Ministerio de Educación

ACUERDO Nro. MINEDUC-ME-2014-00060-A

AUGUSTO X. ESPINOSA A.
MINISTRO DE EDUCACIÓN

CONSIDERANDO:

Que el artículo 227 de la Constitución de la República, dispone 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 Carta Magna en su artículo 212, establece que: *"Serán funciones de la Contraloría General del Estado, además de las que determine la ley: 1. Dirigir el sistema de control administrativo que se compone de auditoría interna, auditoría externa y del control interno de las entidades del sector público y de las entidades privadas que dispongan de recursos públicos. 2. Determinar responsabilidades administrativas y civiles culposas e indicios de responsabilidad penal, relacionadas con los aspectos y gestiones sujetas a su control, sin perjuicio de las funciones que en esta materia sean propias de la Fiscalía General del Estado";*

Que el Reglamento General Sustitutivo para el Manejo y Administración de Bienes del Sector Público, expedido en el Registro Oficial No. 378 de 17 de octubre del 2006, norma entre otros aspectos, el manejo y utilización de los bienes de propiedad de los organismos y entidades del sector público;

Que La Secretaría Nacional de la Administración Pública (SNAP) con fecha 19 de Septiembre del 2013, emite el Acuerdo 166, documento en el cual se establece que las entidades de la Administración Pública que dependen de la Función Ejecutiva deben implementar de forma obligatoria las normas NTE INEN-ISO/ IEC 27000, para la gestión de la Seguridad de la información. El SNAP, solicita a las entidades públicas, la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), que está basado en la norma INEN ISO/IEC 27002, con plazo de hasta marzo de 2014 para las directrices señaladas como prioritarias, y hasta marzo de 2015 para el resto de directrices;

Que el artículo 3 del Reglamento General Sustitutivo para el Manejo y Administración de Bienes del Sector Público, señala que es obligación de la máxima autoridad de cada entidad u organismo, el orientar y dirigir la correcta conservación y cuidado de los bienes públicos que han sido adquiridos o asignados para uso y que se hallen en poder de la entidad a cualquier título: depósito, custodia, préstamo de uso u otros semejantes, de acuerdo con dicho reglamento y las demás disposiciones que dicte la Contraloría General y el propio organismo o entidad;

Que mediante Acuerdo No. 039-CG, publicado en el Suplemento del Registro Oficial No. 87 de 14 de diciembre de 2009, la Contraloría General del Estado, expidió las Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de derecho privado que dispongan de recursos públicos, atribuyendo a la Unidad de Tecnología de Información la definición, documentación y difusión de las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización;

Que el artículo 1 del Acuerdo 039-CG del 16 de noviembre de 2009, establece que: *"[…] Las normas de control interno, que forman parte del presente acuerdo, tienen por objeto propiciar con su aplicación, el mejoramiento de los sistemas de control interno y la gestión pública, en relación a la utilización de los recursos estatales y la consecución de los objetivos institucionales. […]";*

Que el Estatuto Orgánico de Gestión Organizacional por Procesos del MINEDUC, emitido mediante Acuerdo No. 020 de 25 de enero de 2012, en el artículo 25 sobre Gestión Estratégica; establece como misión de la Dirección Nacional de Tecnologías de la Información y Comunicaciones: *"Planear y ejecutar proyectos y procesos de Tecnologías de la Información (TI) para la aplicación de políticas públicas y mejora de la gestión institucional y de los servicios a la ciudadanía, así como garantizar la operación de los sistemas y servicios informáticos, gestionar la seguridad informática, brindar soporte técnico en herramientas, aplicaciones, sistemas y servicios informáticos de la institución[…]";*

Que la Disposición General Primera del Acuerdo No. 020-12 de 25 de enero del 2012, señala que: *"Todas las atribuciones, funciones y productos relacionados a la gestión de tecnologías de información y comunicación y de soporte tecnológico para la gestión institucional interna que conforme el Estatuto Orgánico de Gestión Organizacional por Procesos del MINEDUC , se hallen asignadas a la Dirección Nacional de Tecnologías y Comunicaciones y de la Dirección Nacional Administrativa, y que se enmarquen en la misión determinada en el presente Acuerdo para la Coordinación General de Gestión Estratégica, serán cumplidas por la citada Coordinación General y sus respectivas Direcciones";*

Que el Acuerdo sobre Buen Uso de Recursos Tecnológicos del MINEDUC ACUERDO No. MINEDUC-ME-2014-00005-A de 04 de junio de 2014, establece la responsabilidad de los servidores públicos con respecto al buen uso de los recursos tecnológicos asignados para el trabajo diario de la Servidores Públicos pertenecientes al MINEDUC, así como el respeto a las normas de seguridad informática definidas por la Dirección Nacional de Tecnologías de la Información y Comunicaciones; y,

Que es necesario determinar las políticas y normas que regulen la designación, uso y control de los bienes y servicios tecnológicos y de comunicación que dispone el MINEDUC, de manera que se garantice su oportuna disponibilidad, optimización y calidad; así como la confidencialidad, integridad y disponibilidad de la información que manejen los servidores y servidoras y usuarios externos de la Institución; y, en general para la prestación de servicios de tecnología para la participación y control institucional y ciudadano en las actividades de planificación del Estado a cargo del MINEDUC.

En uso de las atribuciones que le confieren los artículos 154, apartado 1, de la Constitución de la República; 22, literales t) y u), de la Ley Orgánica de Educación Intercultural, y 17 del Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva.

ACUERDA:
Expedir el REGLAMENTO INTERNO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO I
ÁMBITO, OBJETO, ALCANCE, DEFINICIÓN Y POLÍTICA GENERAL

Art. 1.- Ámbito.- Las disposiciones contenidas en el presente reglamento son de cumplimiento obligatorio para todos las/los servidores públicos del MINEDUC a nivel nacional a quienes se les asigne el servicio o el uso del Activo de Información.

Art. 2.- Objetivo.- La presente normativa proporciona los lineamientos y apoyo para la regulación de la seguridad de la información en la institución, permitiendo el manejo de la información a los servidores públicos debidamente autorizados en el MINEDUC, garantizando la disponibilidad, integridad y confidencialidad de la información en todas sus instancias dentro de los procesos institucionales.

Art. 3.- Alcance.- La Política de Seguridad es la protección efectiva y eficiente de la información, que establece los siguientes alcances:
a) Aplica a todos los activos de información e infraestructura tecnológica de propiedad del MINEDUC.
b) Se establece como información sensible o sensitiva, a toda aquella información cuyo mal uso pudiere ocasionar perjuicios al MINEDUC (financieros, legales, imagen, fraudes, pérdidas en general, etc.).
c) Está orientada a garantizar el uso apropiado de los dispositivos tecnológicos durante su ciclo de vida (computadores de escritorio, portátiles, redes, aplicaciones, etc.) y de servicios como Internet y el correo electrónico.
d) Brinda a los servidores públicos pautas para la utilización apropiada de sus recursos, permitiendo minimizar los riesgos de una eventual pérdida de los activos de información.
e) Está orientada al control de protección de los activos de información en todos los ambientes internos y externos.

Art. 4.- Definición.- La Política General Institucional de Seguridad de la Información, se basa en el Sistema de Gestión de la Seguridad de la Información que utiliza las normas NTE INEN-ISO/IEC 27000 “Gestión de Seguridad de la Información” y NTE INEN-ISO/IEC 27002 "Código de Práctica para la Gestión de la Seguridad de la Información", aplicadas en el Esquema Gubernamental de Seguridad de la Información (EGSI), las cuales definen los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de la información del MINEDUC, en los medios físicos o electrónicos y en el tiempo que su legitimidad lo requiera, clasificada como pública, confidencial, reservada y no reservada.

Las y los servidores públicos deben cumplir las medidas y controles que garanticen el acceso, la protección y seguridad de la información y los recursos informáticos que se les ha asignado.

Art. 5.- Política General.- La Política de Seguridad de la Información involucra:
a) A todos las/los servidores públicos del MINEDUC en sus niveles de gestión (central-zonal-distrital), en su interactuación directa o indirecta con los Procesos/Plataformas/Sistemas/ de Información.
b) A todo el personal externo como consultores, contratistas, temporales o terceras partes que accedan a los activos de la información del MINEDUC, quienes están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de seguridad de información que las/los servidores públicos del MINEDUC.
c) Todas las personas que estén involucradas, deberán proteger la información, aún después de terminar su relación con el MINEDUC.

