REF.: Aprueba Política General de Seguridad de la Información y Ciberseguridad de la Comisión Nacional de Energía y deja sin efecto la Resolución Exenta CNE N° 20, de 11 de enero de 2022.

SANTIAGO, 08 de abril de 2025

RESOLUCIÓN EXENTA Nº 167

VISTOS:

a) Lo dispuesto en el artículo 9°, letras c) y h) del D.L. N° 2.224, de 1978, del Ministerio de Minería, que crea el Ministerio de Energía y la Comisión Nacional de Energía, en adelante e indistintamente la "Comisión", la "CNE" o la "Institución";

b) Lo dispuesto en el Decreto Nº 83, del 03 de junio de 2004, 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 requisitos para establecer, implementar, mantener y mejorar de manera continua un Sistema de Gestión de Seguridad de la Información y los requisitos para la evaluación y tratamiento de los riegos que propone la normativa NCh-ISO 27001, Seguridad de la Información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información – Requisitos;

d) La Resolución Exenta CNE N° 487, del 10 de julio de 2018, que Designa Encargado de Seguridad de la Información en la Comisión Nacional de Energía y asigna funciones que indica;

e) La Resolución Exenta CNE N° 656, del 14 de octubre de 2019, que Designa Encargada de Ciberseguridad de la Comisión Nacional de Energía;

f) La Resolución Exenta CNE N° 20, de 11 de enero de 2022, que aprobó la Política General de Seguridad de la Información de la Comisión Nacional de Energía;

g) La Resolución Exenta CNE N° 131, de 21 de marzo de 2025, que Designa integrantes y conforma el Comité de Seguridad de la Información y Ciberseguridad de la CNE y establece sus funciones;

h) Las recomendaciones técnicas del Equipo de Respuesta ante Incidentes de Seguridad Informática - CSIRT de Gobierno;

i) El Decreto N° 12A, de fecha 21 de noviembre de 2022, del Ministerio de Energía, que nombra a don Marco Antonio Mancilla Ayancán en el cargo de Secretario Ejecutivo de 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;

k) El Decreto N° 7, del 19 de mayo de 2023, del Ministerio Secretaría General de la Presidencia, que establece Norma Técnica de Seguridad de la Información y Ciberseguridad conforme a la Ley N° 21.180, en adelante e indistintamente "Decreto N° 7";

l) El Decreto N° 164, del 16 de junio de 2023, del Ministerio del Interior y Seguridad Pública, que aprueba la Política Nacional de Ciberseguridad 2023 – 2028;

m) La Ley N° 21.663, Marco de Ciberseguridad; y,

n) La Resolución Nº 36, de 19 de diciembre de 2024, de la Contraloría General de la República.

CONSIDERANDO:

a) Que, el compromiso adquirido por la Autoridad Superior del Servicio en orden a implementar un proceso de Seguridad de la Información y Ciberseguridad institucional, que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información y/o los sistemas informáticos de la Comisión Nacional de Energía;

b) Que, existe la necesidad de implementar el proceso de seguridad de la información en los sistemas informáticos internos y en los activos y los activos de información, considerando la infraestructura tecnológica, los componentes lógicos de la información, los datos que se manejan en el ciberespacio y las personas que manejan datos, información sensible y/o posean conocimiento relevante, 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 eliminar o minimizar los riesgos y mejorar la seguridad de los activos y los activos de información de la Institución;

c) Que, proteger adecuadamente los sistemas informáticos y la información generada y/o administrada por la Comisión Nacional de Energía es de suma importancia para el Servicio;

d) Que, el 08 de abril de 2024, se publicó en el Diario Oficial la Ley N° 21.663, Marco de Ciberseguridad, que tiene por objetivo establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares;

e) Que, el artículo 5 del Decreto N° 7, dispone que cada órgano de la Administración del Estado deberá elaborar una Política de Seguridad de la Información y Ciberseguridad, aprobada a través de acto administrativo por el respectivo Jefe Superior de Servicio, que tendrá como objetivo establecer las directrices generales en materia de Seguridad de la Información y Ciberseguridad dentro del órgano, además de velar por la seguridad de los componentes de software y hardware, de los sistemas informáticos y de los datos o información que almacenan, procesan e interoperan;

f) Que, en conformidad a lo establecido en la Norma ISO 27001, la alta dirección debe establecer una Política de Seguridad de la Información que proporcione el marco para establecer objetivos de seguridad de la información; y,

g) Que, en el marco del mejoramiento continuo, es necesario actualizar a lo menos cada dos años la Política General de Seguridad de la Información de la Comisión Nacional de Energía.

