Resolución Nro. SGDPN-SGDPN-2023-0014-R

Quito, D.M., 28 de noviembre de 2023

SECRETARÍA DE GESTIÓN Y DESARROLLO DE PUEBLOS Y NACIONALIDADES

EL SECRETARIO DE GESTIÓN Y DESARROLLO DE PUEBLOS Y NACIONALIDADES.

CONSIDERANDO:

Que, la Constitución de la República del Ecuador, en el numeral 1 del artículo 154, dispone que las Ministras y Ministros de Estado además de las atribuciones establecidas en la Ley, les corresponde: *"Ejercer la rectoría de las políticas públicas del área a su cargo y expedir los acuerdos y sus resoluciones administrativas que requieren su gestión (…)";*

Que, la Constitución de la República del Ecuador en el artículo 18, numerales 1 y 2, señala: *"Todas las personas, en forma individual o colectiva, tienen derecho a: 1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior. 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";*

Que, el artículo 82 de la Constitución de la República del Ecuador, establece: *"El derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, clara, públicas y aplicadas por las autoridades competentes";*

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

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

Resolución Nro. SGDPN-SGDPN-2023-0014-R

Quito, D.M., 28 de noviembre de 2023

Que, el Código Orgánico Administrativo en su artículo 130, establece: *"Las máximas autoridades administrativas tienen competencia normativa de carácter administrativo únicamente para regular los asuntos internos del órgano a su cargo, salvo los casos en los que la ley prevea esta competencia para la máxima autoridad legislativa de una administración pública. La competencia regulatoria de las actuaciones de las personas debe estar expresamente atribuida en la ley";*

Que, el numeral 14 del artículo 3 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, establece*: "Las entidades reguladas por esta Ley deberán implementar procesos de mejoramiento continuo de la gestión de trámites administrativos a su cargo, que impliquen al menos un análisis del desempeño real de la gestión del trámite y oportunidades de mejora continua";*

Que, mediante Decreto Ejecutivo Nro. 29 de 24 de mayo de 2021, se creó la Secretaría de Gestión y Desarrollo de Pueblos y Nacionalidades, como una entidad de derecho público, con personalidad jurídica, dotada de autonomía administrativa y financiera, dirigida por un Secretario con rango de Ministro de Estado, quien ejercerá la representación legal, judicial y extrajudicial y será de libre nombramiento y remoción del presidente de la República;

Que, mediante Decreto Ejecutivo Nro. 186, de 7 de septiembre de 2021, se ampliaron las competencias de la Secretaría de Gestión y Desarrollo de Pueblos y Nacionalidades, determinando que tendrá a su cargo la rectoría y asumirá las competencias de plurinacionalidad e interculturalidad;

Que, mediante Decreto Ejecutivo Nro. 664 de 09 de febrero de 2023, se designó como Secretario de Gestión y Desarrollo de Pueblos y Nacionalidades al Antropólogo Jorge Marcelo Córdoba Castro;

Que, mediante Acuerdo Ministerial Nro. 025-2019 de 20 de septiembre de 2019, el Ministro de Telecomunicaciones y de la Sociedad de la Información, expidió el *"Esquema Gubernamental de Seguridad de la Información (EGSI)"*, el cual es de implementación obligatoria en las instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva;

Que, mediante Resolución Nro. SGDPN-2021-008 de 18 de octubre de 2021, se Resuelve expedir *"El Reglamento para la Conformación y Funcionamiento del Comité de Seguridad de la Información (Csi) de la Secretaría de Gestión y Desarrollo de Pueblos y Nacionalidades";*

Que, mediante Resolución Nro. SGDPN-2022-006 de 31 de enero de 2022, se reforma el artículo 5 del Reglamento para la conformación y funcionamiento del Comité de Seguridad de la Información (Csi) de la Secretaría de Gestión y Desarrollo de Pueblos y

Resolución Nro. SGDPN-SGDPN-2023-0014-R

Quito, D.M., 28 de noviembre de 2023

Nacionalidades;