CAPITULO II
GLOSARIO DE TÉRMINOS

Art. 6.- La Política de Seguridad de la Información contiene las siguientes definiciones:

1) Seguridad de la Información.- Conjunto de metodologías, técnicas, estrategias, políticas, normas y procedimientos tendientes a minimizar las amenazas y riesgos continuos a los que está expuesta la información, preservando su disponibilidad, integridad y confidencialidad y el aseguramiento de la continuidad de las operaciones de la Institución.
2.) Seguridad Informática.- Conjunto de metodologías, políticas, técnicas, estrategias y procedimientos orientados a la protección del sistema informático, preservando la integridad, disponibilidad y confidencialidad de la información procesada en un sistema de informático.
3.) Activos de Información.- El activo de información es cualquier elemento que contiene información y represente valor para el soporte institucional. Todos los activos de información deberán estar claramente identificados dentro de un inventario; y pueden ser:
3.1.) Activo en relación con la seguridad de la información.- Se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.
3.2.) Activos de información en medios físicos o electrónicos.- Incluye bases de datos, documentación, manuales, software, hardware, contratos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo: calefacción, iluminación, energía y aire acondicionado y las personas, que son quienes generan, transmiten y destruyen información.
3.3.) Los activos de información se pueden clasificar en: activos de la información tecnológicos, activos de información físicos, activos de información intangibles, activos de entorno.
3.3.1) Activos de Información Tecnológicos.- Comprenden las Plataformas o Sistemas de Información a través de los cuales la institución desarrolla sus actividades y provee recursos y servicios a sus clientes como: recursos de software (aplicaciones, bases de datos, sistemas operativos, utilitarios, paquetes, scripts, firmware, sistemas de seguridad, servicios de comunicación, otros); recursos de hardware (servidores, PCs, firmware, equipos de comunicación, redes LAN, redes WAN, sistemas de respaldo, dispositivos de seguridad, dispositivos de almacenamiento, etc.); servicios computacionales y de comunicaciones; e información lógica sobre:

- Registros de auditoría.
- Información de archivo.
- Datos (en cualquiera de sus formas: archivos, bases de datos, datos cifrados, sonidos, imágenes, videos, otros).
- Meta-datos (estructuras, formatos, códigos, métodos de cifrado).
- Meta-información (información de la información, como por ejemplo, nombre de archivo, autor, versión, otros).

3.3.2.) Activos de Información Físicos: Documentos impresos o manuscritos.

3.3.3.) Activos de Información Intangibles: Ideas, conversaciones, conocimiento, calificaciones, competencias y experiencias.
3.3.4.) Activos de Entorno: Comprende lo siguiente:

- Los activos que se precisan para garantizar la operación de los activos tecnológicos;
- Equipamientos y suministros (energía, climatización); y
- Otros tangibles (edificaciones, mobiliario, instalación física).

4.) Disponibilidad.- Aquella autorización a los servidores públicos para acceder a la información y a los recursos relacionados con ella.

5.) Integridad.- Permite salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento, a través de las medidas de validación que permitirán detectar las modificaciones inapropiadas, la eliminación o la adulteración de los activos de información.
6.) Confidencialidad.- Garantizar que la información sea accesible solo a aquellas personas autorizadas a tener acceso a ella. Los activos de información deben estar debidamente protegidos para evitar la divulgación de la información almacenada, procesada, transmitida o recibida a individuos, entidades o procesos no autorizados.
7.) Autenticidad.- Define cual información es legítima, en caso de que sea interceptada, eventualmente podría ser copiada de su formato original y a pesar de que la información sea idéntica, no sea legítima pues no pertenece al autor original de la misma.
8.) No repudiación.- Improcedencia de la negativa en un proceso de control o seguimiento o transacción desde su inicio, pudiendo reconocerse de dónde provino, quien lo ejecutó y si estaba autorizado para ejecutarla.
9.) Amenaza.- Es el evento que puede provocar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos, que son de dos tipos:
9.1.) Intencionales, en caso de que deliberadamente se intente producir un daño (por ejemplo el robo de información aplicando la técnica de trashing, la propagación de código malicioso y las técnicas de ingeniería social).
9.2.) No intencionales, en donde se producen acciones u omisiones de acciones que ponen en riesgo los activos de información y pueden producir un daño (por ejemplo las amenazas relacionadas con fenómenos naturales).
10.) Vulnerabilidad.- Es un fallo de seguridad, que provoca que los sistemas informáticos funcionen de manera diferente para lo que estaban pensados, afectando a la seguridad de los mismos, pudiendo llegar a provocar entre otras cosas la pérdida y robo de información sensible. La vulnerabilidad de un activo es la potencialidad o posibilidad de ocurrencia de la materialización de una Amenaza sobre dicho Activo.
11.) Impacto.- Es la consecuencia materializada de una amenaza sobre el activo.
12.) Riesgo.- Posibilidad de la materialización de una amenaza en un activo, dominio o en toda la organización y que se aproveche una vulnerabilidad y dañe un activo de información.
13.) Salvaguarda.- Es la acción que reduce el riesgo (servicio de salvaguarda) o el procedimiento o dispositivo físico o lógico que reduce el riesgo (mecanismo de salvaguarda).
14.) SGSI.- Sistema de Gestión de la Seguridad de la Información.
15.) *Batch*.- Archivo electrónico que tiene almacenado una secuencia de comandos que al ejecutarse reemplaza la operación de digitar los comandos en secuencia cada vez que se requiere efectuar una operación. Se utiliza para almacenar operaciones repetitivas.
16.) *Firewall*.- Dispositivo tecnológico que tiene como función el control de acceso lógico en la red de comunicaciones.
17.) Red Privada Virtual – VPN.- Método de conexión a través de una red pública o privada, que permite a los servidores públicos establecer conexiones seguras.
18.) Script.- Es un archivo que contiene una secuencia de comandos que se utiliza para comunicarse en forma automática entre dos aplicaciones.
19.) BCP.- *Business Continuity Planning*. Es el conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los procesos de la Institución, generando un impacto mínimo o nulo ante una contingencia.
20.) Área Segura.- Instalaciones con medidas de control de acceso físico y lógico para reducir el riesgo de acceso no autorizado sobre los activos de información.
21.) Lugar de Trabajo Seguro.- Espacio físico con las debidas medidas de protección para preservar la integridad física de las personas.
22.) Mensajería Electrónica.- Son los servicios tecnológicos utilizados para el intercambio de mensajes de forma electrónica como lo es el correo electrónico.
23.) Paquete de Software.- Conjunto de programas que se comercializan y tienen una función específica. Aplica la definición para el software que apoya procesos de una entidad.

24.) Terceras Partes (Terceros).- Son todos aquellos entes externos o personas que no son servidores públicos del MINEDUC, que tienen acceso a los activos de la información.
25.) Dueños de los Activos de Información.- Son los servidores públicos que tienen un nivel jerárquico dentro de la Institución el cual les habilita para determinar el tipo de información que maneja cada uno de los procesos en los que está involucrada la misma, así como los niveles de riesgo a los cuales está expuesta, de forma que establezca los niveles de confidencialidad aplicables, los responsables de solicitar los niveles de seguridad que deben destinarse a la información, para mantener la confidencialidad, integridad y disponibilidad de la información.
26.) Información sensible.- Es el calificativo que recibe la información de tipo personal privada de un individuo (datos de tipo personal, contraseñas de correo electrónico u otros), usados para distinguir los datos privados relacionados con internet o la informática, sobre todo contraseñas de correo electrónico, conexión a internet, IP privada, sesiones del computador, etc.
27.) Pruebas de penetración externa o interna.- Son actividades técnicas realizadas por profesionales llamados hackers éticos que aplican conocimientos de seguridad para intentar encontrar vulnerabilidades en sistemas, bases de datos, o aplicativos, de forma de documentarlas y definir los niveles de criticidad de las mismas.
28.) Pruebas de ingeniería social.- Son pruebas realizadas por un experto en seguridad que buscan determinar los niveles de reacción de los usuarios ante situaciones que pueden comprometer la entrega de información de tipo confidencial, ejemplo de este tipo de pruebas se pueden considerar cuando un atacante o un *ethical Hacker* solicita información sensible como claves, o acceso a equipos, centros de datos, etc.
29.) Pruebas de desarrollo seguro de aplicaciones y sistemas.- Son pruebas técnicas con o sin el uso de programas de apoyo, que buscan encontrar vulnerabilidades producto del mal uso de lenguajes de programación, uso de componentes no seguros o malas prácticas en cuanto al desarrollo de aplicaciones o sistemas que puedan generar huecos de seguridad que puedan ser aprovechados por atacantes y ocasionar daños.
30.) Pruebas de procedimientos de manejo de vulnerabilidades técnicas.- Se refiere a la validación de las vulnerabilidades encontradas en sistemas, aplicativos, bases de datos, etc. Es una validación detallada del proceso que ha seguido la institución para mitigar las vulnerabilidades, su registro y control de los riesgos detectados.
31.) Identificación de riesgos de seguridad y sus niveles de criticidad hacia los activos de información analizados.- Como parte fundamental de un análisis de seguridad a nivel institucional se debe establecer un proceso de medición de los riesgos a los que se encuentra expuesta la institución tanto a nivel de procesos, tecnología y seguridad, los niveles de criticidad detectados en función de la metodología que se utilice para cuantificar o cualificar los mismos determinará los planes de acción para mitigar o prevenir esos riesgos, así como definir los pasos a seguir para que la implementación de tecnologías de seguridad estén enfocadas a minimizar y controlar los riesgos detectados y su nivel de impacto hacia los activos de información institucionales.

