COORDINADOR
ELÉCTRICO NACIONAL

POLÍTICA INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA

Agosto 2022

Contenido

1. Introducción

El Coordinador Eléctrico Nacional, en adelante Coordinador, como organismo autónomo de derecho público, técnico e independiente, debe velar por una operación segura y económica del conjunto de instalaciones del sistema eléctrico que operan interconectadas entre sí, permitiendo de esta forma abastecer de energía al país y sus habitantes.

En este contexto, y en particular considerando el rol de coordinación de la operación del Sistema Eléctrico Nacional, en adelante SEN, el Coordinador requiere garantizar la continuidad operacional de todos sus procesos, por lo que resulta clave el crear, mantener y propiciar un ambiente que proteja todos sus Activos o Recursos de Información, de las distintas amenazas que puedan poner en riesgo el funcionamiento e integridad de sus instalaciones, plataformas y herramientas, así como de los activos de datos e información que utiliza el para el cumplimiento de las funciones que le asigna la Ley General de Servicios Eléctricos (LGSE).

2. Objetivo

La presente Política de Seguridad de la Información, Ciberseguridad e Infraestructura Crítica, en adelante Política Integral de Seguridad, establece el marco de referencia para las actividades o acciones que se realizan en el Coordinador en materia de seguridad de la información, ciberseguridad e infraestructura critica. Sus principios fundamentales han sido definidos en el Estándar de Ciberseguridad para el Sector Eléctrico en Chile[1], en adelante el Estándar, los cuales establecen el uso, administración y protección contra ataques físicos y ciber ataques, tanto de la información de la organización como de los activos asociados a su tratamiento, protección y preservación de su valor. Se considera que la infraestructura crítica del Coordinador es el conjunto de activos, sean estos edificios, instalaciones, capital humano, sistemas de información, data centers, centros de despacho, sistemas de telecomunicaciones y todos los datos e información de los sistemas (hardware y software) contenidos en ellas. Esta política define los lineamientos, normativa interna y/o procedimientos específicos de seguridad de la información, ciberseguridad e infraestructura crítica para el Coordinador.

3. Alcance

Esta política aplica a toda la organización, siendo responsabilidad del Consejo Directivo, la Dirección Ejecutiva, Gerencias y todo el personal del Coordinador, dar cumplimiento a los lineamientos establecidos en ella. Asimismo, esta política aplica a todos los activos asociados con la creación, monitoreo, recolección, procesamiento y almacenamiento de datos (señales y de control) e información, así como a toda la infraestructura crítica del Coordinador. Finalmente, el conocimiento de las personas en materias propias del quehacer del Coordinador y según el rol organizacional es considerado un activo más de información y está sujeto a los lineamientos de la presente Política Integral de Seguridad.

Las políticas, procedimientos, manuales u otros documentos que apoyen la gestión de seguridad de la información, ciberseguridad e infraestructura crítica ya existentes en el Coordinador y los que se establezcan en el marco de esta Política Integral de Seguridad serán aplicables a terceros que se vinculen con esta política, en el contexto del uso, implementación, suministro o desarrollo de activos o recursos de información, así como en lo referido a la infraestructura crítica del Coordinador, sea esta interacción de forma presencial o remota.

[1] Oficio Ordinario N°5778, de la Superintendencia de Electricidad y Combustibles, de Septiembre de 2020.

4. Definiciones

Para efectos de la presente Política, los términos definidos a continuación se utilizarán en el sentido de las definiciones que se establecen a continuación:

- **Información**: Conjunto organizado de datos que tienen un significado.

- **Seguridad de la información**: Corresponde a asegurar la confidencialidad, integridad y disponibilidad de la información. Con el objetivo de garantizar la continuidad operacional y minimizar consecuencias de incidentes de seguridad de la información.

- **Ciberseguridad**: Condición de estar protegido en contra de consecuencias físicas, digitales o de otro tipo que resultan del fallo, daño, error, accidentes, perjuicios o cualquier otro evento en el ciberespacio que se pueda considerar no deseable.

- **Infraestructura crítica**: Activos de carácter esencial e indispensable cuyo funcionamiento es imprescindible y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los procesos y servicios esenciales para el cumplimiento de las funciones del Coordinador.[2]

- **Sistema de información**: Conjunto de elementos orientados a gestionar datos e información (envío y recepción, tratamiento, almacenamiento y administración de datos e información) en forma organizada y lista para ser utilizada para cubrir una necesidad u objetivo definido.

