactúan, y que, estableciendo Políticas y Objetivos, dirigen y controlan la organización con el fin de lograr dichas metas

Sistemas informáticos: es aquel sistema que aúna por un lado la parte física de la informática y por otra, la parte digital o no tangible de la informática

Tercero: se refiere a todas las personas, jurídicas o naturales, empresas prestadoras de servicios, contratistas, sub contratistas, proveedores, consultores y cualquiera que, por cuenta propia o de terceros, provean servicios, productos o desarrollen trabajos para la Institución.

Mesa de ayuda: Es un servicio integral, que, a través de un punto de contacto, brinda la solución de incidentes y atención de requerimientos relacionados con la tecnología de información, y permite mantener informado al personal del ISSPOL, del estado del proceso de atención a sus necesidades.

ANEXO 2

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN

El (La) Señor (a).....con número de cédula:.....,con el cargo de..... que en adelante se denominará **"EL/LA INTERESADO/A"**, de manera libre y voluntaria, en pleno uso de sus capacidades, suscribe el presente **"Acuerdo de Confidencialidad y No Divulgación de Información"**, en adelante **"Acuerdo"**, al tenor de las siguientes cláusulas:

Cláusula Primera. - ANTECEDENTES:

El artículo 18, numeral 2 de la Constitución de la República del Ecuador, prescribe: *"Todas las personas, en forma individual o colectiva, tienen derecho a: 2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información"*.

La Administración pública y sus servidores, únicamente deben ejercer las competencias y facultades previstas en la Constitución y la Ley, de acuerdo con lo dispuesto en el artículo 226 de la Carta Fundamental del Estado.

La Constitución de la República, en el artículo 227 prescribe que la administración pública constituye un servicio a la colectividad que se rige, entre otros, por el principio de transparencia.

El artículo 5 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, establece: *"Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado."*.

El artículo 6, determina: *"Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 66 y 76 de la Constitución Política de la República.*

El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes (...).".

El artículo 10 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, prescribe: *"Custodia de la Información.- Es responsabilidad de las instituciones públicas, personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley, crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción";*

"Quienes administren, manejen, archiven o conserven información pública, serán personalmente responsables, solidariamente con la autoridad de la dependencia a la que pertenece dicha información y/o documentación, por las consecuencias civiles, administrativas o penales a que pudiera haber lugar, por sus acciones u omisiones, en la ocultación, alteración, pérdida y/o desmembración de documentación e información pública. Los documentos originales deberán permanecer en las dependencias a las que pertenezcan, hasta que sean transferidas a los archivos generales o Archivo Nacional".

El artículo 179 del Código Integral Penal tipifica que: *"La persona que, teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año".*

El artículo 229 del Código Integral Penal tipifica que: *"Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.*

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años".

El artículo 230 del Código Integral Penal tipifica que: *"Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años:*

1. *La persona que, sin orden previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.*

2. *La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal*

manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. *La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.*

4. *La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior".*

El artículo 232 del Código Integral Penal tipifica que: *"Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que:*

1. *Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.*

2. *Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.*

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad"

El último inciso del artículo 22 de la Ley Orgánica de Servicio Público establece como deberes de las o los servidores públicos: *"Custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o comisión tenga bajo su responsabilidad e impedir o evitar su uso indebido, sustracción, ocultamiento o inutilización".*

El Código de Ética del Instituto de Seguridad Social de la Policía Nacional, en el artículo 12 Prevención y prohibición de uso indebido de información prescribe:

"1. Confidencialidad. - La responsabilidad como servidor del ISSPOL exige mantener en reserva la información relacionada con esta, que no deba ser de dominio público, así como abstenerse de aprovecharla para fines particulares; además, guardar absoluta reserva sobre las políticas, procedimientos u operaciones que le sean suministrados o a las que tenga acceso con ocasión de su trabajo".

Cláusula Segunda. - OBJETO:

Mediante el presente instrumento legal, se regula la reserva, confidencialidad, custodia y conservación de la **"INFORMACIÓN CONFIDENCIAL"**, de cualquier tipo, clase o contenido, sea a través de medios documental, físico, digital, etc., que le suministre o pudiera suministrarle el "ISSPOL" al servidor policial y civil, a quienes en adelante se les denominará "EL/LA INTERESADO/A".

La suscripción de "EL/LA INTERESADO/A" en el presente instrumento, le obliga y compromete a su sujeción y aceptación del contenido y tenor literal.

Cláusula Tercera. - DEFINICIÓN DE INFORMACIÓN CONFIDENCIAL:

Para efectos del presente documento, se considerará **"INFORMACIÓN CONFIDENCIAL"**, la 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;

d) Las patentes, derechos de autor y secretos comerciales;

e) Informaciones de carácter médico, técnico, financiero, inversiones bajo cualquier modalidad, legal, fiscal, comercial, datos personales de afiliados y pensionistas, proyectos y operaciones de cualquier carácter propuestas o en fase de estudio, informes, planos, proyecciones de mercado y datos, junto con los análisis y documentos de trabajo, recopilaciones, comparaciones, estudios y en general, toda la información en cualquier forma o medio en que se encuentre.

