Acuerdo Ministerial No. 197

Señora. Lourdes Berenice Cordero
MINISTRA DE INCLUSIÓN ECONÓMICA Y SOCIAL

CONSIDERANDO:

Que, la Constitución de la República del Ecuador en su artículo 18, numerales 1 y 2, prescribe: *"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, la Norma Fundamental en el artículo 154 numeral 1, determina que les corresponde *"A las Ministras y Ministros de Estado, además de las atribuciones establecidas en la ley: Ejercer la rectoría de las políticas públicas del área a su cargo y expedir los acuerdos y resoluciones administrativas que requiera su gestión";*

Que, el artículo 226 de la Carta Magna, dispone 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";*

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

Que, la Ley Orgánica de Transparencia y Acceso a la Información Pública, en el artículo 1 señala: *"Principio de Publicidad de la Información Pública. - El acceso a la información pública es un derecho de las personas que garantiza el Estado.*

Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema materia de la información tengan participación del Estado o sean concesionarios de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no

gubernamentales (ONGs), están sometidas al principio de publicidad, por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley";

Que, la Ley Orgánica de Transparencia y Acceso a la Información Pública, en el artículo 5 establece: ***"Información Pública.*** *- 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";*

Que, el Esquema Gubernamental de Seguridad de la Información EGSI, en su artículo 6 manifiesta que: *"Es responsabilidad de la máxima autoridad de cada entidad mantener la documentación de la implementación del EGSI debidamente organizada y registrada de acuerdo al procedimiento específico que para estos efectos establezca la Secretaría Nacional de la Administración Pública";*

Que, el numeral 1. **POLITICA DE SEGURIDAD DE LA INFORMACION** del mencionado cuerpo normativo en el subnumeral 1.1. Documento de la Política de la Seguridad de la Información, señala:

"a) La máxima autoridad de la institución dispondrá la implementación de este Esquema Gubernamental de Seguridad de la Información (EGSI) en su entidad (*) (1).
b) Se difundirá la siguiente política de seguridad de la información como referencia (*):

"Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental 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".

(1) (*) En todo este documento esta marca significa que se trata de un control/directriz prioritario.

Las entidades públicas podrán especificar una política de seguridad más amplia o específica en armonía con la Constitución, leyes y demás normativa legal propia o relacionada, así como su misión y competencias";

Que, el Esquema Gubernamental de Seguridad de la Información EGSI, en el literal a, subnumeral 1.2. **Revisión de la Política,** dispone:

"a) Para garantizar la vigencia de la política de seguridad de la información en la institución, esta deberá ser revisada anualmente o cuando se produzcan cambios significativos a nivel operativo, legal, tecnológico, económico, entre otros."

Que, el Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Inclusión Económica y Social, expedido mediante Acuerdo Ministerial Nro. 000080, de 9 de abril de 2015, publicado en el Registro Oficial Edición Especial 329, de 19 de junio de 2015, en su artículo 5 establece como misión: *"Definir y ejecutar políticas, estrategias, planes, programas, proyectos y servicios de calidad y con calidez, para la inclusión económica y social, con énfasis en los grupos de atención prioritaria y la población que se encuentra en situación de pobreza y*

vulnerabilidad, promoviendo el desarrollo y cuidado durante el ciclo de vida, la movilidad social ascendente y fortaleciendo a la economía popular y solidaria";

Que, el artículo 9 del referido Estatuto, indica que entre las atribuciones del Ministerio de Inclusión Económica y Social se encuentra:

"1. Ejercer la rectoría de las Políticas Públicas en materia de protección, inclusión y movilidad social y económica para: primera infancia, juventud, adultos mayores, protección especial, al ciclo de vida, personas con discapacidad, aseguramiento no contributivo, actores de la economía popular y solidaria, con énfasis en aquella población que se encuentra en situación de pobreza y vulnerabilidad y los grupos de atención prioritaria";

Que, el numeral 3.1.3 GESTION DE PLANIFICACION Y GESTION ESTRATEGICA, del Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Inclusión Económica y Social, establece como misión: *"Planificar, coordinar, gestionar, controlar y evaluar los procesos de planificación y gestión estratégica institucional, de tal manera que promuevan y permitan incrementar la eficiencia y eficacia operativa, orientados hacia una atención de servicios de excelencia, para el cumplimiento de la misión institucional."*

Que, mediante Acuerdo Ministerial No. 166 de 19 de septiembre de 2013, publicado en el Registro Oficial Segundo Suplemento No 88 de fecha 25 de septiembre de 2013 la Secretaría Nacional de Administración Pública, dispuso a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de la Normas Técnicas Ecuatoriana NTE-INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información;

Que, mediante Acuerdo Ministerial No. 000066 de fecha 21 de enero de 2015, se conforma el comité de Gestión de Seguridad de la Información (CSI) y se emite la política de seguridad de la información del Ministerio de Inclusión Económica y Social (MIES) de acuerdo con el Esquema Gubernamental de Seguridad de la Información (EGSI);

Que, mediante Acuerdo Ministerial No. 000141, de fecha 02 de marzo de 2016, se reforma el Acuerdo Ministerial 000066 correspondiente a la Conformación del Comité de Gestión de la Seguridad de la Información (CSI) y Emisión de la Política de Seguridad de la Información del MIES de acuerdo con el EGSI;

Que, con el Acuerdo Ministerial No. 0001606, publicado en el Registro Oficial No. 775 de fecha 15 de junio de 2016, la Secretaría Nacional de la Administración Pública (SNAP), establece la supresión del artículo 3 del Acuerdo Ministerial No. 166 y la sustitución de las palabras "Comité de Seguridad de la Información-CSI" por la frase "Coordinación General de Planificación y Gestión Estratégica";

Que, mediante memorando No. MIES-CGPGE- 2019- 0387-M de fecha 17 de abril de 2019, la Coordinadora General de Planificación y Gestión Estratégica, remitió a la Coordinación General de Asesoría Jurídica, el Informe Técnico de Viabilidad y la documentación de respaldo para la *"Emisión de la Política de Seguridad de la Información del Ministerio de Inclusión Económica y Social";*

Que, la Administración Pública de forma integral y coordinada debe propender a minimizar o anular riesgos en la información, así como proteger la infraestructura gubernamental, más aún si es estratégica, de los denominados ataques informáticos o cibernéticos;

Que, las Tecnologías de la Información y Comunicación son herramientas imprescindibles para el cumplimiento de la gestión institucional e interinstitucional de la Administración Pública en tal virtud, deben cumplir con estándares de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información;

Que, es importante acoptar políticas, estrategias, normas, procesos, procedimientos, tecnologías y medios necesarios para mantener la seguridad en la información que se genera y custodia en diferentes medios y formatos de las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.

