MINISTERIO DE MINERÍA

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

VERSIÓN: 1.0

JULIO - 2016

QUITO – ECUADOR

ÍNDICE

1. NORMATIVA

La presente Política de Seguridad de la Información se fundamenta en la siguiente normativa:

- Ley Orgánica de Servicio Público
- Reglamento General a la Ley Orgánica del Servicio Publico
- Ley Orgánica de Transparencia y Acceso a la Información Pública en sus artículos 5 y 6:

Art. 5.-" 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 ",*

Art. 6.-" Información Confidencial.- *Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República.*

El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes. No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades, públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución Política de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas".

- Normativa Secundaria de la Contraloría General de Estado que hace referencia a la gestión de Tecnologías de la Información.

410-01 Organización informática

"Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de

"La unidad de tecnología de información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades…".

410-10 Seguridad de tecnología de información

"La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos…"

410-11 Plan de contingencias

"Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado."

410-12 Administración de soporte de tecnología de información

"La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen."

2. OBJETIVOS:

- Proteger todo tipo de información digital y/o electrónica, que se encuentre en cualquier clase de registro o medio, que almacene datos o contenga información del Ministerio de Minería.

- Proteger la información en caso de que exista un desastre natural.

- Elaborar políticas de protección de la información contra pérdida de confidencialidad, integridad o disponibilidad, tanto de forma accidental como intencionada.

La información a la que tenga acceso el personal del Ministerio de Minería, estará regulada a través del acuerdos de confidencialidad que se suscriban, los mismos que demostraran la obligación de los servidores públicos del Ministerio de Minería de **mantener confidencial la información recibida** de parte de la institución y que serán elaborados por la Coordinación General Jurídica, a los que se implementen los elementos de control apropiados y sobre la base de las disposiciones constantes en la Ley Orgánica de Transparencia y Acceso a la Información Pública.

4.2. OBLIGATORIEDAD

Se encuentran sujetos al cumplimiento de las presentes políticas todos los servidores públicos del Ministerio de Minería con nombramiento, contrato, comisión de servicio o licencia, o cualquiera que tenga relación laboral con el Ministerio de Minería, como requisito para tener acceso a la información institucional.

4.3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La información digital constituye un activo del Ministerio de Minería, que debe ser administrada y protegida, para garantizar su disponibilidad, confidencialidad e integridad, por todos los servidores públicos del Ministerio de Minería con nombramiento, contrato, comisión de servicio o licencia, o cualquiera que tenga relación laboral con el Ministerio de Minería, en cumplimiento a los políticas determinadas en la presente política.

4.3.1. Administración de seguridad informática

La administración de la seguridad informática estará a cargo de la Coordinación General de Planificación y Gestión Estratégica a través de la Dirección de Tecnologías de la Información y Comunicaciones, que debe satisfacer requerimientos institucionales como son:

- Garantizar la continua disponibilidad de los sistemas de información;
- Asegurar la integridad de la información almacenada en sus sistemas informáticos y bases de datos;
- Preservar la confidencialidad de todos los datos calificados como "reservados", por el órgano o entidad competente, permitiendo su acceso solo a usuarios autorizados;

Los usuarios deberán utilizar contraseñas de mínimo de ocho caracteres donde no intervenga o haga referencia al nombre o apellido del servidor público (Ejemplos: Dato2015, Planificación013). El personal de la Dirección de Tecnologías de la Información y Comunicaciones, especificará las características que deben tener las contraseñas, de modo que se fortalezca el control de acceso a los equipos y/o sistemas informáticos.

Se prohíbe a los usuarios dar a conocer o difundir sus contraseñas a terceras personas; quien lo hiciere, será responsable de las actividades que se realicen con su cuenta de usuario y contraseña.

En caso de que el usuario sospeche que su contraseña ha sido vulnerada, deberá cambiarla inmediatamente, usando las opciones disponibles para este efecto; o, solicitar soporte técnico inmediato al personal de la Dirección de Tecnologías de la Información y Comunicaciones, notificando del particular.

En caso de que un usuario olvide su contraseña o se produzca un bloqueo de su cuenta de usuario debido a intentos fallidos de ingreso o por olvido de contraseña, deberá solicitar asistencia al personal de la Dirección de Tecnologías de la Información y Comunicaciones, para que se realice el restablecimiento de su cuenta, con el cambio obligatorio de la contraseña.

