COMISIÓN NACIONAL DE ENERGÍA

REF.: Aprueba Política General de Seguridad de la Información de la Comisión Nacional de Energía y deja sin efecto la Resolución Exenta N° 774, de 28 de noviembre de 2018.

SANTIAGO, 06 SEP 2019

RESOLUCION EXENTA Nº 587

VISTOS:

a) Lo dispuesto en el Art. 9°, letras c) y h) del D.L. N° 2.224, de 1978, que crea el Ministerio de Energía y la Comisión Nacional de Energía;

b) Lo dispuesto en el Decreto Supremo Nº 83, del 12 de enero de 2005, del Ministerio Secretaría General de la Presidencia, que aprueba Norma Técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos;

c) Los controles y objetivos de control que propone la normativa NCh-ISO 27001.Of2013, Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información – Requisitos;

d) La Resolución Nº 487, del 10 de julio de 2018, que designa Encargado de Seguridad de la Información en la Comisión Nacional de Energía;

e) La Resolución Exenta 765, del 22 de noviembre de 2018, que modifica Resolución Exenta N° 481, de 09 de julio de 2018, que designó integrantes y conformó el Comité de Seguridad de la Información de la CNE y establece sus funciones;

f) La Resolución Exenta N° 774, de 28 de noviembre de 2018, que aprobó la Política General de Seguridad de la Información de la Comisión Nacional de Energía;

g) Lo establecido en los requisitos técnicos del Sistema de Seguridad de la Información del PMG y la respectiva Guía Metodológica;

h) Las recomendaciones técnicas de la red de expertos del sistema de seguridad de la información del Gobierno de Chile;

i) El Decreto Supremo N° 23 A, de fecha 20 de agosto de 2018, del Ministerio de Energía, que designa Secretario Ejecutivo en la Comisión Nacional de Energía;

j) El instructivo presidencial N° 008 del 23 de octubre de 2018 que imparte instrucciones urgentes en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado; y

k) La Resolución Nº 7, de 2019, de la Contraloría General de la República.

CONSIDERANDO:

a) El compromiso adquirido por la Autoridad Superior del Servicio en orden a implementar un proceso de seguridad de la información institucional, enmarcado en los Programas de Mejoramiento de la Gestión de la Comisión Nacional de Energía;

b) La necesidad de implementar el proceso de seguridad de la información en los sistemas informáticos internos y en los activos de información a través de la identificación, análisis, evaluación, tratamiento y control de las brechas, que permitan a la Autoridad Superior del Servicio, implementar acciones orientadas a mejorar la seguridad de los sistemas y los activos de información institucionales;

c) Las instrucciones específicas que sobre la materia ha impartido la Presidencia de la República a la Administración y las especificaciones y orientaciones técnicas emanadas de la DIPRES, para la implementación de este proceso;

d) La importancia de proteger adecuadamente la información generada y/o administrada por la Comisión Nacional de Energía.

e) En atención a las recomendaciones técnicas realizadas por la red de expertos del sistema de seguridad de la información del Gobierno de Chile, se hace necesario actualizar la presente resolución aprobatoria de la Política General de Seguridad de la Información de la Comisión Nacional de Energía.

f) Las instrucciones impartidas por el Presidente de la República en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos.

COMISIÓN NACIONAL DE ENERGÍA

RESUELVO:

I. APRUÉBESE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA COMISIÓN NACIONAL DE ENERGÍA, en el marco de la Norma ISO 27001 y los requisitos técnicos del Sistema de Seguridad de la Información del PMG y las instrucciones en materia de ciberseguridad, la cual es del siguiente tenor:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

COMISIÓN NACIONAL DE ENERGÍA

TABLA DE CONTENIDOS

COMISIÓN NACIONAL DE ENERGÍA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

COMISIÓN NACIONAL DE ENERGÍA

1. Declaración Institucional

La Comisión Nacional de Energía, CNE, tiene como misión Institucional generar condiciones para el desarrollo confiable, sustentable, inclusivo y de precios razonables de los Mercados Energéticos Chilenos a través de su regulación, monitoreo, análisis, tarificación y dictación de normativas técnicas, económicas y de seguridad, y asimismo asesorar a las autoridades en las materias del Sector Energético, mediante propuestas y análisis de carácter regulatorio.