En uso de las atribuciones conferidas en el artículo 154 numeral 1 de la Constitución de la República del Ecuador y el artículo 17 del Estatuto de Régimen Jurídico Administrativo de la Función Ejecutiva.

ACUERDA:

EXPEDIR LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL ACORDE AL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI) Y SUS ANEXOS.

CAPÍTULO I

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL

ARTÍCULO 1.- OBJETO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MIES.-Son normas, directrices prioritarias para la Gestión de seguridad de la información cuyo objeto es proteger y salvaguardar la información generada por la unidades administrativas del Ministerio de Inclusión Económica y Social (MIES) y los recursos tecnológicos utilizados para su creación, procesamiento y administración, frente a amenazas internas o externas, intencionales o no, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información; implementando mecanismos que garanticen su autenticidad, que sea auditable, que no pueda ser duplicada para fines ajenos a los institucionales y que sus accesos no puedan ser repudiados.

ARTÍCULO 2.- ALCANCE DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MIES. - Todos los servidores/as, funcionarios/as del Ministerio de Inclusión Económica y Social, deben conocer y cumplir sea cual fuere su nivel jerárquico la Política de Seguridad de la Información. Por tanto, su aplicación es obligatoria, inclusive para proveedores externos vinculados a la institución a través de contratos, convenios o acuerdos; y, con apego a la definición de roles y perfiles relacionados con el Esquema Gubernamental de Seguridad de la Información (EGSI).

ARTÍCULO 3.- CONCEPTOS Y DEFINICIONES. - Para efectos del cumplimiento de la Política de Seguridad de la Información, se entenderá por:

a) **ACUERDO DE CONFIDENCIALIDAD:** Es un documento en el que, los funcionarios del MIES 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.

b) **ANÁLISIS DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN:** Es un proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

c) **ADMINISTRACIÓN DE RIESGOS:** Comprende el proceso de control y minimización, o la completa eliminación, de los riesgos de seguridad que podrían afectar a la información de la institución.

d) **EVALUACIÓN DE RIESGOS:** Comprende las acciones realizadas para identificar y analizar las amenazas y/o vulnerabilidades relativas a la información y a los medios de procesamiento de la misma, así como la probabilidad de ocurrencia y el potencial impacto a las operaciones de la institución.

e) **INCIDENTE DE SEGURIDAD INFORMÁTICA:** Es un intento de acceso, uso, divulgación, modificación o destrucción no autorizados de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política de Seguridad de la Información del Ministerio de Inclusión Económica y Social.

f) **INCIDENTE DE SEGURIDAD:** Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

g) **INFORMACIÓN:** Se refiere a toda representación de conocimiento en forma de datos vinculados entre sí. Pudiendo ser textual, numérica, gráfica, cartográfica, narrativa o audiovisual; almacenada en cualquier medio, ya sea magnético, en papel, en medios electrónicos computadoras, audiovisual y otros.

h) **PROPIETARIOS DE LA INFORMACIÓN:** Son las unidades que producen o generan la información, quienes clasifican la información de acuerdo con el grado de sensibilidad y criticidad de la misma.

i) **SISTEMA DE INFORMACIÓN:** Se refiere a un conjunto de recursos organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información, que cumplen con determinadas características propias de la institución, así como con procedimientos que pueden ser automatizados o manuales.

j) **TECNOLOGÍAS DE LA INFORMACIÓN:** Se refiere a equipos de cómputo, aplicativos con desarrollo propio o adquiridos, medios de almacenamiento y comunicaciones, que en conjunto son operados por el Ministerio de Inclusión Económica y Social, o por un tercero, con el objetivo de procesar, almacenar y/o transmitir información para llevar a cabo una función propia de la institución.

k) **SEGURIDAD DE LA INFORMACIÓN:** Para preservar la información, se debe considerar que las características mencionadas a continuación se cumplan:

i. Confidencialidad: La información es accesible únicamente a quien esté autorizado.

ii. Integridad: Salvaguarda la exactitud y la totalidad de la información y los métodos para su creación, recuperación y procesamiento.

iii. Disponibilidad: Los usuarios autorizados tienen acceso a la información y a los recursos relacionados, toda vez que lo requieran.

iv. Autenticidad: Asegura la validez de la información en tiempo, forma y distribución. Así mismo, garantiza el origen de la información al validar el emisor de ésta, para evitar suplantación de identidades.

v. Auditabilidad: Asegura que todos los eventos de un sistema deben quedar registrados, permitiendo su control posterior, ya sea en forma automática o manual.

vi. Protección a la duplicación: Asegura que una transacción sea realizada por única vez, a menos que se especifique lo contrario.

vii. No repudio: Evitar que una entidad que haya interactuado con alguna información alegue ante terceros que no lo ha hecho.

viii. Legalidad: Garantizar el cumplimiento de las leyes, normas, reglamentos o disposiciones.

ix. Confiabilidad: La información debe ser adecuada para sustentar la toma de decisiones y la ejecución de las actividades propias de la Institución.

l) **SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN:** Es un conjunto de políticas de administración de la información, que requiere del diseño, implementación y mantenimiento de un conjunto de procesos y procedimientos que permitan la gestión eficiente de la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de ésta, minimizando los riesgos. Un Sistema de Gestión de Seguridad de la información debe ser eficiente a través del tiempo, adaptándose a los cambios de la institución, así como a los de su entorno.

m) **TERCEROS:** Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

n) **VULNERABILIDADES:** Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la institución (amenazas), las cuales se constituyen en fuentes de riesgo.