Las contraseñas se deberán cambiar trimestralmente, para ello el personal de la Dirección de Tecnologías de la Información y Comunicaciones implementará el sistema informático necesario, que obligue al cambio de contraseña una vez finalizado el tiempo establecido a través de la configuración en los servidores.

Los servidores públicos no deberán escribir ni registrar en ningún medio la contraseña o dejarla en cualquier sitio de fácil acceso.

4.3.4. Creación, mantenimiento y eliminación de usuarios del dominio y de los sistemas del Ministerio de Minería.

4.3.4.1. Creación de usuarios en la red interna.

La cuenta de usuario es la que permite el acceso a los equipos o sistemas de información que posee el Ministerio de Minería. Estas cuentas pueden bloquear el acceso a otras personas que no pertenecen al Ministerio de Minería o que no tienen el permiso suficiente para hacerlo.

electrónico el cese de actividades de servidores públicos del Ministerio de Minería, para proceder con la desactivación de las cuentas y respaldar la información correspondiente.

El servidor/a, que deje de pertenecer al Ministerio de Minería, devolverá al Ministerio de Minería en un estado de conservación aceptable, todos los equipos informáticos que le hayan sido entregados durante el desempeño de sus funciones, para lo cual, el personal de la Dirección de Administrativa revisará el o los equipos con el fin de verificar su funcionamiento y buen estado, lo cual quedará asentado en el formato de paz y salvo para la desvinculación del personal.

4.3.4.3. Mantenimiento de usuarios de la red interna

El mantenimiento de las cuentas de Windows, cuentas de correo electrónico y cuentas de aplicaciones se realizará considerando lo siguiente: cambio de claves, restauración de cuentas, limpieza de buzones de correo, registro actualizado de las cuentas creadas.

4.4. INFORMACIÓN INSTITUCIONAL

4.4.1. Prohibición de divulgación de la información

Se prohíbe expresamente dar a conocer información del Ministerio de Minería, ya sea por medios físicos o digitales tales como: correo electrónico, redes sociales, memorias flash, discos duros externos, etc., salvo previa autorización del Director o Coordinador de cada área y en aquellos casos en los cuales se hubiere dispuesto por la máxima autoridad su difusión o publicación, a través de los canales institucionales.

Los servidores públicos del Ministerio de Minería que realicen intercambio de información de trabajo, deberán tomar las debidas precauciones, para impedir que la información se filtre a personas no autorizadas.

4.4.2. Manejo de dispositivos de Información

A fin de garantizar la integridad, confidencialidad de la información, seguridad y evitar el acceso no autorizado de datos, robo de datos, daño de archivos, etc., el personal de la Dirección de Tecnologías de la Información y Comunicaciones, de forma programada procederá a:

- Se restringirá el uso de internet para: los sistemas públicos de redes sociales, armas, servicios de video y audio; estos servicios estarán sujetos a la aprobación o autorización por parte de la Coordinación General de Planificación y Gestión Estratégica.

- Si un servidor público requiere de acceso a un sitio de internet que se encuentre restringido, deberá remitir una solicitud por correo electrónico o documento físico, misma que deberá estar autorizada por su jefe inmediato o Coordinador de cada área, la cual una vez aprobada y notificada a la Coordinación General de Planificación y Gestión Estratégica, podrá ser habilitada a través de la Dirección de Tecnologías de la Información y Comunicaciones.

- Se prohíbe utilizar el servicio de internet del Ministerio de Minería para establecer conexiones no autorizadas.

- Se prohíbe el uso de cualquier tipo de software que vulnere las seguridades del sistema de firewall del Ministerio, para recibir contenido no autorizado a través del internet.

4.5.2. Uso del correo electrónico

El correo electrónico es la herramienta que se utiliza para las actividades que los servidores públicos del Ministerio de Minería requieran según sus competencias. No obstante, se evitará incurrir en riesgos ocasionados por su inadecuada utilización, por lo cual se tendrá en cuenta las disposiciones de Ley de comercio electrónico, firmas y mensajes de datos y demás, observando las siguientes reglas:

- A los servidores públicos del Ministerio de Minería se les asignará una cuenta de correo electrónico oficial, la cual será proporcionada por la Coordinación General de Planificación y Gestión Estratégica a través del personal de la Dirección de Tecnologías de la Información y Comunicaciones.

