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. 776 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 adoptar 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 electrónicos 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 ente 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/planos y distribución de conexiones de: datos alámbricos/inalámbricas (locales y remotos), 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 auditoria 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.

- 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.

- 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 INFORMACION. -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.

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.

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 N0. 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 2019

Sra. Lourdes Berenice Cordero Molina

MINISTRA DE INCLUSIÓN ECONÓMICA Y SOCIAL

MINISTERIO DE
INCLUSIÓN ECONÓMICA
Y SOCIAL

Toda una Vida

EL
GOBIERNO
DE TODOS

POLÍTICAS

USO DEL CORREO ELECTRÓNICO INSTITUCIONAL EN EL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL

ANEXO 1

Quito, Julio del 2018

DATOS GENERALES		
No. Doc.	MIES-CGTIC-DSIR-POL-2018-0001	
Tipo de documento	Políticas	
Institución	Ministerio de Inclusión Económica y Social	
Dirección Ejecutora	Coordinación General de Tecnologías de Información y Comunicación	
Fecha	24/07/2018	
Versión	2.1	
Elaborado por	**Cargo**	**Firma**
Ing. Katherine Colcha	Analista de Tecnologías de Información	
Revisado por	**Cargo**	**Firma**
Ing. Richarth Pazmiño MBA.	Director de Seguridad, Interoperabilidad y Riesgos	
Ing. Jorge Pichucho MGS.	Director de Infraestructura y Operaciones de TI	
Ing. Soledad Cueva	Director de Soporte a Usuarios de TI (E)	
Ing. Cristian Núñez	Director de Proyectos de TI (E)	
Validado por	**Cargo**	**Firma**
Lic. Rubén Ortega MGS.	Oficial de Seguridad de la Información	
Aprobado por	**Cargo**	**Firma**
Ing. Fabián Vallejo	Coordinador General de Tecnologías de Información y Comunicación	

CONTROL DE VERSIONES			
Fecha	**Versión**	**Responsable**	**Descripción**
11/03/2015	1.0	Ing. Katherine Colcha	Elaboración de las políticas.
13/04/2018	2.0	Ing. Katherine Colcha	Modificación de las políticas.
27/07/2018	2.1	Ing. Katherine Colcha	Modificación de las políticas.

Contenido

1. INTRODUCCIÓN 5
2. ANTECEDENTES 5
3. JUSTIFICACIÓN 5
4. OBJETIVO 6
5. ALCANCE 6
6. RESPONSABILIDADES 6
7. POLÍTICAS 7
   - 7.1. Estructura de las cuentas de correo electrónico institucional 7
   - 7.2. Estructura para el envío interno de correo electrónico 7
   - 7.3. Formato de correo electrónico institucional 8
   - 7.4. Pie de página 9
   - 7.5. Perfiles de Correo Electrónico Institucional 9
   - 7.6. Asignación de perfiles a los usuarios de la Institución 9
   - 7.7. Sitio de acceso para el correo electrónico institucional 10
   - 7.8. Creación de cuentas de correo electrónico institucional 10
   - 7.9. Aceptación de políticas de correo electrónico 10
   - 7.10. Disponibilidad del servicio de correo electrónico institucional 11
   - 7.11. Monitoreo de correos electrónicos institucionales 11
   - 7.12. Depuración de plataforma de correo electrónico 11
   - 7.13. Confiabilidad e integridad de los correos electrónicos 11
   - 7.14. Respuestas automáticas 12
   - 7.15. Reseteo de claves 12
   - 7.16. Responsabilidad de actividades realizadas en el correo electrónico institucional 12
   - 7.17. Envío de archivos adjuntos 13
   - 7.18. Permisos de envío de correo electrónico institucional masivo 13
   - 7.19. Seguridad del correo del usuario 14
   - 7.20. Restricciones 14
   - 7.21. Casos especiales 15
   - 7.22. Casos excepcionales de acceso al correo electrónico de un funcionario 15
   - 7.23. Eliminación de cuentas de correo electrónico 15
   - 7.24. Bloqueo de cuentas de correo electrónico 16
   - 7.25. Archivo y almacenamiento 16
   - 7.26. Respaldo de cuentas de correo electrónico 16
8. AMONESTACIONES 16
9. VALIDEZ Y GESTIÓN DE DOCUMENTOS 17

10. POLÍTICAS, PROCEDIMIENTOS Y MANUALES RELACIONADOS.....17
11. ADVERTENCIA.....17

1. INTRODUCCIÓN

El Correo Electrónico Institucional es proporcionado con el objeto de apoyar las funciones de comunicación entre los servidores y las servidoras públicas del Ministerio de Inclusión Económica y Social y agilizar la gestión de procesos de cada unidad administrativa. El acceso a estos recursos está condicionado a la aceptación de la Política de Uso.

Toda organización que utiliza el servicio de correo electrónico institucional debe tener políticas que regulen y controlen el uso de este.

Las políticas explican el uso apropiado del servicio de correo electrónico institucional y las medidas para preservar los recursos tecnológicos.

Cuando las políticas se ejecutan adecuadamente, pueden aumentar la productividad de los empleados y proteger la información en la red interna y la imagen institucional.

Los usuarios del servicio de correo electrónico son absolutamente responsables por el contenido al que accedan, los correos que envíen o distribuyan usando la red ministerial o fuera de ella. El uso del servicio de correo electrónico debe estar normado bajo términos legales, éticos y de requerimientos laborales.

2. ANTECEDENTES

La provisión del servicio de correo electrónico institucional administrada por parte de la Coordinación General de Tecnologías de Información y Comunicación, se encuentra alineada a las políticas de control, regulación y optimización de los recursos tecnológicos vigentes, lo cual permite la correcta administración de la plataforma y el buen uso de este servicio por parte de los servidores y las servidoras en cada una de sus cuentas.

Se ha tomado el Esquema Gubernamental de Seguridad de la Información como guía de referencia en temas de seguridad informática.

3. JUSTIFICACIÓN

El establecimiento de políticas es fundamental para alcanzar los objetivos institucionales.

Las políticas de correo electrónico proveen los lineamientos a las y los servidores públicos de la Institución de utilizar este recurso para disminuir riesgos de seguridad por manejo indebido, así como también controlar y precautelar el rendimiento de la red institucional para evitar su saturación y mantener la disponibilidad de los servicios.

El Esquema Gubernamental de Seguridad de la Información en el punto 3. GESTION DE LOS ACTIVOS, 3.2. Responsable de los activos, dispone:

d) Reglamentar el uso de correo electrónico institucional (*):

- Este servicio debe utilizarse exclusivamente para las tareas propias de las funciones que se desarrollan en la institución y no debe utilizarse para ningún otro fin.

- Cada persona es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte.
- Todos los mensajes deben poder ser monitoreados y conservados permanentemente por parte de la institución.
- Toda cuenta de correo electrónico debe estar asociada a una única cuenta de usuario.
- La conservación de los mensajes se efectuará en carpetas personales, para archivar la información de acceso exclusivo del usuario y que no debe compartirse con otros usuarios. Debe definirse un límite de espacio máximo.
- Toda la información debe ser gestionado de forma centralizados y no en las estaciones de trabajo de los usuarios.
- Todo sistema debe contar con las facilidades automáticas que notifiquen al usuario cuando un mensaje enviado por él no es recibido correctamente por el destinatario, describiendo detalladamente el motivo del error.
- Deben utilizarse programas que monitoreen el accionar de virus informáticos tanto en mensajes como en archivos adjuntos, antes de su ejecución.
- Todo usuario es responsable por la destrucción de los mensajes con origen desconocido, y asume la responsabilidad por las consecuencias que pueda ocasionar la ejecución de los archivos adjuntos. En estos casos, no deben contestar dichos mensajes y deben enviar una copia al Oficial de Seguridad de la Información para que efectúe el seguimiento y la investigación necesaria.
- Para el envío y la conservación de la información, debe implementarse el cifrado (criptografía) de datos.
- Todo usuario es responsable de la cantidad y tamaño de mensajes que envíe. Debe controlarse el envío no autorizado de correos masivos.

Es fundamental que estas políticas sean configuradas en la plataforma de correo electrónico institucional y aplicado por cada servidor y servidora de esta Institución logrando así una mejor gestión y control del servicio.

4. OBJETIVO

Definir y reglamentar las normas generales de administración y uso responsable del Correo Electrónico Institucional del Ministerio de Inclusión Económica y Social.

5. ALCANCE

Las políticas de correo electrónico institucional aplican a las y los servidores públicos, asesores y empleados en general, que pertenezcan o tengan cuenta de correo electrónico institucional en esta Cartera de Estado. En adelante, a todas las personas que cuenten con cuenta de correo electrónico institucional, se los denominará *"usuario"*.

6. RESPONSABILIDADES

El Ministerio de Inclusión Económica y Social proporcionará la plataforma de correo electrónico que será utilizada en toda la Institución.

Cada usuario tiene la responsabilidad de cumplir con esta política.

Las autoridades institucionales son responsables de controlar el cumplimiento de esta política por parte de los usuarios bajo su unidad.

7. POLÍTICAS

- A cada funcionario se le asigna una sola cuenta de correo electrónico institucional, la cual será creada bajo el estándar definido la Dirección de Soporte a Usuarios de TI
- Las cuentas de correo electrónico institucional son asignadas de manera personal e intransferible
- Todo usuario que trabaja en el MIES, debe utilizar solo el correo institucional asignado para el envío y recepción de documentación institucional
- Las cuentas de correo electrónico institucional asignadas a los usuarios son propiedad del Ministerio de Inclusión Económica y Social y son exclusivamente para las tareas propias de la función desarrollada en la Institución
- Toda cuenta de correo electrónico institucional debe estar asociada a una única cuenta de usuario
- Toda información que se almacene o pase a través del sistema de correo electrónico institucional es de propiedad de la Institución y debe cumplir con la normativa o reglamentación que para su efecto haya determinado la autoridad competente, tanto en el ámbito interno de la Institución, así como las requeridas por las entidades de regulación y/o control externas
- El sistema de correo debe permitir controlar el envío de correos masivos

7.1. Estructura de las cuentas de correo electrónico institucional

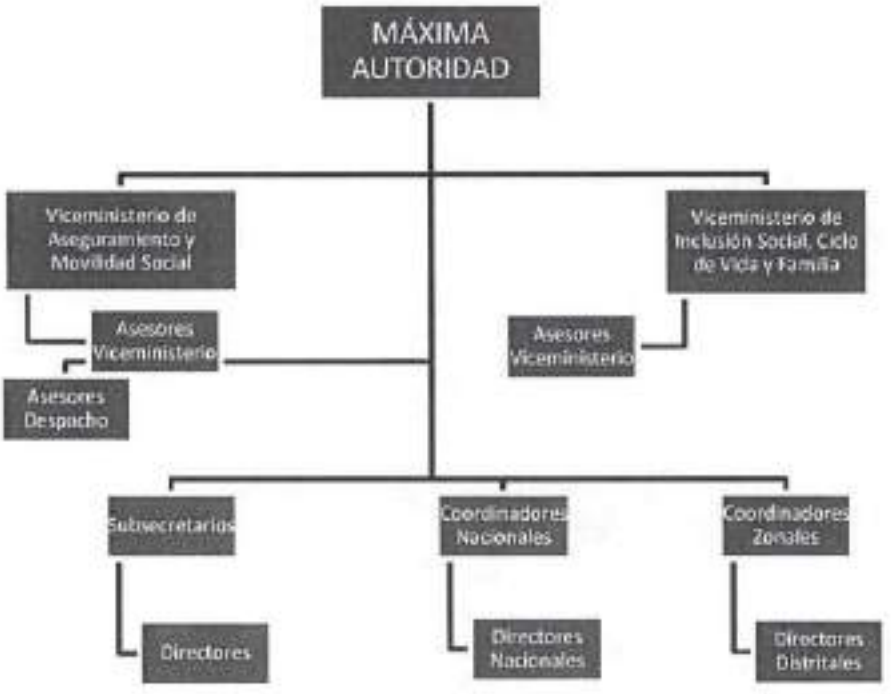
Las cuentas de correo electrónico de cada usuario están formadas por la siguiente estructura:

primernombre.primerapellido@inclusion.gob.ec

En caso de existir homónimos en los nombres, la nueva cuenta se creará con el segundo nombre del usuario solicitante o en su defecto se analizará la estructura de ese correo para la creación debido a que no pueden existir correos electrónicos repetidos.

7.2. Estructura para el envío interno de correo electrónico.

Las y los servidores públicos de esta Cartera de Estado deberán enviar correos electrónicos en el orden de jerarquía, de acuerdo a la estructura detallada a continuación:



7.3. Formato de correo electrónico institucional

Todo correo electrónico enviado desde la cuenta institucional deberá cumplir con un formato mínimo definido por la Dirección de Soporte a Usuarios de TI.

7.4. Pie de página

El emisor de un correo electrónico debe identificar sus datos en el pie de firma para el conocimiento de los mismos por parte del destinatario.

Datos
Saludos Cordiales,
Nombres y Apellidos completos
Cargo actual
Nombre de la Institución
Logo Institucional
Dirección donde se encuentra ubicado el funcionario
Teléfonos: Ext:
www.inclusion.gob.ec
Mensaje: Cuidado al Planeta

"Cláusula de Confidencialidad: La información contenida en cada mensaje de correo electrónico y sus anexos puede ser confidencial o privilegiada y solo puede ser utilizada por el destinatario a quien esté dirigida. Si usted no es el destinatario de este correo electrónico, cualquier uso de esta información se encuentra prohibido. Si recibió este correo por error, por favor informe inmediatamente a la persona que se lo envió y borre el correo electrónico y las copias de su computador.