ARTÍCULO 4.- POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. - A efectos de salvaguardar la información que se genera en los medios tecnológicos institucionales, esta Cartera de Estado ha diseñado las siguientes políticas de seguridad de información:

a) **Política de uso del correo electrónico institucional en el Ministerio de Inclusión Económica y Social:** Define y reglamenta la administración y uso responsable del Correo Electrónico Institucional, para ello todo servidor/a, funcionario/a debe cumplir de manera estricta lo determinado en esta Política, respetando la estructura de envío interno de correo electrónico. (Anexo 1).

b) **Política de Seguridad de la Información:** Regula la gestión de la seguridad de la información al interior de la entidad, logrando niveles adecuados de integridad, confidencialidad y disponibilidad de toda la información institucional; para este efecto, todos/as los servidores/as, funcionarios de esta Cartera de Estado deben aplicar y cumplir lo establecido en esta política. (Anexo 2).

c) **Política de Control de Accesos a Servicios Tecnológicos:** Establece normas generales para el control de acceso a los servicios informáticos, tiene por objeto mejorar la seguridad de la información en la Institución, considerando el tipo de usuario, cargo y funciones asignadas como servidor o funcionario público acorde al régimen laboral en que se encuentre. (Anexo 3)

d) **Política de Pantallas y Escritorios Limpios**: Establece que la información generada o almacenada en la institución en diferentes medios es de propiedad del MIES y debe ser utilizada exclusivamente para las tareas propias de las funciones que desarrollan en la institución; el cumplimiento de esta política es responsabilidad de cada usuario. (Anexo 4).

e) **Política de Resguardo y Recuperación de la Información de los Sistemas que Administra el MIES**: Establece los lineamientos de respaldo para proteger la información, configuraciones y aplicaciones de software en caso de presentarse alguna contingencia y posibilitar la recuperación de la información en el menor tiempo posible garantizando la confidencialidad, integridad y disponibilidad de los datos en el Ministerio de Inclusión y Social. (Anexo 5).

f) **Política de uso de Dispositivos Propios (BYOD)**: Establece que el uso de dispositivos propios está únicamente contemplado para el nivel Jerárquico Superior que preste servicios a la Institución. Los datos que se procesan o transfieren en los dispositivos propios, siguen perteneciendo a la Institución. La autorización del uso de estos debe ser otorgada por el jerárquico superior inmediato; esta política, es de estricto cumplimiento para todos los funcionarios/as del MIES (Anexo 6).

El Ministerio de Inclusión Económica y Social MIES, podrá crear otras políticas vinculadas al cumplimento del EGSI acorde a las necesidades institucionales, las mismas que será de estricto cumplimiento de los/as servidores/as públicos y funcionarios de esta Cartera de Estado.

ARTÍCULO 5.-LINEAMIENTOS GENERALES DE LAS POLÍTICAS.- La Seguridad de la información, es un factor clave para el correcto desarrollo institucional, en este sentido, el Ministerio de Inclusión Económica y Social (MIES), ha establecido los lineamientos generales para la aplicación de las Políticas de Seguridad de la Información, que es de cumplimiento obligatorio para los/las servidoras y funcionarios, proveedores externos vinculados a la institución a través de contratos, convenios o acuerdos, y otras partes interesadas. Así mismo, se considera que la Gestión de la Seguridad de la información, es uno de los pilares en los que se fundamenta las actividades de la institución, por ello, es política del MIES:

- Cumplir con todas las leyes, reglamentos, disposiciones y mandatos, así como las obligaciones contractuales.
- Realizar actividades de formación y concienciación en materia de los procesos de Seguridad de la información para todas las servidoras y servidores públicos que presta sus servicios en el Ministerio.
- Determinar que la información generada o almacenada en diferentes medios, es de propiedad del MIES y debe ser utilizada exclusivamente para las tareas propias de la función desarrollada en la institución.
- En el MIES, la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.
- Establecer que para el manejo de la información institucional debe tener relación laboral con la institución, o contar con la autorización escrita del funcionario del nivel jerárquico superior competente.
- 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 desconcentrado.
- Monitorear cambios significativos de los riesgos que afecten a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Designar a los custodios y responsables de la información de cada una de las unidades administrativas donde se genera la misma.

- Velar por la aplicación de la normativa relacionada a las normas técnicas ecuatorianas INEN ISO/IEC 27000 conforme al ámbito de cada institución.
- Se establezca los objetivos de control correspondientes para mitigar los riesgos detectados.
- Establecer la responsabilidad, y sanciones a los servidores o funcionarios 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.

El Oficial de Seguridad de la Información (OSI) es el responsable directo del mantenimiento de esta política; los directores de las unidades administrativas podrán analizar y plantear reformas conforme las condiciones lo ameriten.

CAPITULO II

GESTIONES INTERNAS ACORDE AL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN, VINCULADO A LAS POLITICAS INTERNAS

ARTÍCULO 6.- GESTIÓN DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- **Ministra/o:** dispone la difusión e implementación del Esquema Gubernamental de Seguridad de la Información, así como las Políticas de Seguridad de la Información del MIES.
- **Coordinador/a General de Planificación y Gestión Estratégica:** Cumple funciones enfocadas a mantener la política y normas institucionales particulares en materia de seguridad de la información, gestionar la aprobación y puesta en vigencia por parte de la máxima autoridad de la institución, así como el cumplimiento por parte de los servidores/as, funcionarios/as de la institución, para ello será el responsable de:

  a) Monitorear cambios significativos de los riesgos que afectan a los recursos de información, frente a las amenazas más importantes.

  b) Tomar conocimiento en la investigación y monitoreo de los incidentes relativos a la seguridad.

  c) Aprobar las iniciativas para incrementar la seguridad de la información, de acuerdo con las competencias y responsabilidades asignadas a cada área.

d) Promover la difusión y apoyo a la seguridad de la información dentro de la institución.

e) Designar a los custodios o responsables de la información de las diferentes áreas de la entidad, que deberá ser formalizada en un documento físico o electrónico.

f) Gestionar la provisión permanente de recursos económicos, tecnológicos y humanos para la gestión de la seguridad de la información.

g) Designar formalmente al Director/a de Servicios, Procesos y Calidad como Oficial de Seguridad de la Información. El Oficial de Seguridad no pertenecerá al área de Tecnologías de la Información y reportará las novedades a la máxima autoridad de la institución.

h) Designar formalmente al Director/a de Seguridad, Interoperabilidad y Riesgos como responsable de seguridad del área de Tecnologías de la Información en articulación con el Coordinador General de Tecnologías de la Información y Comunicación de la institución.