- La cuenta de correo electrónico será individual, a la cual se accederá mediante la clave personal entregada por la Dirección de Tecnologías de la Información y Comunicaciones, y será una herramienta de uso obligatorio en temas institucionales.

- La cuenta de correo electrónico será responsabilidad exclusiva de su titular.

- Cada usuario de correo electrónico será responsable del almacenamiento de mensajes y anexos válidos, siendo su obligación eliminar elementos innecesarios.

Se debe considerar las siguientes instrucciones para el manejo de las computadoras de escritorio o portátiles y más dispositivos móviles:

- Se prohíbe utilizar los equipos informáticos de propiedad del Ministerio de Minería para asuntos personales, aunque dicho manejo se realice fuera del horario de trabajo.

- Queda prohibido obtener por cualquier medio, sin el debido consentimiento, información de uno de los computadores o de la red informática del Ministerio de Minería, para ser utilizada de forma personal o para terceros, con fines ajenos a los propósitos de la entidad.

- Está prohibido manipular los equipos informáticos institucionales, así como instalar, extraer, cambiar dispositivos externos o internos, accesorios y elementos que sean de propiedad del Ministerio de Minería.

- Se prohíbe instalar en los equipos informáticos, programas diferentes a los utilizados en las actividades del Ministerio de Minería, tales como: servidores de correo, aplicaciones web, archivos ejecutables, proxy o similares, juegos y en general cualquier tipo de software, sea éste de licencia libre o propietaria, que pueda dañar los equipos o sistemas del Ministerio de Minería.

- Está prohibido instalar, enviar o utilizar archivos, imágenes, documentos o programas de contenido ofensivo, inapropiado o discriminatorio.

- Está prohibido conectar equipos de cómputo que no sean del Ministerio de Minería a la red local, que pretendan acceder a información no autorizada o manipular archivos o bases de datos que contengan información confidencial o reservada. Considerando información confidencial o reservada a la información expresamente establecida como reservadas en leyes vigentes.

- Se sugiere a los funcionarios, que al ausentarse de su puesto de trabajo, bloqueen o apaguen el computador asignado, o que soliciten al personal de la Dirección de Tecnologías de la Información y Comunicaciones la implementación del bloqueo automático de los equipos después de diez minutos o menos de no haber sido utilizados.

- Se prohíbe borrar de los equipos informáticos, archivos, programas o cualquier otro medio la información almacenada que tenga relación con el Ministerio de Minería.

- Si por cuestiones estrictamente institucionales, fuere preciso instalar algún programa o aplicación informática de la que no disponga el Ministerio, el usuario deberá contactar con el

electrónico a la Coordinación General de Planificación y Gestión Estratégica que el servidor público entregará para su resguardo el computador portátil a su superior inmediato.

- Cada usuario precautelará la integridad del computador que le haya sido asignado, así como la información y programas almacenados en el mismo. En caso de pérdida o sustracción, este evento debe ser reportado inmediatamente al superior inmediato y se debe realizar un informe que será presentado a la Coordinación General Jurídica, quienes realizarán la respectiva denuncia, para presentarla luego a la Coordinación General Administrativa Financiera y continuar de esta manera con el trámite correspondiente para la reposición del bien.

4.5.4. Uso de las impresoras, copiadoras y escáner

Las impresoras, copiadoras y escáner son recursos informáticos, que se encuentran a cargo de una o varias Coordinaciones y están a disposición de los servidores públicos del Ministerio de Minería, por lo que deben ser utilizados pensando siempre en la optimización de los recursos públicos, por consiguiente se deben aplicar las siguientes normas:

- A los servidores públicos del Ministerio de Minería, se les asignará los respectivos equipos necesarios para el desarrollo de las labores en tanto sea posible, los equipos que lo permitan, serán activados a través de claves;

- El personal de la Dirección de Tecnologías de la Información y Comunicaciones, implementará los mecanismos que permitan monitorear el uso adecuado de los recursos de las impresoras, tales como la frecuencia de cambio de tóner y mantenimiento de equipos, para ello se procederá, según la necesidad de cada Coordinación.

- Los servidores públicos del Ministerio de Minería serán responsables de la información que impriman.