Que, mediante memorando Nro. SGDPN-SGDPN-2023-0384-M, de 13 de septiembre de 2023, el Director de Planificación y Gestión Estratégica, Encargado, señala: *"De acuerdo a lo establecido en el Acuerdo Ministerial No. 025-2019, del Ministerio de Telecomunicaciones y Sociedad de la Información, publicado mediante registro oficial el 10 de enero de 2020, en su artículo 7, señala: "El Comité de Seguridad de la Información (CSI) designará al interior de su institución a un funcionario como Oficial de Seguridad de la Información (OSI)".*

"Por lo antes manifestado y de conformidad a lo establecido en el numeral 5, del artículo 7 de la
resolución Nro. SGDPN-2021-008, de fecha 18 de octubre de 2021, Funciones del Presidente del
Comité de Seguridad de la Información: "Notificar el nombramiento como Oficial de Seguridad de la Información al funcionario seleccionado en el Comité de Seguridad de la Información", se procede a notificar a Usted Srta. María Silvia Umajinga Ante, el nombramiento como Oficial de Seguridad de la Información de esta cartera de Estado.

Por lo antes mencionado, dentro de las responsabilidades del Oficial de Seguridad de la Información, se registran las siguientes:

1. *Identificar todas las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI:*

k) l) Informar al Comité de Seguridad de la Información, el avance de la implementación del
Esquema Gubernamental de Seguridad de la Información (EGSI), así como las alertas que
impidan su implementación (…)";

Que, mediante reunión extraordinaria del Comité de Seguridad de la Información para la aprobación de la Política de Seguridad de la Información de la SGDPN y acta de reunión Nro. SGDPN-UCS-CSI-2023 de 23 de noviembre de 2023, se certifica*; "(…) aprobado la Política de Seguridad de la Información de la SGDPN, el presidente del Comité de Seguridad de la Información, Eco. Ricardo Reinoso, da por concluida la reunión extraordinaria del Comité de Seguridad de la Información (…),* en el mismo documento se acuerda el compromiso de la; *"Elaboración de la Resolución de la Política de Información de la SGDPN.";*

En ejercicio de las atribuciones constitucionales, legales y reglamentarias:

Resolución Nro. SGDPN-SGDPN-2023-0014-R

Quito, D.M., 28 de noviembre de 2023

RESUELVE:

Artículo 1.- APROBAR la Política de Seguridad de la Información de la Secretaría de Gestión y Desarrollo de Pueblos y Nacionalidades, las mismas que serán de cumplimiento obligatorio para todos/as los/las servidores/as y funcionarios/as que tenga relación con la Secretaría de Gestión y Desarrollo de Pueblos y Nacionalidades.

Las políticas de seguridad de la información, serán elaboradas y emitidas por el Comité de Seguridad de la Información (EGSI).

Artículo 2.- El/la Oficial de Seguridad de la Información de ser necesario identificará y definirá nuevas políticas de carácter específico y particular para diferentes procesos que se implementen en la SGDPN, con la aprobación de la máxima autoridad y serán incorporadas en las siguientes actualizaciones de la Política de Seguridad de la Información.

Artículo 3.- ENCARGAR a el/la Oficial de Seguridad de la Información conjuntamente con la Unidad de Comunicación Social, responsables de elaborar estrategias de difusión y capacitación a todos los/las servidoras/ y funcionarios/as de la Secretaría de Gestión y Desarrollo de Pueblos y Nacionalidades, sobre la Política de Seguridad de la información.

Artículo 4.- El/la Oficial de Seguridad de la Información, presentará un informe semestral a la máxima autoridad, respecto de novedades, seguimiento y cumplimiento de las presentes políticas.

Artículo 5.- Encárguese a la Unidad de Comunicación Social la publicación de la presente Resolución.

Artículo 6.- Declarar la presente Resolución de ejecución inmediata.

Dada en la ciudad de Quito, Distrito Metropolitano, el 27 de noviembre de 2023.

Antrop. Jorge Marcelo Córdoba Castro
SECRETARIO DE GESTIÓN Y DESARROLLO DE PUEBLOS Y NACIONALIDADES.