CAPITULO III
GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Art. 7.- Dominios de la Norma NTE INEN-ISO/IEC 27000.- Conforme a disposición del Secretaría Nacional de la Administración Pública (SNAP) a través del acuerdo 166, se dispone la necesidad de la aplicación de dos normas de seguridad de la información vigentes al momento y que han sido debidamente homologadas en el Ecuador, estas son: NTE INEN-ISO/IEC 27000 “Gestión de Seguridad de la Información” y NTE INEN-ISO/IEC 27002 "Código de Práctica para la Gestión de la Seguridad de la Información".

Estas normativas establecen lo que se conocen como dominios o capítulos que deben ser cubiertos por el sistema de gestión de seguridad de la información, así como la aplicación de buenas prácticas en cuanto a aplicación de controles de seguridad de la información de forma institucional, estos dominios a saber son:

a) **Política de seguridad**: Se estipulan las políticas de seguridad de la información para El MINEDUC.
b) **Organización de la seguridad:** Gestionar la seguridad de la información dentro del MINEDUC. (Roles, compromisos, autorizaciones, acuerdos, manejo con terceros).
c) **Gestión de activos:** Es el mantenimiento y protección apropiados de todos los activos de información.
d) **Seguridad del Talento Humano:** Busca asegurar que el servidor público, contratistas y terceros entiendan sus responsabilidades de conformidad a los roles que van a desempeñar, minimizando los riesgos relacionados con personal.
e) **Seguridad Física y del entorno:** Busca prevenir accesos físicos no autorizados (perímetro), daños o interferencias a las instalaciones del MINEDUC y a su información.
f) **Gestión de comunicaciones y operaciones:** Se busca asegurar la correcta y segura operación de las áreas de procesamiento de información (actividades operativas y concernientes a la plataforma tecnológica).
g) **Control de acceso:** Es el control físico o lógico de los accesos a los activos de la información.
h) **Adquisición, desarrollo y mantenimiento de sistemas de información:** Asegurar la inclusión de todos los controles de seguridad en los sistemas de información (infraestructura, aplicaciones, servicios, etc.).
i) **Gestión de incidentes de seguridad:** Es la comunicación de los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información para tomar una acción correctiva adecuada y en el momento indicado.
j) **Gestión de la continuidad del negocio:** Enfocado en reaccionar en contra de interrupciones a las actividades del MINEDUC y en proteger los procesos críticos contra fallas mayores en los sistemas de información o desastres, y por otro lado, asegurar que se recuperen a tiempo.
k) **Cumplimiento:** Busca prevenir el incumplimiento total o parcial de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

Art. 8.- Observancia.- La observación y cumplimiento de la Política de Seguridad de la Información institucional es obligatorio, ningún servidor público o tercero (contratista, proveedor, *outsourcing*) está exento de esta obligación. El servidor público que por negligencia o intencionalmente incumpliere las disposiciones de las políticas de seguridad del MINEDUC será sancionado de conformidad a los procesos establecidos en los reglamentos internos y las leyes vigentes aplicables al sector público.

En caso de que el incumplimiento o negligencia sea causado por terceros, éstos se acogerán a lo estipulado en las cláusulas del acuerdo de confidencialidad que describen sanciones o terminaciones de contratos de acuerdo a las leyes vigentes.

CAPÍTULO IV
PREMISAS DE LA SEGURIDAD DE LA INFORMACIÓN

Art. 9.- Principios Básicos.- La Política de Seguridad de la Información para la infraestructura tecnológica del MINEDUC se fundamenta en los siguientes principios básicos:

1.) Protección de la Información.- Los activos de información serán protegidos con el nivel necesario en proporción a su valor y el riesgo para la institución. La protección debe concentrarse en los aspectos de confidencialidad, integridad y disponibilidad de los activos de información.

Las y los servidores públicos del MINEDUC, así como los terceros proveedores de servicios, soluciones, capacitaciones, u otros, deberán firmar de forma obligatoria el Acuerdo de Confidencialidad para servidores públicos y/o terceros, respectivamente, de conformidad a las Normas de Seguridad.

2.) Clasificación de la Información.- La información deberá ser clasificada de acuerdo a sus niveles de acceso como pública, confidencial o de acceso restringido, para lo cual cada responsable de los activos de información a su cargo deberá establecer esta clasificación usando un modelo base que permita definir este proceso. Todas las tecnologías asociadas a este proceso estarán destinadas a mantener la confidencialidad, disponibilidad e integridad de la información. La Dirección Nacional de Tecnologías de la Información y Comunicaciones será responsable de proveer las soluciones tecnológicas apropiadas para estos efectos.

3.) Protección de los Recursos Tecnológicos.- Los recursos tecnológicos serán protegidos con el nivel necesario en proporción a su valor y el riesgo para la Institución. Dichos recursos deben ser utilizados exclusivamente para desarrollar las actividades laborales establecidas a los servidores públicos, contratistas y en contratos de terceros, así mismo su utilización se hará en forma adecuada, con el máximo de eficiencia y con ejemplar racionalidad.

4.) Autorización de servidores públicos.- Todos los servidores públicos deben ser identificados independientemente con permisos de acceso, específicos e individuales, autorizados por razones básicas de la Institución. Los métodos de acceso de servidores públicos deben exigir un proceso robusto de autenticación, autorización apropiada y auditoría confiable.

5.) Responsabilidad.- Los servidores públicos, dueños y custodios de los activos de información del MINEDUC, son responsables por su uso apropiado, protección y privacidad. Los sistemas de información del MINEDUC generarán y mantendrán pistas apropiadas de auditoría para identificar a los servidores públicos y documentar los eventos relacionados con temas de seguridad.

6.) Esfuerzo de Equipo.- Para la efectiva seguridad de la información, debe existir la participación activa de todos los servidores(as) públicos que tengan interacción con los activos de la información del MINEDUC.

7.) Revisiones de seguridad.- En forma periódica el MINEDUC debe efectuar las revisiones necesarias para evaluar el cumplimiento de las diferentes políticas de seguridad.

Las revisiones de seguridad podrán incluir a:
a) Pruebas de penetración externa o interna;
b) Pruebas de ingeniería social;
c) Pruebas de desarrollo seguro de aplicaciones y sistemas;
d) Pruebas de procedimientos de manejo de vulnerabilidades técnicas; y,
e) Identificación de riesgos de seguridad y sus niveles de criticidad hacia los activos de información analizados.

8.) Propiedad de la Información.- La información soportada por la infraestructura

tecnológica del MINEDUC es de su exclusiva propiedad la que podrá ser suministrada a los entes de control pertinentes cuando estos lo requieran, previa autorización expresa y aprobada por las Direcciones del MINEDUC.
Para efectos de control del flujo de la información de los procesos del MINEDUC, se asignarán como responsables de la información a los Directores de área, quienes controlarán el acceso a la información que genere su área, con el fin de lograr un buen nivel de segregación de funciones y acceso a la información.

En caso de divulgación no autorizada de la información de propiedad del MINEDUC, se realizarán las investigaciones pertinentes para establecer sanciones. Estas investigaciones serán realizadas por el dueño de la información y las sanciones serán evaluadas y aplicadas por el área encargada de aplicar procesos disciplinarios internos.

CAPÍTULO V
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN CUMPLIMIENTO DE LA NORMA NTE INEN-ISO/IEC 27000

Art. 10.- Política de Seguridad.- La Política de Seguridad del MINEDUC especifica las directrices que deben cumplir los servidores públicos, proveedores, contratistas y terceros, con el fin de asegurar un adecuado nivel de confidencialidad, integridad y disponibilidad en sus activos de información.

La Política de Seguridad de la Información seguirá el proceso establecido en la Institución para su aprobación, publicación y comunicación a todo el personal y partes externas.

La Política de Seguridad de la Información será revisada de forma anual o cuando se produzcan cambios significativos identificados en procesos, infraestructura, software, aplicaciones y todo aspecto que influya considerablemente en la misión del MINEDUC, con el fin de garantizar que ella sigue siendo suficiente y eficaz.

El desarrollo de cada una de los procedimientos técnicos de la Política de Seguridad de la Información se encuentra detallado en el documento anexo al presente Acuerdo Ministerial.

Art. 11.- Organización de la seguridad de la Información.- Para que la Seguridad de la Información esté debidamente estructurada, se definirán los elementos de organización del personal a cargo y los responsables del mantener el compromiso institucional, para que conozcan sus funciones y responsabilidades, además de proveer los parámetros necesarios para asegurar que la Política de Seguridad de la Información sea conocida y difundida tanto a nivel interno como externo.
El MINEDUC adoptará las buenas prácticas que permitan una correcta organización de la seguridad de la información.

1) Organización Interna.- Las directrices de gestión de la seguridad de la información dentro de MINEDUC, se puede dar a través de.
1.1.) Compromiso de las Direcciones.- Cada Dirección es responsable de la seguridad de los activos de información a su cargo, que será continuamente revisada y actualizada por parte del MINEDUC a través del sistema SGSI (EGSI).
1.2.) Coordinación de la Seguridad de la Información con el apoyo del personal con perfiles y funciones laborales pertinentes para ello.
1.3.) Autorización para los Servicios de Procesamiento de Información.
d.) La suscripción de acuerdos de confidencialidad e integridad de la información con los

servidores públicos y terceras partes.
1.4.) Contactos con las autoridades para identificar los organismos externos que ejercen autoridad.
1.5.) Contactos con grupos de interés especiales, para identificar comunidades y grupos de interés.
1.6.) Revisión periódica y planificada de las políticas de controles, procesos y procedimientos de seguridad de la información, por parte de un organismo o consultor externo o del MINEDUC.