Para contribuir al logro de la referida misión, es necesario generar las condiciones necesarias de resguardo y protocolos de seguridad, mediante la adecuada identificación de las acciones y situaciones de riesgo de seguridad de la información. Lo anterior enmarcado en un contexto normativo que responde al D.S N°83 y la NCh ISO 27001.

2. Objetivo de la Gestión de Seguridad de la Información dentro de la CNE

La información es un recurso que, como el resto de los activos, tiene valor para la CNE y por consiguiente debe ser debidamente protegida. La aplicación de las políticas o normas de Seguridad de la Información protegerán de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas y de los objetivos institucionales, minimizar los riesgos y asegurar el eficiente cumplimiento de los objetivos institucionales. Es importante que los principios de la Política General de Seguridad de la Información sean parte de la cultura organizacional.

La presente Política de Seguridad de la Información pretende servir de ayuda en el proceso de gestión de la seguridad de la Comisión Nacional de Energía (CNE), el cual se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico, proteger los recursos de información y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Esta política general de seguridad de la información cubre los siguientes objetivos:

- Establecer las expectativas de la Secretaría Ejecutiva con respecto al correcto uso de los recursos de información de la Comisión Nacional de Energía, así como de las medidas que se deben adoptar para la protección de estos recursos.
- Establecer para todo el personal de la organización la necesidad de la seguridad de la información y promover la comprensión de sus responsabilidades individuales.
- Determinar las medidas esenciales de seguridad de la información que la CNE debe adoptar, para protegerse apropiadamente contra amenazas que podrían afectar en

alguna medida la confidencialidad, integridad y disponibilidad de la información, ocasionando alguna de las siguientes consecuencias:

  - Pérdida o mal uso de los activos de información (datos, equipos, documentación impresa, etc.).
  - Interrupción total o parcial de los procesos que soportan el negocio.

- Proporcionar a todo el personal de la CNE una herramienta que facilite la toma de decisiones apropiada, en situaciones relacionadas con la preservación de la seguridad de la información.

3. Alcance de la Política de Seguridad

El alcance del Sistema de Gestión de Seguridad de la Información está determinado por los procesos que dan soporte a los productos estratégicos de la Comisión Nacional de Energía, definidos en la Ficha de Definiciones Estratégicas (Formulario A1) vigente.

Esta Política General de Seguridad de la Información debe ser conocida y aplicada por todos quienes trabajan en la CNE, en cualquier nivel jerárquico, ya sean funcionarios de planta, contratados asimilados a grados, honorarios o en cualquier calidad que se desempeñen, que laboren o cumplan funciones dentro de las áreas y departamentos de la institución, así como los proveedores, terceros autorizados o cualquiera que use o tenga acceso a los activos de información de la Institución.

4. Referencias

- Norma NCh ISO 27001:2013 Tecnología de la Información – Técnicas de Seguridad – Sistema de Gestión de Seguridad de la Información – Requerimientos.
- DS N° 83 Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los documentos electrónicos.

5. Definiciones

Información	Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
Confidencialidad	Es la propiedad de la información por la que se garantiza que es accesible sólo para aquellas personas debidamente autorizadas.
Integridad	Es la propiedad de la información que busca salvaguardar la precisión y completitud de la información y los métodos de procesamiento.