RESUELVO:

I. APRUÉBESE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DE LA COMISIÓN NACIONAL DE ENERGÍA, en cumplimiento de las leyes y regulaciones relacionadas con la seguridad de la información y ciberseguridad, cuyo texto es el siguiente:

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD COMISIÓN NACIONAL DE ENERGÍA

1. Declaración Institucional

La Comisión Nacional de Energía, CNE, tiene como misión Institucional "Generar condiciones para el desarrollo seguro, sostenible, diversificado y de precios justos de los Mercados Energéticos Chilenos a través de la generación de propuestas al Ministerio de Energía de carácter regulatorio que permitan cumplir los objetivos de política pública, monitoreo, análisis, tarificación y dictación de normativas técnicas, económicas y de seguridad, contribuyendo con ello a establecer las condiciones necesarias para que la energía aporte al bienestar y a la vida digna de las personas".

Para contribuir al logro de la referida misión, es necesario generar las condiciones de resguardo y protocolos de seguridad, mediante la adecuada identificación de las acciones y situaciones de riesgo de seguridad de la información y ciberseguridad, aplicando una estrategia de mejora continua, basada en las mejores prácticas y controles sobre los activos y los activos de información, asegurando el cumplimiento de las leyes y regulaciones relacionadas con la seguridad de la información y ciberseguridad.

La CNE se compromete a custodiar y proteger sus activos y activos de Información, considerando la infraestructura tecnológica, los componentes lógicos de la información, los datos que se manejan en el ciberespacio y las personas que manejan datos, información sensible y/o posean conocimiento relevante, con el objetivo de mantener su confiabilidad, integridad y disponibilidad frente a riesgos o amenazas, internas o externas, deliberadas o accidentales, a través de la constante implementación de medidas tendientes a asegurar la continuidad de las operaciones de la CNE.

2. Objetivo de la Política de Seguridad de la Información y Ciberseguridad

La presente Política tiene por objetivo establecer las directrices generales en materia de Seguridad de la Información y Ciberseguridad dentro de la Institución, además, de velar por la seguridad de los componentes de software y hardware, de los sistemas informáticos y de los datos o información que almacenan, procesan e interoperan.

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 y Ciberseguridad 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 y Ciberseguridad sean parte de la cultura organizacional.

La presente Política se enmarca en el proceso de gestión de la Seguridad de la Información y Ciberseguridad de la Comisión, 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, permitiendo evaluar todo tipo de riesgos o amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información y la infraestructura informática que soporta sus procedimientos administrativos, considerando estándares de Seguridad de la Información y Ciberseguridad.

3. Objetivos específicos de la Política de Seguridad de la Información y Ciberseguridad

La Política General de Seguridad de la Información y Ciberseguridad cubre los siguientes objetivos específicos:

- 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 y promover la comprensión de las responsabilidades individuales de todo el personal de la CNE.

- Establecer normas generales que regulen el uso y manejo de los activos y los activos de información de la Institución, con el fin de asegurar la confidencialidad, integridad y disponibilidad de los mismos.

- Determinar las medidas esenciales de Seguridad de la Información y Ciberseguridad que la CNE debe adoptar, para eliminar o minimizar los riesgos y/o amenazas que podrían afectar en alguna medida la confidencialidad, integridad y disponibilidad de la información y la infraestructura informática que soporta sus procedimientos administrativos, ocasionando alguna de las siguientes consecuencias:

    - Pérdida o mal uso de los activos y los activos de información (infraestructura tecnológica, componentes lógicos de la información, datos que se manejan en el ciberespacio, documentación impresa, las personas que manejan datos, información sensible y/o posean conocimiento relevante, 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 y Ciberseguridad.