Esta información no debe ser distribuida, ni copiada total o parcialmente por ningún medio sin la autorización de la MIES; misma que no asume responsabilidad sobre la información, opiniones o criterios contenidos en este correo electrónico.

Nota: Tipo de fuente: Calibri, Tamaño: 8.0, Color: Negro, Estilo: Normal

7.5. Perfiles de Correo Electrónico Institucional

El sistema de correo institucional debe contar con perfiles y niveles de usuario para su administración.

- ***Acceso Súper Administrador:*** Este perfil tiene control total de la plataforma, permite crear, modificar y eliminar correos electrónicos, áreas y listas de distribución. Posee acceso a la consola de administración total de la plataforma, así como también a la generación de reportes
- ***Acceso Administrador:*** Este perfil permite la creación, modificación o eliminación de las cuentas de correo electrónico, áreas y listas de distribución
- ***Acceso Estándar:*** Este perfil permite acceder únicamente a la cuenta a la que se le ha designado al usuario y hacer uso de las funcionalidades que ofrece la interfaz de la plataforma dentro de su cuenta

7.6. Asignación de perfiles a los usuarios de la Institución

Se asignarán los permisos de acuerdo a los siguientes niveles:

Tipo de perfil	Asignación de perfiles	Área
Súper Administrador	Responsables de la administración total de la plataforma	Dirección de Infraestructura y Operaciones de TI.
Administrador	Técnicos de TIC a nivel nacional	Dirección de Soporte a Usuarios de TI. Áreas de Tecnologías de Información a nivel zonal.
Estándar	Resto de usuarios a nivel nacional que no tienen perfil de administrador	Todas las áreas a nivel nacional

Los funcionarios asignados deben ser identificados y registrados para control y auditorías.

7.7. Sitio de acceso para el correo electrónico institucional

El sitio oficial para acceder al correo electrónico institucional de cada usuario es: https://mail.inclusion.gob.ec

Los usuarios de servicios deben ingresar al correo electrónico institucional desde: https://cz.inclusion.gob.ec

7.8. Creación de cuentas de correo electrónico institucional

Desde la Dirección de Administración de Recursos Humanos se envía una solicitud a la Dirección de Soporte a Usuarios de TI para la activación de creación de usuarios y claves para los sistemas utilizados en el MIES, mismos que son fundamentales en la actividad diaria de cada usuario.

Dentro de esta solicitud se encuentra especificada la información básica del usuario.

Entre los sistemas activados se encuentra el correo electrónico institucional. La creación de cuentas está alineada a los tipos de perfiles de acuerdo al puesto que ocupa cada usuario en la Institución.

Nombre de usuario: El nombre de usuario para todos los usuarios de la Institución está generado de acuerdo a lo mencionado en el punto:

7.1. Estructura de las cuentas de correo electrónico institucional

Clave: La clave que se establece como valor inicial, será determinada por la Dirección de Soporte a Usuarios de TI y deberá ser cambiada la primera vez que el usuario ingrese al correo. Cada usuario deberá cambiar su clave cada 60 días; se enviará una notificación de cambio para realizar este proceso.

7.9. Aceptación de políticas de correo electrónico

Todos los usuarios del Ministerio de Inclusión Económica y Social que ingresan a la Institución deben utilizar la plataforma de correo institucional establecida.

Al momento de ingresar a su correo institucional, cada usuario está aceptando la responsabilidad y confidencialidad del uso y manejo de información institucional.

7.10. Disponibilidad del servicio de correo electrónico institucional

La Dirección de Infraestructura y Operaciones de TI, trabajará con el objetivo de minimizar la indisponibilidad del servicio de correo electrónico institucional, debido a la posibilidad de incidentes de la red de Internet y otros contingentes de fuerza mayor. En este último caso la Coordinación General de Tecnologías de Información y Comunicación, no será responsable de pérdidas de datos.

7.11. Monitoreo de correos electrónicos institucionales

Los correos electrónicos institucionales de todos los usuarios del Ministerio de Inclusión Económica y Social pueden ser monitoreados por la Coordinación General de Tecnologías de Información y Comunicación en caso de identificar anomalías que estén afectando el buen uso del correo electrónico institucional o anomalías que intervengan en la alta disponibilidad de este servicio se deben tomar las notificaciones y correctivos necesarios.

7.12. Depuración de plataforma de correo electrónico

- El servidor de correo electrónico institucional será depurado de manera periódica por las direcciones que son responsables de la administración
- Considerando que el espacio y la memoria, tanto en los servidores de datos de la Institución como en las computadoras asignadas a los usuarios es limitado, se hace mandatorio que los usuarios realicen una revisión continua y depuren los correos que no son relevantes para no afectar el espacio de almacenamiento en el servidor
- Todos los usuarios deben vaciar frecuentemente las papeleras de su cuenta con el mismo objetivo de mantener el mayor espacio disponible en el servidor

7.13. Confiabilidad e integridad de los correos electrónicos

- La Institución se compromete a no ceder ni vender a terceros la información registrada en los correos electrónicos de cada usuario
- Con el objetivo de mantener la confidencialidad e integridad de los correos electrónicos, todos los funcionarios tienen la obligación de mantener confidenciales sus claves de acceso y utilizar claves robustas, las cuales deben contener mayúsculas, minúsculas, números y caracteres especiales, con una extensión mínima de 8 caracteres
- Será responsabilidad del usuario de una cuenta de correo electrónico institucional, modificar su clave de acceso si considera que podría haber sido vulnerada
- Será responsabilidad del remitente toda la información transmitida por correo electrónico institucional
- Todos los correos electrónicos institucionales de los usuarios del servicio de correo de la MIES podrán ser utilizados en cualquier clase de litigio, previa orden judicial
- Es importante mencionar que quien incumpla con alguno de los puntos estipulados en esta política será sujeto de sanción de acuerdo a la gravedad de la falta incurrida

7.14. Respuestas automáticas

Será responsabilidad del usuario, personalizar un mensaje de respuesta automática en caso de ausencia, sea por vacaciones o cualquier otra situación que le impida recibir y responder sus correos por un plazo de tiempo superior a 3 días.

7.15. Reseteo de claves

- El sistema debe ser configurado para que solicite reseteo automático de claves cada 60 días como máximo
- Para solicitar una clave de acceso al correo electrónico institucional extraviada, se deberá enviar esta solicitud a través del sistema de gestión de servicios tecnológicos (mesa de servicios) que se encuentre vigente en la Coordinación General de Tecnologías de Información y Comunicación

7.16. Responsabilidad de actividades realizadas en el correo electrónico institucional

- Los usuarios del Ministerio de Inclusión Económica y Social son responsables de todas las actividades realizadas con sus cuentas de correo electrónico institucional
- El usuario responsable del buzón debe dar un trámite ágil al correo electrónico recibido (responder, eliminar, archivar mensajes en el disco duro local)
- Los buzones de correo configurados son de uso exclusivo del usuario al que fue asignado y serán de su responsabilidad todos aquellos mensajes enviados en su nombre
- El usuario es responsable de mantener o archivar los mensajes enviados y/o recibidos para efectos de soportar ante terceros (internos o externos) la ejecución de operaciones o acciones
- El usuario es responsable de hacer limpieza / depuración a su buzón de correo institucional, con el fin de no exceder el máximo tope de almacenamiento asignado.
- Todos los mensajes que se envíen a través del correo electrónico institucional deben estar enmarcados en normas de respeto
- Si un funcionario debiera cambiar de equipo, ya sea por reemplazo del mismo o por traslado a otra unidad, la Dirección de Soporte a Usuarios de TI, será responsable de realizar la migración del buzón personal local al nuevo equipo que usará el funcionario, para conservar sus correos electrónicos en caso de requerirlos
- Todo usuario es responsable por la destrucción de los mensajes con origen desconocido, y asume la responsabilidad por las consecuencias que pueda ocasionar la ejecución de los archivos adjuntos. En estos casos, no deben contestar dichos mensajes y deben notificar a soporte a usuarios para que efectúe el seguimiento, direccionamiento y la investigación necesaria de ser el caso
- Todo usuario es responsable de la cantidad y tamaño de mensajes que envíe, por lo que debe optimizar el tamaño de sus mensajes y/o adjuntos. Se considerará como una violación a esta política cuando se encuentre en circulación un mensaje de correo electrónico que no cumpla con la optimización requerida
- El usuario es responsable de la administración de su correo por lo que en el caso de que el usuario borre accidentalmente algún correo o carpeta de su cuenta de correo, la Coordinación General de Tecnologías de Información y Comunicación, no garantiza la reposición

- La solicitud de creación de cuentas genéricas y listas de distribución es responsabilidad de las diferentes direcciones que requiera dicha funcionalidad. Éstas deberán ser asignadas a un funcionario, el cual será responsable de la cuenta y aparecerá como tal. Las listas de distribución sólo podrán contener correos institucionales

7.17. Envio de archivos adjuntos

Los archivos adjuntos que se envíen en los correos electrónicos institucionales deberán corresponder exclusivamente a temas laborales que competan a la Institución y no deberán sobrepasar los límites establecidos.

Cuando los archivos adjuntos son de gran tamaño, deberá solicitar por Mesa de Servicio el soporte técnico de la Dirección de Soporte a Usuarios de TI.

7.18. Permisos de envio de correo electrónico institucional masivo.

El correo electrónico institucional no es una herramienta de difusión de información, por lo que es prohibido distribuir de forma masiva grandes cantidades de mensajes a usuarios del Ministerio o fuera de él, directamente desde la bandeja de entrada del correo electrónico institucional del usuario.

Están autorizados de enviar mails masivos: Ministro(a), Viceministros(as), Subsecretarios(as), Coordinadores(as), Directores(as).

Adicionalmente con el objeto de optimizar los recursos del MIES y eliminar respuestas masivas; se debe enviar a los destinatarios en copia oculta.

7.19. Seguridad del correo del usuario

- Todo incidente de seguridad o desempeño del correo electrónico, debe ser notificado a la Coordinación General de Tecnologías de Información y Comunicación, empleando los canales establecidos para tal fin
- Se debe realizar un análisis de virus, con la herramienta asignada para tal fin, de todos los archivos adjuntos que son enviados o recibidos por correo electrónico.

7.20. Restricciones

El correo electrónico institucional es una herramienta para el intercambio de información entre los usuarios del Ministerio de Inclusión Económica y Social, así como también se lo usa para intercambio de información con personas ajenas a la Institución únicamente para temas relacionados a lo laboral. Están completamente prohibidas las siguientes actividades:

- Queda estrictamente prohibida la utilización de otro sistema de correo electrónico para fines institucionales
- Uso del correo electrónico institucional para cualquier propósito comercial o financiero
- Uso del correo electrónico para propósitos políticos, religiosos o temas similares
- Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para la Institución
- Está prohibido enviar cartas, cadenas o mensajes con bromas desde un correo del MIES, así como enviar alertas o correos masivos a menos que se tenga autorización de su autoridad jerárquica superior
- Envíos masivos pueden enviar únicamente la Dirección de Comunicación Social, Dirección de Soporte a Usuarios de TI, Dirección de Administración de Recursos Humanos y el jerárquico superior de acuerdo a la estructura detallada en el punto 7.18
- El correo electrónico institucional no debe ser utilizado por terceros (clientes o proveedores) sin previa autorización

- No está permitido la parametrización de los mensajes a enviar, que contengan fondos, imágenes o logos no institucionales
- Los usuarios de la Institución no deben utilizar versiones escaneadas de firmas hechas a mano para dar la impresión de que un mensaje de correo electrónico o cualquier otro tipo de comunicación electrónica ha sido firmada por la persona que la envía
- No se debe abrir o revisar correo que tenga procedencia de remitentes desconocidos
- En forma general no está permitido imprimir los mails, ya que esta herramienta fue creada para tener un archivo electrónico, agilitar las comunicaciones, descartar en la medida de lo posible el archivo tradicional y lograr un ahorro en suministros y papelería
- Los funcionarios no podrán utilizar su correo personal para el envío, almacenamiento, compartición de información de la Institución, porque solo es un medio de gestión centralizada

7.21. Casos especiales

En ciertas ocasiones o casos especiales, esta política no se podrá aplicar en su totalidad, estos casos deberán ser analizados por la Dirección de Soporte a Usuarios de TI, quienes evaluarán la pertinencia y los riesgos asociados y permitirán o negarán la excepción.

Dichos casos especiales deberán ser informados de manera escrita a la Dirección de Seguridad, Interoperabilidad y Riesgos para su registro y evaluación.

7.22. Casos excepcionales de acceso al correo electrónico de un funcionario

La Dirección de Infraestructura y Operaciones de Tecnología de la Información, podrá acceder al contenido del correo electrónico de sus funcionarios, sólo en los siguientes casos excepcionales de:

- Fallecimiento, enfermedad temporal o definitiva, que no le permita acceder al correo electrónico, con la previa autorización del jefe inmediato de la Unidad Administrativa
- Expresa voluntad de la persona, previamente autorizado por escrito

En los casos mencionados, el contenido del correo electrónico será entregado al jefe inmediato superior, quien asegurará la custodia de la información. La finalidad de este acceso excepcional es el de permitir que la unidad a la cual pertenece dicho funcionario, pueda continuar con sus labores habituales.