2.) Control de la seguridad.- Garantizar el control de la seguridad de la información y los servicios de procesamiento de información a partes externas, con la correspondiente autorización de acceso.
2.1.) Identificación de los riesgos relacionados con partes externas.- El Control del acceso de terceras partes a los activos de la información de MINEDUC, se autorizará, previa identificación de los riesgos asociados a ese acceso en virtud de la estructura de Seguridad de la Información.
2.2.) Consideraciones de seguridad para conexión de los clientes.- El acceso de los clientes a los activos de la información de MINEDUC, será autorizado únicamente cuando se cumplan con las políticas de seguridad de la información y se hayan establecidos los controles respectivos.
2.3.) Consideraciones de la seguridad en los acuerdos con terceras partes.- El acceso, procesamiento, comunicación o gestión de la información de los activos del MINEDUC requerido por terceras partes, debe ser autorizado únicamente cuando estos se comprometan de forma escrita a cumplir con la política de seguridad de la información y los controles establecidos por MINEDUC.

Art. 12.- Gestión de los activos de información.- Esta Política establece los mecanismos a través de los cuales el MINEDUC define y clasifica los activos de información institucionales, designa a los dueños o propietarios de la información, su nivel de responsabilidad ante los mismos; y, requiere de la implementación de un proceso de clasificación de la información de forma que pueda determinar posibles usos inadecuados de la misma.

1.) Responsabilidad por los activos.- Este control tiene como objetivo lograr y mantener la protección adecuada de los activos de la información del MINEDUC.

2.) Inventario de Activos.- Todos los activos de información deben ser claramente identificados, referenciados, inventariados y constantemente actualizados en el sistema correspondiente.

3.) Propiedad de los activos.- Designar formalmente a los dueños de los activos de información asociados con los servicios de procesamiento de información.

4.) Uso aceptable de los activos.- Usar de forma aceptable la información y los activos asociados con los servicios de procesamiento de la información.

5.) Clasificación de la información.- Este control tiene como finalidad asegurar que la información reciba el nivel de protección adecuado y se define de acuerdo a las normativas vigentes, los tipos de información y los niveles de confidencialidad de la misma, así mismo busca la aplicación de mecanismos de protección que aseguren sus correcto acceso, respaldo, y tránsito ante todas las instancias internas o externas que requieran tener acceso a la información de acuerdo a los permisos y derechos de acceso que hayan sido autorizados por los Dueños de los Activos de la Información, a través de dos circunstancias:

5.1.) Directrices de clasificación.- Por las que se realiza procesos de clasificación de la información para asegurar que esta reciba el nivel de protección adecuado.
5.2.) Etiquetado y manejo de información.- a través de la cual se define y estandariza el correcto etiquetado de la información.

Art. 13.- Seguridad del Talento Humano.- La Dirección Nacional de Talento Humano o la unidad desconcentrada que haga sus veces serán los responsables de asegurar que, los servidores públicos, contratistas y terceros, entiendan sus responsabilidades y sean preparados en el desempeño de sus roles, para reducir el riesgo sobre robos, fraudes o uso no adecuado de las instalaciones o de la información.

1.) Roles y responsabilidades.- A través del correcto proceso de selección, se busca garantizar que todos los nuevos servidores públicos, conozcan, entiendan y asuman sus responsabilidades con respecto a la seguridad de la información, según el rol a desempeñar. Esta misma responsabilidad será cumplida por todos los servidores públicos del MINEDUC con anterioridad a la elaboración de este documento.

2.) Vinculación de personal.- Se refiere a la verificación de antecedentes de los candidatos a ser próximos servidores públicos, contratistas o servidores públicos de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos de la misión, la función, la clasificación de la información a la cual se va a tener acceso y a los riesgos percibidos.

3.) Términos y condiciones laborales y contractuales.- Los servidores públicos, contratistas y servidores públicos de terceras partes deben firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las del MINEDUC con relación a la seguridad de la información.

4.) Responsabilidades de la Dirección.- La Institución debe exigir que los servidores públicos, contratistas y servidores públicos de terceras partes, apliquen la seguridad según las políticas y los procedimientos establecidos por el MINEDUC.

5.) Educación, formación y concientización sobre la seguridad de los activos de información.- El MINEDUC definirá las mejores prácticas para garantizar un proceso ordenado de educación, formación y concientización a sus servidores públicos de forma continua en los temas de seguridad de los activos de información, para asegurar el cumplimiento de los procedimientos del modelo de seguridad adoptado.

6.) Proceso disciplinario.- El incumplimiento de la política de seguridad de la información o de alguno de los procedimientos establecidos en el modelo de seguridad de la información SGSI del MINEDUC que conlleve a un incidente de seguridad, implicará la realización de un proceso disciplinario para establecer la responsabilidad del servidor público involucrado y en consecuencia, establecer las sanciones a que haya lugar.

7.) Terminación o cambio de la vinculación laboral o contractual.- Este protocolo de seguridad busca asegurar que los servidores públicos o terceras partes terminen su vinculación laboral o contractual con el MINEDUC en estricto cumplimiento de lo establecido en la legislación ecuatoriana.

8.) Responsabilidades en la terminación de la vinculación laboral o contractual.- Se establecen los procedimientos para llevar a cabo la terminación o el cambio de la vinculación laboral o contractual con sus servidores públicos.

9.) Devolución de activos.- El MINEDUC adopta buenas prácticas para garantizar que todos sus servidores públicos y terceras partes devuelvan los activos que estén en su poder y pertenezcan al MINEDUC, al finalizar su vinculación laboral o contractual.

10.) Retiro de los derechos de acceso.- El MINEDUC retirará a las personas que sean desvinculadas laboral o contractualmente, todos los derechos de acceso a sus activos de información.

Art. 14.- Seguridad Física y del Entorno.- El MINEDUC a través de las Dirección Nacional Administrativa y la Dirección Nacional de Tecnologías de la Información y Comunicaciones implementarán buenas prácticas de seguridad física y del entorno, con el propósito de evitar el acceso no autorizado o el daño e interferencia a sus instalaciones y activos de información.

El MINEDUC para mantener y controlar la seguridad en las instalaciones y su perímetro físico adoptará las siguientes prácticas:

1. Utilización de perímetros de seguridad física (paredes, puertas y otros) para proteger las áreas que contienen los activos de información.

2. Control de ingreso del personal autorizado y acceso restringido a las áreas seguras y protegidas.

3. Aplicación de las recomendaciones de diseño e implementación de la seguridad física para oficinas, recintos e instalaciones.

4. Protección de las instalaciones contra daño por incendio, inundaciones, sismos, explosión, actos malintencionados por terceros, manifestaciones sociales y otras formas de desastre natural o artificial.

5. Trabajo en áreas seguras y mecanismos de trabajo seguros.

6. Implementación de controles de acceso a los puntos por donde pueda ingresar personal no autorizado a las instalaciones tales como el área de almacén, parqueaderos y sótanos.

7. Ubicación y protección de los activos de información propios, así como los que se encuentran bajo la responsabilidad del MINEDUC (comodato, arrendamiento) para reducir el riesgo debido a amenazas o peligros del entorno y las oportunidades de acceso no autorizado.

8. Protección de sus activos de información, o los que se encuentran bajo su responsabilidad, contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios.

9. Protección el cableado de energía eléctrica, de voz y datos contra interceptaciones y daños.

10. Mantenimiento de su plataforma tecnológica para asegurar su continua disponibilidad e integridad.

11. Seguridad a los equipos cuando sean requeridos o utilizados fuera de las instalaciones de MINEDUC.

12. Eliminación completa de la información contenida en equipos que se reutilizan o se dan de baja.

13. Prevención de que ningún equipo, información ni software se retiren sin autorización previa.

14. Respaldo de la información ubicada en el centro de cómputo de la Dirección Nacional de Tecnologías de la Información y Comunicaciones, para la custodia de la información.

15. Los Centros de Cómputo del MINEDUC definen la necesidad de establecer y controlar los mecanismos de seguridad necesarios para la correcta protección de la información, de manera que se mantenga la confidencialidad, integridad y disponibilidad de la información que se procesa.

Art. 15.- Gestión de comunicaciones y operaciones.- El MINEDUC proporcionará los mecanismos y controles necesarios para garantizar el acceso a los activos de información a través de los medios de comunicación establecidos en forma segura, de manera que la operación de los mismos corresponda a los niveles y compromisos determinados institucionalmente.

El MINEDUC adoptará las mejores prácticas para mantener y controlar la operación de las comunicaciones y operaciones a través de:

1.) Procedimientos operacionales y responsabilidades.- En este apartado se definen las políticas para garantizar la correcta y segura operación de los servicios de procesamiento de información dentro de MINEDUC, a través de:
1.1.) Documentación de los procedimientos operativos relacionados con la información.
1.2.) Gestión del Cambio en los servicios y los sistemas de procesamiento de información
1.3.) Distribución de funciones y áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de información.
1.4.) Separación de ambientes de Prueba, Desarrollo y Producción, aplicando para cada uno, los procedimientos, para reducir los riesgos de acceso o cambios no autorizados en los sistemas.