- Los equipos deberán estar ubicados en sitios de fácil acceso.

- Se prohíbe usar las impresoras, escáner, copiadoras y equipos en general, en funciones diferentes a las institucionales impuestas por el Ministerio de Minería.

- Queda prohibido el manipular los equipos informáticos por personal diferente a los técnicos de la Dirección de Tecnologías de la Información y Comunicaciones, autorizados para el efecto;

El personal de la Dirección de Tecnologías de la Información y Comunicaciones, será el área encargada de coordinar el mantenimiento preventivo y correctivo con el responsable de bienes institucionales, así como de dar soluciones a los problemas que se presenten con los equipos informáticos y el soporte a los usuarios en el uso del software que el Ministerio de Minería disponga para las actividades de los funcionarios

4.6. CONTROL DE RECURSOS INFORMÁTICOS Y DE TELECOMUNICACIONES

Todos los equipos, aplicaciones y herramientas informáticas de propiedad del Ministerio de Minería, puestos a disposición de los servidores/as, deberán ser utilizados por éstos con fines exclusivamente institucionales y relacionados con las funciones que desempeñan. El Ministerio de Minería se reserva el derecho de comprobar, en el momento que considere necesario, si su utilización se ajusta a dicha finalidad y a lo previsto en este reglamento.

4.6.1. Tipos de control

- **Control concurrente.-** De manera permanente, solo los servidores autorizados por la Coordinación General de Planificación y Gestión Estratégica, monitorearán y brindarán soporte y seguridad, revisarán y verificarán, a través de la red interna del Ministerio de Minería, los programas instalados y los servicios puestos a disposición de los servidores/as de la institución, precautelando la privacidad, integridad y confidencialidad de la información, siempre enmarcados dentro de las actividades propias que son de su competencia.

- **Control a través del acceso físico a los equipos informáticos.-** El control por parte de los responsables del Ministerio de Minería podrá ser realizado a través del acceso físico a los equipos informáticos de las y los servidores, ante indicios de eventuales usos indebidos de los equipos asignados. Dicho control deberá efectuarse, de ser el caso, mediante una revisión de tecnología informática. El acceso podrá realizarse en función de las circunstancias presentadas. El proceso de control que se realice, garantizará la legalidad, legitimidad, privacidad y confidencialidad de la información contenida en el equipo, de acuerdo al siguiente procedimiento:

  - La revisión se hará por parte de un profesional en materia informática de la Dirección de Tecnologías de la Información y Comunicaciones.

  - Se hará en presencia del servidor/a al que esté asignado el equipo informático que sea objeto de control, dentro de la jornada de trabajo. Si el servidor/a se niega a estar presente durante el control y revisión de su equipo, se hará constar esta circunstancia en el acta en la cual se detallará la revisión que se efectuó y todas las circunstancias que se presentaron.

4.7. REGLAS ESPECIALES PARA LA REVISIÓN DEL CORREO ELECTRÓNICO

El servicio de correo electrónico que el Ministerio de Minería brinda a las y los servidores, deberá ser usado para propósitos institucionales y no deberá comprometer la imagen institucional.

El Ministerio de Minería, a través de la Coordinación General de Planificación y Gestión Estratégica, establecerá la metodología necesaria para que las y los servidores realicen un buen uso y manejo de las direcciones electrónicas que la entidad dispone para la comunicación interna y externa.

Únicamente, las unidades administrativas o personal autorizado por la Coordinación General de Planificación y Gestión Estratégica, podrán realizar envíos de correos masivos, sea dentro o fuera de la institución.

La Coordinación General de Planificación y Gestión Estratégica a través de la Dirección de Tecnologías de la Información y Comunicaciones, una vez que identifique los correos que no contengan información institucional, comunicará a la máxima autoridad o su delegado, quien dispondrá a través del personal autorizado que se realice una indagación informática, aplicada en los siguientes casos:

- Cuando existan claros indicios del cometimiento de infracciones que impliquen la indebida utilización del correo electrónico institucional; y,

- Cuando se presuma que mediante la utilización del correo electrónico, existe acoso o cualquier otro tipo de comportamiento indebido que pudiera ocasionar perjuicio a servidores/as, proveedores y personas vinculadas o no con la institución.

