Acuerdo MERNNR-MERNNR-2019-0033-AM Emítese la Política de Seguridad de la Información

MINISTRO DE ENERGÍA Y RECURSOS NATURALES NO RENOVABLES

Considerando:

Que, el numeral 1 del artículo 154 de la Constitución de la República confiere a los ministros de Estado, además de las atribuciones establecidas en la ley, la rectoría de las políticas del área a su cargo, así como la facultad de expedir acuerdos y resoluciones administrativas;

Que, el artículo 226 de la Carta Magna señala que las instituciones del Estado, sus organismos, dependencias, los servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la Ley debiendo coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución;

Que, el artículo 227 de la Constitución de la República, establece: "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, mediante Acuerdo Ministerial No. 166 de 19 de septiembre de 2013, publicado en el Registro Oficial Suplemento No. 88 del 25 de septiembre de 2013, el Secretario Nacional de la Administración Pública, acuerda: "Art. 1.- Disponer a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.";

Que, el artículo 7 del Acuerdo Ministerial No. 166, dispone que las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos de su institución, en base a la norma INENISO/IEC 27005 Gestión del Riesgo en la Seguridad de la Información;

Que, el Anexo 1 del antedicho Acuerdo, referente al Esquema Gubernamental de Seguridad de la Información (EGSI) en la sección introductoria, numeral 2.1., literal c), establece como compromiso de la máxima autoridad de la institución en cuanto a la seguridad de la información, la conformación oficial del Comité de Gestión de la Seguridad de la Información de la institución (CSI) y designar a sus integrantes;

Que, el Anexo 1 del Acuerdo Ministerial No. 166, de 19 de septiembre de 2013, señala:

"I. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1.1. Documento de la Política de la Seguridad de la Información

a. La máxima autoridad de la institución dispondrá la implementación de este Esquema Gubernamental de Seguridad de la Información (EGSI) en su entidad (*) (1).

b. Se difundirá la siguiente política de seguridad de la información como referencia (*):

"Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada

como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera".

"2.2. Coordinación de la Gestión de la Seguridad de la Información

a) La coordinación estará a cargo del Comité de Gestión de Seguridad de la Información el cual tendrá las siguientes funciones:

- Definir y mantener la política y normas institucionales particulares en materia de seguridad de la información y gestionar la aprobación y puesta en vigencia por parte de la máxima autoridad de la institución así como el cumplimiento por parte de los funcionarios de la institución".

Que, el artículo 12 del Acuerdo Ministerial No. 1606 de fecha 17 de mayo de 2016, publicado en Registro Oficial No. 776 de 15 de junio de 2016, dispone: "Suprímase la frase de "Comités de Gestión de Seguridad de la Información" de la Disposición General Tercera del Acuerdo Ministerial No. 166 de 19 de septiembre de 2013, publicado en el Segundo Suplemento del Registro Oficial No. 88 de 25 de septiembre de 2013".

Que, el artículo 13, del Acuerdo Ministerial No. 1606, manifiesta: "Todas las atribuciones y responsabilidades conferidas al "Comité de Seguridad de la Información - CSI" en el Esquema Gubernamental de Seguridad de la Información -EGSI, emitido a través del Acuerdo Ministerial No. 166, de 19 de septiembre de 2013, publicado en el Segundo Suplemento del Registro Oficial No. 88 del 25 de septiembre de 2013, serán asumidas por la Unidad de Gestión Estratégica o quien haga sus veces en cada entidad de la Administración Pública Central, Institucional y que depende de la Función Ejecutiva;

o por la unidad encargada de la Gestión de Riesgos Institucionales o Seguridad de la Información, cuando se cuente con aquella dependencia en la estructura orgánica institucional".

Que, mediante Memorando Nro. MH-DM-2016-0074-ME de 17 de junio de 2016, el entonces Ministro de Hidrocarburos informó sobre la eliminación de los Comités de Gestión de Seguridad de la Información y delega las atribuciones y responsabilidades conferidas del citado Comité, a la Coordinación General de Planificación y Gestión Estratégica, en cumplimiento de lo señalado en el artículo 13 del Acuerdo Ministerial No. 1606.

Que, mediante Decreto Ejecutivo No. 8 de 24 de mayo de 2017, el Sr. Presidente de la República, Lic. Lenin Moreno, designa como Ministro de Hidrocarburos al Sr. Ing. Enrique Pérez García.