4. Alcance de la Política de Seguridad de la Información y Ciberseguridad

La Política General de Seguridad de la Información y Ciberseguridad es aplicable a todos los procesos de negocio y de soporte de la Comisión Nacional de Energía, con especial énfasis en los activos y los activos de información y la infraestructura tecnológica, componentes lógicos de la información, datos que se manejan en el ciberespacio, documentación impresa, las personas que manejan datos, información sensible y/o posean conocimiento relevante.

Esta Política General de Seguridad de la Información y Ciberseguridad 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, unidades y departamentos de la institución. También es aplicable a los proveedores, terceros autorizados o cualquiera que use o tenga acceso a los activos y los activos de información de la Institución.

Asimismo, esta Política es aplicable independientemente del lugar en que los funcionarios de la CNE ejercen sus funciones, ya sea bajo la modalidad presencial, teletrabajo, cometido funcionario, comisiones de servicio u otra de las condiciones que se establezca, de acuerdo a la legislación vigente, abarcando a toda la Institución independiente de su ubicación geográfica.

5. Referencias

- Norma NCh-ISO IEC 27001:2023, Seguridad de la Información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información – Requisitos.
- Decreto N° 83, de 03 de junio de 2004, 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.
- Oficio Ord. N° 008, de 23 de octubre de 2018, del Presidente de la República, 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.
- Ley N° 21.663, Marco de Ciberseguridad.
- Decreto N° 7, de 19 de mayo de 2023, del Ministerio Secretaría General de la Presidencia, que establece Norma Técnica de Seguridad de la Información y Ciberseguridad conforme a la Ley N° 21.180.
- Decreto N° 164, del 16 de junio de 2023, del Ministerio del Interior y Seguridad Pública, que aprueba la Política Nacional de Ciberseguridad 2023 – 2028.

6. Definiciones

Activo	Todo elemento lógico o físico, componente de hardware, equipamiento o sistema relacionado con la información, que permita su generación, almacenamiento, soporte, envío o intercambio, sea a otros órganos de la Administración del Estado o con personas naturales o jurídicas.

Activos de información	Datos o información cuyo tratamiento es esencial para el funcionamiento y desarrollo del órgano de la Administración del Estado que lo utiliza, genera, almacena, envía o intercambia, y que deben ser protegidos en su confidencialidad, integridad, disponibilidad u otros factores de importancia.
Amenaza(s)	Circunstancia desfavorable que puede ocurrir y que, cuando sucede, tiene consecuencias negativas sobre los activos y los activos de información, provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad en un activo o aprovechando su existencia, puede derivar en un incidente de seguridad de la información o ciberseguridad.
Ciberataque(s)	Intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático
Ciberseguridad y Seguridad de la Información	Conjunto de acciones, políticas, medidas preventivas y reactivas destinadas a la prevención, mitigación, manejo, respuesta y estudio de las amenazas y riesgos de incidentes de seguridad de la información o ciberseguridad, a la reducción de sus efectos y el daño causado; antes, durante y después de su ocurrencia; respecto de los activos y activos de información y la continuidad de servicios, con el fin de proteger, preservar y restablecer la confidencialidad, integridad y disponibilidad de aquellos y de las plataformas electrónicas de los órganos de la Administración del Estado, aumentando su resiliencia en el tiempo.
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.
Confidencialidad	Propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.
Disponibilidad	Propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado.
Evento de seguridad	Suceso o situación que puede comprometer la Seguridad de la Información o Ciberseguridad Institucional.
Incidente de Seguridad de la Información o Ciberseguridad	Todo evento de seguridad o una serie de ellos, de carácter indeseado o inesperado, que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas informáticos, los activos y activos de información, datos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y que puedan afectar al normal funcionamiento de los mismos.