7.23. Eliminación de cuentas de correo electrónico

El espacio de las cuentas incide directamente sobre el espacio del servidor, por lo que se establecen que:

- Cuando un funcionario se desvincula completamente de la Institución, la Dirección de Administración de Recursos Humanos envía mediante correo electrónico a la Dirección de Soporte a Usuarios de TI, el requerimiento de eliminación de la cuenta de correo electrónico institucional asignado del servidor público saliente

- De igual manera en el caso de un cambio administrativo, la Dirección de Administración de Recursos Humanos deberá realizar la notificación formal a la Dirección de Soporte a Usuarios de TI para que sus datos sean actualizados en la cuenta de correo electrónico institucional

7.24. Bloqueo de cuentas de correo electrónico

- En el caso que se detecte que a través de la cuenta de usuario se está efectuando un ataque informático malicioso al correo institucional, se procederá a bloquear la cuenta del usuario
- Para habilitar de nuevo la cuenta, el usuario debe comunicarse con la Dirección de Soporte a Usuarios de TI del MIES

7.25. Archivo y almacenamiento

El servicio de correo electrónico institucional debe ser utilizado exclusivamente como un medio de transmisión de información y no de almacenamiento o gestión de información. En consecuencia, cada funcionario es responsable de almacenar la información relevante en carpetas de trabajo personales creadas directamente en su equipo. Es decisión del funcionario la forma de organizar su correo y su archivo en carpetas personales.

El tamaño de correos, tamaño de archivos adjuntos y cantidad de destinatarios se indican en la siguiente tabla:

Cargos	Tamaño de correo	Cantidad de destinatarios	Tamaño de Adjuntos
Autoridades	5 GB	20	10 MB
Directores (Asistentes de Dirección) y Asesores	3 GB	20	10 MB
Servidores Públicos	1 GB	20	10 MB

7.26. Respaldo de cuentas de correo electrónico

- Cada usuario es responsable de respaldar la información que se considere importante. *(Para tener conocimiento en la manera como generar respaldos en el equipo de cada usuario, descargar manual de generación de respaldos alojado en la Intranet de la Institución)*
- La Dirección de Infraestructura y Operaciones es responsable de respaldar el Sistema de correo electrónico integral de forma periódica

8. AMONESTACIONES

Se sancionará a los usuarios que no hagan buen uso del correo electrónico institucional de acuerdo a la presente política; se aplicará la sanción correspondiente en coordinación con la Dirección de Administración de Recursos Humanos de acuerdo a lo que especifique la Ley vigente.

9. VALIDEZ Y GESTIÓN DE DOCUMENTOS

Este documento es válido desde su implementación y socialización.

Este documento está validado por el Oficial de Seguridad de Información (Director de Procesos) del MIES.

El propietario del documento es el área de Seguridad, Interoperabilidad y Riesgos del MIES, para la verificación, y si es necesario actualización del presente documento.

10. POLÍTICAS, PROCEDIMIENTOS Y MANUALES RELACIONADOS

- Acuerdo Ministerial 000080 de fecha 9 de Abril de 2015
- Acuerdo Ministerial 166, EGSI, y su última modificación del 15 de junio de 2016

11. ADVERTENCIA

Cualquier usuario del Ministerio de Inclusión Económica y Social, que sea encontrado realizando actividades que contravenga la presente política podrá ser investigado y puede ser causal de sanciones, sin perjuicio de las acciones disciplinarias y/o jurídicas.

MINISTERIO DE
INCLUSIÓN ECONÓMICA
Y SOCIAL

Toda una Vida

EL
GOBIERNO
DE TODOS

POLÍTICAS
SEGURIDAD DE LA INFORMACIÓN

ANEXO 2

Quito, Mayo del 2018

DATOS GENERALES		
No. Doc.	MIES-CGTIC-DSIR-POL-2018-0002	
Tipo de documento	Politicas	
Institución	Ministerio de Inclusión Económica y Social	
Dirección Ejecutora	Coordinación General de Tecnologías de Información y Comunicación	
Fecha	22/05/2018	
Versión	1.0	
Elaborado por	**Cargo**	**Firma**
Ing. Katherine Colcha	Analista de Tecnologías de Información	
Revisado por	**Cargo**	**Firma**
Ing. Richarth Pazmiño MBA.	Director de Seguridad, Interoperabilidad y Riesgos	
Ing. Jorge Pichucho MGS.	Director de Infraestructura y Operaciones de TI	
Ing. Soledad Cueva	Director de Soporte a Usuarios de TI (E)	
Ing. Cristian Núñez	Director de Proyectos de TI (E)	
Validado por	**Cargo**	**Firma**
Lic. Rubén Ortega MGS	Oficial de Seguridad de la Información	
Aprobado por	**Cargo**	**Firma**
Ing. Fabián Vallejo	Coordinador General de Tecnologías de Información y Comunicación	

CONTROL DE VERSIONES			
Fecha	**Versión**	**Responsable**	**Descripción**
22/05/2018	1.0	Ing. Katherine Colcha	Elaboración de las políticas.

Contenido

1. INTRODUCCIÓN 4
2. ANTECEDENTES 4
3. JUSTIFICACIÓN 4
4. OBJETIVO 4
5. ALCANCE 5
6. RESPONSABILIDADES 5
7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 5
8. GESTIÓN DE LA POLÍTICA Y OTROS DOCUMENTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 5
9. ROLES Y RESPONSABILIDADES 6
9.1. Responsabilidades frente a la Seguridad de la Información y al Sistema de Gestión de Seguridad 7
9.1.1. Responsabilidades – Direcciones de la Coordinación General de Tecnología de Información y Comunicación (CGTIC) 7
9.1.2. Responsabilidades – Propietarios de la Información 8
9.1.3. Responsabilidades – Funcionarios, Contratistas y Practicantes Usuarios de la Información 8
9.1.4. Responsabilidad de Usuarios 9
9.1.5. Casos Especiales 9
10. COMPROMISO DE TODO EL PERSONAL DE LA INSTITUCIÓN 10
11. IDENTIFICACIÓN DE RIESGOS 10
12. AMONESTACIONES 10
13. VALIDEZ Y GESTIÓN DE DOCUMENTOS 10
14. POLÍTICAS, PROCEDIMIENTOS Y MANUALES RELACIONADOS 11
15. GLOSARIO 11

1. INTRODUCCIÓN

La información es un recurso importante dentro del Ministerio de Inclusión Económica y Social en el cumplimiento de los objetivos estratégicos por cuanto permite la toma de decisiones a las autoridades encargadas de la gestión de servicios a los usuarios internos y externos.

Establecer un marco en el cual se asegure que la información es protegida de una manera adecuada cuando sea manejada, procesada, transportada o almacenada.

2. ANTECEDENTES

El Ministerio de Inclusión Económica y Social entrega servicios tecnológicos a los servidores públicos que laboran en la Institución a través de los cuales se gestiona información confidencial de los usuarios que reciben los servicios institucionales, misma que debe ser manejada con total sigilo para evitar su mala utilización.

El Esquema Gubernamental de Seguridad de la Información EGSI determina la necesidad de aplicar normas y procedimientos para seguridad de la información, e incorporar a la cultura y procesos institucionales la gestión permanente de la misma.

El EGSI establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la Administración Pública. El EGSI no reemplaza a la norma INEN ISO/IEC 27002 sino que marca como prioridad la implementación de algunas directrices.

3. JUSTIFICACIÓN

El establecimiento de políticas es fundamental para alcanzar los objetivos institucionales.

Las políticas de seguridad de la información, incrementará la seguridad de la información manejada en los servicios tecnológicos entregados por el MIES.

El EGSI establece: "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".

4. OBJETIVO

Establecer la política de seguridad de la información en el Ministerio de Inclusión Económica y Social, con el fin de regular la gestión de la seguridad de la información al interior de la entidad, logrando niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información institucional relevante, asegurando continuidad operacional de los procesos y servicios.

5. ALCANCE

Las políticas de seguridad de la información aplican a las y los servidores públicos que laboran en el Ministerio de Inclusión Económica y Social y a los usuarios que utilizan servicios tecnológicos provistos por la misma.

Esta política abarca los siguientes controles definidos en la norma ISO/IEC 27002:2013

- 5.1.1 Conjunto de políticas para la seguridad de la información
- 5.1.2 Revisión de las políticas para la seguridad de la información

6. RESPONSABILIDADES

El Ministerio de Inclusión Económica y Social a través de la Coordinación General de Tecnologías de Información y Comunicación proporcionará los servicios tecnológicos y los lineamientos que en temas de seguridad informática deben ser utilizados en la Institución.

Cada usuario tiene la responsabilidad de cumplir con esta política.

Las autoridades institucionales son responsables de controlar el cumplimiento de esta política por parte de los usuarios bajo su unidad.

7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

- La información generada o almacenada en medios de la Institución es de propiedad del MIES y deben ser utilizadas exclusivamente para las tareas propias de la función desarrollada en la Institución
- Para el manejo de la información institucional debe tener relación laboral con la Institución, o contar con la autorización escrita de un funcionario del jerárquico superior
- 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
- Los funcionarios, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información del MIES, 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

8. GESTIÓN DE LA POLÍTICA Y OTROS DOCUMENTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Conforme a lo dispuesto en el Acuerdo Ministerial No. 166 del Esquema Gubernamental de Seguridad de la Información – EGSI, donde dispone a las entidades de la Administración Pública Central, Institucional y que dependen de las Funciones Ejecutivas el uso obligatorio

de las Normas Técnicas Ecuatorianas NTE INEN –ISO/IEC 27000, es necesario aclarar que se basan en la Norma Internacional ISO/IEC 27001:2013 del Sistema de Seguridad de la Información para el MIES, la estructura documental de ese sistema está compuesto por una Política General de Seguridad de la Información, políticas específicas de seguridad de la información, procedimientos de operación, instructivos y registros.

La referida estructura documental aplicable al MIES debe ser aprobada por la Coordinación General de Planificación y Gestión Estratégica, será revisada y de ser el caso modificar la política cada dos años por el Oficial de Seguridad de la Información.

La documentación aplicable al MIES debe asegurar:

- Cumplir con la normativa definida en el Acuerdo Ministerial No. 166 del Esquema Gubernamental de Seguridad de la Información – EGSI, del 25 de septiembre del 2013
- Cumplir las normas legales y reglamentarias referidas a seguridad, tanto para la información, como para los medios que la contienen
- Que la información cumpla con los niveles de autorización y responsabilidad correspondientes para su utilización, divulgación, administración, seguimiento y custodia
- Que la información, sus medios de procesamiento, conservación y transmisión estén protegidos del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotajes, espionaje, violación de la privacidad y otras acciones que pudieran perjudicarla
- Que los medios de procesamiento, conservación y comunicación de la información cuenten con medidas de protección física que eviten el acceso y/o utilización indebida por personal no autorizado
- Que los derechos de propiedad sobre la información y sistemas estén establecidos
- Que las comunicaciones internas y externas cuenten con mecanismos que protejan la integridad, disponibilidad y confidencialidad en la transmisión de información
- Que se delimiten los ámbitos físicos de acción de las políticas de seguridad, dependiendo de los distintos niveles de riesgo que presentan los medios de procesamiento, conservación y comunicación
- Que las actividades y uso de recursos críticos, relacionados con productos y servicios, sean monitoreados y su información sea conocida en forma oportuna por los niveles correspondientes
- Las versiones vigentes de la normativa del Sistema de Gestión de Seguridad de la Información SGSI y los documentos de apoyo, serán publicados en la intranet del MIES (https://www.inclusion.gob.ec/).

9. ROLES Y RESPONSABILIDADES

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Institución. Las autoridades institucionales aprueban esta política y son responsables de la autorización de sus modificaciones.

La estructura organizacional para la gestión de la seguridad de la información en el MIES, estará compuesta por:

- **Oficial de Seguridad de la Información:** Es el responsable de revisar y proponer a las autoridades institucionales para su aprobación, el texto de la Política de Seguridad de la Información y la estructuración, recomendación, 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 materia de seguridad de la información y de coordinar las acciones, impulsando la implementación y cumplimiento de la presente política.

  A lo que se refiere el Acuerdo No. 166 del Esquema Gubernamental de Seguridad de la Información – EGSI, con fecha 25 de septiembre del 2013, tiene los roles y responsabilidades que se definen en el número 2.3 de dicho Acuerdo.

- **Dirección de Administración de Recursos Humanos:** El Director de Recursos Humanos cumplirá la función de notificar a todo el personal que se vincula a la Institución, las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de Seguridad de la Información. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de los acuerdos de Confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el Oficial de Seguridad de la Información

  A lo que se refiere el Acuerdo No. 166 del Esquema Gubernamental de Seguridad de la Información – EGSI, con fecha 25 de septiembre del 2013, tiene los roles y responsabilidades que se definen en el número 4.1 de dicho Acuerdo

- **Dirección de Asesoría Jurídica:** Asesorará en materia legal a la Institución en lo que se refiere a la Seguridad de la Información. Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

9.1. Responsabilidades frente a la Seguridad de la Información y al Sistema de Gestión de Seguridad

9.1.1. Responsabilidades – Direcciones de la Coordinación General de Tecnología de Información y Comunicación (CGTIC)

- Establecer, mantener y divulgar 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 a 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 de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la Institución a la CGTIC, las diferentes Direcciones de la Institución, así como a los entes de control e investigación que tienen injerencia sobre la misma
- Proporcionar 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 CGTIC y las diferentes direcciones
- Implementar los mecanismos de control necesarios y pertinentes para verificar el cumplimiento de la presente política

9.1.2. Responsabilidades – Propietarios de la Información

Son propietarios de la información cada uno de los servidores públicos que la genera, procesa, recibe y almacena en cualquier medio, esto incluye:

- Valorar y clasificar la información que está bajo su administración y/o generación, siguiendo los lineamientos establecidos por la Dirección de Secretaría General
- 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 acceder a consultar, crear o modificar parte o la totalidad de la información, así como la aceptación de acuerdos de confidencialidad establecidos
- Determinar los tiempos de retención de la información en conjunto con las áreas que se encarguen de su protección y almacenamiento de acuerdo a las determinaciones y políticas de la entidad como de los entes externos y las normas o leyes vigentes
- 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 los requisitos de esta política a todos los funcionarios, contratistas y practicantes en las diferentes dependencias de la Institución

9.1.3. Responsabilidades – Funcionarios, Contratistas y Practicantes Usuarios de la Información

- Manejar la información de la Institución y rendir cuentas por el uso y protección de tal información, mientras que este bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio
- Proteger la información a la cual accedan y procesen, para evitar su pérdida,

alteración, destrucción o uso indebido
- Evitar la divulgación no autorizada o el uso indebido de la información
- 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 intencional o no justificada y de la divulgación no autorizada
- Reportar los Incidentes de seguridad, eventos sospechosos y el 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 CGTIC
- Se debe utilizar software autorizado que haya sido 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 CGTIC
- Aceptar y reconocer que en cualquier momento y sin previo aviso, la Dirección de Seguridad, Interoperabilidad y Riesgos de la CGTIC 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 institucionales 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 auditoria 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. El MIES 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.