2.) Gestión de la prestación del servicio por terceras partes.- En este apartado se definen las políticas para implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras partes, como son:
2.1.) Prestación del servicio.- El MINEDUC, mediante la acción de la Estructura de Seguridad de la Información que se defina, exige y vigila que los controles de seguridad, las definiciones del servicio y sus niveles de prestación incluidos en los contratos o convenios suscritos con terceras partes, sean implementados, mantenidos y operados por éstas.
2.2.) Monitoreo y revisión de los servicios por terceras partes.- Se realizará controles e implementará las herramientas necesarias para realizar la verificación de los servicios, generar reportes y mantener registros relacionados con seguridad de la información que son suministrados por terceras partes.
2.3.) Gestión de los cambios en los servicios por terceras partes.- Se mantendrá procesos de control para que los cambios en la prestación de los servicios incluyendo mantenimiento y mejora de las políticas existentes de seguridad de la información, en los procedimientos, se gestionen teniendo en cuenta la importancia de los sistemas y procesos de la misión funcional involucrados, así como la reevaluación de los riesgos, por parte de la Estructura de Seguridad de la Información que se defina en el MINEDUC .

3.) Planificación y aceptación del sistema.- En este apartado se definen las políticas para minimizar el riesgo de fallas de los sistemas, que involucra:
3.1.) Gestión de la capacidad.- El personal técnico definido del MINEDUC monitoreará continuamente a sus servidores, sistemas de almacenamiento, redes y sistemas de información incluyendo los sistemas de respaldo, con el fin de establecer adecuados niveles de capacidad y desempeño en el presente y a futuro.
3.2.) Aceptación del sistema.- Se establecerán criterios de aceptación para los nuevos sistemas de información, actualizaciones y nuevas versiones, y la realización de las pruebas respectivas antes de su aceptación.

4.) Protección contra código malicioso y móvil.- En este apartado se definen las políticas para proteger la integridad del software y de la información, que involucra:
4.1.) Controles contra código malicioso.- Se Implementarán los controles para la detección, prevención y recuperación a fin de proteger los activos de información contra códigos maliciosos, y aplicarán procedimientos apropiados de concientización de los servidores públicos, para control de códigos maliciosos.
4.2.) Controles contra códigos móviles.- Se definirán los mecanismos y procedimientos para que la autorización de utilización de códigos móviles, sea configurada de forma que se asegure que dichos códigos operan de acuerdo con la política de seguridad definida, y evitar la ejecución de los códigos móviles no autorizados.

5.) Respaldo de la información.- Se implementará una política de respaldo por medio de copias de seguridad siguiendo el procedimiento adecuado según el componente.

6) Gestión de la seguridad de las redes.- En este apartado se definen las políticas para asegurar la protección de la información en las redes y la protección de la infraestructura de soporte de MINEDUC, a través de:
6.1.) Control de las redes.- Se mantendrá y controlará las redes, protegiéndolas de las amenazas y mantener la seguridad de los activos de información que usan la red.
6.2.) Seguridad de los servicios de red.- Se identificará e incluirá las características de seguridad en los acuerdos sobre los servicios de la red, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en MINEDUC o se contratan externamente.

7.) Manejo de medios.- Se definirán las políticas para evitar la divulgación, modificación, retiro o destrucción de información propiedad de MINEDUC de forma no autorizada, a través de las siguientes prácticas:

7.1.) Gestión de los medios removibles.
7.2.) Eliminación de los datos y archivos en forma segura y sin riesgo de los medios que ya no son requeridos.
7.3.) Se definirán los Procedimientos para el manejo **y** almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.
7.4.) Se protegerá la documentación de los sistemas y aplicativos contra el acceso no autorizado.

8.) Intercambio de información.- Para mantener la seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa, se definirán las siguientes políticas.
8.1.) Políticas y procedimientos para el intercambio de información**,** para proteger la información que circula en todo tipo de servicios de comunicaciones.
8.2.) Acuerdos para el intercambio**,** para garantizar el intercambio de información y del

software entre la organización y partes externas.
8.3.) Protección de los medios físicos en tránsito **o** medios que contienen información contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de MINEDUC.
8.4.) Protección de la información contenida en la mensajería electrónica.
8.5.) Protección de los Sistemas de información asociada con la interconexión de los sistemas de información de MINEDUC.

9.) Información disponible al público.- Se buscará asegurar la protección de la integridad de la información que se pone a disposición de terceras partes, para evitar la modificación no autorizada de la misma.

10.) Monitoreo.- Se definen las políticas para detectar actividades de procesamiento de la información no autorizada, a través de:
10.1) Registro de auditorías.- Se registrará y conservará con fines de auditoría y conforme a la normatividad aplicable, las actividades de los funcionarios y terceras partes, excepciones y eventos de seguridad de la información sobre los servidores, redes, sistemas de respaldo, computadores personales y sistemas de información.
10.2.) Monitoreo del uso del sistema.- Se establecerán los procedimientos para el monitoreo del uso de los servicios de procesamiento de información y sus resultados se revisarán periódicamente conforme al riesgo calculado de las aplicaciones.
10.3.) Protección de la información de los registros.- Se protegerán los servicios y la información de la actividad de registro contra el acceso o la manipulación no autorizados.
10.4.) Registros del administrador y operador.- Se registrarán las actividades del personal que administra y opera los sistemas de información, servidores, equipos de comunicaciones y bases de datos.
10.5.) Registros de falla.- Se registrarán, analizarán y tomarán las acciones pertinentes sobre las fallas en los servicios, según se describe en el anexo al presente Acuerdo Ministerial, en el apartado denominado “Gestión de comunicaciones y operaciones”.
10.6.) Sincronización de relojes.- Se implementarán procedimientos que permitan la sincronización de los relojes de todos sus sistemas de procesamiento de información.

Art. 16.- Control de Acceso.- El MINEDUC establece que para manejar un acceso autorizado a los activos de la información Institucionales se deberán definir mecanismos, procedimientos y medios a través de los cuales se pueda aprobar el acceso a los mismos, así mismo y las cuentas de acceso a sistemas y aplicativos, incluyendo el uso adecuado de claves de acceso a los diferentes sistemas.

El MINEDUC para garantizar el acceso, control y auditoría de los Activos de Información institucionales, adoptará las siguientes mejores prácticas:

1.) Requisitos del negocio para el control de acceso.- En este apartado se definen la política de control de acceso para prevenir el acceso no autorizado a los activos de información de MINEDUC.

2.) Gestión de Acceso para Servidores Públicos:
2.1.) Registro de Servidores Públicos.- Se llevará un control del registro, modificación y cancelación de las cuentas de servidores públicos con el fin de conceder, actualizar o revocar el acceso a todos los sistemas y servicios de Información.
2.2.) Gestión de privilegios.- Se restringirá y controlará la asignación y uso de privilegios.
2.3.) Gestión de contraseñas para servidores públicos.- Se controlará la asignación de contraseñas a través de un proceso formal de gestión.

2.4.) Revisión de los derechos de acceso de los servidores públicos.- Se revisará periódicamente los derechos de acceso de los servidores públicos.

3.) Responsabilidades de los servidores públicos.- Esta política define las directrices para evitar el acceso de servidores públicos no autorizados, el robo, puesta en peligro de la información y de los servicios de procesamiento de información, que involucra:
3.1.) Uso de la contraseña.- Se aplicará un procedimiento para la correcta selección y el uso de las contraseñas.
3.2.) Equipo de servidor público desatendido.- Se asegurará que a los equipos desatendidos de los Servidores Públicos se les brindará la protección apropiada.
3.3.) Política de escritorio y pantalla despejados.- Se regularizará el manejo del escritorio y pantalla despejados, con el propósito de asegurar la protección de la información confidencial.

4.) Control de acceso a las redes.- El objetivo de esta política es evitar el acceso no autorizado a los servicios de red, a través de:
4.1.) Política de uso de los servicios de red.- Se controlará y auditará que los servidores públicos solo tengan acceso a los servicios para cuyo uso están específicamente autorizados.
4.2.) Autenticación de Servidores Públicos para conexiones externas.- Se usará mecanismos de autenticación para controlar el acceso de servidores públicos remotos.
4.3.) Identificación de los equipos en las redes.- Se garantizará la identificación automática de los equipos para autenticar conexiones de equipos y ubicaciones específicas.
4.4.) Protección de los puertos de configuración y diagnostico remoto.- Se garantizará el control del acceso lógico y físico a los puertos de configuración y diagnóstico.
4.5.) Separación en las redes.- Se separará las redes en los grupos de servicios de información, servidores públicos y sistemas de información.
4.6.) Control de conexión a las redes.- Se garantizará que se restringe la capacidad de los servidores públicos para conectarse a la red, de acuerdo con la política de control de acceso y los requisitos de aplicación del negocio.
4.7.) Control de enrutamiento de la red.- Se controlará el enrutamiento en las redes con el fin de asegurar que las conexiones entre equipos computacionales y los flujos de información no incumplan la política de control de acceso de las aplicaciones del negocio.