- **Clasificación de la Información**: Es el proceso bajo el cual se identifica la importancia que cada dato o información tiene para el Coordinador, en función del posible daño que puede producir al Coordinador, si la información es mal utilizada o divulgada sin autorización. Se reconocen cuatro categorías de clasificación:
    - Pública: no se producen daños si la información es utilizada o conocida fuera del Coordinador.
    - Uso Interno: no se producen daños si la información es utilizada o conocida dentro del ámbito del Coordinador, pero sí puede existir daño si es utilizada o conocida por terceros al exterior de la organización.
    - Confidencial: se producen daños si la información es conocida fuera del Coordinador, sin su autorización.
    - Sensible: datos o información que requiere autorización explícita del Comité de Seguridad para su utilización, uso o intervención.

- **Política de seguridad**: Declaración documentada de lineamientos y gobierno de una organización en materia de seguridad con un enfoque integral que incluye la seguridad de la información, la ciberseguridad y la infraestructura crítica como ámbitos fundamentales desde el diseño, planificación, gestión, control, implementación, monitoreo de la estrategia de seguridad y nivel madurez, así como su mejoramiento continuo en el tiempo.

- **Ciberespacio**: Entorno complejo que resulta de la interacción de personas, software y servicios en internet por medio de dispositivos y redes de tecnología conectados a éste, los que no existen en forma física.

- **Proceso**: Conjunto de actividades interrelacionadas o que interactúan, que transforman elementos de entrada en elementos de salida.

[2] Los activos que forman la infraestructura crítica del Coordinador se detallan en el Anexo de esta política.

- **Activo de Información**: Comprende las instalaciones físicas y/o cualquier elemento, equipamiento, red, instrumento, aplicación, plataforma o tecnología utilizada para los procesos que permiten la continuidad operacional del Coordinador, cuya afectación, degradación, denegación, interrupción o destrucción podría impedir la continuidad y seguridad operacional del sistema eléctrico y el cumplimiento de la función de operador de red y de mercado eléctrico del Coordinador.

- **Disponibilidad**: Propiedad de la información consistente en estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **Integridad**: Propiedad de la información relativa a su exactitud y completitud.

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

- **Entidad Responsable**: Se refiere a las empresas Coordinadas (o Coordinados), al Coordinador, y a todo otro organismo al cual le apliquen los requerimientos establecidos en el presente estándar.

- **Incidente de Ciberseguridad Reportable (ICR)**: Incidente de Ciberseguridad que ha comprometido o interrumpido:
    - Un Ciber Sistema SEN que desempeña una o más funciones asociadas a mantener la seguridad y confiabilidad del SEN por parte de las Entidades Responsables.
    - Un Perímetro se Seguridad Electrónica (PSE) de un Ciber Sistema SEN de Impacto Alto o Medio.
    - Un Sistema de Monitoreo o Control de Acceso Electrónico (SMCAE) de un Ciber Sistema SEN de Impacto Alto o Medio.

  Los incidentes que comprometan o interrumpan Ciber Sistemas o perímetros de seguridad según se indica en los puntos anteriores, se deberán reportar como ICR, produzcan o no interrupción a los coordinados del SEN, con la periodicidad y tiempos definidos en el Protocolo de Notificación de Incidentes de Ciberseguridad para el Sector Eléctrico[3].

- **Incidente de seguridad (IC)**: Corresponden a aquellos actos maliciosos o eventos que:
    - Amenacen o intenten compromete, un Perímetro de Seguridad Electrónica (PSE), un Perímetro de Seguridad Física (PSF) o un Sistema de Monitoreo o Control de Acceso Electrónico (SMCAE) para un Ciber Sistema SEN de Impacto Alto o Medio.
    - Amenacen o intenten interrumpir la operación de un Ciber Sistema SEN, sea que esté calificado como de impacto alto, medio o bajo.

- **NERC CIP**: North American Electric Reliability Corporation - Critical Infrastructure Protection.

- **CSIRT**: Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas.

[3] Protocolo-de-Notificacion-de-Ciberincidentes.pdf (coordinador.cl)

5. Principios Básicos

El Coordinador se encuentra sometido a diversos riesgos inherentes en las actividades que desarrolla, que pueden impedir o limitar el logro de sus objetivos y ejecutar sus estrategias con éxito. Toda actuación dirigida a controlar y mitigar los riesgos cibernéticos que afecten la disponibilidad, integridad y confidencialidad de la información y de su infraestructura crítica y no crítica, se regirá por los siguientes principios básicos.