- **Oficial de Seguridad de la Información:** Es el responsable de revisar y proponer a la máxima autoridad para su aprobación el texto de la Política de Seguridad de la Información, la estructuración, seguimiento y mejora del Sistema de Gestión de Seguridad de la institución.

  Es responsabilidad del Oficial de Seguridad de la Información, definir las estrategias de capacitación en coordinación con la unidad de Administración de Recursos Humanos en materia de seguridad de la información y coordinar las acciones, impulsando la implementación y cumplimiento de la presente política.

  El Oficial de Seguridad de la Información, controla la aplicación de la política de protección de datos y privacidad de la información personal e implementa medidas técnicas y organizacionales apropiadas para gestionar de manera responsable la información personal de acuerdo con la legislación vigente y a lo establecido en el Acuerdo No. 166 del Esquema Gubernamental de Seguridad de la Información – EGSI, de fecha 25 de septiembre del 2013, referente a los roles y responsabilidades que se define en el numeral 2.3.

- **Coordinadora/or General de Tecnologías de Información y Comunicación:** Se encarga de establecer mantener y dar a conocer las políticas y procedimientos de los servicios de tecnología, incluida esta política de seguridad de la información y todos sus capítulos; el uso de los servicios tecnológicos en toda la institución, de acuerdo a las mejores prácticas y lineamientos institucionales y normativa vigente.

Mantener la custodia de la información que reposa en los diferentes sistemas, bases de datos y aplicativos de la institución.

Informa de los eventos que están en contra de la seguridad de la información e infraestructura tecnológica de la Institución a la Coordinación General de Tecnologías de Información y Comunicación, a las diferentes direcciones de la institución, así como a los entes de control e investigación que tiene injerencia sobre la misma.

El Oficial de Seguridad, de manera conjunta con las unidades administrativas de la Coordinación General de Tecnologías de Información y Comunicación, implementa mecanismos de carácter organizacional y tecnológico para autorización al acceso, e intercambio de datos personales o ciudadanos en custodio de las entidades públicas. Prima el principio que los datos personales pertenecen a los ciudadanos y no a las instituciones, éstas custodian al amparo de la normativa legal vigente.

Proporciona medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la institución.

- **Directora/or de Administración de Recursos Humanos:** El Director de la unidad de Recursos Humanos cumplirá la función de notificar a todo el personal que se vincula a la institución acerca de las obligaciones respecto del cumplimiento de las Políticas de Seguridad de la Información y demás normativa interna, procedimientos y prácticas que se generan.

  De igual forma es responsable de socializar al personal, los cambios en las políticas de seguridad de la información que se presente y de la suscripción del Acuerdo de Confidencialidad al personal que se vincula a la institución.

  Directora/or de Asesoría Jurídica: Verifica el cumplimiento de la presente política en la gestión de todos los contratos, acuerdos u otros instrumentos que determinen derechos, obligaciones y responsabilidades de y para la institución, y con terceros. Asesora en materia legal a la máxima autoridad, al Oficial de Seguridad y a la institución en lo referente a Seguridad de la Información.

- **Coordinadora/or, Directora/or de Unidades Administrativas desconcentradas del Ministerio de Inclusión Económica y Social:** Son responsables de clasificar la información de acuerdo con el grado de sensibilidad y criticidad; de 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; otorga los permisos de acceso a la información de acuerdo con sus funciones y competencias.

ARTÍCULO 7.- REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN. - El Oficial de Seguridad de la Información y Responsable de Seguridad del Área de Tecnologías de la

información, ejecutan revisiones independientes de la gestión de seguridad en las áreas que manejan información confidencial de esta Cartera de Estado en intervalos planificados o cuando ocurran cambios. Identifican las oportunidades de mejora y la necesidad de cambios con enfoque de seguridad, incluyendo la política y los objetivos de control.

ARTÍCULO 8.- CONSIDERACIONES DE LA SEGURIDAD CUANDO SE TRATA CON CIUDADANOS O CLIENTES. -Previó a la entrega de información a ciudadanos o clientes de entidades gubernamentales, las unidades responsables de proveer la información solicitada deberán consideran los siguientes criterios:

- Tipo de información solicitada.
- Protección de activos de información.
- Protección de datos en base a la Constitución, Ley del Sistema Nacional de Registro de Datos Públicos, LOTAIP y demás Leyes nacionales aplicable a los planes, programas y proyectos del MIES, 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.
- 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 entidad.

ARTÍCULO 9.- GESTIÓN DE LOS ACTIVOS FIJOS. -El Ministerio de Inclusión Económica y Social a través de las unidades de la Coordinación Administrativa Financiera, son responsables de la coordinación y manejo de activos que tienen valor para la institución, en colaboración con otras unidades y serán responsables de:

- Inventariar activos primarios en formatos físicos y/o electrónicas conforme lo establece el Esquema de Seguridad de la Información y el Reglamento Administración y Control de Bienes del Sector Público.
- Inventariar los activos de Hardware, conforme lo establece el Esquema Gubernamental de la Información, donde consten equipos móviles, fijos, periféricos de salida, periféricos de entrada, dispositivos, sistemas entre otros vinculados a las acciones que ejecuta el MIES y que permitan dar continuidad al negocio.
- Inventariar los activos de Software, Redes y demás aplicativos informáticos del negocio.

- Los/as funcionarios/as y servidores/as públicos del MIES son responsables del manejo y uso de los activos de la institución que utiliza para sus actividades diarias.

- El uso aceptable de los activos de la institución se enmarca en la utilización adecuada de los mismos y el cumplimiento de las normativas y políticas establecidas por la institución.

ARTÍCULO 10.- GESTIÓN DE SEGURIDAD DE LOS RECURSOS HUMANOS. - El Ministerio de Inclusión Económica y Social, mediante sus unidades responsables ejecutan las siguientes acciones vinculadas al cumplimiento del Esquema Gubernamental de la Información EGSI.