9.1.4. Responsabilidad de Usuarios

- Los usuarios del Ministerio de Inclusión Económica y Social son responsables de los usuarios, contraseñas y servicios tecnológicos que son asignados
- Si un funcionario debiera cambiar de equipo, ya sea por reemplazo del mismo o por traslado a otra unidad, el funcionario deberá solicitar apoyo tecnológico a la Dirección de Soporte a Usuarios mediante la Mesa de Servicio

9.1.5. Casos Especiales

En ciertas ocasiones o casos especiales, esta política no se podrá aplicar en su totalidad, estos casos deberán ser analizados por las Direcciones de Tecnología involucradas,

quienes evaluarán la pertinencia y los riesgos asociados y permitirán o negarán la excepción.

Dichos casos especiales deberán ser informados de manera escrita a la Dirección de Seguridad, Interoperabilidad y Riesgos para su registro y evaluación.

10.COMPROMISO DE TODO EL PERSONAL DE LA INSTITUCIÓN

El personal de la Institución acepta esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información del MIES.

El personal de la Institución demuestra su compromiso a través de:

- La aceptación de las Políticas de Seguridad de la Información contenidas en este documento
- La promoción activa de una cultura de seguridad
- Facilitar la socialización de este documento a todos los funcionarios de la entidad
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información
- La verificación del cumplimiento de las políticas

11.IDENTIFICACIÓN DE RIESGOS

En cumplimiento al Acuerdo No. 166 del Esquema Gubernamental de Seguridad de la Información – EGSI, en el Artículo 7 "Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos, en base a la norma INEN ISO/IEC:27005 "Gestión del Riesgo en la Seguridad de la Información".

12.AMONESTACIONES

Cualquier usuario del MIES, que sea encontrado realizando actividades que contravenga esta política podrá ser investigado y puede ser causal de sanciones, sin perjuicio de las acciones disciplinarias y/o jurídicas.

13.VALIDEZ Y GESTIÓN DE DOCUMENTOS

Este documento es válido desde su implementación y socialización.

Este documento está validado por el Oficial de Seguridad de Información (Director de Procesos) del MIES.

El propietario del documento es el área de Seguridad, Interoperabilidad y Riesgos del MIES, para la verificación, y si es necesario actualización del presente documento.

14.POLÍTICAS, PROCEDIMIENTOS Y MANUALES RELACIONADOS

- Acuerdo Ministerial 000080 de fecha 9 de Abril de 2015
- Acuerdo Ministerial 166, EGSI, y su última modificación del 15 de junio de 2016

15. GLOSARIO

ACTIVO DE INFORMACIÓN: Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Institución y, en consecuencia, debe ser protegido.

ACUERDO DE CONFIDENCIALIDAD: Es un documento en los 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 dentro de la misma.

CUSTODIO DEL ACTIVO DE LA INFORMACIÓN: Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

DISPONIBILIDAD: Es la propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

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).

INTEGRIDAD: Es la protección de la exactitud y estado completo de los activos.

SEGURIDAD DE LA INFORMACIÓN – SI: Es la preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad (accountability), no repudio y fiabilidad.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: Es el conjunto de datos que se organizan en una institución y otorgan valor añadido para ésta, de forma independiente de la forma en la que se guarde o transmita, el origen que tenga o la fecha de elaboración.

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

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.

TI: Hace referencia a las Tecnologías de la Información.

MINISTERIO DE
INCLUSIÓN ECONÓMICA
Y SOCIAL

Toda una Vida

EL
GOBIERNO
DE TODOS

POLÍTICAS

CONTROL DE ACCESOS A SERVICIOS TECNOLÓGICOS

ANEXO 3

Quito, Junio del 2018

DATOS GENERALES		
No. Doc.	MIES-CGTIC-DSIR-POL-2018-0003	
Tipo de documento	Políticas	
Institución	Ministerio de Inclusión Económica y Social	
Dirección Ejecutora	Coordinación General de Tecnologías de Información y Comunicación	
Fecha	26/06/2018	
Versión	1.0	
Elaborado por	**Cargo**	**Firma**
Ing. Katherine Colcha	Analista de Tecnologías de Información	
Revisado por	**Cargo**	**Firma**
Ing. Richarth Pazmiño MBA.	Director de Seguridad, Interoperabilidad y Riesgos	
Ing. Jorge Pichucho MGS.	Director de Infraestructura y Operaciones de TI	
Ing. Soledad Cueva	Director de Soporte a Usuarios de TI (E)	
Ing. Cristian Núñez	Director de Proyectos de TI (E)	
Validado por	**Cargo**	**Firma**
Lic. Rubén Ortega MGS.	Oficial de Seguridad de la Información	
Aprobado por	**Cargo**	**Firma**
Ing. Fabián Vallejo	Coordinador General de Tecnologías de Información y Comunicación	

CONTROL DE VERSIONES			
Fecha	**Versión**	**Responsable**	**Descripción**
26/06/2018	1.0	Ing. Katherine Colcha	Elaboración de las políticas

Contenido

1. INTRODUCCIÓN 4
2. ANTECEDENTES 4
3. JUSTIFICACIÓN 4
4. OBJETIVO 5
5. ALCANCE 5
6. RESPONSABILIDADES 5
7. POLÍTICAS DE CONTROL DE ACCESO A SERVICIOS TECNOLÓGICOS 5
7.1. GESTIÓN DE ACCESOS 5
7.1.1. Solicitud de acceso a los servicios tecnológicos 5
7.1.2. Creación de usuarios de servicios tecnológicos 6
7.1.3. Asignación de Permisos 6
7.1.4. Perfiles de Servicios Tecnológicos 6
7.1.5. Asignación de perfiles a los usuarios de la Institución 6
7.2. RESPONSABILIDADES DE USUARIO 7
7.3. CONTROL DE ACCESO A LA RED 7
7.3.1. Utilización de los servicios de red 7
7.3.2. Autenticación de usuarios para conexiones externas 8
7.3.3. Identificación de equipos en la Red 8
7.3.4. Protección de los puertos de configuración y diagnóstico remoto 8
7.3.5. Separación de redes 8
7.3.6. Control de conexión de las redes 8
7.3.7. Control de enrutamiento de red 9
7.4. CONTROL DE ACCESO AL SISTEMA OPERATIVO 9
7.4.1. Registro de inicio seguro 9
7.4.2. Gestión de contraseñas 9
7.4.3. Uso de utilitarios del Sistema 10
7.5. CONTROL DE ACCESO A LAS APLICACIONES E INFORMACIÓN 10
7.6. MONITOREO DE SERVICIOS INFORMÁTICOS INSTITUCIONALES 10
7.7. DEPURACIÓN DE LOS ACCESOS EXISTENTES 10
7.8. CASOS ESPECIALES 11
8. AMONESTACIONES 11
9. VALIDEZ Y GESTIÓN DE DOCUMENTOS 11
10. POLÍTICAS, PROCEDIMIENTOS Y MANUALES RELACIONADOS 11
11. GLOSARIO 12

1. INTRODUCCIÓN

Las políticas de control de acceso informático refieren a la autorización de las personas para acceder a las instalaciones o sistemas que contienen información. La implementación de una política de control de acceso físico ayuda a prevenir el robo y la divulgación no autorizada de información y otros problemas que puedan presentarse.

Los servicios tecnológicos son proporcionados con el objeto de apoyar las funciones que desempeñan los servidores y las servidoras públicas del Ministerio de Inclusión Económica y Social y agilizar la gestión de procesos de cada unidad administrativa.

Las políticas explican el uso apropiado de los servicios tecnológicos institucionales y las medidas para optimizar su utilización.

Cuando las políticas se ejecutan adecuadamente, aumentan la productividad de los servidores y servidoras públicas y protegen la información en la red interna e imagen institucional.

2. ANTECEDENTES

El Ministerio de Inclusión Económica y Social entrega servicios tecnológicos a los servidores públicos que laboran en la Institución, estos son administrados por parte de la Coordinación General de Tecnologías de Información y Comunicación, misma que se encuentra alineada a las políticas de control, regulación y optimización de los recursos tecnológicos vigentes, lo cual permite la correcta gestión de acuerdo a las necesidades institucionales.

Se ha tomado el Esquema Gubernamental de Seguridad de la Información como guía de referencia en temas de seguridad informática.

Los principales servicios tecnológicos entregados actualmente son:

- Internet
- Correo institucional
- Aplicativos Gubernamentales
- Sistemas informáticos institucionales
- Aplicativos provistos por terceros
- Telefonía IP

3. JUSTIFICACIÓN

El establecimiento de políticas es fundamental para alcanzar los objetivos institucionales.

Las políticas de control de accesos a servicios tecnológicos institucionales permitirán utilizar los recursos de forma efectiva, disminuyendo el riesgo y propendiendo a la entrega eficiente de los recursos informáticos tanto a los servidores públicos como a la ciudadanía.

El Esquema Gubernamental de Seguridad de la Información en el punto 7. CONTROL DE ACCESO, 3.2. Responsable de los activos, establece con (*) los aspectos que se deben considerar como primordiales de cumplimiento para una buena gestión de control de accesos.

Es fundamental que estas políticas sean socializadas y cumplidas por cada servidor y servidora pública de esta Institución para de esta manera mejorar la seguridad en la gestión de los servicios tecnológicos en el MIES.

4. OBJETIVO

Definir y reglamentar las normas generales de control de acceso a los servicios informáticos, mejorando la seguridad de la información en la Institución.

5. ALCANCE

Las políticas de control de accesos aplican a las y los servidores públicos que laboran en el Ministerio de Inclusión Económica y Social y utilizan servicios tecnológicos provistos por la misma.

Entre los temas tratados se encuentra: Gestión de accesos; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones e información.

6. RESPONSABILIDADES

El Ministerio de Inclusión Económica y Social a través de la Coordinación General de Tecnologías de Información y Comunicación proporcionará los servicios tecnológicos que serán utilizados en toda la Institución.

Cada usuario tiene la responsabilidad de cumplir con esta política.

Las autoridades institucionales son responsables de controlar el cumplimiento de esta política por parte de los servidores públicos bajo su unidad.

7. POLÍTICAS DE CONTROL DE ACCESO A SERVICIOS TECNOLÓGICOS

- La información generada o almacenada en medios institucionales es de propiedad del MIES y debe ser utilizada exclusivamente para las tareas propias de las funciones desarrollada en la Institución
- Para acceder a los servicios tecnológicos la persona debe tener relación laboral con la Institución, o contar con la autorización escrita de un funcionario del jerárquico superior

7.1. GESTIÓN DE ACCESOS

7.1.1. Solicitud de acceso a los servicios tecnológicos

Desde la Dirección de Administración de Recursos Humanos se envía una solicitud a la Dirección de Soporte a Usuarios de TI para la habilitación de usuarios y claves en los sistemas informáticos utilizados en el MIES, de acuerdo al cargo y funciones asignadas al servidor público. En cuanto al uso de los sistemas institucionales la solicitud debe ser remitida por el Jefe Inmediato informando los perfiles que utilizará.

Dentro de esta solicitud se encuentra especificada la información básica del usuario.

Nombres Completos	Cédula de Ciudadanía	Ubicación Geográfica (Planta Central, Zona, Distrito)	Unidad Asignada (Dirección)	Cargo (Funciones)

7.1.2. Creación de usuarios de servicios tecnológicos

Nombre de usuario: El nombre de usuario de servicios tecnológicos está generado de la siguiente forma:

primer nombre.primer apellido@inclusion.gob.ec

En caso de existir homónimos en los nombres, el usuario se creará con el segundo nombre del usuario solicitante o en su defecto se analizará la estructura para evitar usuarios repetidos.

En el caso de tener una estandarización diferente en los sistemas; debe ser documentada, socializada y aprobada por el Director responsable donde se administre el sistema, aplicación, etc.