La seguridad de la información y protección de la infraestructura critica:

- Es un atributo esencial para mantener la confianza pública.
- Es un elemento clave para la continuidad operacional del Coordinador.
- Busca proteger la Confidencialidad, Integridad y Disponibilidad de los Activos o Recursos de Información del Coordinador, de amenazas y vulnerabilidades internas y externas.
- Se basa en la identificación y gestión permanente de riesgos o vulnerabilidades y sus costos se justifican en función de los resultados esperados de las medidas de mitigación propuestas para eliminar esos riesgos o vulnerabilidades.
- Está alineada con los objetivos estratégicos y prioridades del Coordinador, con los requerimientos y estándares normativos asociados y con las buenas prácticas de la industria.
- Es responsabilidad de todos los trabajadores del Coordinador, y debe ser gestionada por los responsables de cada proceso del Coordinador.
- Es una materia para la cual el Coordinador reconoce la importancia de mantener una constante y efectiva sensibilización, capacitación y entrenamiento de su personal.
- Busca garantizar la correcta utilización de las herramientas de control, que darán cobertura a los riesgos de ciberseguridad y seguridad de la información, y su correcto registro.
- Implica informar con transparencia sobre los riesgos de ciberseguridad y seguridad de la información del Coordinador y el funcionamiento de las medidas desarrolladas para su control al Consejo Directivo, manteniendo los canales adecuados para favorecer la comunicación.
- Busca asegurar un cumplimiento adecuado de las políticas, procedimientos y sistemas, y su actualización y mejora continua en el marco de las mejores prácticas de transparencia y gobierno corporativo, e instrumentar su seguimiento y medición.

6. Gobierno de Seguridad, Roles y Responsabilidades

La Gobernanza de la Seguridad de la Información, Ciberseguridad e Infraestructura Crítica del Coordinador Eléctrico Nacional es ejercida desde el Consejo Directivo, a través de la Unidad de Ciberseguridad e Infraestructura Crítica, y su alcance comprende desde el diseño de las políticas en estas materias hasta el monitoreo continuo de su cumplimiento en toda la organización y terceros que se vinculen con esta política.

Las instancias formales a través de las cuales el Coordinador ejerce el gobierno de la Seguridad de la Información, Ciberseguridad e Infraestructura Crítica, son las siguientes:

i. Comité de Tecnología y Seguridad de la Información

- Objetivo: Monitoreo bimensual de la Estrategia de Tecnología y Seguridad Integral.
- Participantes: Consejo Directivo, Unidad de Ciberseguridad e Infraestructura Crítica, Dirección Ejecutiva, Gerencia de Tecnología y Sistemas y Departamento de Seguridad de la Información.

ii. Comité de Seguridad de la Información, Ciberseguridad e Infraestructura Crítica

- Objetivo: Monitoreo quincenal de la Estrategia de Seguridad Integral.
- Participantes: Dirección Ejecutiva con sus Gerencias, Departamento de Seguridad de la Información, Gerencia de Personas y Administración (Seguridad Física) y la Unidad de Ciberseguridad e Infraestructura Crítica.

iii. Unidad de Ciberseguridad e Infraestructura Crítica y Oficial de Seguridad

- Responsable del monitoreo del cumplimiento e informe a la SEC, según corresponda, del Estándar y otros definidos por la autoridad en materia de ciberseguridad, tanto para el Coordinador como para las empresas Coordinadas.
- Como Oficial de Seguridad es responsable de monitorear la Política integral de Seguridad dentro del Coordinador y proponer, impulsar y controlar el desarrollo e implementación de la normativa interna e iniciativas de seguridad de la información, ciberseguridad e infraestructura crítica en el Coordinador. Es responsable, además de informar a la autoridad y dar seguimiento a los incidentes de seguridad detectados.

iv. Dirección Ejecutiva / Encargado CIP

- Responsable de liderar y gestionar la implementación y continuo cumplimento de los requerimientos establecidos en el Estándar.

v. Gerencia de Tecnología y Sistemas

- Responsable de la ejecución de las tareas, actividades e implementación de la política, procedimientos y planes en materia de seguridad de la información y ciberseguridad.
- Encargado del cumplimiento y gestión operativa de la seguridad de la información y ciberseguridad. Además de la creación de: campañas de concientización, manuales, protocolos, y/o instructivos que implementen la seguridad de la información y ciberseguridad.

vi. Gerencia de Personas y Administración / Seguridad Física

- Responsable de la creación de campañas de concientización, manuales, protocolos, y/o instructivos que implementen esta política integral de seguridad. Asimismo, es responsable de implementar las medidas de protección en lo que respecta a la seguridad física de la infraestructura crítica del Coordinador.