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.
Integridad	Propiedad que consiste en que la información no ha sido modificada o destruida sin autorización.
Inventario de Activos de Información	Instrumento utilizado para la identificación y análisis de los activos y los activos de información, con la finalidad de determinar su criticidad, considerando su confidencialidad, integridad y disponibilidad.
Responsable de los activos de información	Responsable de la identificación y clasificación, así como gestionar el riesgo y niveles de seguridad asociados a los activos y los activos de información.
Riesgo(s)	Posibilidad de ocurrencia de un incidente seguridad de la información o ciberseguridad; la magnitud de un riesgo es cuantificada en términos de la probabilidad de ocurrencia del incidente y del impacto de las consecuencias del mismo.
Servicios esenciales	Son servicios esenciales aquellos provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional; los prestados bajo concesión de servicio público, y los proveídos por instituciones privadas que realicen las siguientes actividades: generación, transmisión o distribución eléctrica; transporte, almacenamiento o distribución de combustibles; suministro de agua potable o saneamiento; telecomunicaciones; infraestructura digital; servicios digitales y servicios de tecnología de la información gestionados por terceros; transporte terrestre, aéreo, ferroviario o marítimo, así como la operación de su infraestructura respectiva; banca, servicios financieros y medios de pago; administración de prestaciones de seguridad social; servicios postales y de mensajería; prestación institucional de salud por entidades tales como hospitales, clínicas, consultorios y centros médicos, y la producción y/o investigación de productos farmacéuticos.
Sistema(s) informático(s)	Conjunto de componentes lógicos y físicos que, interactuando entre sí, permiten que su totalidad o una parte de ellos, realicen la función para la cual fueron diseñados.
Vulnerabilidad	Debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.

7. Activos y Activos de Información

Se distinguirán 3 niveles básicos de activos y 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.

Los activos y los activos de información de la CNE son identificados, clasificados y analizados en el "Inventario de Activos de Información", permitiendo obtener el nivel de criticidad de éstos, considerando su confidencialidad, integridad y disponibilidad.

Dicho inventario permite identificar atributos tales como:

- Tipo de activo/activo de información y su ubicación,
- Responsable de los activos/activo de información,
- Personas autorizadas para manipular,
- Personas autorizadas para copiar,
- Medio de almacenamiento,
- Tiempo de retención antes de eliminarse,
- Disposición final,
- Criterio de búsqueda,
- Niveles de Confidencialidad, Integridad y Disponibilidad.

De esta forma, la CNE gestiona sus activos y activos de información, considerando la asignación de responsabilidades sobre su tratamiento, a través de un proceso de análisis, evaluación de riesgos de Seguridad de la Información y Ciberseguridad y la evaluación de la efectividad de las medidas implementadas para garantizar la seguridad de la información sobre los diversos procesos y productos estratégicos de la institución.

7.1 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 y Ciberseguridad, 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 y los activos de información.

- 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.

7.2 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 sólo estará disponible al personal de la CNE debidamente autorizado.

8. Roles y Responsabilidades

8.1 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 de la CNE que así lo requieran, con el propósito de proteger la confidencialidad, integridad y disponibilidad de la información que se maneja en la Institución y la infraestructura informática que soporta sus procedimientos administrativos. El detalle de sus responsabilidades en relación al Sistema de Gestión de Seguridad de la Información estará establecido en el acto administrativo de nombramiento correspondiente.

8.2 Comité de Seguridad de la Información y Ciberseguridad

El Comité de Seguridad de la Información y Ciberseguridad, está 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 tendientes a proteger la información y los sistemas informáticos de la Institución contra posibles ciberataques y amenazas. El detalle de sus responsabilidades en relación con el Sistema de Gestión de Seguridad de la Información y Ciberseguridad estará establecido en el acto administrativo de designación de sus integrantes y su conformación correspondiente.

8.3 Encargado/a de Ciberseguridad

Es la persona que cumple la función de supervisar el cumplimiento de las medidas de seguridad para proteger los sistemas informáticos de la Institución contra posibles ciberataques y amenazas, 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 el acto administrativo de nombramiento correspondiente.