Disponibilidad	Es la capacidad de asegurar que las personas autorizadas tengan acceso a la información y bienes asociados cuando lo requieran.
Sistema informático	Conjunto de uno o más computadores, software asociado, periféricos, terminales, usuarios, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información y/o transferencia de información.
Seguridad de la Información	Todas aquellas medidas preventivas y reactivas que permitan resguardar y proteger los activos de información, buscando mantener la confidencialidad, integridad y disponibilidad de los mismos.
Claves de acceso	Combinación de letras, números y signos que debe teclearse para obtener acceso a un programa o partes de un programa determinado, un terminal u ordenador personal, un punto en la red, etc.
Ciberseguridad	Conjunto de herramientas, políticas, métodos de gestión de riesgos, prácticas, y tecnologías que pueden utilizarse para proteger los activos de información de la organización y sus usuarios en el entorno digital, buscando garantizar la disponibilidad, integridad y confidencialidad de la información.
Amenaza	Evento generado a partir de un agente externo o interno de la institución, que tenga el potencial de generar algún grado de daño (ya sea en relación a la confidencialidad, integridad o disponibilidad) en uno o más activos de información institucional.
Vulnerabilidad	Se refiere a alguna condición de debilidad o fragilidad que se encuentra presente en el activo identificado. Usualmente se traduce en una debilidad o ausencia de control, que posibilita la ocurrencia de un incidente y que pueden afectar a uno o más activos de información.
Riesgos	Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones.
Riesgo de seguridad de la información	Corresponde a una amenaza potencial que podría afectar activos de información, vinculados a los procesos de provisión de Productos Estratégicos (bienes y servicios) establecidos en las definiciones estratégicas institucionales (Formulario A1), y por tanto causar daño a la organización.

6. Activos de Información

Se distinguirán 3 niveles básicos de activos de Información: La **Información** propiamente tal, en sus múltiples formatos, los **equipos/sistemas/infraestructura** que soportan esta información y las **personas** que utilizan la información y que tienen el conocimiento de los procesos institucionales, es decir, aquellos funcionarios en calidad de Planta, Contrata o personal a Honorarios que cumplan sus funciones en dependencias de la CNE, así como el personal vinculado a tareas de apoyo o asesoría externa a la CNE.

6.1 Información Interna

- La información interna de la CNE debe ser protegida, por sus custodios, de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en las políticas específicas de seguridad de la información, sus procedimientos asociados y en las recomendaciones dadas por el responsable designado de dicha información. Para ello, la CNE deberá proveer los recursos que permitan implementar los controles necesarios para otorgar el nivel de protección correspondiente al valor de los activos.
- Toda la información creada o procesada por la organización debe ser considerada como de "Uso Interno", a menos que el dueño de la información considere otro nivel de clasificación.
- La Comisión Nacional de Energía proveerá los mecanismos para que la información sea accedida y utilizada por el personal que de acuerdo a sus funciones así lo requiera. Sin embargo, se reserva el derecho de revocar al personal, el privilegio de acceso a la información y tecnologías que la soportan, si la situación y las condiciones lo ameriten.

6.2 Información Externa

- La Comisión Nacional de Energía procesa y mantiene información de sus usuarios externos, que se asume como información valiosa y confidencial, por lo cual la organización se compromete a asegurar que esta información no será divulgada sin previa autorización y estará protegida de igual manera que la información interna.
- Esta información solo estará disponible al personal de la CNE debidamente autorizado.

7. Roles y Responsabilidades

7.1 Encargado/a de Seguridad de la Información

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran. El detalle de sus responsabilidades en relación al Sistema de Gestión de Seguridad de la Información estará establecido en la Resolución de nombramiento correspondiente.

7.2 Comité de Seguridad de la Información

El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas de la Institución, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad. El detalle de sus responsabilidades en relación con el Sistema de Gestión de Seguridad de la Información estará establecido en la Resolución de designación de integrantes y conformación correspondiente.

7.3 Encargado/a de Ciberseguridad

Es la persona que cumple la función de supervisar el cumplimiento de la normativa y controles de ciberseguridad y de asesorar en materia de ciberseguridad al Jefe Superior del Servicio y a los integrantes de la Institución que así lo requieran. El detalle de sus responsabilidades quedará establecido en la Resolución de nombramiento correspondiente.