7.1.3. Asignación de Permisos

- Los permisos concedidos son asignados de manera personal e intransferible
- La Coordinación General de Tecnologías de Información y Comunicación determina y asigna los servicios tecnológicos básicos de uso general para todos los servidores públicos del MIES
- Para el caso de requerir servicios tecnológicos especiales, se debe proceder de acuerdo al Instructivo Autorización de Accesos Especiales, a través de la Mesa de Servicios

7.1.4. Perfiles de Servicios Tecnológicos

- ***Acceso Súper Administrador:*** Este perfil tiene control total de la plataforma, permite crear, modificar y eliminar
- ***Acceso Administrador:*** Este perfil permite la creación, modificación o eliminación de usuarios
- ***Acceso estándar:*** Este perfil permite acceder únicamente a los permisos asignados a su usuario y hacer uso de las funcionalidades básicas que ofrece el servicio tecnológico

7.1.5. Asignación de perfiles a los usuarios de la Institución

Se asignarán los permisos de acuerdo a los siguientes perfiles:

Tipo de perfil	Asignación de perfiles	Área
Súper Administrador	Responsables de la administración total de la plataforma	Direcciones de la CGTIC
Administrador	Técnicos de TIC a nivel nacional	Áreas de Tecnologías de Información a nivel zonal y distrital
Estándar	Usuarios a nivel nacional que no tienen perfil de administrador	Todas las áreas a nivel nacional

Todo usuario creado debe tener incluido el número de cedula y nombre en el sistema, aplicación, etc. En el caso de utilizar usuarios genéricos se debe justificar e ingresar la identificación y el nombre del usuario responsable.

7.2. RESPONSABILIDADES DE USUARIO

- Todos los usuarios del Ministerio de Inclusión Económica y Social que ingresan a la Institución deben utilizar los servicios tecnológicos provistos por la Institución.
- Al momento de ingresar a los sistemas, aplicaciones institucionales, cada usuario está aceptando la responsabilidad y confidencialidad del uso y manejo de los servicios e información institucional.
- Los servidores públicos del Ministerio de Inclusión Económica y Social son responsables de los usuarios, contraseñas y servicios tecnológicos asignados.
- Si un funcionario debiera cambiar de equipo, ya sea por reemplazo del mismo o por traslado a otra unidad, el funcionario deberá solicitar apoyo tecnológico a la Dirección de Soporte a Usuarios mediante la Mesa de Servicios.
- Todos los funcionarios o terceros que tengan un usuario en la plataforma tecnológica de la Institución, deberán conocer y cumplir con esta política, donde se dictan pautas sobre derechos y deberes con respecto al uso adecuado de los servicios tecnológicos proporcionados por el MIES.

7.3. CONTROL DE ACCESO A LA RED

Las conexiones no seguras a los servicios de red pueden afectar a toda la institución, por lo tanto, se debe controlar 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.

Las reglas de acceso a la red a través de los puertos, estarán basadas en la premisa: "todo está restringido, a menos que este expresamente permitido".

7.3.1. Utilización de los servicios de red

Las Direcciones de la Coordinación General de TIC, deben desarrollar procedimientos para la activación y desactivación de permisos de acceso a las redes y servicios, los cuales comprenderán principalmente:

- Controlar el acceso a los servicios de red tanto internos como externos
- Identificar las redes y servicios de red a los cuales se permite el acceso
- Autorización de acceso entre redes

- Establecer controles de administración para proteger el acceso y servicios de red

7.3.2. Autenticación de usuarios para conexiones externas

La Dirección de Infraestructura y Operaciones de TI contempla como servicios de conexiones externas SSL (Capa de conexión segura), VPN (Redes privadas virtuales) y primarios para funcionarios que requieran conexión remota a la red de datos institucional.

La autenticación a los servicios VPN para usuarios con conexiones externas, debe estar documentado mediante un procedimiento de Utilización del Acceso Remoto VPN.

7.3.3. Identificación de equipos en la Red

Las direcciones de TIC responsables identificarán y controlarán los equipos conectados a su red, mediante el uso de controladores de dominio, estandarización de nombres de equipos o dispositivos, asignación de IP y portales cautivos en el caso de conexiones inalámbricas.

7.3.4. Protección de los puertos de configuración y diagnóstico remoto

Los puertos que permitan realizar mantenimiento y soporte remoto a los equipos de red, servidores y equipos de usuario final, estarán restringidos a los administradores de red. Para el caso del diagnóstico remoto, los usuarios finales deben permitir tomar el control remoto de sus equipos por parte de la Dirección de Soporte a Usuarios, teniendo en cuenta, no mantener archivos con información sensible a la vista y no desatender el equipo mientras que se tenga el control del equipo por un tercero.

7.3.5. Separación de redes

La Dirección de Infraestructura y Operaciones TI utilizará dispositivos de seguridad perimetral, para controlar el acceso de una red a otra y proteger la información más crítica o vulnerable.

La segmentación se realizará en equipos de conectividad.

Las redes inalámbricas, contarán con restricciones de políticas a nivel de los equipos de comunicaciones.

7.3.6. Control de conexión de las redes

La capacidad de descarga de cada usuario final debe ser limitada y controlada.

La seguridad para las conexiones WiFi será WPA2 o superior.

Dentro de la red de datos institucional se restringirá el acceso a:

- Mensajería instantánea y redes sociales
- La telefonía a través de internet
- Correo electrónico comercial no autorizado

- Descarga de archivos de sitio peer to peer o repositorios no autorizados.
- Conexiones a sitios de streaming no autorizado.
- Acceso a sitios de pornografía.
- Violencia contra niños, niñas y adolecentes
- Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de la misma.

7.3.7. Control de enrutamiento de red

El acceso a redes desde y hacia afuera de la Institución cumplirá con los lineamientos del Control de acceso a la red y adicionalmente se utilizarán métodos de autenticación de protocolo de enrutamiento, translación de direcciones IP y listas de control de acceso.

7.4. CONTROL DE ACCESO AL SISTEMA OPERATIVO

7.4.1. Registro de inicio seguro

El acceso a los sistemas operativos estará protegido, mediante un inicio seguro de sesión, que contemplará las siguientes condiciones:

- No mostrar información del sistema, hasta que el proceso de inicio se haya completado.
- No suministrar mensajes de ayuda, durante el proceso de autenticación.
- Validar los datos de acceso, una vez que se han diligenciado todos los datos de entrada.
- Limitar el número de intentos fallidos de conexión auditando los intentos no exitosos
- No mostrar las contraseñas digitadas.
- Las contraseñas deben almacenarse en los sistemas en forma encriptada.
- No transmitir la contraseña en texto claro.

7.4.2. Gestión de contraseñas

- La generación de contraseña del servidor público debe cumplir una complejidad media y alta que consiste en la utilización de con letras mayúsculas, minúsculas, con caracteres especiales. (Hito 7.6 – Uso de contraseñas – Esquema Gubernamental de Seguridad de la Información)
- Para la asignación y cambio de contraseñas se deberá controlar a través de un proceso formal de gestión de contraseñas, a cargo de la Dirección de Soporte a Usuarios de TI.
- La contraseña que se establece como valor inicial es la cédula del usuario y esta deberá ser cambiada la primera vez que ingrese al servicio. Cada usuario deberá cambiar su clave cada 60 días; los sistemas deberán enviar una notificación de cambio para realizar este proceso.
- Las contraseñas no deben estar escritas y expuestas a que otras personas las vean
- Controlar el cambio de contraseña de los usuarios y del personal de tecnología y de los administradores de tecnología, en rangos de tiempo y complejidad.
- Forzar el cambio de contraseña en el primer registro de acceso o inicio de sesión.

- Generar un procedimiento formal para la administración y custodia de las contraseñas de acceso de administración e información crítica de la institución.
- Documentar el control de acceso para los usuarios temporales.
- Almacenar y transmitir las contraseñas en formatos protegidos (encriptados o codificados.

7.4.3. Uso de utilitarios del Sistema

- Se establecerá una política a nivel del controlador de dominio, que no permita la instalación de software y cambios de configuración del sistema. Ningún usuario final, deberá tener privilegios de usuario administrador.
- Después de diez (10) minutos de inactividad del sistema, se considerará tiempo muerto y se bloqueará la sesión, sin cerrar las sesiones de aplicación o de red (Ítem 7.20. Tiempo de inactividad de la sesión – EGSI).
- Los usuarios procederán a bloquear sus sesiones, cuando deban abandonar temporalmente su puesto de trabajo.
- Las estaciones de trabajo deberán quedar apagadas al finalizar la jornada laboral o cuando una ausencia temporal supere dos (2) horas

7.5. CONTROL DE ACCESO A LAS APLICACIONES E INFORMACIÓN

- El control de acceso a la información, se realizará a través de roles que administren los privilegios de los usuarios por cada sistema, aplicativo o servicio, mismos que deben contar en un registro incluido en carpetas compartidas con acceso solo a personal de tecnología autorizado.
- El control de acceso a información física o digital, se realizará teniendo en cuenta los niveles de clasificación y el manejo de intercambio de información determinado por las autoridades.
- La Coordinación General de Tecnologías de Información y Comunicación, identificará según los niveles de clasificación de información cuales sistemas considera sensibles y que deberían gestionarse desde ambientes tecnológicos aislados e independientes. Al aislar estos sistemas se debe prever el intercambio seguro de información, con otras fuentes de datos, ya que no se permite duplicar información en otros sistemas, siguiendo las directrices de fuentes únicas de datos.
- Los funcionarios que se desvinculan de la Institución, se desactivarán una vez que la Coordinación General de Tecnología de Información y Comunicación, reciba el listado respectivo por parte de la Dirección de Administración de Recursos Humanos.

7.6. MONITOREO DE SERVICIOS INFORMÁTICOS INSTITUCIONALES

El Ministerio de Inclusión Económica y Social a través de la Coordinación General de Tecnologías de Información y Comunicación monitoreará los servicios tecnológicos entregados con el fin de evitar anomalías que interfieran en la alta disponibilidad de los mismos.

7.7. DEPURACIÓN DE LOS ACCESOS EXISTENTES

- La Coordinación General de Tecnologías de Información y Comunicación realizará una depuración de los accesos otorgados a los servidores públicos.

- Se deberá realizar las depuraciones respectivas de los accesos de los usuarios, determinando un periodo máximo de 60 dias; en casos de presentar cambios estructurales, esta gestión deberá hacerse inmediatamente que se ejecute el cambio organizacional (Hito 7.5. Revisión de los derechos de acceso de los usuarios, EGSI).
- Considerando la optimización del espacio de almacenamiento y la memoria, tanto en los servidores de datos de la Institución como en las computadoras asignadas a los usuarios, es limitado, se hace mandatorio que los usuarios realicen una revisión continua de sus archivos y depuren la información no relevante.

7.8. CASOS ESPECIALES

En ciertas ocasiones o casos especiales, esta política no se podrá aplicar en su totalidad, estos casos deberán ser analizados por las Direcciones de la Coordinación de TIC involucradas, quienes evaluarán la pertinencia y los riesgos asociados y permitirán o negarán la excepción.

Los casos especiales son los que no se encuentren contemplados en ésta política y deberán ser informados de manera escrita a la Dirección de Seguridad, Interoperabilidad y Riesgos para su registro y evaluación.

8. AMONESTACIONES

Cualquier servidor público del MIES, que sea encontrado realizando actividades que contravenga esta política podrá ser investigado y puede ser causal de sanciones, sin perjuicio de las acciones disciplinarias y/o jurídicas.

9. VALIDEZ Y GESTIÓN DE DOCUMENTOS

Este documento es válido desde su implementación y socialización.

Este documento está validado por el Oficial de Seguridad de Información (Director de Procesos) del MIES.

El propietario del documento es el área de Seguridad, Interoperabilidad y Riesgos del MIES, para la verificación, y si es necesario actualización del presente documento.

10. POLÍTICAS, PROCEDIMIENTOS Y MANUALES RELACIONADOS

- Acuerdo Ministerial 000080 de fecha 9 de Abril de 2015.
- Acuerdo Ministerial 166, EGSI, y su última modificación del 15 de junio de 2016.
- Acuerdo Ministerial 013, Código Cero Tolerancia a la Corrupción del MIES de fecha 26 febrero de 2018.

11. GLOSARIO

PORTAL CAUTIVO: es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal. El programa intercepta todo el tráfico HTTP hasta que el usuario se autentifica

MESA DE SERVICIOS: Es la herramienta destinada para la gestión y solución de todas las posibles incidencias y requerimientos de recursos y servicios de tecnológicos.

PERFIL: Es un entorno personalizado específicamente para un usuario o grupo de usuarios. Contiene configuración de los programas de acuerdo a las características por área de trabajo y responsabilidad.

PLATAFORMA: Es un sistema que sirve como base para hacer funcionar determinados módulos de hardware o de software con los que es compatible. Dicho sistema está definido por un estándar alrededor del cual se determina una arquitectura de hardware y una plataforma de software (incluyendo entornos de aplicaciones).

USUARIO: Es una persona que utiliza un sistema informático. Para que los usuarios puedan obtener seguridad, acceso al sistema, administración de recursos, etc., dichos usuarios deberán identificarse.

DOMINIO: Es el conjunto de computadoras conectadas en una red informática que confían a uno de los equipos de dicha red, la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en dicha red.

SEGMENTACIÓN: Es dividir la red en varias subredes para mantener una mejor administración de recursos y proporcionar seguridad de forma dinámica.