8.4 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.

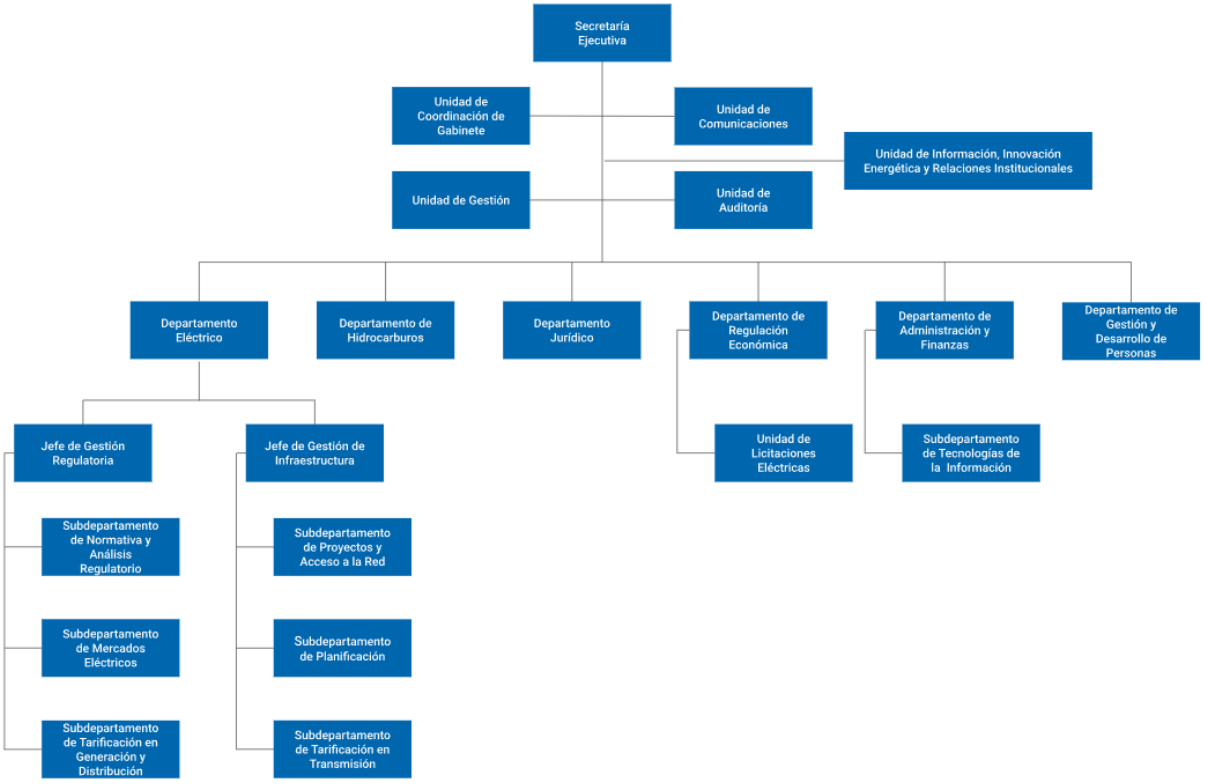
- El personal está en la obligación de alertar, de manera oportuna y adecuada, cualquier incidente de Seguridad de la Información o Ciberseguridad que atente contra lo establecido en esta política.

- 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.

- El personal está obligado a reportar la ocurrencia de cualquier evento que pueda afectar la integridad, confidencialidad o disponibilidad de los activos y los activos de información, con el objeto de identificar posibles anomalías, fallas o eventos precursores que pudieran derivar en un incidente de Seguridad de la Información o Ciberseguridad.