Resolución Nro. SGDPN-SGDPN-2023-0014-R

Quito, D.M., 28 de noviembre de 2023

Documento firmado electrónicamente

Antrop. Jorge Marcelo Córdoba Castro
SECRETARIO DE GESTIÓN Y DESARROLLO DE PUEBLOS Y NACIONALIDADES

Referencias:
- SGDPN-DPGE-2023-0465-M

Anexos:
- A1 Resolución Nro. SGDPN-2021-008
- A2 Resolución Nro. SGDPN-2022-006
- A3 Acta aprobación PSI
- Política de Seguridad de la Información-signed
- política_de_seguridad_de_la_información-signed-signed.pdf

Copia:
Señorita Magíster
Angelita Andrea Suarez Pacheco
Directora de Asesoría Jurídica

Señorita
Maria Silvia Umajinga Ante
Oficial de Seguridad de la Información

lh/as

Firmado electrónicamente por:
JORGE MARCELO CORDOBA CASTRO

Secretaría de Gestión y Desarrollo de
Pueblos y Nacionalidades

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (EGSI)

Comité de Seguridad de la Información

Noviembre 2023

República del Ecuador
Gobierno del Ecuador
GUILLERMO LASSO
PRESIDENTE

Secretaría de Gestión y Desarrollo de Pueblos y Nacionalidades

DATOS GENERALES

Código del documento:	CSI-P001-PO	
Tipo de documento:	Política	
Institución:	Secretaría de Gestión y Desarrollo de Pueblos y Nacionalidades	
Unidad ejecutora:	Comité de Seguridad de la Información	
Fecha:	23-11-2023	
Versión:	1.0	
ACCIÓN	**NOMBRE/CARGO**	**SUMILLA**
Revisado y aprobado por:	Marco Ricardo Reinoso Villamil Director de Planificación y Gestión Estratégica (E)	Firmado electrónicamente por: MARCO RICARDO REINOSO VILLAMIL
	Lilian de los Ángeles Sánchez Saavedra Directora Administrativa	Firmado electrónicamente por: LILIAN DE LOS ANGELES SANCHEZ SAAVEDRA
	Norma Gioconda Urquizo Déleg Directora de Administración del Talento Humano	Firmado electrónicamente por: NORMA GIOCONDA URQUIZO DELEG
	Daniel Antonio Riera Suárez Director de Tecnologías de la Información y Comunicaciones (E)	Firmado electrónicamente por: DANIEL ANTONIO RIERA SUAREZ
	Alex Vicente Valdez Chamba Director de Registro de Comunidades, Pueblos, Nacionalidades, Fundaciones y Organizaciones sin Fines de Lucro (E)	Firmado electrónicamente por: ALEX VICENTE VALDEZ CHAMBA
	Jorge Patricio Silva Delgado Director de Políticas Públicas de los Pueblos y Nacionalidades	Firmado electrónicamente por: JORGE PATRICIO SILVA DELGADO
	Denisse Estefanía Sevillano Calderón Directora de Desarrollo de Proyectos a Comunas, Comunidades, Pueblos, Nacionalidades	Firmado electrónicamente por: DENISSE ESTEFANIA SEVILLANO CALDERON
	David Patricio Muenala Amaguaña Director de Fortalecimiento de los Pueblos y Nacionalidades	Firmado electrónicamente por: DAVID PATRICIO MUENALA AMAGUANA
	Angelita Andrea Suárez Pacheco Directora de Asesoría Jurídica	Firmado electrónicamente por: ANGELITA ANDREA SUAREZ PACHECO
	Jaime Rodrigo León Pomaquiza Analista de Comunicación 2	Firmado electrónicamente por: JAIME RODRIGO LEON POMAQUIZA
Elaborado por:	María Silvia Umajinga Ante Oficial de Seguridad de la Información	Firmado electrónicamente por: MARIA SILVIA UMAJINGA ANTE

CONTROL DE CAMBIOS

Versión	Descripción del Cambio	Fecha	Responsable del Cambio
1.0	Versión inicial	23/11/2023	Comité de Seguridad de la Información

CONTENIDO

1. Antecedentes:

El numeral 1 del Artículo 154 de la Constitución de la República del Ecuador establece que a los Ministros de Estado les corresponde: "*Ejercer la rectoría de las políticas públicas del área a su cargo y expedir los acuerdos y resoluciones administrativas que requiera su gestión".*