5.) Control de acceso al sistema operativo.- Esta política tiene como objetivo evitar el acceso no autorizado a los sistemas operativos.
5.1.) Procedimiento de ingresos seguros.- Se controlará el acceso a los sistemas operativos mediante un procedimiento de registro de inicio seguro.
5.2.) Identificación y autenticación de Servidores Públicos.- Se asegurará que todos los servidores públicos tengan un identificador único (ID del usuario) por medio del uso de una técnica apropiada de autenticación para comprobar la identidad declarada de un servidor público.
5.3.) Sistemas de Gestión de contraseñas.- Se garantizará que los sistemas de gestión de contraseñas sean interactivos y aseguren la calidad y fortaleza de las mismas.
5.4.) Uso de las utilidades del sistema.- Se desarrollará prácticas seguras para restringir y controlar estrictamente el uso de programas utilitarios que puedan anular los controles del sistema y de la aplicación.
5.5.) Tiempo de inactividad de la sesión.- Se asegurará que las sesiones inactivas se suspenden después de un periodo definido de inactividad.

6.) Limitación del tiempo de conexión.- Se restringirá y controlará los tiempos de conexión con el propósito de ofrecer seguridad adicional para las aplicaciones de alto riesgo.

7.) Control de acceso a las aplicaciones y a la información.- Esta política tiene como objetivo evitar el acceso no autorizado a la información contenida en los sistemas de información, que comprende:

7.1.) Restricción de acceso a la información.- Se restringirá el acceso a la información y a las funciones del sistema de aplicación por parte de los servidores públicos y del personal de soporte de acuerdo con las funciones desempeñadas.
7.2.) Aislamiento de sistemas sensibles.- Se asegurará que los sistemas sensibles tengan un entorno informático dedicado (aislados).

8.) Computación móvil y de trabajo remoto.- Esta política tiene como objetivo garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto.
8.1.) Computación y comunicaciones móviles.- Se protegerá contra los riesgos generados por el uso de dispositivos de computación y comunicación móviles.
8.2.) Trabajo remoto.- Se controlará las actividades de trabajo remoto.

Art. 17.- Adquisición, desarrollo y mantenimiento de sistemas de información.- El MINEDUC debe garantizar que los procesos de adquisición, desarrollo y mantenimiento de sistemas de información que hayan sido adquiridos a través de terceros o desarrollados internamente con recursos y personal propios del MINEDUC, cuenten con medidas de seguridad establecidas para garantizar la seguridad de los productos generados, así como se apliquen las mejores prácticas en cuanto a desarrollo seguro.

Esta política establece los procesos que generen sistemas y aplicaciones fortalecidos, y que puedan garantizar a la Institución el cumplimiento de la confidencialidad, disponibilidad e integridad de la información, a través de las siguientes medidas:

1.) Requisitos de seguridad de los sistemas de información.- Esta política tiene como objetivo garantizar que la seguridad sea parte integral de los sistemas de información. Se asegurará que las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes, especifican los requisitos para los controles de seguridad.

2.) Procesamiento correcto de las aplicaciones.- Esta política tiene como objetivo evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.
2.1.) Validación de los datos de entrada.- Se aplicará una validación de los datos de entrada en todas las aplicaciones para asegurar que dichos datos son correctos y apropiados.
2.2.) Control de procesamiento interno.- Se incorporarán verificaciones de validación en las aplicaciones con el fin de detectar cualquier corrupción de la información por errores de procesamiento deliberados.
2.3.) Integridad del mensaje.- Se asegurará y protegerá la autenticidad y la integridad del mensaje en las aplicaciones.
2.4.) Validación de los datos de salida.- Se definirán procesos de validación de los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.

3.) Controles criptográficos.- Esta política tiene como objetivo proteger la confidencialidad e integridad de la información.
3.1.) Política sobre el uso de los controles criptográficos.- Se usarán controles criptográficos para la protección de la información.

3.2.) Gestión de llaves.- Se aplicarán mecanismos adecuados para la gestión de llaves para apoyar el uso de las técnicas criptográficas aplicadas.

4.) Seguridad de los archivos del sistema.- Esta política tiene como objetivo proteger la confidencialidad e integridad de la información, a través de:
4.1.) Control de instalación del software en sistemas operativos.
4.2.) Protección y control de los datos de prueba del sistema.
4.3.) Control de acceso al código fuente de los programas.- Se restringirá el acceso indiscriminado y no autorizado al código fuente de los programas.
5.) Seguridad en los procesos de desarrollo y soporte.- Esta política tiene como objetivo mantener la seguridad del software y de la información del sistema de aplicaciones, a través de:

5.1.) Procedimientos de control de cambios.- Se controlará la implementación de cambios utilizando procedimientos formales de control de cambios.
5.2.) Revisión técnica de las aplicaciones después de los cambios en el sistema operativo.- Se controlará y auditará los cambios a los sistemas operativos para garantizar que las aplicaciones críticas para el negocio se revisen y sometan a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de MINEDUC.
5.3.) Restricción en los cambios a los paquetes de software.- Se aplicarán controles para desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y mantener un estricto control de la totalidad de los cambios.
5.4.) Fuga de información.- Se desarrollarán los controles adecuados para evitar la fuga de información cuando se cambian los sistemas operativos.
5.5.) Desarrollo de software contratado externamente.- Se supervisará y monitoreará el desarrollo de software contratado externamente.

6.) Gestión de la vulnerabilidad técnica.- Esta política tiene como objetivo reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.
6.1.) Control de vulnerabilidades técnicas.- Se aplicarán los controles y medidas necesarias para obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.

Art. 18.- Gestión de los incidentes de la seguridad de la información.- Esta política define como el MINEDUC deberá proceder ante el aparecimiento, identificación, catalogación, y resolución de incidentes de seguridad, para aplicar medidas correctivas o preventivas oportunas, lograr una disminución de los riesgos de seguridad.

El Ministerio llevará un control y registro detallado de los incidentes para establecer mecanismos de solución y de revisión para tomar acciones legales de ser el caso.

Para garantizar el acceso adecuado, controlados y debidamente auditado a los activos de Información institucionales, el MINEDUC adoptará las mejores prácticas:

1.) Reporte sobre los eventos y las debilidades de la seguridad de la información.- Esta política tiene como objetivo asegurar que los eventos y las debilidades de la seguridad de la información asociados con los activos de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente, así:
1.1.) Reporte sobre los eventos de la seguridad de la información.- Se definirán los procesos adecuados para informar a través de los canales de gestión apropiados, tan pronto como sea posible, los eventos de seguridad asociados a sus activos de información.

1.2.) Reporte sobre las debilidades de la seguridad de la información.- Se definirán los procedimientos para exigir a todos los funcionarios y terceras partes responsables de los activos de información, que observen y reporten todas las debilidades encontradas al realizar sus actividades.

2.) Gestión de los incidentes y las mejoras en la seguridad de la información.- Esta política tiene como objetivo asegurar que se aplique un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información, a través de:
2.1.) Responsabilidades y procedimientos.- Se establecerán las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad sobre sus activos de información.
2.2.) Aprendizaje debido a los incidentes de seguridad de la Información.- Se definirán mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.
2.3.) Recolección de evidencia.- Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información, implique acciones legales (civiles o penales), el MINEDUC adoptará buenas prácticas para que esta evidencia se recolecte, se mantenga y se presente con el fin de cumplir con las reglas para la recolección de evidencia establecidas en la jurisdicción pertinente.

Art. 19.- Gestión de la continuidad del negocio.- El MINEDUC desarrollará los planes de continuidad de negocio y de recuperación ante desastres tecnológicos usando metodologías actuales y adecuadas a la realidad de la institución, realizará las pruebas del caso de los mencionados planes considerando los riegos más críticos a ser probados, los sistemas y procesos a ser recuperados en prioridad conforme el impacto a la institución en cuanto a la materialización de los riesgos.

El control de seguridad de activos de información tiene como propósito suplir las interrupciones en las actividades de función misional y proteger sus procesos críticos contra los efectos de fallas importantes en los activos de información o desastres, y asegurar su recuperación oportuna e incluye los siguientes aspectos:

1.) Inclusión de la seguridad de los activos de información en el proceso de gestión.- Se determinará el marco general de los requisitos de seguridad de los activos de información para desarrollar un proceso de gestión Institucional que garanticen la continuidad del negocio de MINEDUC.
2.) Continuidad del negocio y evaluación de riesgos.- Se definirá un proceso que le permita identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de los activos de la información.
3.) Desarrollo e implementación del plan de continuidad que incluya la seguridad de la información.- Se desarrollarán e implementarán los planes necesarios para mantener y recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempos establecidos después de la interrupción o falla de los procesos críticos para el negocio.
4.) Estructura para la planificación de la continuidad del negocio.- Se mantendrá una sola estructura del plan de continuidad del negocio, para asegurar que éste sea consistente e incluya los requisitos de seguridad de los activos de información e identifiquen las prioridades para pruebas y mantenimiento del mismo.
5.) Pruebas, mantenimiento y reevaluación del plan de continuidad de MINEDUC.- El plan de continuidad de MINEDUC se someterá a pruebas y revisiones periódicas para asegurar su actualización y eficiencia.