La Unidad de Administración de Recursos Humanos, verifica la información entregada por los candidatos previos a su contratación y entrega de manera formal las funciones y responsabilidades de los servidores y funcionarios contratados. Los funcionarios, servidores, empleados, contratistas, usuarios y terceras personas deberán firmar un acuerdo de confidencialidad y de no divulgación, para acceder a la información confidencial.

La Dirección de Recursos Humanos, Dirección de Seguridad, Interoperabilidad y Riesgos, Oficial de Seguridad de la Información, deberán brindar una inducción a los nuevos funcionarios y servidores que se integran a esta Cartera de Estado, donde expliquen las funciones, responsabilidades respecto a la seguridad de la información, acceso a la información, uso de contraseñas con sistemas de información confidencial.

Las Subsecretarías, Coordinaciones y Direcciones, se encargan de explicar y definir las funciones y responsabilidades respecto a la seguridad de la información. Previa la terminación de un contrato laboral se debe realizar la transferencia de la documentación e información de la que fue responsable el servidor/a o funcionario/a al servidor/a que designe el jefe inmediato; para garantizar la continuidad de las operaciones importantes dentro de la institución.

ARTÍCULO 11.- GESTIÓN DE SEGURIDAD FÍSICA Y DEL ENTORNO -Esta Cartera de Estado mediante las unidades responsables, deberán encargarse de velar por el acceso y seguridad física de las áreas restringidas, así como de los equipos tecnológicos y personal; el acceso deberá ser controlado y restringido para el personal ajeno a estas áreas o usuarios externos, para lo cual se puede implementar normas, controles y/o registros de acceso.

Se debe definir un área de recepción, con personal y otros medios que permitan controlar el acceso físico, supervisión de la permanencia de los visitantes en las áreas restringidas, debiendo registrar la hora, fecha de ingreso y salida.

Deben establecerse directrices restrictivas en las áreas de procesamiento de información como: prohibición de ingerir alimentos, fumar, utilizar equipos de grabación, cámaras, equipos de video y audio, dispositivos móviles entre otros dispositivos que ponen en riesgo la conservación de la información, más aún si no se encuentran autorizados.

Establece un sistema de suministro de energía sin interrupción (UPS) o al menos permitir el cierre/apagado ordenado de los servicios y equipos que soportan las operaciones de los servicios informáticos de la institución.

Debe disponer de documentación, diseños/planes y distribución de conexiones de: datos alámbricos/inalámbricas (locales y remotas), voz, eléctricas polarizadas, etc.

ARTÍCULO 12.- GESTIÓN DE COMUNICACIONES Y OPERACIONES. -Establece las normas que regulan la Gestión de las Comunicaciones y Operaciones, con el propósito de proteger la información almacenada en los computadores dentro de la infraestructura tecnológica de la institución y minimizar los riesgos ante las amenazas que puedan surgir, para ello las unidades administrativas que conforman la Coordinación General de Tecnologías de la Información y Comunicación deben ejecutar lo siguiente:

- Documentar los contactos de soporte y analizar los reportes de servicio, reportes de incidentes elaborados por terceros.
- Monitorear los niveles de desempeño de los servicios; realizar proyecciones de necesidad institucional respecto de capacidad operativa y tecnológica para asegurar el desempeño de los servicios del MIES.
- Revisar y verificar los registros y pruebas de auditoría de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionadas con el servicio prestado.
- Emitir norma reglamentaria de uso de software autorizados por la institución, que para el efecto se encargará a la unidad responsable de seguridad de información.
- Debe instalar y actualizar de forma periódica software antivirus y contra código malicioso, además debe, implementar soluciones que proporcionen valor agregado a las conexiones y servicios de red como: firewalls, antivirus y demás mecanismos, se encarga a la unidad responsable del área tecnológica la ejecución de dichas tareas.
- El Oficial de Seguridad de la información, los responsables del Área de Tecnologías y el propietario de la información, deben determinar los procedimientos, etiquetado para el resguardo y contención de la información.
- La Coordinación General de Tecnologías de la Información a través de sus unidades administrativas es la responsable de documentar los incidentes y eventos incluyendo la hora, fecha, e información del evento, así como el registro y cuenta del administrador y operador que estuvo involucrado; además son corresponsables de la aplicación de políticas y normas para registrar los accesos, tipos de accesos, protocolos de red, sistemas de protección como antivirus y sistemas de detección de intrusos y demás instrumentos que permita el manejo adecuado del negocio.

- La Coordinación General de Tecnologías de la Información a través de sus unidades administrativas deben gestionar y normar las actividades vinculadas al numeral 6 del Esquema Gubernamental de Seguridad de la Información.

ARTÍCULO 13.- GESTIÓN DE CONTROL DE ACCESO. - El Ministerio de Inclusión Económica y Social, mediante las unidades administrativas de la Coordinación General de Tecnologías de Información y Comunicación deberá regular el proceso de administración y control de accesos lógicos a los sistemas de información, con el fin de mitigar los riesgos de accesos y uso indebido de los mismos; para ello, se aplicarán las siguientes medidas:

- Deberá contribuir en la socialización de la Política de Control de Accesos para usuarios a los sistemas de información acorde al nivel y tipo.
- Establecer normas y procesos formales para la asignación y cambio de contraseñas.
- Determinar, diseñar y especificar el manejo de usuarios/as contraseñas y características especiales para la creación y uso de contraseñas como: uso de letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, que cumplan una complejidad media y alta para evitar contraseñas en blanco.
- Controlar el cambio periódico de contraseñas e implementar medidas en el caso de que el usuario no está realizando ningún trabajo, el equipo se bloquee y lo desbloquee únicamente si el usuario ingresa nuevamente su clave.
- Definir mecanismos para asegurar que la información transmitida por los canales de conexión remota, sean usando técnicas como encriptación de datos, redes virtuales privadas y otros que asegure la información.
- Eliminar o deshabilitar los puertos, servicios que no requiera la institución.
- Establecer un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros de alarmas cuando se violan las políticas de seguridad del sistema.
- Identificar y documentar los equipos que se encuentran en las redes, así como realizar una evaluación de riesgos para identificar los segmentos de red donde se encuentra los activos críticos para la institución.