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

El artículo 227 de la Constitución de la República del Ecuador manifiesta que: *"La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación".*

El artículo 47 del Código Orgánico Administrativo, prescribe *"La máxima autoridad administrativa de la correspondiente entidad pública ejerce su representación para intervenir en todos los actos, contratos y relaciones jurídicas sujetas a su competencia. Esta autoridad no requiere delegación o autorización alguna de un órgano o entidad superior, salvo en los casos expresamente previstos en la ley".*

La Ley Orgánica de Telecomunicaciones en su artículo 140, establece: *"Rectoría del sector. - El Ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información es el órgano rector de las telecomunicaciones y de la sociedad de la información, informática, tecnologías de la información y las comunicaciones y de la seguridad de la información. A dicho órgano le corresponde el establecimiento de políticas, directrices y planes aplicables en tales áreas para el desarrollo de la sociedad de la información, de conformidad con lo dispuesto en la presente Ley, su Reglamento General y los planes de desarrollo que se establezcan a nivel nacional".*

Mediante Decreto Ejecutivo Nro. 29 de 24 de mayo de 2021, el Presidente de la República del Ecuador dispone: *"Artículo 1.- Créase la Secretaría de Gestión y Desarrollo de Pueblos y Nacionalidades, como una entidad de derecho público, con personalidad jurídica, dotada de autonomía administrativa y financiera. Estará dirigida por un Secretario con rango de Ministro de Estado, quien ejercerá la representación legal, judicial y extrajudicial y será de libre nombramiento y remoción del Presidente de la República".*

Mediante Decreto Ejecutivo Nro. 186, de 07 de septiembre del 2021, el Presidente Constitucional de la República del Ecuador dispuso lo siguiente: *"Artículo 1.- La Secretaría de Gestión y Desarrollo de Pueblos y Nacionalidades tendrá a su cargo la rectoría y asumirá las competencias de plurinacionalidad e interculturalidad".*

A través del Acuerdo Ministerial Nro. 025-2019, el Ministerio de Telecomunicaciones y de la Sociedad de la Información expidió el Esquema Gubernamental de Seguridad de la Información - EGSI versión 2.0, el cual es de implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.

Mediante Acuerdo Ministerial Nro. 025-2019 se establece: *"Es responsabilidad de la máxima autoridad de cada institución gestionar la implementación de esta normativa asignando los recursos necesarios".*

Las instituciones de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesas, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera.

El Secretario de Gestión y Desarrollo de Pueblos y Nacionalidades, mediante resolución Nro. SGDPN-2021-008, de 18 de octubre de 2021 resuelve expedir el "Reglamento para la Conformación y Funcionamiento del Comité de Seguridad de la Información (CSI) de la Secretaría de Gestión y Desarrollo de Pueblos y Nacionalidades".

Mediante resolución Nro. SGDPN-2022-006, de 31 de enero de 2022, en su artículo 1 resuelve: *"Refórmese el artículo 5 del REGLAMENTO PARA LA CONFORMACIÓN Y FUNCIONAMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (CSI) DE LA SECRETARÍA DE GESTIÓN Y DESARROLLO DE PUEBLOS Y NACIONALIDADES (…)"*.

2. Política de Seguridad de la Información:

2.1. Descripción de la Política

Para las instituciones es importante contar con una Política de Seguridad de la Información, ya que a través de este documento se guiará el comportamiento personal y profesional de los servidores, trabajadores, funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la institución,

así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la institución.

La máxima autoridad y el Comité de Seguridad de la Información de la Secretaría de Gestión y Desarrollo de Pueblos y Nacionalidades, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la institución.