Art. 20.- Cumplimiento.- El MINEDUC aplicará esta política para evitar el incumplimiento, de las leyes y decretos, reglamentos, contratos y cualquier requisito de seguridad por parte de los servidores públicos.

El cumplimiento de las Políticas de Seguridad de la Información es obligatorio. Ningún servidor(a) público o funcionario(a) o tercero (contratista, proveedor, *outsourcing*) está exento del cumplimiento de estas políticas.

Si un servidor(a) o funcionario(a) transgrede las disposiciones de las Políticas de Seguridad de la Información del MINEDUC, por negligencia o intencionalmente, se acogerá a las sanciones establecidas de la Ley Orgánica del Servicio Público y su Reglamento General, Código de Ética Institucional, Reglamento Interno del MINEDUC, y demás normativa pertinente, de acuerdo al tipo de falta que se configure.

En caso de Terceros, al ser detectados incumplimientos por negligencia o intencionalmente de las políticas de seguridad de la información en el MINEDUC, se acogerán a lo estipulado en las cláusulas del acuerdo de confidencialidad y a las sanciones y terminación de los contratos debidamente suscritos entre las partes.

El MINEDUC adopta e implementará los procedimientos necesarios para garantizar la protección de la información, a través de:

1.) Identificación de las leyes aplicables.- Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes a cada sistema de información, así como el enfoque del MINEDUC, están explícitamente documentados y se mantendrán actualizados.

2.) Derechos de propiedad intelectual.- El MINEDUC implementará procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

3) Protección de los registros de MINEDUC.- Los registros de información institucional de MINEDUC se protegerán contra eventos no autorizados: acceso, divulgación, modificación, duplicidad, destrucción; o actos de alteración, sustracción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del objetivo organizacional.

4.) Protección de los datos y privacidad de la información personal.- El MINEDUC procura garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si aplica, con las cláusulas del contrato.

5.) Prevención del uso inadecuado de los servicios de procesamiento de información.- El uso inadecuado de los servicios de procesamiento de información y de los activos de información está prohibido en el MINEDUC, el cual además adopta los mecanismos de difusión y actos disciplinarios que considera apropiados para disuadir a los servidores públicos de utilizar los servicios de procesamiento de información para propósitos no autorizados.

6.) Reglamentación de los controles criptográficos.- El MINEDUC utiliza controles criptográficos bajo el estricto cumplimiento de todos los acuerdos, las leyes y los reglamentos pertinentes.

7.) Cumplimiento con las políticas y normas de seguridad.- Todos los Servidores Públicos de MINEDUC son responsables del cumplimiento de la política, normas y procedimientos de seguridad establecidos. El MINEDUC designará en los Directores de cada Área la responsabilidad de controlar que los funcionarios a su cargo cumplan los procedimientos de seguridad definidos.

8.) Verificación del cumplimiento técnico.- El MINEDUC, a través del Oficial de Seguridad de la Información, verifica periódicamente el cumplimiento de las normas de implementación de seguridad.

9.) Auditoría a los activos de información.- Se planificará y realizarán las actividades de auditoría a los activos de información para hacerlas recomendaciones necesarias a fin de minimizar los riesgos sobre la confidencialidad, integridad y disponibilidad de los procesos de la Compañía.

10.) Protección de las herramientas de auditoría de los sistemas de información.- El acceso a las herramientas de auditoría de los activos de información se encuentra debidamente protegido y limitado a servidores públicos autorizados, para evitar su uso inadecuado o no autorizado.

11.) Protección Legal.- El MINEDUC conserva el derecho de retirar de los sistemas de información cualquier material que pueda ser considerado ofensivo o potencialmente ilegal.

El MINEDUC, a través del Oficial de Seguridad de la Información o la Dirección Nacional de Tecnologías de la Información y Comunicaciones, se reserva el derecho de monitorear o inspeccionar en cualquier momento, todos los sistemas de información de MINEDUC.

La evaluación, monitoreo e inspección se realizará con o sin el consentimiento, presencia o conocimiento de los funcionarios involucrados. Los sistemas de información sujetos a tal examen incluyen pero no están limitados a: sistemas de archivo de correo electrónico, archivos en discos duros de computadores personales, archivos de correo de voz, archivos en colas de impresión, y salidas de máquinas de fax.

MINEDUC contará con un contrato de respaldo alterno de equipos, para ser utilizado en caso de contingencia.

12.) Normatividad.- Ningún servidor público, inclusive aquellos pertenecientes a la Dirección Nacional de Tecnologías de la Información y Comunicaciones, leerá o facilitará a otra persona que lea el contenido de cualquier archivo de correo electrónico del personal, sin obtener el permiso del servidor público o jefe inmediato por escrito; excepto en caso que exista un motivo razonable para hacerlo. Dichos motivos pueden incluir, sin limitarse a ello, mantener la integridad del sistema (tal como la eliminación de virus), cumplir obligaciones legales (tal como citaciones judiciales) y efectuar ciertas funciones de administración del sistema (tal como remitir los mensajes con direcciones erróneas).

Sin embargo de lo anterior, el MINEDUC puede obtener acceso a la información de los servidores públicos y/o terceros en caso que se requiera dicha información para investigaciones, en caso de presentarse incidentes de seguridad, bajo requerimiento del Oficial de Seguridad de la Información o en caso de emergencia, como por ejemplo, si el empleado y/o tercero está ausente durante un período prolongado de tiempo debido a enfermedad u otro motivo, previa autorización escrita del jefe inmediato, para necesidades del servicio y de la Dirección Nacional de Tecnologías de la Información y Comunicaciones para las respectivas

investigaciones.

El MINEDUC se reserva el derecho de interceptar o vigilar cualquier tráfico de información que pase a través de los sistemas o aplicaciones de la institución como parte de sus actividades de vigilancia, mantenimiento, investigación, auditoria o seguridad del desempeño del sistema. Todo el personal debe ser informado respecto este derecho previo al uso los sistemas de tecnologías de información del MINEDUC.

Es responsabilidad del dueño del activo de información definir los periodos de retención y la frecuencia de sus respaldos a fin de garantizar el cumplimiento de sus obligaciones legales y sus propios fines.

Las políticas de seguridad de la información del MINEDUC están diseñadas para ajustarse o exceder, sin contravenir, las medidas de protección establecidas en las leyes y regulaciones; si algún empleado y/o tercero del MINEDUC considera que alguna política de seguridad de información está en conflicto con las leyes y regulaciones existentes, lo debe reportar en forma inmediata al Oficial de Seguridad de la Información de la Información.

CAPÍTULO VI

DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Art. 21:- Comité de Seguridad de la Información.- Créase el Comité de Seguridad de la Información institucional, el que consiste de un equipo humano multidisciplinario que se reúne con el objetivo de definir, revisar, aprobar, políticas de seguridad, aplicación de controles, aprobación de proyectos relacionados con seguridad de la información, así como analizar y priorizar mecanismos y actividades de mitigación de los riesgos críticos que afecten a la institución. Este Comité estará conformado por los siguientes miembros o sus delegados:

1. Ministro de Educación, quien participara con voz y voto.

2. Viceministros, quien participara con voz y voto.

3. Coordinador/a General de Gestión Estratégica, quien participará con voz y voto.

4. Coordinador/a General de Asesoría Jurídica, quien participara con voz y voto.

5. Coordinador/a General Administrativo y Financiero, quien participara con voz y voto.

6. Director Nacional de Tecnología de la Información y Comunicaciones, quien participara con voz.

7. Director de Talento Humano, quien participara con voz y voto.

8. Director Nacional de Auditoría Interna quien participara con voz; y,

9. Oficial de Seguridad de Información, quien participara con voz y a además actuará como Coordinador/a del Comité.

Este Comité se reunirá una vez al mes por convocatoria del Coordinador/a General de Gestión Estratégica. Podrá contar además con la presencia de más miembros con voz pero sin voto, en relación a los temas que vayan a tratarse en cada reunión. El comité emitirá un reglamento

para regular su funcionamiento.

Art. 22.- Atribuciones.- El Comité de Seguridad de la Información tendrá las siguientes atribuciones:

a. Revisar y aprobar la Política y las normas en materia de seguridad de la información.
b. Monitorear cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
c. Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
d. Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
e. Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
f. Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
g. Promover la difusión y apoyo a la seguridad de la información dentro de la institución.
h. Coordinar el proceso de administración de la continuidad de la operación de los sistemas de procesamiento de la información de la institución frente a incidentes de seguridad imprevistos.
i. Designar a los custodios de la información de las diferentes áreas de la entidad, que deberá ser formalizada en un documento. Cualquier cambio de custodio de la información deberá ser notificado al Oficial de Seguridad de la Información (coordinador del CSI) y formalizado nuevamente de manera individual, como alcance al documento inicial.
j. Gestionar la provisión permanente de recursos económicos, tecnológicos y humanos para la gestión de la seguridad de la información.