4.8. MECANISMOS DE SEGURIDAD

Se refiere a las configuraciones propias sobre los equipos y sistemas informáticos de propiedad del Ministerio de Minería, con el ánimo de prevenir posibles eventos que atenten contra la estabilidad de un equipo o sistema, así como la fuga de información.

Dentro de las medidas de seguridad que los sistemas de gestión de base de datos permiten, una vez que el Ministerio de Minería cuente con bases de datos, se monitoreará y se administrará los usuarios que accedan a los datos almacenados, se les asignará permisos de acuerdo a sus funciones y se aplicarán las siguientes medidas de seguridad:

Físicas

Controlar el acceso a los servidores, el acceso solo lo tendrá el personal técnico de la Dirección de Tecnologías de la Información y Comunicaciones.

Software

Identificación y autentificación de gestión de base de datos, donde existen diversos elementos que ayudan a controlar el acceso a los datos, y en primera instancia el sistema deberá identificar y autentificar a los usuarios utilizando alguno de los siguientes métodos:

- Código y contraseña.
- Identificación por hardware.

Dentro de la identificación se especificará los privilegios que el usuario tendrá sobre la base de datos:

- Consultar datos.
- Actualizar datos.
- Crear o actualizar objetos.
- Ejecutar procedimientos almacenados.

4.8.3.2. Tipos de usuario en la base de datos

Para el acceso a las bases de datos, el personal de la Dirección de Tecnologías de la Información y Comunicaciones asignará los perfiles de usuarios que permitan gestionar, monitorear, modificar y evitar la pérdida de los datos almacenados en las bases de datos del Ministerio de Minería, considerando las siguientes categorías:

- Usuarios súper administradores que permitan crear usuarios, asignar perfiles y generar respaldos de datos.

- Usuarios administradores que permitan crear, borrar y modificar objetos, y que además puedan conceder privilegios a otros usuarios sobre los objetos que han creado.

- Usuarios operadores nivel 1 que permitan crear y modificar objetos.

- Coordinar los mantenimientos preventivos de los equipos considerados críticos.

4.10. RESPALDOS DE INFORMACIÓN DIGITAL

Para realizar respaldos de seguridad de la información, se clasificar en crítica y no crítica.

Información crítica es toda aquella que es indispensable para el buen funcionamiento del Ministerio de Minería, como lo son las bases de información de los siguientes sistemas internos:

- Sistema de correo electrónico
- Sistema biométrico
- Desarrollo interno de aplicaciones
- Demás sistemas que adquiera el Ministerio de Minería para su operación

Información no crítica es aquella generada por los usuarios y la que ellos consideran importante para el desarrollo de sus actividades.

- Archivos de office
- Archivos pdf
- Documentos en general, generados por los usuarios

La frecuencia de generación de respaldos de la información se realizará de manera semanal a través del sistema de respaldos back ups, en el caso de disponer de los fondos para contar con esta herramienta, de lo contrario se realizará manualmente de forma mensual, por parte de los técnicos de la Dirección de Tecnologías de la Información y Comunicaciones.

El respaldo mensual incluirá todos los días del mes que finaliza en lo posible, en caso de que existan sistemas que cierran las operaciones los siguientes días del próximo mes, el respaldo se generará considerando la fecha de cierre.

5. RÉGIMEN SANCIONADOR

5.1. INCUMPLIMIENTO DE OBLIGACIONES

El incumplimiento de las obligaciones previstas en la presente política, viabilizará la aplicación de las Normas Internas por parte de la Dirección de Administración de Recursos Humanos del Ministerio de Minería, según corresponda, sin perjuicio de las responsabilidades administrativas, civiles o penales, en las que pudiere incurrir la o el servidor público por el mismo hecho. Así como aquellas personas que ocasionalmente presten sus servicios en la entidad y tengan acceso a la información institucional.

7. REVISIÓN

REVISADO POR:	Freddy Gallardo	**Coordinador General de Planificación y Gestión Estratégica**	
REVISADO POR:	Alejandro Estrada	**Director de Tecnologías de la Información y Comunicaciones, Subrogante**	
ELABORADO POR:	Estefanía Molina	**Analista de Tecnologías de la Información y Comunicaciones**	

8. APROBACIÓN

APROBADO POR:	Javier Córdova	**Máxima Autoridad Ministerio de Minería**	