Cláusula Cuarta. - OBLIGACIONES:

"EL/LA INTERESADO/A" tiene conocimiento y acepta que la información y documentos de carácter técnico, económico, financiero, legal, estadístico, de planificación y/o información de terceros (ejecutores, beneficiarios, promotores, contratistas, etc.), que administre, tenga acceso, o le proporcione el "ISSPOL", a

través del presente acuerdo, es de propiedad exclusiva de la Institución, debiendo protegerla y mantenerla de manera reservada, por lo que, no podrá ser divulgada por cualquier medio, verbal, escrito u otros, salvo en los casos de autorización expresa del "ISSPOL", y podrá ser utilizada con fines consultivos, investigativos, estadísticos, por parte de "EL/LA INTERESADO/A".

"EL/LA INTERESADO/A" se responsabiliza por el buen uso de la "INFORMACIÓN CONFIDENCIAL", mediante el uso de las herramientas tecnológicas, para lo cual, declara que su utilización se limitará al desarrollo de las actividades institucionales, siendo de su absoluta y personal responsabilidad, cualquier utilización indebida o perjudicial para el "ISSPOL", aceptando que el uso inadecuado de la información generaría responsabilidad administrativa, civil e inclusive penal.

"EL/LA INTERESADO/A", acepta conocer: la Constitución de la República, la Ley Orgánica de Transparencia y Acceso a la Información Pública, la Ley Orgánica del Servicio Público, el Código Orgánico Integral Penal; el Código de Ética del ISSPOL y el Reglamento Interno de Administración de Talento Humano que se cree para el efecto. Además de las implicaciones legales por su incumplimiento, previstas para el efecto en el marco jurídico vigente.

"EL/LA INTERESADO/A", conoce y acepta que las obligaciones inherentes a la confidencialidad de la información a la que tenga acceso persistirán indefinidamente, mientras la información mantenga el carácter de confidencial.

El/LA INTERESADO/A", Se compromete a cumplir con todas las leyes, regulaciones y normativas aplicables inherentes a la confidencialidad y no divulgación de la información, así como aquellas relacionadas con la prevención del soborno y otras actividades ilícitas; se abstendrá de participar en prácticas corruptas o ilegales debiendo aplicar principios éticos y de cumplimiento.

Cláusula Quinta. - TRATAMIENTO DE LA INFORMACIÓN CONFIDENCIAL:

"EL/LA INTERESADO/A", no podrá hacer uso de la "INFORMACIÓN CONFIDENCIAL" para ningún propósito distinto a lo establecido en el presente acuerdo. En todo momento, "EL/LA INTERESADO/A" tomará y mantendrá las medidas apropiadas de seguridad de la información, a fin de proteger la "INFORMACIÓN CONFIDENCIAL" según los términos de este Acuerdo.

"EL/LA INTERESADO/A", conoce y acepta que toda la información provista por el ISSPOL es de propiedad exclusiva o se encuentra bajo custodia del ISSPOL.

"EL/LA INTERESADO/A", ha sido informado y acepta que en virtud de la naturaleza de la información y a los riesgos que el mal uso y/o divulgación de la misma implican para la ISSPOL, la inobservancia de este acuerdo se considera como un incidente de seguridad de la información.

Cláusula Sexta. - INCUMPLIMIENTO:

En el evento de que se produzca la inobservancia y/o incumplimiento de la "**Política de Seguridad de la Información**" o alguna de las cláusulas estipuladas en el presente acuerdo, se notificará del incumplimiento a la máxima autoridad de la institución, sin perjuicio de que el ISSPOL pueda iniciar las acciones y sanciones previstas en la cláusula séptima.

Cláusula Séptima. - SANCIONES:

"EL/LA INTERESADO/A", será sancionado de la siguiente manera:

- **Servidor público policial:** De conformidad con lo determinado en el Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público y demás normativa conexa.

- **Servidor público civil:** De conformidad con lo determinado en la Ley Orgánica del Servicio Público y demás normativa conexa.

Cláusula Octava. - VIGENCIA:

El presente acuerdo entrará en vigencia a partir de su suscripción y finalizará una vez que "EL/LA INTERESADO/A" cumpla con el proceso formal de desvinculación del ISSPOL, de acuerdo a lo establecido en el Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público y su reglamento y la Ley Orgánica del Servicio Público, LOSEP y su reglamento general, según corresponda.

Cláusula Novena. - ACEPTACIÓN:

"EL/LA INTERESADO/A" acepta el contenido de todas y cada una de las cláusulas del presente acuerdo, por lo que, se compromete a cumplirlas en toda su extensión y como muestra de aquello, se suscribe en 2 (dos) ejemplares del mismo tenor y efecto, en la ciudad de Quito, Distrito Metropolitano, el dd de mm de aaaa.

Firma de responsabilidad y aceptación

"EL/LA INTERESADO/A"
INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICIA NACIONAL DEL ECUADOR

Señor, Coronel de Policía de E.M.
Lcdo. Renato González Peñaherrera
DIRECTOR GENERAL
INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICIA NACIONAL

ANEXO 3

Toda política específica para la gestión de seguridad de la información basada en la aplicación del estándar internacional ISO/IEC: 27001 podrá contener la siguiente estructura y en el marco de las directrices que emita la Gestión de Planificación Estratégica y Calidad:

1. ESTRUCTURA (Referencia)

TABLA DE CONTENIDO

TABLAS