Art. 23.- Coordinador del Comité.- Serán competencias del Coordinador del Comité de Seguridad de la Información, las siguientes:

a. Coordinar el Comité de Seguridad de la Información.

b. Implementar y controlar el Esquema Gubernamental de Seguridad de la Información.

c. Definir procedimientos para el control de cambios a los procesos operativos, los sistemas e instalaciones, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.

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

e. Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.

f. Controlar los mecanismos de distribución y difusión de información dentro de la institución.

g. Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso, garantizar la seguridad de los datos y los servicios conectados a las redes de la institución.

h. Desarrollar procedimientos adecuados de concienciación de Servidores Públicos en materia de seguridad, controles de acceso al sistema y administración de cambios; e,

i. Verificar el cumplimiento de las normas, procedimientos y controles de seguridad establecidos.

Art. 24.- De las sanciones a los servidores públicos del MINEDUC.- En el caso de que se determinare que algún servidor público del MINEDUC utilice de manera indebida los equipos, servicios o activos tecnológicos institucionales o que en su defecto se produjeran daños graves a los sistemas institucionales por efecto del incumplimiento de las disposiciones dadas en el presente reglamento, sea por negligencia, irresponsabilidad y/o mal uso de los privilegios otorgados para la administración de servicios de parte del personal de la Dirección Nacional de Tecnologías de la Información y Comunicaciones, el Oficial de Seguridad de la Información informará a la Dirección Nacional de Talento Humano a fin de que se inicie el proceso y/o sumario respectivo.

En el caso de que se detecte lo señalado en el inciso anterior en relación a un contratista externo, consultor o proveedor el Oficial de Seguridad informará, según corresponda, al Director Nacional de Tecnología de la Información y Comunicaciones o a la Dirección Nacional de Patrocinio, para que se proceda al establecimiento de las acciones administrativas o legales a que haya lugar por el uso inadecuado de activos de información y de soporte que generen incidentes de seguridad.

Art 25.- De las acciones en contra de los ciudadanos y a los servidores de otras entidades.- En el caso de los ciudadanos y servidores públicos de otras entidades que no cumplieren con lo que establece este reglamento, el MINEDUC revocará de inmediato el acceso a los bienes y/o servicios tecnológicos que fueron prestados temporalmente y emprenderá las acciones administrativas, civiles y/o penales que corresponda de acuerdo con el perjuicio causado a la institución o a terceros.

Art. 26.- Notificación.- La revocatoria de los servicios informáticos será notificada al ciudadano o servidor correspondientes, por parte de la Dirección Nacional de Tecnologías de la Información y Comunicaciones, explicando las razones que justifiquen las medidas adoptadas.

DISPOSICIONES GENERALES

PRIMERA.- La Dirección Nacional de Cambio de Cultura Organizacional será la responsable a través del Oficial de Seguridad de la Información institucional de elaborar un plan de Seguridad de la Información anual. Este plan incluirá el levantamiento de las necesidades de seguridad de la Información de los servidores públicos, a efecto de implementar las modificaciones técnicas necesarias o adquirir nuevas tecnologías, funcionalidades y controles que permitan garantizar el uso óptimo de recursos, así como la definición de las mejores prácticas recomendadas por los fabricantes o proveedores de los equipos tecnológicos, y las acciones, correcciones o implementaciones que se deban realizar para asegurar la optimización de recursos institucionales sin afectar las labores cotidianas de los servidores públicos del MINEDUC de acuerdo a las Políticas de Seguridad de la Información.

SEGUNDA.- La Coordinación General Administrativa y Financiera del MINEDUC deberá analizar la factibilidad económica para el otorgamiento de firma digital a todos los servidores públicos del MINEDUC, y presentar un informe al Comité de Seguridad de la Información para determinar su viabilidad técnica y económica para evitar la emisión física de informes y

otros documentos, implementando mecanismos cero papeles en la institución.

TERCERA.- La movilización hacia el exterior de la institución de equipos informáticos asignados a los servidores públicos o de uso institucional solo puede ser autorizada por la Dirección Nacional Administrativa o quien haga sus veces en cada unidad administrativa desconcentrada.

CUARTA.- La Dirección Nacional de Tecnologías de la Información y Comunicaciones, en coordinación con la Dirección Nacional de Talento Humano, será responsable de capacitar de manera permanente al personal del MINEDUC sobre el buen uso de recursos y herramientas tecnológicas utilizadas en la institución, a través de plataformas tecnológicas que permitan a los servidores públicos acceder constantemente a entrenamientos en línea, capacitándolos en el uso autorizado, adecuado y razonable de las mismas. Estas capacitaciones incluirán evaluaciones individuales, cuyos resultados serán almacenados en la carpeta individual de cada servidor/a.

La Dirección Nacional de Cambio de Cultura Organizacional y el Oficial de Seguridad de la Información en coordinación con la Dirección Nacional de Talento Humano capacitarán al personal institucional sobre las Políticas de Seguridad de la Información y absolverán cualquier duda sobre la aplicación del presente reglamento.

QUINTA.- La Dirección Nacional de Tecnologías de la Información y Comunicaciones es responsable de:

a) Cumplir y ejecutar las Políticas de Seguridad de la Información que sean aprobadas por el Comité de Seguridad de la información del MINEDUC, e implementar los controles tecnológicos adecuados.

b) Apoyar en la difusión de las Políticas de Seguridad de la Información y procedimiento técnicos de Seguridad informática referidas a los activos, servicios y equipos tecnológicos a todos los Servidores Públicos del MINEDUC y a los Servidores Públicos/as finales que acceden a los recursos e información de la institución por las actividades relacionadas con la Institución.

SEXTA.- La Dirección Nacional de Cambio de Cultura Organizacional, en coordinación con la Dirección Nacional de Tecnologías de la Información y Comunicaciones exigirá la suscripción y firma del Acuerdo de Confidencialidad de la Información previa la facilitación de los servicios y equipos tecnológicos institucionales.

La suscripción de este acuerdo de confidencialidad de información y de las Políticas de Seguridad de la Información deberá ser extensiva a los proveedores, consultores, contratistas y demás servidores públicos externos y/o terceros que utilicen recursos tecnológicos e información de la institución.

El contenido del Acuerdo de Confidencialidad de Información y de las Políticas de Seguridad de la Información deberá ser elaborado y aprobado por el Comité de Seguridad de la Información del MINEDUC, creado por el presente reglamento.

SÉPTIMA.- Encárguense la Ejecución del presente reglamento a los titulares de la Coordinación General Administrativa Financiera del MINEDUC y de la Dirección Nacional de Tecnologías de la Información y Comunicaciones del MINEDUC.

DISPOSICIONES TRANSITORIAS

PRIMERA.- En el plazo no mayor a sesenta días desde la expedición del presente reglamento, el Comité de Seguridad de la Información del MINEDUC presentará a la Dirección Nacional de Talento Humano el Acuerdo de Confidencialidad de Información para servidores públicos para su aplicación y remisión a la unidad que haga sus veces en las diferentes unidades desconcentradas institucionales. Asimismo, las unidades que contraten servicios que impliquen la provisión o conexión a sistemas informáticos instituciones o el uso de información de tipo confidencial, deberán requerir la firma del Acuerdo de Confidencialidad y las Normas de seguridad para Terceros.

SEGUNDA.- Hasta el 31 de Diciembre del 2014 todos los servidores públicos, terceros y proveedores que actualmente acceden a los recursos y equipos tecnológicos del MINEDUC, deberán suscribir el Acuerdo de Confidencialidad de Información, así como la indicación expresa de conocimiento y aceptación de las Políticas de Seguridad del MINEDUC, caso contrario la Dirección Nacional de Tecnologías de la Información y Comunicaciones revocará los servicios otorgados. Este acuerdo se archivará en la carpeta personal que mantiene la Dirección Nacional de Talento Humano y en el registro que para el efecto deberá llevar la Dirección Nacional de Cambio de Cultura Organizacional, según corresponda.

TERCERA.- En el plazo no mayor a sesenta días tras la expedición del presente reglamento, la Dirección Nacional de Tecnologías de la Información y Comunicaciones, en coordinación con la Dirección Nacional de Talento Humano, emitirá el documento técnico de asignación de perfiles y categorías de navegación de los cargos institucionales a las y los servidores públicos definidos en la Política de Seguridad de la Información.

CUARTA.- En el plazo no mayor a noventa días desde la expedición del presente reglamento, la Dirección Nacional de Tecnologías de la Información y Comunicaciones presentará para la aprobación de la máxima autoridad un Plan de Capacitación a los Servidores Públicos del MINEDUC sobre el uso y control de las tecnologías y servicios brindados por la Institución. La ejecución de este plan deberá ser validada y aprobada conjuntamente con la Dirección Nacional de Talento Humano y la coordinación de la Dirección Nacional de Gestión de Cambio de Cultura Organizacional.

DISPOSICION FINAL.- El presente reglamento entrará en vigencia a partir de la fecha de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

COMUNÍQUESE Y PUBLÍQUESE.- Dado, en el Distrito Metropolitano de Quito, a

Dado en Quito, D.M., a los 15 día(s) del mes de Octubre de dos mil catorce.

Documento firmado electrónicamente

AUGUSTO X. ESPINOSA A.
MINISTRO DE EDUCACIÓN