MINISTERIO DE
INCLUSIÓN ECONÓMICA
Y SOCIAL

Toda una Vida

EL
GOBIERNO
DE TODOS

POLÍTICAS
PANTALLAS Y ESCRITORIOS LIMPIOS

ANEXO 4

Quito, Julio del 2018

DATOS GENERALES		
No. Doc.	MIES-CGTIC-DSIR-POL-2018-0004	
Tipo de documento	Políticas	
Institución	Ministerio de Inclusión Económica y Social	
Dirección Ejecutora	Coordinación General de Tecnologías de Información y Comunicación	
Fecha	05/07/2018	
Versión	1.0	
Elaborado por	**Cargo**	**Firma**
Ing. Katherine Colcha	Analista de Tecnologías de Información	
Revisado por	**Cargo**	**Firma**
Ing. Richarth Pazmiño MBA.	Director de Seguridad, Interoperabilidad y Riesgos	
Ing. Jorge Pichucho MGS.	Director de Infraestructura y Operaciones de TI	
Ing. Soledad Cueva	Director de Soporte a Usuarios de TI (E)	
Ing. Cristian Núñez	Director de Proyectos de TI (E)	
Validado por	**Cargo**	**Firma**
Lic. Rubén Ortega MGS.	Oficial de Seguridad de la Información	
Aprobado por	**Cargo**	**Firma**
Ing. Fabián Vallejo	Coordinador General de Tecnologías de Información y Comunicación	

CONTROL DE VERSIONES			
Fecha	**Versión**	**Responsable**	**Descripción**
05/07/2018	1.0	Ing. Katherine Colcha	Elaboración de las políticas

Contenido

1. INTRODUCCIÓN 4
2. ANTECEDENTES 4
3. JUSTIFICACIÓN 4
4. OBJETIVO 5
5. ALCANCE 5
6. RESPONSABILIDADES 5
7. POLÍTICAS DE PANTALLAS Y ESCRITORIOS LIMPIOS 5
   - 7.1. UBICACIÓN Y PROTECCIÓN DEL EQUIPAMIENTO 5
   - 7.2. ESCRITORIOS LIMPIOS Y SEGUROS 6
   - 7.3. PANTALLAS TRANSPARENTES / LIMPIAS 6
   - 7.4. EQUIPO DESATENDIDO DEL USUARIO 6
   - 7.5. EQUIPOS DE REPRODUCCIÓN DE INFORMACIÓN 6
   - 7.6. SALAS Y PIZARRAS LIMPIAS 7
   - 7.7. RESPONSABILIDADES DE USUARIO 7
8. MONITOREO DE SERVICIOS INFORMÁTICOS INSTITUCIONALES 7
9. CASOS ESPECIALES 7
10. AMONESTACIONES 8
11. VALIDEZ Y GESTIÓN DE DOCUMENTOS 8
12. POLÍTICAS, PROCEDIMIENTOS Y MANUALES RELACIONADOS 8
13. GLOSARIO 8

1. INTRODUCCIÓN

Las políticas de pantallas y escritorios limpios se refieren a la protección de cualquier tipo de información utilizada por los servidores públicos para el desarrollo de sus actividades.

Las políticas son proporcionadas con el objeto de apoyar las funciones que desempeñan los servidores y las servidoras públicas del Ministerio de Inclusión Económica y Social, explican el uso apropiado de la información institucional y las medidas consideradas para mantener un nivel aceptable de seguridad.

Cuando las políticas se ejecutan adecuadamente, aumentan la productividad de los servidores y servidoras públicas y protegen la información en la red interna e imagen institucional.

2. ANTECEDENTES

El Ministerio de Inclusión Económica y Social entrega servicios tecnológicos a los servidores públicos que laboran en la Institución, estos son administrados por parte de la Coordinación General de Tecnologías de Información y Comunicación, misma que se encuentra alineada a las políticas de control, regulación y optimización de los recursos tecnológicos vigentes, lo cual permite la correcta gestión de acuerdo a las necesidades institucionales.

Se ha tomado el Esquema Gubernamental de Seguridad de la Información como guía de referencia en temas de seguridad informática.

La información puede estar contenida en:

- Escritorios
- Estaciones de trabajo
- Computadores portátiles
- Medios ópticos
- Medios magnéticos
- Documentos en papel
- Etc.

3. JUSTIFICACIÓN

El establecimiento de políticas es fundamental para alcanzar los objetivos institucionales.

Las políticas de pantallas y escritorios limpios permitirán otorgar seguridad a la información, disminuyendo el riesgo y propendiendo a la entrega eficiente de los recursos informáticos tanto a los servidores públicos como a la ciudadanía.

El Esquema Gubernamental de Seguridad de la Información en el punto 7. CONTROL DE ACCESO, 7.8. Política de puesto de trabajo despejado y pantalla limpia, establece con (*) los aspectos que se deben considerar como primordiales de cumplimiento para una buena gestión de control de accesos.
Es fundamental que estas políticas sean socializadas y cumplidas por cada servidor y servidora pública de esta Institución para de esta manera mejorar la seguridad en la gestión de los servicios tecnológicos en el MIES.

4. OBJETIVO

Definir y reglamentar las normas generales de pantallas y escritorios limpios, mejorando la seguridad de la información en la Institución.

5. ALCANCE

Las políticas de pantallas y escritorios limpios aplican a las y los servidores públicos que laboran en el Ministerio de Inclusión Económica y Social y utilizan servicios tecnológicos provistos por la misma.

Entre los temas tratados se encuentra: Ubicación y protección de equipos, Pantallas y Escritorios Limpios, Equipo desatendido.

6. RESPONSABILIDADES

El Ministerio de Inclusión Económica y Social a través de la Coordinación General de Tecnologías de Información y Comunicación proporcionará los servicios tecnológicos que serán utilizados en toda la Institución.

Cada usuario tiene la responsabilidad de cumplir con esta política.

Las autoridades institucionales son responsables de controlar el cumplimiento de esta política por parte de los servidores públicos bajo su unidad.

7. POLÍTICAS DE PANTALLAS Y ESCRITORIOS LIMPIOS

- La información generada o almacenada en medios institucionales es de propiedad del MIES y debe ser utilizada exclusivamente para las tareas propias de las funciones desarrollada en la Institución
- Para acceder a la información interna la persona debe tener relación laboral con la Institución, o contar con la autorización escrita de un funcionario del jerárquico superior

7.1. UBICACIÓN Y PROTECCIÓN DEL EQUIPAMIENTO

- Los lugares de trabajo de los funcionarios y personal que prestan servicios en la Institución deben localizarse preferentemente en ubicaciones que no queden expuestas al acceso de personas externas. De esta forma se protege tanto el equipamiento tecnológico como los documentos que está utilizando el funcionario
- Los equipos que estén ubicados cerca de zonas de atención o tránsito de público, deben situarse de forma que las pantallas no puedan ser visualizadas por personas no autorizadas y deben ser asegurados mediante candado de seguridad u otro medio que impida que sean sustraídos
- No se deben ingerir alimentos o bebidas cerca de los equipos o dispositivos de procesamiento de información, así como no colocar o manipular líquidos en su cercanía

7.2. ESCRITORIOS LIMPIOS Y SEGUROS

Un puesto de trabajo que posee un escritorio desordenado es un sitio vulnerable, ya que la información personal y profesional con carácter confidencial o sensible puede estar expuesta. Por tal razón se debe tomar las siguientes acciones:

- Al finalizar la jornada de trabajo, el funcionario debe guardar en un lugar seguro los documentos, medios magnéticos u óptico removible que contengan información confidencial o de uso interno
- No utilizar hojas con información confidencial para reciclaje
- Utilizar los recursos asignados, para almacenar los activos de información sensible.
- Queda terminantemente prohibido tener sustancias y/o líquidos en su escritorio que pudieran dañar documentos originales y/o equipo de trabajo y la información almacenada en ellos
- Destruir en forma efectiva los documentos sensibles que tiró al canasto de basura (usar máquinas picadoras de papel)

7.3. PANTALLAS TRANSPARENTES / LIMPIAS

- Las estaciones de trabajo y equipos portátiles deben tener aplicado el estándar relativo a protector de pantalla definido por la Institución, de forma que se active luego de cinco minutos (5') de inactividad
- La pantalla de autenticación a la red de la Institución debe requerir solamente la identificación de la cuenta, clave y no entregar más información
- El escritorio de la computadora no debe poseer archivos o carpetas con accesos directos que faciliten la ubicación de información
- El único fondo de pantalla autorizado para los usuarios que utilizan equipos o logotipos, son los que defina la Institución

7.4. EQUIPO DESATENDIDO DEL USUARIO

- Toda vez que un funcionario se ausenta de su lugar de trabajo, para asistir a alguna reunión, capacitación, entre otros, debe bloquear su equipo y verificar que no exista información sensible o documentos sobre el escritorio; esto evitará vulnerabilidades y pérdidas de información
- Todos los usuarios deben apagar su equipo de cómputo al finalizar su jornada de trabajo

7.5. EQUIPOS DE REPRODUCCIÓN DE INFORMACIÓN

- Los equipos de reproducción de información (por ejemplo: impresoras, fotocopiadoras), deben estar ubicados en lugares con acceso controlado y cualquier documentación confidencial o sensible se debe retirar inmediatamente del equipo
- Restringir el uso de fotocopiadoras y otra tecnología de reproducción a usuarios no autorizados
- Implementar el control de uso de fotocopiado y escaneo con el uso de clave, en los equipos que tengan esas funcionalidades. Para futuras adquisiciones se debe contar con equipos con estas funcionalidades

7.6. SALAS Y PIZARRAS LIMPIAS

- Las salas o áreas de reuniones, salas de conferencias y de capacitación, deben quedar limpias de todo el material utilizado
- Después de las reuniones en que se utilicen pizarras, estas deben quedar limpias de la información que se ha expuesto en ellas
- En caso que se utilice una computadora para presentaciones, si éste fuera de uso común, debe eliminarse la información antes presentada
- Velar que las salas de reuniones permanezcan cerradas y será exclusivo para reuniones de trabajo
- Todo equipo (computadoras, proyector, aire acondicionado, ventiladores, y otros) que fuere utilizado en las salas de reuniones, deben permanecer apagados, así mismo se deben retirar los documentos utilizados para evitar exposición y/o pérdida de información y desperdicio de energía eléctrica

7.7. RESPONSABILIDADES DE USUARIO

- Todos los usuarios del Ministerio de Inclusión Económica y Social que ingresan a la Institución deben utilizar los servicios tecnológicos provistos por la Institución
- Al momento de utilizar información, sistemas o aplicaciones institucionales, cada usuario está aceptando la responsabilidad y confidencialidad del uso y manejo de los servicios e información institucional
- Los servidores públicos del Ministerio de Inclusión Económica y Social son responsables de los usuarios, contraseñas, servicios tecnológicos e información utilizados
- Si un funcionario debiera cambiar de equipo, ya sea por reemplazo del mismo o por traslado a otra unidad, el funcionario deberá solicitar apoyo tecnológico a la Dirección de Soporte a Usuarios mediante la Mesa de Servicios
- Todos los funcionarios o terceros que tengan un usuario o manejen información de la Institución, deberán conocer y cumplir con esta política, donde se dictan pautas sobre derechos y deberes con respecto al manejo apropiado de información el MIES

8. MONITOREO DE SERVICIOS INFORMÁTICOS INSTITUCIONALES

El Ministerio de Inclusión Económica y Social a través de la Coordinación General de Tecnologías de Información y Comunicación monitoreará los servicios tecnológicos entregados con el fin de evitar anomalías que interfieran en la alta disponibilidad de los mismos.

9. CASOS ESPECIALES

En ciertas ocasiones o casos especiales, esta política no se podrá aplicar en su totalidad, estos casos deberán ser analizados por las Direcciones de la Coordinación de TIC involucradas, quienes evaluarán la pertinencia y los riesgos asociados y permitirán o negarán la excepción.

Los casos especiales son los que no se encuentren contemplados en ésta política y deberán ser informados de manera escrita a la Dirección de Seguridad, Interoperabilidad y Riesgos para su registro y evaluación.

10.AMONESTACIONES

Cualquier servidor público del MIES, que sea encontrado realizando actividades que contravenga esta política podrá ser investigado y puede ser causal de sanciones, sin perjuicio de las acciones disciplinarias y/o jurídicas.

11.VALIDEZ Y GESTIÓN DE DOCUMENTOS

Este documento es válido desde su implementación y socialización.

Este documento está validado por el Oficial de Seguridad de Información (Director de Procesos) del MIES.

El propietario del documento es el área de Seguridad, Interoperabilidad y Riesgos del MIES, para la verificación, y si es necesario actualización del presente documento.

12.POLÍTICAS, PROCEDIMIENTOS Y MANUALES RELACIONADOS

- Acuerdo Ministerial 000080 de fecha 9 de Abril de 2015
- Acuerdo Ministerial 166, EGSI, y su última modificación del 15 de junio de 2016
- Acuerdo Ministerial 013, Código Cero Tolerancia a la Corrupción del MIES de fecha 26 febrero de 2018

13. GLOSARIO

ACTIVOS DE INFORMACIÓN: Información de propiedad del MIES, sus medios de almacenamiento y procesamiento, que son considerados críticos para el cumplimiento de los procesos y objetivos de la Institución.

INFORMACIÓN SENSIBLE: es aquella a la cual la ley tiene prohibido divulgar, ya que perjudica la seguridad nacional, o la intimidad personal; por ejemplo, ciertos datos personales y bancarios, contraseñas de correos electrónicos. Estos son datos personales que solo pueden ser revelados con autorización del titular.

USUARIO: Es cualquier persona que acceda a los servicios de la Institución, y ello implica su adhesión plena e incondicional a estas Políticas, por lo tanto es responsabilidad del Usuario leerlas previamente, de tal manera que esté consciente de que se sujeta a ellas y a las modificaciones que pudieran sufrir.

PANTALLA LIMPIA: Es la protección de las computadoras, dispositivos móviles, u otros dispositivos, mediante un bloqueo de pantalla o desconexión cuando no están en uso.

ESCRITORIO LIMPIO: Es la protección de los papeles y dispositivos removibles de información, almacenados y manipulados en estaciones de trabajo (escritorio, oficina, etc.), de accesos no autorizados, pérdida y/o daño de la información durante y fuera de las horas normales de trabajo.

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.

TI: Tecnologías de la Información.

MEDIOS ÓPTICOS: Los discos ópticos son un producto de almacenamiento de datos que guarda el contenido en formato digital; estos discos se pueden escribir y leer mediante un láser que generalmente se encuentra en su computadora.