Que, mediante Decreto Ej ecutivo No. 3 99, de 15 de mayo de 2018 el Presidente Constitucional de la República decreta la fusión por absorción al Ministerio de Hidrocarburos, las siguientes instituciones: Ministerio de Electricidad y Energía Renovable, Ministerio de Minería y la Secretaría de Hidrocarburos. Una vez concluido el proceso de fusión por absorción, Modifíquese la denominación del Ministerio de Hidrocarburos a "Ministerio de Energía y Recursos Naturales No Renovables".

Que, la Disposición General Segunda, del antedicho Decreto Ejecutivo manifiesta: "Una vez concluido el proceso de fusión por absorción, en la normativa vigente en donde se haga referencia al "Ministerio de Electricidad y Energía Renovable", al "Ministerio de Minería", al Ministerio de Hidrocarburos"; y a la "Secretaría de Hidrocarburos", léase "Ministerio de Energía y Recursos Naturales No Renovables".

Que, mediante Decreto Ejecutivo Nro. 471, de 08 de agosto de 2018 el presidente constitucional de la República decreta el plazo para la fusión por absorción es ampliado por treinta (30) días contados a partir de la entrada en vigencia del presente Decreto Ejecutivo.

Que, el señor Presidente Constitucional de la República, mediante Decreto Ejecutivo Nro. 472 del 08 de agosto de 2018, dispone la creación adicional de los Viceministerios de Minas y de Electricidad y Energía Renovable, dentro de la estructura orgánica del Ministerio de Hidrocarburos, excepcionando lo previsto en el Decreto Ejecutivo 1121 de 18 de julio de 2016.

Que, Mediante Acuerdo Ministerial No. MERNNR 2018-0025-AM de fecha 28 de septiembre del 2018, se expidió el Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Energía y Recursos Naturales No Renovables.

Que, la Coordinación General de Planificación y Gestión Estratégica del Ministerio de Energía y Recursos Naturales No Renovables, recibió a través de memorando No. MERNNR-COGEAF-2019-0265-ME de 25 de abril de 2019, la propuesta de la Política de Seguridad de la Información por parte de la Coordinadora General Administrativa Financiera, y resolvió ponerla a consideración del Ministro de Energía y Recursos Naturales No Renovables.

Que, mediante Acción de Personal No. DATH-2019-247 vigente a partir del 23 de mayo de 2019, se nombró al Ing. Juan Carlos Bermeo Calderón como Viceministro de Hidrocarburos del Ministerio de Energía y Recursos Naturales No Renovables;

Que, con Acción de Personal No. DATH-2019-249 vigente a partir del 21 de mayo de 2019, se nombró al Ing. Juan Carlos Bermeo Calderón como Ministro de Energía y Recursos Naturales No Renovables, Subrogante desde el 31 de mayo hasta el 1 de junio de 2019;

En ejercicio de las facultades y atribuciones que le confieren los artículos 154 de la Constitución de la República; 17 del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva, Acuerdo Ministerial No. MERNNR-2019-0024-AM de 14 de mayo de 2019;

Acuerda:

Art. 1.- Emitir la Política de Seguridad de la Información del Ministerio de Energía y Recursos Naturales No Renovables, la misma que es de aplicación obligatoria para todos los funcionarios y servidores de la Institución, así como para terceras personas; y, que consta como Anexo al presente Acuerdo.

Art. 2.- De la ejecución del presente Acuerdo Ministerial encárguese a la Coordinación General de Planificación y Gestión Estratégica, al Oficial de Seguridad de la Información y al Responsable de Seguridad del Área de Tecnologías de la Información y Comunicación.

Art. Final.- El presente Acuerdo entrará en vigencia a partir de su expedición, sin perjuicio de su publicación en el Registro Oficial.

Dado en Quito, D.M. , a los 03 día(s) del mes de Junio de dos mil diecinueve.

f.) Sr. Ing. Carlos Enrique Pérez García, Ministro de Energía y Recursos Naturales No Renovables.

MINISTERIO DE ENERGÍA Y RECURSOS NATURALES NO RENOVABLES.- Es fiel copia del original.- 06 de junio de 2019.- f.) Ilegible, Secretaria General.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE ENERGÍA Y RECURSOS NATURALES NO RENOVABLES

Contenido

1. OBJETIVO

Establecer la política general que regirá y normará la Seguridad de la Información que garantice la confidencialidad, integridad y disponibilidad, mediante el desarrollo y aplicación de reglas, procesos, procedimientos y tecnologías en el Ministerio de Energía y Recursos Naturales No Renovables.