ARTÍCULO 14.- GESTIÓN DE ADQUISICIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN. Las unidades administrativas de la Coordinación General de Tecnologías de la Información y Comunicación son responsables de establecer normas de seguridad y controles durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan, por ello se realizará lo siguiente:

- La Coordinación General de Tecnologías de la Información mediante sus unidades administrativas implementa de manera conjunta con el Oficial de Seguridad de la Información, la política de controles y gestión de claves, así como su generación.

- Emite y socializa la Política sobre el uso de controles criptográficos acorde a los requerimientos de seguridad de la información y el tipo de información.

- Establece normas de controles de cifrado (criptográficos) que se adoptan, para la implementación eficaz en toda la institución; establece la solución a usar para cada proceso del negocio.

- Evalúa los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas por falla o falta de seguridad.

CAPITULO III

ROLES Y RESPONSABILIDADES

La Política de Seguridad de la información es de aplicación obligatoria para todo el personal de la institución y nivel central y desconcentrado. Las autoridades institucionales aprueban esta política y son responsables de la autorización para sus modificaciones.

ARTÍCULO 15.- Designación del Oficial de Seguridad de la Información. -El/la director/a de Servicios Procesos y Calidad, es designado como Oficial de Seguridad de la información (OSI) del Ministerio de Inclusión Económica y Social.

ARTÍCULO 16.- Responsable de Seguridad del Área de Tecnologías de la Información. - Es el /la Director/a de Seguridad Interoperabilidad y Riesgos, velará por la Seguridad del Área de Tecnologías en el ámbito de sus competencias, conjuntamente con los directores de las unidades que conforman la Coordinación General de Tecnologías de la Información.

ARTÍCULO 17.- El Oficial de Seguridad de la Información (OSI). -Tiene las siguientes responsabilidades: Define procedimientos para el control de cambios a los procesos operativos, los sistemas e instalaciones y verifica su cumplimiento, de manera que no afecte la seguridad de la información.

- Establece criterios de seguridad para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas antes de su aprobación definitiva.

- Define procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.

- Controla los mecanismos de distribución y difusión de información dentro y fuera de la institución.

- Implementar los mecanismos de controles necesarios y pertinentes para verificar el cumplimiento de la presente política.

ARTÍCULO 20.- RESPONSABILIDADES DE LOS PROPIETARIOS DE LA INFORMACIÓN. – Los servidores/as y funcionarios/as públicos de esta Cartera de Estado, que manejan, generan, procesan, reciben y almacenan en cualquier medio la información institucional, son responsables de:

- Velar, valorar y clasificar la información que está bajo su administración y/o generación, siguiendo los lineamientos establecidos por la Constitución de la República del Ecuador, Ley Orgánica de Transparencia y Acceso a la Información Pública, y el Esquema de Seguridad de la Información.

- Autorizar, restringir y delimitar a los demás usuarios de la institución el acceso a la información de acuerdo a sus roles y responsabilidades y a los diferentes funcionarios, contratistas o practicantes que por sus actividades requieran consultar, crear o modificar parte o la totalidad de la información, así como la solicitud y aceptación de acuerdos de confidencialidad establecidos en el documento denominado Instructivo para la Clasificación y Entrega de Información Pública Confidencial del Ministerio de Inclusión Económica y Social.

- Determinar los tiempos de retención de la información juntamente con las áreas que se encarguen de su protección y almacenamiento de acuerdo con las normas vigentes y a las políticas de la entidad.

- Determinar y evaluar de forma periódica los riesgos asociados a la información, así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de la misma.

- Acoger e informar sobre las políticas de seguridad de la información a todos los funcionarios, contratistas y practicantes en las diferentes dependencias de la institución, sobre su aplicación obligatoria.

ARTÍCULO 21- RESPONSABILIDADES DE FUNCIONARIOS/AS, CONTRATISTAS, PRACTICANTES Y USUARIOS DE LA INFORMACIÓN. -En el manejo y uso de la información, los servidores/as, funcionarios/as, contratistas y/o terceras personas que generan o acceden a la información del MIES, tienen las siguientes responsabilidades:

- Manejar la información de la institución y rendir cuentas por el uso y protección de la misma, mientras esté bajo su conocimiento y custodia, la que puede ser física o electrónica o almacenada en cualquier medio.

- Proteger la información a la cual accedan o procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

- No divulgar la información que no esté autorizada su uso, por las autoridades competentes.

- Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma.

- Informar a sus superiores sobre la violación de estas políticas.

- Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición, de la destrucción o alteración y de la divulgación no autorizada.

- Reportar a la autoridad competente, los incidentes de seguridad, eventos sospechosos y mal uso de los recursos que identifique.

- 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 al MIES, 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 Dirección competente de la Coordinación General de Tecnologías de Información y Comunicación.

- Utilizar software autorizado adquirido legalmente por la institución; no está permitido la instalación ni uso de software diferente al institucional sin el consentimiento de sus superiores y visto bueno de la Dirección competente de la Coordinación General de Tecnologías de Información y Comunicación.

- Aceptar y reconocer que en cualquier momento y sin previo aviso, la Dirección de Seguridad, Interoperabilidad y Riesgos de la Coordinación General de Tecnologías de Información y Comunicación 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 MIES, 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 actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales.

- Proteger y resguardar su información personal que no esté relacionada con sus funciones en la institución.

- La institución no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito al utilizar la infraestructura tecnológica facilitada por la institución.

- Define y documenta 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.
- Desarrolla procedimientos adecuados de concienciación de usuarios en materia de seguridad, controles de acceso a los sistemas.
- Verifica el cumplimiento de las políticas, normas, procedimientos y controles de seguridad institucional establecidos y vinculados al EGSI.
- Coordina la gestión de eventos de seguridad con otras entidades gubernamentales.