Para la Secretaría de Gestión y Desarrollo de Pueblos y Nacionalidades, la protección de la información busca la disminución del impacto generado sobre sus activos, 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 la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo a lo expuesto, esta política aplica a la Institución según como se define en el alcance: sus servidores, trabajadores, nivel directivo, terceros, proveedores y la ciudadanía en general, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

2.2. Objeto

Establecer la Política de Seguridad de la Información de la Secretaría de Gestión y Desarrollo de Pueblos y Nacionalidades-SGDPN

, frente a amenazas internas o externas, intencionales o no, para asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

2.3. Ámbito de Aplicación

La Política de Seguridad de la Información de la SGDPN, es de aplicación y cumplimiento obligatorio para todos los servidores, trabajadores, funcionarios, practicantes o cualquier persona que tenga relación con la institución tanto a nivel

central y desconcentrado, así como también proveedores, instituciones públicas y privadas, sistemas o procesos que creen, utilicen, comparten, almacenen y transfieran información en medio electrónico, escrito o verbal, clasificada conforme lo determinen las leyes y normas vigentes.

2.4. Alcance

Se aplica para la protección de toda la información contenida, registrada, transmitida o procesada por y hacia la Secretaría de Gestión y Desarrollo de Pueblos y Nacionalidades, que se encuentre en medios físicos, digitales, en sistemas de información, en gestión de procesos gobernantes, sustantivos, adjetivos y cadena de valor; del nivel central y desconcentrado de la institución.

2.5. Roles y Responsabilidades

La máxima autoridad a través del Comité de Seguridad de la Información (CSI) es la responsable de asegurar que la seguridad de la información se gestione adecuadamente en toda la institución.

Cada funcionario líder de la unidad (NJS), es responsable de garantizar que los servidores que trabajan bajo su control, protejan la información de acuerdo con las normas establecidas por la institución.

El Oficial de Seguridad de la Información (OSI) asesora al equipo directivo, proporciona apoyo especializado al personal de la institución y garantiza que los informes sobre la situación de la seguridad de la información estén disponibles.

Cada uno de los funcionarios, servidores, trabajadores, practicantes o cualquier persona que tenga relación con la institución tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.

2.6. De la Institución:

- El Oficial de la Seguridad de la Información y el responsable de la Gestión de Infraestructura y Seguridad de la Información de la Dirección de Tecnologías de la Información y Comunicaciones, tendrán a cargo las funciones relativas a la seguridad de los sistemas de información de la SGDPN, lo cual incluye la supervisión de todos los aspectos inherentes a la seguridad de la información, cualquiera sea el medio de almacenamiento, tratados en la presente Política.

- El Comité de Seguridad de la Información realizará revisiones independientes sobre la vigencia e implementación de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas de la SGDPN reflejen adecuadamente sus disposiciones.

- La creación, mantenimiento y resguardo de la información y/o documentación será responsabilidad de cada Dirección dueña de la información y/o documentación, para el efecto deben mantener espacios físicos y digitales adecuados.

- Los expedientes físicos o digitales generados por las distintas unidades de la Secretaría, que ya no son de uso continuo pero que deben ser conservados por normativa, deben ser enviados al Archivo Central.

- La SGDPN adopta una política de puesto de trabajo despejado y pantalla limpia para proteger documentos en papel y dispositivos de almacenamiento extraíbles y a través de las pantallas limpias en las instalaciones de procesamiento de información, tiene como fin el reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo. Se aplicarán los siguientes lineamientos:
  1. Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
  2. Guardar bajo llave la información sensible o crítica de la SGDPN, cuando no está en uso, especialmente cuando no hay personal en la oficina.
  3. Apagar los equipos de computación, impresoras, cuando están desatendidas. Las mismas deben ser protegidas mediante, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de TICS mantendrán un registro de las contraseñas de seguridad utilizadas.

- El equipamiento, la información y el software no serán retirados de las oficinas, sin autorización formal del de su jefe inmediato. Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la SGDPN. El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones.

- El Comité de Seguridad de la Información, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades de la SGDPN.

  Este Comité tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información de la SGDPN frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

  1. Identificar y priorizar los procesos críticos de las actividades de la SGDPN.
  2. Asegurar que todos los integrantes de la SGDPN comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad de la SGDPN.
  3. Elaborar y documentar una estrategia de continuidad de las actividades de la SGDPN consecuente con los objetivos y prioridades acordados.
  4. Proponer planes de continuidad de las actividades de la SGDPN de conformidad con la estrategia de continuidad acordada.
  5. Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
  6. Coordinar actualizaciones periódicas de los planes y procesos implementados.
  7. Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades de la SGDPN.
  8. Proponer las modificaciones a los planes de contingencia.