2. ALCANCE

Esta política se aplica para todos los bienes y activos de la información pertenecientes al Ministerio de Energía y Recursos Naturales No Renovables y será responsabilidad en forma general y obligatoria para todas las autoridades, funcionarios, servidores y trabajadores de la institución; así como para terceros.

3. BASE LEGAL

3.1. Constitución de la República del Ecuador

1. Numeral 19 del articulo 66.- "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de es le carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley":

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

3.2 Ley de Transparencia y Acceso a la Información

3.2.1. Art. 5.- "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 ";

3 2.2. 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 [...]";

3.2.3. Art. 17.- "No procede el derecho a acceder a la información pública, exclusivamente en los siguientes casos: […] b) Las informaciones expresamente establecidas como reservadas en leyes vigentes". El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes.";

3.3 El artículo 22 de la Ley Orgánica de Servicio Público, LOSEP, establece los deberes de las y los servidores públicos.

3.4. Mediante Acuerdo Ministerial 166, emitido por la Secretaria Nacional de la Administración Publica, publicado en el Registro Oficial No. 88 del 26 de septiembre del 2013, se dispuso el uso obligatorio de las normas nacionalesINEN ISO/IEC 27000 para Gestión de la Seguridad de la Información en todas las entidades de la Administración Publica.

3.5. El artículo 15 del Reglamento Interno de Administración del Tálenlo Humano del Ministerio, emitido a través de Acuerdo Ministerial Nro. MRNNR-DM-2014-0576-AM de 28 de abril de 2014., en su numeral 12, señala: "Guardar reserva de información, datos y resoluciones que tengan ese carácter propio de la función que desempeña, de conformidad como lo establece la LOSEP y su Reglamento General;"

4. TÉRMINOS Y DEFINICIONES

- **Activo de información:** Es la información en cualquier forma que esta se manifieste, la misma que se almacena, procesa, resguarda, gestiona, transmite y que tiene valor para la institución y el Estado. Un activo de información, además, es aquel elemento que contiene, transmite o manipula información, corno puede ser: Bases de Datos, servidores, PC's, canales de comunicación y demás componentes tecnológicos.

- **Confidencialidad:** Propiedad de la Información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

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

- **EGSI:** Esquema Gubernamental de Seguridad de la Información.

- **Incidente de la seguridad de la información:** Es un evento adverso en un sistema de computadoras, red de computadoras, procedimiento, leyes o políticas vigentes, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

- **Información Confidencial:** Es toda información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales.

- **Información Pública:** Es todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere la Ley. contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado.

- **Información Reservada:** Es toda información declarada como confidencial, estratégica y sensible a los intereses de la institución, desde el punto de vista tecnológico, comercial y de mercado.

- **Integridad:** Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- **MERNNR:** El Ministerio do Energía y Recursos Naturales No Renovables de la República de Ecuador.

- **Normativa:** Lineamientos específicos que afianzan al cumplimiento de la política; conjunto de reglas generales que cumplen con un objetivo.

- **Procedimiento:** Conjunto de actividades detalladas alineadas a un objetivo que genera un resultado específico.

- **Seguridad de la Información:** Son todas aquellas medidas preventivas y reactivas de las personas, de las instituciones y de los sistemas de información que permitan resguardar y proteger la información buscando mantener la confidencialidad; la disponibilidad y la integridad de la misma.

- **Sistema de información:** Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

- **Tercero:** Cualquier persona ya sea natural o jurídica, que se de la firma de un contrato o convenio, hace uso de los sistemas de información para el desarrollo de las actividades que relacionan la generación, procesamiento y resguardo de la información y ello implica su adhesión plena e incondicional a estas Políticas.

- **TI:** hace referencia a las Tecnologías de la Información.

- **Usuario:** Cualquier persona que acceda a los servicios de la Dirección de Tecnologías de la Información Comunicación, bajo cualquier relación de dependencia con la Institución hace uso de los sistemas de información para el

desarrollo de las actividades que relacionan la generación, procesamiento y resguardo de la información y ello implica su adhesión plena e incondicional a estas Políticas, por lo tanto es responsabilidad del Usuario leerías previamente, de tal manera que esté consciente de que se sujeta a ellas y a las modificaciones que pudieran sufrir.

5. POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

5. El Ministerio de Energía y Recursos Naturales No Renovables, al generar, utilizar, procesar, compartir y/o almacenar información en medio electrónico o escrito, que se clasifica como pública, confidencial, reservada o no reservada, aplicará el Esquema Gubernamental de Seguridad de la Información (EGSI) y las normativas, políticas o cualquier cuerpo normativo vigentes en los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad o disponibilidad de la información, de acuerdo a las necesidades de la Institución,

5. La información, como activo principal de la Institución, debe mantenerse bajo métodos formales de salvaguarda para acceder, producir, procesar, intercambiar y/o gestionar en cualquier medio que esta se encuentre: verbal, escrita, electrónica, en las aplicaciones informáticas, incluyendo el conocimiento de los funcionarios que por la naturaleza de sus funciones han adquirido y su revelación ponga en riesgo a personas y activos de información.

5. Los equipos, sistemas y recursos informáticos solo podrán ser utilizados para funciones propias de la institución.

5.4. La información generada por los servidores en el desempeño de sus actividades asignadas son de propiedad exclusiva del MERNNR y deberá permanecer únicamente en los medios de almacenamiento establecidos por la institución.

6. RESPONSABILIDAD

6.1. Cada servidor tiene la responsabilidad de cumplir con esta política. Los funcionarios de nivel jerárquico superior impartirán disposiciones para controlar el cumplimiento de esta política por parte de los servidores bajo su dirección.

6. Es responsabilidad do todas las autoridades, funcionarios, servidores y trabajadores de la institución, cumplir con todas las políticas, normativas y regulaciones vigentes establecidas para la Seguridad de la Información, actuando de manera oportuna, proactiva y coordinada, a fin de prevenir, contrarrestar las amenazas y mitigar los riesgos que atenten contra la información de la Institución.

6. Toda la Información de la Institución es de responsabilidad del servidor que la genere, procese o custodie; por lo que se deberá cumplir con los mandatos que la ley establece para el manejo de la información clasificada y velar por la protección de la misma.

Las responsabilidades de emitir, mantener, implementar, administrar, controlar y ejecutar las políticas, normas, procedimientos del Esquema Gubernamental de Seguridad de la Información serán realizadas conforme a lo establecido en el Acuerdo No. 166 y sus reformas, con el apoyo de los

responsables de las áreas correspondientes, quienes serán los encargados, conforme a su competencia, de velar por la implantación de las medidas relativas a la seguridad de la información, además de desarrollar las tareas necesarias para el mantenimiento y mejora continua de estas medidas.

7. INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

7. Las áreas usuarias deberán informar de manera íntegra e inmediata al Oficial de Seguridad de la Información, sobre la existencia de un potencial incidente de seguridad que afecte a los activos de información críticos de la Institución o del Estado.

7. Para dar repuesta y mitigar un incidente de Seguridad de la información, se deberá seguir el procedimiento establecido.

8. SANCIONES PREVISTAS POR INCUMPLIMIENTO

8. El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido y de acuerdo a la ley vigente en la República del Ecuador. Podría generar el correspondiente proceso disciplinario, por tanto, en caso de identificar que algún usuario ha incurrido en el incumplimiento de la política, se tomará como falta administrativa y el MERNNR. de ser el caso, adoptará las medidas que legalmente amparen la protección de sus derechos, sin eximir de las responsabilidades civiles y penales.

8. Cualquier usuario del MERNNR que sea encontrado realizando actividades que contravengan estas políticas podrá ser investigado y puede ser causal de sanción, sin perjuicio de las acciones disciplinarias y/o jurídicas quo pudieran ser emprendidas por las entidades de control del estado. Además de la responsabilidad civil y penal que hubiere podido generarse especialmente cuando los actos involucren reproducción, distribución o uso no autorizado de programas de computación e información.

9. REVISIÓN DE LA POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

9.1. Revisar anualmente o cuando se produzcan cambios significativos a nivel operativo, legal, tecnológico, económico, entre otros, la política de seguridad de la información en la institución.

10. VIGENCIA

10.1. Esta política, y las guías que la .acompañen tendrán vigencia desde la fecha de su expedición.