ARTÍCULO 18.- RESPONSABLE DE SEGURIDAD DEL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN. - Acorde al numeral 2.3 del EGSI, el/la Responsable de Seguridad del Área de Tecnologías de la Información posee los compromisos siguientes:

- Controla la existencia de documentación física y/o electrónica actualizada relacionada con los procedimientos de comunicaciones, operaciones y sistemas.
- Evalúa el posible impacto operativo a nivel de seguridad de los cambios previstos a sistemas y equipamiento y verifica su correcta implementación.
- Administra los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
- Monitorea las necesidades de capacidad de los sistemas en operación y proyecta futuras demandas de capacidad para soportar potenciales amenazas de seguridad a la información.
- Controla la obtención de copias de resguardo de información; así como la prueba periódica de su restauración.
- Asegura el registro de las actividades realizadas por el personal operativo de seguridad de la información, para su posterior revisión.
- Desarrolla y verifica el cumplimiento de procedimientos para comunicar fallas en el procesamiento de la información o los sistemas de comunicaciones que permita tomar medidas correctivas.
- Implementa y Verifica los controles de seguridad definidos.
- Define e implementa procedimientos para la administración de medios informáticos de almacenamiento e informes impresos y verificar la eliminación o destrucción segura de los mismos.
- Gestiona los incidentes de seguridad de la información de acuerdo con los procedimientos.

- Otras vinculadas a su naturaleza en la gestión de seguridad de la información.

ARTÍCULO 19.- RESPONSABILIDADES DE LAS DIRECCIONES DE LA COORDINACIÓN GENERAL DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN. -Las Direcciones de las Unidades Administrativas de la Coordinación General de Tecnologías de la Información y Comunicación cumplen con las siguientes responsabilidades:

- Las Direcciones de la Coordinación General de Tecnologías de la Información y Comunicación participan en el establecimiento, mantenimiento y divulgación de las políticas y procedimientos de servicios de tecnología, incluida esta política de seguridad de la información y todos sus capítulos, el uso de los servicios tecnológicos en toda la Institución de acuerdo con las mejores prácticas y lineamientos institucionales y normativa vigente a nivel del Gobierno
- Mantener la custodia de la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la Institución.
- Informar los eventos que esté en contra de la seguridad de la información y de la infraestructura tecnológica de la Institución a la Coordinación General de Tecnologías de la Información y Comunicación, a las diferentes Direcciones de la Institución, así como a los entes de control e investigación que tienen injerencia sobre la misma.
- Proporcionar las medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la Institución.
- Garantizar las condiciones tecnológicas óptimas para la implementación de las políticas de seguridad de información institucional.
- Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio del MIES.
- Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los datos e información gestionados en la institución.
- Resolver de común acuerdo con las áreas y los propietarios de la información los conflictos que se presenten por la propiedad de la información al interior de la Institución, esto incluye los posibles medios de acceso a la información, los datos derivados del procesamiento de la información a través de cualquier aplicación o sistema, los datos de entrada a las aplicaciones y los datos que son parte integral del apoyo de la solicitud.
- Habilitar/Deshabilitar el reconocimiento y operación de dispositivos de almacenamiento externo de acuerdo con las directrices emitidas de parte de la Coordinación General de Tecnologías de la Información y Comunicación y diferentes direcciones.

CAPITULO IV

ADMINISTRACIÓN DE RIESGOS

ARTÍCULO 22.- GESTIÓN DE INCIDENTES INFORMÁTICOS. -El Ministerio de Inclusión Económica y Social, ha establecido los lineamientos generales para la gestión efectiva de incidentes de seguridad que afecten a la institución y al cumplimiento de su misión y objetivos, con la finalidad de prevenir y responder de forma idónea, para lo cual, la Coordinación General de Tecnologías de la Información y Comunicaciones mediante sus unidades administrativas realiza las siguientes acciones:

- Implementar y ejecutar el procedimiento formal para el reporte de eventos de seguridad informáticos junto al procedimiento de escalada y respuesta al incidente que amenace la seguridad informática. Este procedimiento inicia mediante la mesa de servicios.
- Mantener una bitácora de registro de incidentes y el reporte de vulnerabilidades de la seguridad de la información, el monitoreo de los sistemas, alertas y las vulnerabilidades, se establece y ejecuta un procedimiento para la gestión de incidentes.
- Identificar y clasificar los diferentes tipos de incidentes de seguridad de la información mediante la mesa de servicios y con la utilización de la matriz de asignación de responsabilidades-matriz RACI.
- Identifica y analiza las posibles causas de un incidente producido.
- Planificar e implementar acciones correctivas para evitar la recurrencia del incidente.
- El funcionario/a de turno responsable del equipo o sistema afectado debe identificar, registrar el incidente en la bitácora incluyendo datos, fecha y hora, así como el tipo de incidente suscitado y el nivel de severidad del mismo.
- En caso de que el funcionario/a de turno no pueda solucionarlo, el escalamiento debe ser registrado en la bitácora de escalamiento de incidentes, se notificará al jefe inmediato.
- Establecer procesos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la institución.

ARTÍCULO 23.- GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN. - En caso de que los incidentes informáticos que produzcan afectación en la Seguridad de la Información de esta Cartera de Estado, el Oficial de Seguridad de la Información es el contacto para el reporte de los eventos de seguridad de la información. Los servidores/as, funcionarios/as, contratistas y usuarios contratados por los proveedores deben reportar todos los eventos de inseguridad de la información lo más pronto posible.

Los servidores/as, funcionarios/as, contratistas y usuarios contratados por los proveedores del MIES, deben informar los asuntos de las debilidades en la seguridad al Director/ra o al su proveedor del servicio tan pronto como sea posible. Cuando se detecte alguna vulnerabilidad o debilidad en un equipo o sistema se debe:

- Informar y notificar a su jefe inmediato y este al Oficial de Seguridad de la información la debilidad o vulnerabilidad encontrada.

- El Oficial de Seguridad de la información debe llevar el reporte de vulnerabilidades y debilidades de seguridad de la información, que contendrá la fecha, hora, apellidos, nombres del funcionario/a que detectó la debilidad, descripción de la misma, detalle de posibles incidentes de seguridad que pudieran ocurrir como producto de la vulnerabilidad.

- El Oficial de Seguridad de la información debe emitir un reporte del o los incidentes ocurridos a los jefes de las unidades donde se produjo el incidente.