MEDIOS MAGNÉTICOS: Son dispositivos que utiliza materiales magnéticos para archivar información digital, tales como los disquetes, los discos duros o los CD que almacenan grandes volúmenes de datos en un espacio físico pequeño.

MINISTERIO DE
INCLUSIÓN ECONÓMICA
Y SOCIAL

Toda una Vida

EL
GOBIERNO
DE TODOS

POLÍTICAS

RESPALDO, RESGUARDO Y RECUPERACIÓN DE LA INFORMACIÓN DE LOS SISTEMAS QUE ADMINISTRA EL MIES

ANEXO 5

Quito, Julio del 2018

DATOS GENERALES		
No. Doc.	MIES-CGTIC-DSIR-POL-2018-0005	
Tipo de documento	Políticas	
Institución	Ministerio de Inclusión Económica y Social	
Dirección Ejecutora	Coordinación General de Tecnologías de Información y Comunicación	
Fecha	30/07/2018	
Versión	1	
Elaborado por	**Cargo**	**Firma**
Ing. Katherine Colcha	Analista de Tecnologías de Información	
Revisado por	**Cargo**	**Firma**
Ing. Richarth Pazmiño MBA.	Director de Seguridad, Interoperabilidad y Riesgos	
Ing. Jorge Pichucho MGS.	Director de Infraestructura y Operaciones de TI	
Ing. Soledad Cueva	Director de Soporte a Usuarios de TI (E)	
Ing. Cristian Núñez	Director de Proyectos de TI (E)	
Validado por	**Cargo**	**Firma**
Lic. Rubén Ortega MGS.	Oficial de Seguridad de la Información	
Aprobado por	**Cargo**	**Firma**
Ing. Fabián Vallejo	Coordinador General de Tecnologías de Información y Comunicación	

CONTROL DE VERSIONES			
Fecha	**Versión**	**Responsable**	**Descripción**
30/07/2018	1.0	Ing. Katherine Colcha	Elaboración de las políticas.

Contenido

1. INTRODUCCIÓN 4
2. ANTECEDENTES 4
3. JUSTIFICACIÓN 4
4. OBJETIVO 4
5. ALCANCE 5
6. RESPONSABILIDADES 5
7. POLÍTICAS DE RESPALDO, RESGUARDO Y RECUPERACIÓN DE LA INFORMACIÓN DE LOS SISTEMAS QUE ADMINISTRA EL MIES 5
7.1. Definición de Activos Críticos 5
7.2. Etiquetado 6
7.3. Registros de Auditoria 6
7.4. Frecuencia y Tipo de Respaldos 6
7.5. Vigencia y Retención de los Respaldos 6
7.6. Respaldos de Estaciones de Trabajo 7
7.7. Medios de Almacenamiento 7
7.8. Manejo y Seguridad de Medios de Almacenamiento 7
7.9. Protección de la información en medios de respaldo 7
7.10. Pruebas de Restauración 8
8. COMPROMISO DE TODO EL PERSONAL DE LA INSTITUCIÓN 8
9. IDENTIFICACIÓN DE RIESGOS 9
10. AMONESTACIONES 9
11. VALIDEZ Y GESTIÓN DE DOCUMENTOS 9
12. POLÍTICAS, PROCEDIMIENTOS Y MANUALES RELACIONADOS 9
13. GLOSARIO 9

1. INTRODUCCIÓN

La información es un recurso importante dentro del Ministerio de Inclusión Económica y Social para el cumplimiento de los objetivos estratégicos porque permite la toma de decisiones a las autoridades encargadas de la gestión de servicios a los usuarios internos y externos.

Mediante la presente política se establece el marco referencial con lineamientos generales aplicables a la información sensible, de alta criticidad o confidencial del Ministerio de Inclusión Económica y Social, referente a los procedimientos de respaldo, resguardo y recuperación de la información, que se debe realizar en la Institución.

2. ANTECEDENTES

El Ministerio de Inclusión Económica y Social entrega servicios en los cuales se gestiona información confidencial de grupos de atención prioritaria y la población que se encuentra en situación de pobreza y vulnerabilidad que reciben los servicios institucionales, la cual debe ser manejada y respaldada de forma segura y oportuna.

El Esquema Gubernamental de Seguridad de la Información EGSI establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información.

3. JUSTIFICACIÓN

El establecimiento de políticas de respaldo, resguardo y recuperación es fundamental para garantizar la continuidad de los servicios institucionales para los usuarios internos y externos.

Las políticas de respaldo, resguardo y recuperación de la información, incrementará la seguridad de la información manejada en los servicios tecnológicos del MIES.

El EGSI establece: "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".

4. OBJETIVO

Establecer 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 Económica y Social.

5. ALCANCE

Esta política es aplicable a toda la información electrónica contenida en los servidores, estaciones de trabajo y equipos comunicacionales que contengan información, configuraciones, aplicativos y servicios críticos del MIES.

Esta política se aplica a todos los funcionarios del MIES, independientemente del tipo de régimen laboral en que se encuentren, y a terceros que presten servicios al Ministerio de Inclusión Económica y Social.

Esta política debe ser revisada y/o actualizada anualmente, o cuando se considere necesario por la Dirección de Seguridad, Interoperabilidad y Riesgos de la Coordinación General de Tecnologías de Información y Comunicación.

6. RESPONSABILIDADES

El Ministerio de Inclusión Económica y Social a través de la Coordinación General de Tecnologías de Información y Comunicación proporcionará los servicios tecnológicos y los lineamientos que en temas de manejo seguro de la información del MIES.

Cada usuario tiene la responsabilidad de cumplir con esta política.

Las autoridades institucionales son responsables de controlar el cumplimiento de esta política por parte de los usuarios bajo su unidad.

7. POLÍTICAS DE RESPALDO, RESGUARDO Y RECUPERACIÓN DE LA INFORMACIÓN DE LOS SISTEMAS QUE ADMINISTRA EL MIES

Aplicar el EGSI para el manejo, respaldo, restauración y recuperación de activos informáticos del MIES.

7.1. Definición de Activos Críticos

Los responsables de las unidades del MIES, serán los encargados de identificar los activos críticos de aquella información que sus departamentos necesitan para mantener operativo sus procesos, durante eventuales eventos de restauración. La Coordinación General de TIC a través de sus direcciones establecerá un esquema de prioridad y periodicidad de respaldo, resguardo y recuperación de los activos informáticos generados u obtenidos, cuyo proceso debe ser validado por el técnico responsable de la administración del activo, de acuerdo a un procedimiento establecido internamente en el área.

Para todos los sistemas del MIES, se debe definir el procedimiento que incluyan principalmente:

- Generación de copias de respaldo de la información, aplicaciones, configuraciones, etc
- Restauración de los respaldos

- Inventario de los respaldos y bitácoras de respaldos

7.2. Etiquetado

Todas las copias de respaldo deberán estar claramente identificadas, con etiquetas que indiquen como mínimo:

- Nombre del servidor
- Identificación (Nombre que identifique lo que contiene)
- Tipo de respaldo (completo, incremental o diferencial)
- Frecuencia: (anual, mensual, semanal, diario)
- Fecha de respaldo
- Responsable designado

7.3. Registros de Auditoria

Toda ejecución de respaldo, ya sea de forma manual o automática, debe generar un registro (logs) en el equipo, que permita la revisión del resultado de la ejecución.

7.4. Frecuencia y Tipo de Respaldos

Las direcciones que conforman la Coordinación General de TIC y las direcciones que sean responsables de manejos de información son responsables de establecer el Plan de Respaldos, determinar los procedimientos de respaldo, resguardo y recuperación de los activos informáticos, su implementación y actualización. Se deberá contemplar de manera obligatoria, respaldos de bases de datos, logs, aplicaciones y configuraciones.

Las direcciones responsables deberán planificar la obtención o ejecución de los respaldos, de tal manera que no afecte la disponibilidad de los servicios del MIES.

Tipos de respaldos:

1. **Respaldo completo o Total:** Considera toda la información comprendida en el servidor
2. **Respaldo Incremental:** Se respaldarán los archivos creados a diario
3. **Respaldo Diferencial:** Se respaldarán todos los archivos modificados y creados en la semana

7.5. Vigencia y Retención de los Respaldos

Las direcciones responsables conjuntamente con los dueños o responsables técnicos de los activos de información, debe definir los periodos de retención de la información en función de la naturaleza de la misma, con el fin de garantizar la continuidad del negocio y la consulta histórica de su información, esta información debe estar contemplada en el Plan de Respaldos, considerando como base el artículo 10 .- Conservación de documentación, del Reglamento de Archivos de Contraloría General del Estado, que indica que, "La documentación sujeta a control y seguimiento institucional, deben ser conservadas durante 7 años, contados a partir de la fecha de emisión de la misma, sea

formato físico o digital".

Es responsabilidad de los dueños o responsables técnicos de los activos de información, constatar de forma periódica, el valor y la utilidad de la información almacenada.

7.6. Respaldos de Estaciones de Trabajo

Es responsabilidad de cada servidor público, el debido respaldo de la información contenida en el computador asignado (estaciones de trabajo o portátiles), para lo cual la Dirección de Infraestructura y Operaciones de TI asignará una carpeta o recurso compartido para cada usuario, con un límite de cuota en el servidor de repositorio de datos.

Cualquier necesidad de respaldo urgente, debe ser solicitada formalmente por el jefe de la unidad administrativa mediante la Mesa de Servicio.

7.7. Medios de Almacenamiento

Las direcciones responsables deberán definir los medios de almacenamiento a utilizar acorde a las necesidades de la Institución, llevando un control de su uso y vigencia.

El uso y aprovechamiento de los medios de respaldo será destinado únicamente para las funciones que son propias de la Institución.

Queda estrictamente prohibido almacenar en los respaldos, archivos de juegos, música, videos y cualquier otra información ajena a la Institución.

Ante cambios tecnológicos que se produzca en los medios de respaldos, que pueda generar obsolescencia tecnológica, deben generarse las acciones necesarias de resguardo de información en ellos.

7.8. Manejo y Seguridad de Medios de Almacenamiento

Las direcciones responsables deben implementar una bitácora de respaldos, en la que se lleve el registro de todos los respaldos realizados de los servicios tecnológicos.

Los medios de almacenamiento con información sensible o copias de respaldo, debe ser manipulado, custodiados única y exclusivamente por el personal delegado por el director de la dirección responsable de realizar los respaldos.

Los sitios donde se almacenan las copias de respaldo deben ser físicamente seguros, con los controles físicos y ambientales según normas y estándares, en el caso de no poseer esta infraestructura se debe transferir a un tercero (proveedor) que garantice este servicio.

7.9. Protección de la información en medios de respaldo

El MIES debe respaldar la información, en un sitio lejano, localizado a una distancia tal, que sea suficiente para evitar cualquier daño producido por desastres en la sede principal

de la Institución. Dicho respaldo debe tener registros exactos y completos de las copias; como también procedimientos documentados de recuperación.

Las direcciones responsables deberán mantener un inventario actualizado de la información almacenada en el sitio lejano.

Solamente el técnico asignado por el director de la dirección responsable es el encargado de la entrega y retiro de los respaldos de información del sitio lejano.

Toda información de respaldos que es almacenada fuera de la Institución, debe ser trasladada con los elementos de seguridad adecuados de acuerdo al procedimiento definido por la dirección responsable.

7.10. Pruebas de Restauración

Se debe efectuar pruebas planificadas de recuperación o restauración de las copias de respaldo por parte de los responsables técnicos de los activos y el custodio de los soportes de almacenamiento; al menos una vez al mes en un ambiente de pruebas adaptado para tal fin, con el objetivo de garantizar que la información almacenada y protegida, se pueda extraer de forma confiable de los diferentes medios de almacenamiento en caso de una eventual restauración.

Las pruebas de recuperación se deben formalizar en un acta escrita y firmada por el responsable técnico y el custodio de los soportes de almacenamiento siguiendo un procedimiento establecido.

La Dirección de Seguridad, Interoperabilidad y Riesgos, verificará o realizará el seguimiento del procedimiento de restauración de forma periódica o cuando lo requiera.

8. COMPROMISO DE TODO EL PERSONAL DE LA INSTITUCIÓN

El personal de la Institución acepta esta Política de Respaldo, Resguardo y Recuperación como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información del MIES.

El personal de la Institución demuestra su compromiso a través de:

- La aceptación de las Políticas de Respaldo, Resguardo y Recuperación de la Información de los Sistemas que Administra el MIES contenidas en este documento
- La promoción activa de una cultura de seguridad
- Facilitar la socialización de este documento a todos los funcionarios de la entidad
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de Respaldo, Resguardo y Recuperación de la Información de los Sistemas que Administra el MIES
- La verificación del cumplimiento de las políticas

9. IDENTIFICACIÓN DE RIESGOS

En cumplimiento al Acuerdo No. 166 del Esquema Gubernamental de Seguridad de la Información – EGSI, en el Artículo 7 "Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos, en base a la norma INEN ISO/IEC:27005 "Gestión del Riesgo en la Seguridad de la Información".

10. AMONESTACIONES

Cualquier usuario del MIES, que sea encontrado realizando actividades que contravenga esta política podrá ser investigado y puede ser causal de sanciones, sin perjuicio de las acciones disciplinarias y/o jurídicas.

11. VALIDEZ Y GESTIÓN DE DOCUMENTOS

Este documento es válido desde su implementación y socialización.

Este documento está validado por el Oficial de Seguridad de Información (Director de Procesos) del MIES.

El propietario del documento es el área de Seguridad, Interoperabilidad y Riesgos del MIES, para la verificación, y si es necesario actualización del presente documento.