- Todos los servidores, trabajadores, funcionarios, practicantes o cualquier persona que tenga relación con la institución tanto a nivel central y desconcentrado de la SGDPN deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan acceso con motivo del ejercicio de sus funciones.

  A través de una “Acta de Confidencialidad”, la cual deberá ser suscrita por todos los que tengan acceso a información clasificada como confidencial o secreta. La copia firmada del compromiso será retenida en forma segura por la SGDPN.

  Mediante este instrumento el suscriptor se comprometerá a utilizar la información solamente para el uso específico al que está destinada y a no

comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización.

2.7. De la Tecnología:

- Los nuevos recursos de procesamiento de información serán autorizados por los responsables de las unidades adjetivas, sustantivas y oficinas técnicas involucradas conjuntamente con el responsable de la Gestión de Infraestructura y Seguridad de la Información, considerando su propósito y uso, a fin de garantizar que se cumplan todas las políticas y requerimientos de seguridad pertinentes. Cuando corresponda se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas de la SGDPN.

- El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado en cada caso por el comité de seguridad de la información o por el responsable de Seguridad Informática.

- Cuando exista la necesidad de otorgar acceso a terceras partes a información de la SGDPN, La Dirección de Tecnologías de la Información y Comunicaciones a través del responsable de la Gestión de Infraestructura y Seguridad de la Información, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:
  - ✓ El tipo de acceso requerido (físico/lógico y a qué recurso). Los motivos para los cuales se solicita el acceso.
  - ✓ El valor de la información.
  - ✓ Los controles empleados por la tercera parte.
  - ✓ La incidencia de este acceso en la seguridad de la información de la SGDPN.

- La Dirección de Tecnologías de la Información y Comunicaciones establecerá procedimientos para la comunicación y corrección de anomalías de software.

- Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes.

- El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la SGDPN, será autorizado por el Director de cada área. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la SGDPN para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma. Se respetarán permanentemente las instrucciones respecto del cuidado del equipamiento. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito de la SGDPN.

- La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda. La Dirección de TICS, elaborará un procedimiento la desafectación segura de los medios de almacenamiento.

- Los responsables de los Sistemas de Información documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Director de TICS.

- El responsable de Infraestructura y Seguridad de la Información, conjuntamente con el responsable Soporte Técnico definirán controles de detección y prevención para la protección contra software malicioso.

    1. Prohibir el uso de software no autorizado por la SGDPN.

    2. Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.

    3. Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.

    4. Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).

    5. Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la SGDPN,

investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.

6. Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.

7. Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.

8. Concientizar al personal acerca del problema de los falsos virus y de cómo proceder frente a los mismos.

- El responsable de Infraestructura y Seguridad de la Información implementará controles para reducir los riesgos de incidentes de seguridad en el correo electrónico.

- Política y procedimiento para mensajería electrónica, se definirán y documentarán normas y procedimientos claros con respecto al uso del correo electrónico institucional, teniendo en cuenta que la seguridad de la cuenta del correo electrónico, es responsabilidad de cada uno de los servidores, trabajadores, funcionarios, practicantes o cualquier persona que tenga relación con la institución tanto a nivel central, como desconcentrado; para lo cual la institución deberá aplicar controles que aseguren el uso correcto del correo electrónico de tal manera que la información transmitida por este medio esté protegida adecuadamente.

- En la aplicación de controles de acceso, se contemplarán los siguientes aspectos:

  1. Identificar los requerimientos de seguridad de cada una de las aplicaciones.

  2. Identificar toda la información relacionada con las aplicaciones.

  3. Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes.

  4. Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.

5. Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.

6. Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

- Con el objetivo de impedir el acceso no autorizado a la información. Se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

- La asignación de contraseñas se controlará a través de un proceso de administración formal, en el que deberán incorporar medidas de gestión y protección de las contraseñas de acuerdo a los procedimientos definidos por la Dirección de Tecnologías de la Información y Comunicaciones. La DTIC, a través de sus gestiones serán los responsables del proceso de asignación de contraseñas.

- Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

- Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

  Los equipos instalados en áreas de usuarios, por ejemplo, estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

  Las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

- Las conexiones no seguras a los servicios de red pueden afectar a toda la SGDPN, por lo tanto, el responsable de Infraestructura y Seguridad de la Información controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan

acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El responsable de Infraestructura y Seguridad de la Información tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del jefe inmediato, que lo solicite para personal de su incumbencia.

- El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

  El responsable de la Infraestructura y Seguridad de la Información creará un documento que permita solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el responsable a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

- Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información de la SGDPN.

- El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo a la SGDPN.

  El trabajo remoto en los Sistemas de información o en los Activos de Información sólo será autorizado por el jefe inmediato a la cual pertenezca, y comunicado al Director de TICS verificando que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo que se cumpla con la política, normas y procedimientos existentes.

2.8. Del Recurso Humano:

- En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la SGDPN, La Dirección de Administración del Talento Humano, La Dirección de Tecnologías de la Información y Comunicaciones, el Responsable de Seguridad Informática y el Responsable del Área Legal establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar. En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto

se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

- El responsable de la Dirección Talento Humano llevará a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que a tal efecto.

- Como parte de sus términos y condiciones iniciales de empleo, los funcionarios, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la SGDPN. La copia firmada del Compromiso deberá ser retenida en forma segura por la Dirección Talento Humano. Asimismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo.

- Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información. Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la matriz u oficinas técnicas de la SGDPN y del horario normal de trabajo. Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo, en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo.

- Todos los funcionarios de la SGDPN y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la SGDPN, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la SGDPN. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

  El personal que ingrese a la SGDPN recibirá capacitación, en el que se le indicará el comportamiento esperado en lo que respecta a la seguridad de la información, antes de ser le otorgados los privilegios de acceso a los sistemas que correspondan. Por otra parte, el responsable de la Dirección de TICS arbitrará los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

2.9. De la Protección Física:

- La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las oficinas en la Planta Central y Oficinas Técnicas de SGDPN donde exista procesamiento de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo: una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera serán definidas por el responsable de la Dirección Administrativa con el asesoramiento de la Dirección de TICS, de acuerdo a la evaluación de riesgos efectuada. Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:
  1. Definir y documentar claramente el perímetro de seguridad.
  2. Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo: no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción).
  3. Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados.
  4. Verificar la existencia de un área de recepción atendida por personal. El acceso a las oficinas estará restringido y solo será exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.
  5. Identificar claramente todas las puertas de incendio de un perímetro de seguridad.

- Se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan las edificaciones. Se establecen las siguientes medidas de protección para áreas protegidas:
  1. Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
  2. Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.

3. Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, computadoras, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.
4. Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia.
5. Implementar mecanismos de control para la detección de intrusos. Estos mecanismos de control comprenderán todas las puertas exteriores y ventanas accesibles.
6. Separar las instalaciones de procesamiento de información administradas por la SGDPN de aquellas administradas por terceros.
7. Almacenar los materiales peligrosos o combustibles en lugares seguros a una distancia prudencial de las áreas protegidas de la SGDPN. Los suministros, como los útiles de escritorio, no serán trasladados a las Oficinas hasta que sean requeridos.
8. Almacenar los equipos redundantes y la información de resguardo (backup) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

- El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas, se contemplarán el disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.

- El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño, estas acciones son administradas por CNT e INMOBILIAR.

2.10. De los Terceros:

- El Comité de Seguridad de la información, a través del Titular de la Dirección de Asesoría Jurídica o su delegado revisará los contratos o acuerdos existentes o que se efectúen con terceros, teniendo en cuenta la necesidad de aplicar los siguientes controles:
  1. Cumplimiento de la Política de seguridad de la información de la SGDPN.
  2. Protección de los activos de la SGDPN, incluyendo:

a) Procedimientos para proteger los bienes de la SGDPN, abarcando los activos físicos, la información y el software.

b) Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.

c) Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.

d) Restricciones a la copia y divulgación de información.

3. Descripción de los servicios disponibles.
4. Nivel de servicio esperado y niveles de servicio aceptables.
5. Permiso para la transferencia de personal cuando sea necesario.
6. Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.
7. Existencia de Derechos de Propiedad Intelectual.
8. Definiciones relacionadas con la protección de datos.
9. Acuerdos de control de accesos que contemplen:

a) Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.

b) Proceso de autorización de accesos y privilegios de usuarios.

c) Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

10. Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.

11. Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.

12. Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.

13. Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.

14. Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.

15. Proceso claro y detallado de administración de cambios.

16. Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.

17. Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.

18. Controles que garanticen la protección contra software malicioso.

19. Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

20. Relación entre proveedores y subcontratistas.

3. Comunicación de la Política de Seguridad de la Información.

La presente Política de Seguridad de la Información será difundida mediante inducciones físicas o virtuales a todos los servidores de la SGDPN, también será incluida en la intranet institucional y a través del correo electrónico institucional.

4. Documentos de referencia

A continuación, se detallan todos los documentos que respaldan la elaboración del presente documento de Política de Seguridad de la Información.

- Constitución de la República del Ecuador
- Código Orgánico Administrativo
- Ley Orgánica de Telecomunicaciones
- Acuerdo Ministerial 025-2019
- Esquema Gubernamental de Seguridad de la Información (EGSI v2.0)
- Alcance del Esquema Gubernamental de Seguridad de la Información
- Decreto Ejecutivo Nro. 29 de 24 de mayo de 2021

- Decreto Ejecutivo Nro. 186, de 07 de septiembre del 2021
- Resolución Nro. SGDPN-2021-008, de 18 de octubre de 2021
- Resolución Nro. SGDPN-2022-006, de 31 de enero de 2022

5. Terminología

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

Activos: cualquier objeto tangible o intangible que represente un valor para la Institución.

Activo de información: es todo aquello que la Institución considera importante o de alta validez para la misma ya que puede contener importante información.

Acuerdo de confidencialidad: es un documento en el que los integrantes de la Secretaría de Gestión y Desarrollo de Pueblos y Nacionalidades o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la institución, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la institución.

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

Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Contraseña: es una cadena de caracteres que se puede usar para iniciar sesión en un equipo y obtener acceso a archivos, programas y otros recursos.

Controles: el medio por el cual se gestiona el riesgo al proporcionar garantías mediante procedimientos, directrices, o gestión.

Desastre: es un hecho natural o provocado por el ser humano que conlleva daño, pérdida o destrucción.

Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Evaluación de riesgos: es el proceso global de la identificación y determinación de las vulnerabilidades a las que están expuestos los activos de información.

Incidente de seguridad de la información: es un único evento o una serie de eventos de seguridades de la información, inesperadas o no deseadas, que tienen una propiedad significativa de comprometer las operaciones institucionales y de amenazar la seguridad de la información.

Información: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Información sensible: es el nombre que recibe la información personal privada de un individuo, por ejemplo ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos. Aunque lo más común es usar este término para designar datos privados relacionados con internet o la informática, sobre todo contraseñas, tanto de correo electrónico, conexión a Internet, IP privada, sesiones del PC, etc.

Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la SGDPN.

Medios electrónicos: Cualquier tecnología que permita la transmisión, generación, almacenamiento, envío, resguardo, transformación, modificación, comunicación pública o privada sin limitar tecnologías actuales o futuras.

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

Riesgo: se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Los factores que lo componen son la amenaza y la vulnerabilidad.

Seguridad de la Información: la seguridad de la información se entiende como la preservación de las siguientes características: confidencialidad, integridad, disponibilidad, autenticidad y auditabilidad.

Sistema de Información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Usuario: son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.

Terceros: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que proveas servicios o productos a la entidad.

Vulneración de la Seguridad de la Información: una violación de la seguridad de los datos se produce cuando los datos de los que ustedes son responsables sufren un incidente de seguridad que da lugar a la violación de la confidencialidad, disponibilidad o integridad de los datos.

6. Sanciones disciplinarias

Cualquier violación de la presente Política de Seguridad de la Información puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con el proceso interno de la Secretaría de Gestión y Desarrollo de Pueblos y nacionalidades. Es responsabilidad de todos los servidores, trabajadores, funcionarios, practicantes o cualquier persona que tenga relación con la institución tanto a nivel central y desconcentrado notificar al Oficial de Seguridad de la Información cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.