- El Oficial de Seguridad de la Información en coordinación con el Responsable de Tecnologías de la Información realizarán una evaluación del impacto generado por el o los incidentes de seguridad de la información producidos donde se evidencie el tipo de incidente, el número de incidentes graves, el tiempo medio de resolución de incidentes, costo promedio de incidentes, frecuencia del incidente

CAPITULO V

SANCIONES POR INCUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 24.- En caso de detectar incumplimiento de esta política, la/el Directora/r de la unidad administrativa pondrá en conocimiento del Oficial de Seguridad de la Información OSI la transgresión de la Política de Seguridad establecida en el presente instrumento y demás normativa relacionada, para ello el Oficial de Seguridad de la Información levantará un informe que será puesto en conocimiento de la Dirección de Administración de Talento Humano y a la máxima autoridad para las acciones pertinentes.

Cuando los responsables de las unidades administrativas de planta central y del nivel desconcentrado omitan notificar al Oficial de Seguridad de la información - OSI - sobre las transgresiones de la Política de Seguridad de la Información e instrumentos vinculantes, se pondrá en conocimiento de la máxima autoridad para los fines pertinentes.

Acuerdo Ministerial No.

Señora. Lourdes Berenice Cordero
MINISTRA DE INCLUSIÓN ECONÓMICA Y SOCIAL

CONSIDERANDO:

Que, la Constitución de la República del Ecuador en su artículo 18, numerales 1 y 2, prescribe: *"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, la Norma Fundamental en el artículo 154 numeral 1, determina que les corresponde *"A los Ministras y Ministros de Estado, además de las atribuciones establecidas en la ley: ejercer la rectoría de las políticas públicas del área a su cargo y expedir los acuerdos y resoluciones administrativas que requiera su gestión";*

Que, el artículo 226 de la Carta Magna, dispone 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";*

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

Que, la Ley Orgánica de Transparencia y Acceso a la Información Pública, en el artículo 1 señala: *"Principio de Publicidad de la Información Pública. - El acceso a la información pública es un derecho de las personas que garantiza el Estado.*

Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema materia de la información tengan participación del Estado o sean concesionarios de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no

gubernamentales (ONGs), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley";

Que, la Ley Orgánica de Transparencia y Acceso a la Información Pública, en el artículo 5 establece: ***"Información Pública.** - 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";*

Que, el Esquema Gubernamental de Seguridad de la Información EGSI, en su artículo 6 manifiesta que: *"Es responsabilidad de la máxima autoridad de cada entidad mantener la documentación de la implementación del EGSI debidamente organizada y registrada de acuerdo al procedimiento específico que para estos efectos establezca la Secretaría Nacional de la Administración Pública";*

Que, el numeral 1. **POLITICA DE SEGURIDAD DE LA INFORMACION** del mencionado cuerpo normativo en el subnumeral 1.1. Documento de la Política de la Seguridad de la Información, señala:

"a) La máxima autoridad de la institución dispondrá la implementación de este Esquema Gubernamental de Seguridad de la Información (EGSI) en su entidad (*) (1).
b) Se difundirá la siguiente política de seguridad de la información como referencia (*):

"Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental 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",

(1) (*) En todo este documento esta marca significa que se trata de un control/directriz prioritario.

Las entidades públicas podrán especificar una política de seguridad más amplia o específica en armonía con la Constitución, leyes y demás normativa legal propia o relacionada, así como su misión y competencias";

Que, el Esquema Gubernamental de Seguridad de la Información EGSI, en el literal a, subnumeral 1.2. **Revisión de la Política,** dispone.

"a) Para garantizar la vigencia de la política de seguridad de la información en la institución, esta deberá ser revisada anualmente o cuando se produzcan cambios significativos a nivel operativo, legal, tecnológico, económico, entre otros."

Que, el Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Inclusión Económica y Social, expedido mediante Acuerdo Ministerial Nro. 000080, de 9 de abril de 2015, publicado en el Registro Oficial Edición Especial 329, de 19 de junio de 2015, en su artículo 5 establece como misión: *"Definir y ejecutar políticas, estrategias, planes, programas, proyectos y servicios de calidad y con calidez, para la inclusión económica y social, con énfasis en los grupos de atención prioritaria y la población que se encuentra en situación de pobreza y*

DISPOSICIONES GENERALES

PRIMERA.- La Coordinación General de Planificación y Gestión Estratégica a través de la Dirección de Gestión del Cambio y Cultura Organizativa conjuntamente con la Dirección de Comunicación Social, serán responsables de elaborar estrategias de socialización y capacitación a todos los servidores y funcionarios del MIES, sobre el Esquema Gubernamental de la Información (EGSI) y de la Política de Seguridad de la Información del MIES y sus Anexos, en un plazo de 60 días a partir de la vigencia del presente Acuerdo Ministerial.

SEGUNDA - Las políticas elaboradas y emitidas por la Coordinación General de Tecnologías de la Información vinculadas al cumplimiento del Esquema de Seguridad de la Información (EGSI) validadas por el Oficial de Seguridad de la Información, serán de cumplimiento obligatorio para todos/as los y las servidores y funcionarios/as de esta Cartera de Estado.

DISPOSICIÓN DEROGATORIA

Deróguese íntegramente los Acuerdos Ministeriales No. 000066 de fecha 21 de enero de 2015 referente a la Conformación del Comité de Gestión de la Información y Emisión de la Política de Seguridad de la Información; y, el Acuerdo Ministerial ND. 000141 de fecha 02 de marzo de 2016 relativo a la Reforma al Acuerdo Ministerial No. 000066 correspondiente al Comité de Gestión de la Seguridad (CSI) y Emisión de la Política de Seguridad de la Información del Ministerio de Inclusión Económica y Social de Acuerdo al Esquema Gubernamental de Seguridad de la Información (EGSI).

DISPOSICIÓN FINAL

El presente Acuerdo Ministerial entrará en vigencia a partir de la suscripción, sin perjuicio de su publicación en el Registro Oficial.

Dado en la ciudad de San Francisco de Quito, Distrito Metropolitano, a 15 MAYO 2018

Sra. Lourdes Berenice Cordero Molina

MINISTRA DE INCLUSIÓN ECONÓMICA Y SOCIAL