12. POLÍTICAS, PROCEDIMIENTOS Y MANUALES RELACIONADOS

- Acuerdo Ministerial 000080 de fecha 9 de Abril de 2015
- Acuerdo Ministerial 166, EGSI, y su última modificación del 15 de junio de 2016
- NTC ISO 17799: "Seguridad de la Información" Punto 10.5 "Las copias de respaldo de información y software deberían ser realizadas y probadas con regularidad, conforme a la política de seguridad y de continuidad de negocio"
- NTC ISO 27001 basado en el código de buenas prácticas y objetivos de control el Anexo A, dominio de Control A.12 Seguridad en la Operación - Numeral: A.12.3. Copias de Seguridad, A.12.3.1. Copias de seguridad de la Información, cuyo objetivo es mantener la integridad y disponibilidad de los servicios de tratamiento de información y comunicación.
- Ley Orgánica de Transparencia y Acceso a la Información Pública.

13. GLOSARIO

RESGUARDO: Es proteger la información del computador, hacer una copia de seguridad o copia de respaldo de datos de tal forma que estas copias adicionales puedan restaurar un sistema después de una pérdida de información.

DISPONIBILIDAD: Es la propiedad en la cual la información sea accesible y utilizable por

solicitud de una entidad autorizada.

INTEGRIDAD: Es la protección de la exactitud y estado completo de los activos.

PROPIETARIO DE LA INFORMACIÓN: Es la persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.

SEGURIDAD DE LA INFORMACIÓN – SI: Es la preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad (accountability), no repudio y fiabilidad.

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

MINISTERIO DE
INCLUSIÓN ECONÓMICA
Y SOCIAL

EL GOBIERNO DE TODOS

POLÍTICAS

USO DE DISPOSITIVOS PROPIOS
(Bring Your Own Device – BYOD)

ANEXO 6

Quito, Septiembre del 2018

DATOS GENERALES		
No. Doc.	MIES-CGTIC-DSIR-POL-2018-0006	
Tipo de documento	Políticas	
Institución	Ministerio de Inclusión Económica y Social	
Dirección Ejecutora	Coordinación General de Tecnologías de Información y Comunicación	
Fecha	27/09/2018	
Versión	1	
Elaborado por	**Cargo**	**Firma**
Ing. Katherine Colcha	Analista de Tecnologías de Información	
Revisado por	**Cargo**	**Firma**
Ing. Richarth Pazmiño MBA.	Director de Seguridad, Interoperabilidad y Riesgos	
Ing. Jorge Pichucho Mgs.	Director de Infraestructura y Operaciones de TI	
Ing. Soledad Cueva	Director de Soporte a Usuarios de TI (E)	
Ing. Cristian Núñez	Director de Proyectos de TI (E)	
Validado por	**Cargo**	**Firma**
Lic. Rubén Ortega Mgs.	Oficial de Seguridad de la Información	
Aprobado por	**Cargo**	**Firma**
Ing. Fabián Vallejo	Coordinador General de Tecnologías de Información y Comunicación	

CONTROL DE VERSIONES			
Fecha	**Versión**	**Responsable**	**Descripción**
27/09/2018	1.0	Ing. Katherine Colcha	Elaboración de las políticas.

Contenido

1. INTRODUCCIÓN 4
2. ANTECEDENTES 4
3. JUSTIFICACIÓN 4
4. OBJETIVO 4
5. ALCANCE 5
6. RESPONSABILIDADES 5
7. POLÍTICAS DE USO DE DISPOSITIVOS PROPIOS – BYOD 5
   - 7.1. Política BYOD 5
   - 7.2. Uso de dispositivos propios 6
     - 7.2.1. Utilización BYOD 6
     - 7.2.2. Dispositivos contemplados en el BYOD 6
     - 7.2.3. Uso aceptable 6
   - 7.3. Prohibiciones 6
   - 7.4. Reembolso 6
   - 7.5. Derechos Especiales 7
   - 7.6. Guía de Conducta – Violaciones de Seguridad 7
   - 7.7. Acuerdo 7
8. COMPROMISO DE TODO EL PERSONAL DE LA INSTITUCIÓN 7
9. IDENTIFICACIÓN DE RIESGOS 7
10. AMONESTACIONES 8
11. VALIDEZ Y GESTIÓN DE DOCUMENTOS 8
12. POLÍTICAS, PROCEDIMIENTOS Y MANUALES RELACIONADOS 8
13. GLOSARIO 8

1. INTRODUCCIÓN

Las siglas BYOD (Bring your own device – Traiga su propio dispositivo), se refiere a que el usuario o empleado lleve su propio dispositivo a su lugar de trabajo para tener acceso a recursos de la Institución, tales como correos electrónicos y archivos en equipos informáticos así como datos y aplicaciones personales. También se le conoce como «bring your own technology» (BYOT, trae tu propia tecnología), de esta manera se expresa un ámbito mucho más amplio porque ya que no sólo cubre el equipo, sino que también cubre al software.

Mediante la presente política se establece el marco referencial con lineamientos generales en la utilización de dispositivos observando la protección de la información.

2. ANTECEDENTES

El Ministerio de Inclusión Económica y Social entrega servicios en los cuales se gestiona información confidencial de grupos de atención prioritaria y la población que se encuentra en situación de pobreza y vulnerabilidad que reciben los servicios institucionales, la cual debe ser manejada y respaldada de forma segura y oportuna.

El Esquema Gubernamental de Seguridad de la Información EGSI establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información.

En este documento se identifica los dispositivos BYOD permitidos dentro de la Institución.

3. JUSTIFICACIÓN

El establecimiento de políticas de uso de dispositivos propios es fundamental para determinar los parámetros de utilización de dispositivos tecnológicos por servidores públicos del Ministerio de Inclusión Económica y Social y usuarios externos autorizados para el uso de servicios tecnológicos institucionales.

El EGSI establece: "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".

4. OBJETIVO

Definir lineamientos para el uso de dispositivos propios en el Ministerio de Inclusión Económica y Social.

5. ALCANCE

Esta política se aplica a todos los dispositivos personales autorizados para conectarse a la red institucional, sea de forma inalámbrica o cableada.

Esta política se aplica a todos los funcionarios del MIES, independientemente del tipo de régimen laboral en que presten servicios al Ministerio de Inclusión Económica y Social.

La política debe ser revisada y/o actualizada anualmente, o cuando se considere necesario por la Dirección de Seguridad, Interoperabilidad y Riesgos de la Coordinación General de Tecnologías de Información y Comunicación.

6. RESPONSABILIDADES

El Ministerio de Inclusión Económica y Social a través de la Coordinación General de Tecnologías de Información y Comunicación proporciona los servicios tecnológicos y los lineamientos en temas de manejo seguro de la información del MIES.

La Dirección de Seguridad, Interoperabilidad y Riesgos se encargará de revisar y gestionar la aprobación de los permisos de accesos especiales a la red e internet.

Cada usuario tiene la responsabilidad de cumplir con esta política.

Las autoridades institucionales son responsables de cumplir y controlar el cumplimiento de esta política por parte de los usuarios bajo su unidad.

7. POLÍTICAS DE USO DE DISPOSITIVOS PROPIOS – BYOD

Las políticas se aplican para los BYOD que contengan información institucional, dentro o fuera de las instalaciones de MIES.

7.1. Política BYOD

El uso de dispositivos propios está permitido únicamente para el Jerárquico Superior y está prohibido para el resto de servidores públicos del MIES y terceros que presten servicios a la Institución.

Los dispositivos propios solo podrán ser utilizados previa autorización; para lo cual es indispensable enviar un requerimiento mediante la Mesa de Servicios con el respectivo formulario de SOLICITUD DE ACCESOS ESPECIALES A LA RED E INTERNET, con la debida justificación.

En caso de requerir algún funcionario, solamente podrá autorizar el jerárquico superior inmediato, con la debida justificación.

Los datos que se almacenan, transfieren o procesan en BYOD siguen perteneciendo a la

Institución, la cual tiene el derecho de controlar, aunque no sea propietaria del dispositivo.

7.2. Uso de dispositivos propios

7.2.1. Utilización BYOD

La Dirección de Soporte a Usuarios de TI debe mantener un registro actualizado de los funcionarios, equipos, permisos y fechas en las que se permite la utilización de los BYOD.

7.2.2. Dispositivos contemplados en el BYOD

Laptops, teléfonos inteligentes, tablets, etc.

7.2.3. Uso aceptable

A los funcionarios que tienen autorizado el uso de los Dispositivos BYOD se recomienda que:

- Los dispositivos deben estar protegidos contra códigos maliciosos y virus.
- La información sensible de la Institución que se encuentre en los dispositivos BYOD debe estar encriptada o con clave de acceso.
- Los dispositivos deben estar configurados con usuario, contraseña y bloqueo automático; lo cual es responsabilidad del propietario.
- Cuando se utiliza BYOD fuera de la Institución, el propietario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- Evitar conectarse a redes inalámbricas desconocidas.
- Los sistemas operativos y las aplicaciones de los dispositivos BYOD debe estar actualizados, lo cual es responsabilidad del propietario del dispositivo.

7.3. Prohibiciones

Es prohibido realizar lo siguiente con los dispositivos propios (BYOD):

- Permitir el acceso a la información de la Institución a cualquier persona que no sea el propietario del BYOD o funcionario de la Institución.
- Compartir o almacenar claves de los sistemas del MIES.

7.4. Reembolso

El Ministerio de Inclusión Económica y Social no pagará a los funcionarios (los propietarios de BYOD) ningún costo por el uso del dispositivo con fines laborales, robo o daño de los mismos.

7.5. Derechos Especiales

La Institución tiene el derecho de ver, editar y borrar todos los datos de la Institución que se encuentran almacenados, transferidos o procesados en los dispositivos (BYOD).

La Dirección de Soporte a Usuarios de TI está autorizada a configurar cualquier dispositivo propio en conformidad con la presente política.

La Dirección de Seguridad, Interoperabilidad y Riesgos está autorizada a controlar el uso de dispositivos BYOD a través de herramientas tecnológicas institucionales.

El Ministerio de Inclusión Económica y Social tiene el derecho de realizar el borrado completo de todos los datos del BYOD, si considera que es necesario para la protección de la información de la Institución, sin el consentimiento del propietario del dispositivo.

7.6. Guía de Conducta – Violaciones de Seguridad

Todas las violaciones de seguridad relacionadas con BYOD deben ser reportadas inmediatamente a la Dirección de Seguridad, Interoperabilidad y Riesgos a través del correo electrónico: seguridad.interoperabilidad@inclusion.gob.ec.

7.7. Acuerdo

La solicitud de uso de dispositivos BYOD debe ser ingresada mediante la Mesa de Servicios, adjuntando el respectivo formulario de SOLICITUD DE ACCESOS ESPECIALES A LA RED E INTERNET, con la debida justificación e indicando el tiempo requerido

8. COMPROMISO DE TODO EL PERSONAL DE LA INSTITUCIÓN

El personal de la Institución acepta esta Política de Uso de Dispositivos Propios – BYOD como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información del MIES.

El personal de la Institución demuestra su compromiso a través de:

- La aceptación de las Políticas de Uso de Dispositivos Propios – BYOD contenidas en este documento
- El cumplimiento de las políticas de Uso de Dispositivos Propios

9. IDENTIFICACIÓN DE RIESGOS

En cumplimiento al Acuerdo No. 166 del Esquema Gubernamental de Seguridad de la Información – EGSI, en el Artículo 7 "Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos, en base a la norma INEN ISO/IEC:27005 "Gestión del Riesgo en la Seguridad de la Información".

10. AMONESTACIONES

Cualquier usuario del MIES, que sea encontrado realizando actividades que contravenga esta política podrá ser investigado y puede ser causal de sanciones, sin perjuicio de las acciones disciplinarias y/o jurídicas.

11. VALIDEZ Y GESTIÓN DE DOCUMENTOS

Este documento es válido desde su implementación y socialización.

Este documento está validado por el Oficial de Seguridad de Información (Director de Procesos) del MIES.

El propietario del documento es el área de Seguridad, Interoperabilidad y Riesgos del MIES, para la verificación, y si es necesario actualización del presente documento.

12. POLÍTICAS, PROCEDIMIENTOS Y MANUALES RELACIONADOS

- Acuerdo Ministerial 000080 de fecha 9 de Abril de 2015
- Acuerdo Ministerial 166, EGSI, y su última modificación del 15 de junio de 2016
- Acuerdo Ministerial 013, Cero Tolerancia a la Corrupción.

13. GLOSARIO

BYOD – Bring Your Own Device: Son herramientas basadas en tecnologías de gestión de movilidad que permiten la protección de estos dispositivos. Incorporan mecanismos de autenticación accediendo a las aplicaciones y datos en cualquier dispositivo.
DISPOSITIVO MÓVIL: se puede definir como un aparato de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, que ha sido diseñado específicamente para una función, pero que puede llevar a cabo otras funciones más generales.
INFORMACIÓN SENSIBLE: Es aquella a la cual la ley tiene prohibido divulgar, ya que perjudica la seguridad nacional, o la intimidad personal; por ejemplo, ciertos datos personales y bancarios, contraseñas de correos electrónicos. Estos son datos personales que solo pueden ser revelados con autorización del titular.
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.
SOFTWARE: Son los programas informáticos que hacen posible la realización de tareas específicas dentro de un computador.
USUARIO: Es cualquier persona que acceda a los servicios de la Institución, y ello implica su adhesión plena e incondicional a esta Política, por lo tanto, es responsabilidad del Usuario leerlas previamente, de tal manera que esté consciente de que se sujeta a ellas y a las modificaciones que pudieran sufrir.
TI: El termino TI hace referencia a Tecnologías de la Información.