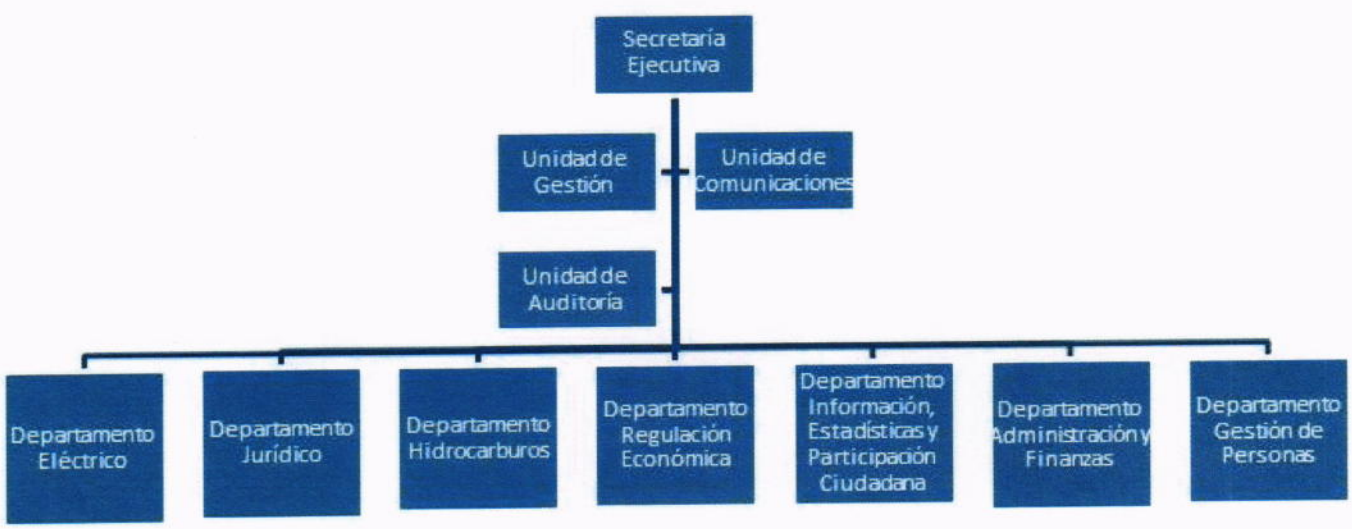
7.4 Personal

Todo el personal de la Comisión Nacional de Energía es responsable de la implementación de las normas de Seguridad promovidas por la CNE dentro de sus áreas de responsabilidad, así como del cumplimiento por parte de su equipo de trabajo. En particular se debe considerar que:

- La información y las tecnologías de información deben ser usadas sólo para propósitos relacionados con el servicio y autorizados por las jefaturas directas, debiéndose aplicar criterios de buen uso en su utilización.
- Las claves de acceso a la información y a las tecnologías de información son individuales, intransferibles y de responsabilidad única de su propietario.
- El personal está en la obligación de alertar, de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta política.
- Está absolutamente prohibido al personal divulgar cualquier información interna de la CNE, salvo que sea explícitamente autorizado por el responsable de la información, quien deberá hacerse responsable de esta divulgación.

7.5 Unidades afectadas.

Todos los Departamentos, unidades, funcionarios y personal de la CNE.



8. Cumplimiento y Difusión

La presente Política General de Seguridad de la Información entrará en vigencia una vez oficializada por el Secretario Ejecutivo y será difundida mediante correo electrónico a todos los funcionarios de la CNE.

9. Actualización de la Política

- La mantención de la presente política será realizada por el Encargado de Seguridad de la Información y sus cambios serán aprobados por el Secretario Ejecutivo de la CNE.
- La presente política se reevaluará cada dos años como máximo y su cumplimiento se revisará en forma anual, en reunión de Comité de Seguridad de la Información, con la finalidad de asegurar el cumplimiento e incorporación de todas las políticas, normas y procedimientos necesarios de implementar en el marco de la Seguridad de la Información.

II. Déjese sin efecto la Resolución Exenta N° 774, de 28 de noviembre de 2018, de la Comisión Nacional de Energía.

ANÓTESE Y NOTIFÍQUESE

JOSÉ VENEGAS MALUENDA
SECRETARIO EJECUTIVO
COMISIÓN NACIONAL DE ENERGÍA

LCE/MAJ/JGS/RAG/frb

Distribución:
- Secretaría Ejecutiva CNE
- Unidad de Gestión CNE
- Oficina de Partes CNE