8.5 Unidades afectadas.

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


Secretaría Ejecutiva
Unidad de Coordinación de Gabinete
Unidad de Comunicaciones
Unidad de Información, Innovación Energética y Relaciones Institucionales
Unidad de Gestión
Unidad de Auditoría
Departamento Eléctrico
Departamento de Hidrocarburos
Departamento Jurídico
Departamento de Regulación Económica
Departamento de Administración y Finanzas
Departamento de Gestión y Desarrollo de Personas
Jefe de Gestión Regulatoria
Jefe de Gestión de Infraestructura
Unidad de Licitaciones Eléctricas
Subdepartamento de Tecnologías de la Información
Subdepartamento de Normativa y Análisis Regulatorio
Subdepartamento de Mercados Eléctricos
Subdepartamento de Tarificación en Generación y Distribución
Subdepartamento de Proyectos y Acceso a la Red
Subdepartamento de Planificación
Subdepartamento de Tarificación en Transmisión

9. Gestión de la Seguridad de la Información y Ciberseguridad

Para el cumplimiento de esta Política, la CNE debe contar con directrices generales vinculadas a la Seguridad de la Información y Ciberseguridad, las que se aplicarán de manera transversal en los procesos de negocios y de gestión interna, a través de la definición e implementación de Políticas y Procedimientos tendientes a establecer las acciones necesarias para llevar a cabo la implementación del Sistema de Seguridad de la Información y Ciberseguridad al interior de la CNE.

Se deberá adoptar los requisitos de la Norma ISO 27001 para el marco de gobernabilidad de la seguridad de la información, así como los lineamientos presidenciales y normativos de la Seguridad de la Información y Ciberseguridad del Estado.

El Encargado de Seguridad de la Información y el Encargado de Ciberseguridad deberán velar por la existencia, implementación y actualización de políticas y documentos de Seguridad de la Información y Ciberseguridad al interior de la CNE, así como el cumplimiento de las medidas por parte de los proveedores externos.

Del mismo modo deberán desarrollar e implementar las acciones necesarias para gestionar de manera oportuna todos los eventos de Seguridad de la Información y Ciberseguridad, con el propósito detectar, analizar, responder, mitigar y recuperar los incidentes, asimismo identificar y proponer medidas o acciones que permitan mejoras futuras.

Adicionalmente, deberán velar por la implementación de un monitoreo continuo de la seguridad, en el cual los servidores y sus plataformas electrónicas deben contar con medidas adecuadas para la protección contra código malicioso. Deberán, además, velar por la implementación de las acciones necesarias para restablecer cualquier capacidad, plataforma electrónica, sistema electrónico, servidor, red o servicio en general, que se haya visto afectado debido a un incidente de Seguridad de la Información o Ciberseguridad.

El Encargado de Seguridad de la Información y el Encargado de Ciberseguridad deberán mantener contacto con las autoridades pertinentes y grupos de interés especial en materias vinculadas con la Seguridad de la Información y Ciberseguridad.

10. Cumplimiento y Difusión

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

11. Actualización de la Política

- La mantención de la presente política será realizada por el Encargado de Seguridad de la Información junto al Encargado de Ciberseguridad y sus cambios serán aprobados por el Secretario Ejecutivo de la CNE.

- La presente política será revisada periódicamente y actualizada cada dos años como máximo, en función de la normativa vigente o cuando el Comité de Seguridad de la

Información y Ciberseguridad, el Encargado de Seguridad de la Información y/o el Encargado de Ciberseguridad así lo determinen. Lo anterior, 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 y Ciberseguridad.

II. Déjese sin efecto la Resolución Exenta N° 20, del 11 de enero de 2022, de la Comisión Nacional de Energía.

Anótese y notifíquese

MARCO ANTONIO MANCILLA AYANCAN

Firmado digitalmente por MARCO ANTONIO MANCILLA AYANCAN
Nombre de reconocimiento (DN): c=CL, title=ING CIVIL INDUSTRIAL, cn=MARCO ANTONIO MANCILLA AYANCAN, email=MMANCILLA@CNE.CL, serialNumber=10213184-3
Fecha: 2025.04.08 16:03:29 -04'00'

SECRETARIO EJECUTIVO
COMISIÓN NACIONAL DE ENERGÍA

MFH/MAJ/JGS/RAG/MAS

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