7. Modelo Integral de Seguridad

El modelo de gestión de seguridad integral debe desenvolverse en tres etapas del ciclo de vida de los riesgos que impacten la continuidad operacional del Coordinador, que son la prevención, la respuesta, y la mitigación. Este enfoque permite que la seguridad integral se gestione y mejore continuamente antes, durante y después de que una amenaza se transforme en un incidente.

Esta Política Integral de Seguridad se basa en la normativa vigente aplicable, principalmente en el Estándar de Ciberseguridad para el Sector Eléctrico de Chile. Además, serán referencias complementarias para este modelo la familia de normas ISO/IEC 27000 y NIST, las cuales en su conjunto entregan las bases del Sistema de Gestión de Seguridad de la Información; e ISO 22301 del Plan de Continuidad del Negocio (BCP), que tendrán como finalidad fortalecer la resiliencia del Coordinador.

8. Lineamientos de la Política de Seguridad

- El Coordinador mantendrá debidamente actualizado un catálogo con los activos o recursos de información de la organización, en base a criterios definidos en el Estándar.
- Los recursos de información del Coordinador definidos como críticos deberán ser protegidos de cualquier riesgo o amenaza, física o informática, que afecte su funcionamiento y/o la obtención de los resultados esperados por el Coordinador.
- La Seguridad de la Información deberá ser un elemento esencial para tener en consideración en el diseño, implementación, operación y mantenimiento de los procesos, sistemas, redes y servicios del Coordinador, tanto para aquellos de uso interno como para los ofrecidos por el Coordinador a la Autoridad, Coordinados, o terceros.
- Todo el personal del Coordinador, sin excepción, es personalmente responsable por la custodia y protección de los activos o recursos de Información que utiliza en el desempeño de sus funciones.
- El personal sólo tendrá acceso a los activos y recursos de información sensible que sean estrictamente necesarios para el cumplimiento de sus funciones.
- Las tareas, funciones, actividades, procesos y sistemas que se relacionen o afecten plataformas críticas, datos o información, en particular información sensible, deberán contar con etapas o niveles de revisión/autorización que aseguren una clara definición de responsabilidades desde el punto de vista de Seguridad de la Información, de manera de garantizar el acceso confiable a los datos o información que requiere el personal del Coordinador para el desarrollo de sus funciones.
- El Coordinador protegerá los datos e Información, clasificándolos conforme a su importancia en cuanto a los efectos negativos que pueda producir para la continuidad operacional y prestigio del Coordinador, el uso malicioso o errado de estos datos e información, velando especialmente por su disponibilidad, integridad y confidencialidad.
- El Coordinador tendrá procedimientos de contingencia establecidos y probados para procurar la Seguridad de la Información y su continuidad operacional, en caso de ocurrir un desastre que afecte la integridad, disponibilidad y confidencialidad de esta.
- Los Activos o Recursos informáticos del Coordinador sólo deberán ser utilizados para las funciones propias del Coordinador.
- El personal del Coordinador sólo podrá utilizar elementos personales para las labores o funciones propias que desarrolla en el Coordinador, cuando hayan sido autorizadas por el Oficial de Seguridad y siempre que cumplan estrictamente con la presente Política Integral de Seguridad, la normativa interna de seguridad de la información y con todas las normas internas de la organización.
- El personal del Coordinador tiene la obligación de notificar al Oficial de Seguridad ante cualquier incidente, actividad o situación que, a su entender, pueda estar afectando la seguridad de los activos o recursos de Información, conforme al procedimiento que se defina para tal efecto.
- Los incumplimientos a las normas internas de Seguridad de la Información, Ciberseguridad e Infraestructura Crítica, e Incidentes de Seguridad, serán gestionados por el Oficial de Seguridad.
- El Coordinador implementará un sistema de gestión de la seguridad de la información y utilizará la Política Nacional de Ciberseguridad, el estándar NERC CIP, u otra que establezca la normativa aplicable, como guía de referencia para la Gestión de Seguridad de la Información al objeto de mitigar y reducir de manera efectiva y permanente los riesgos de Seguridad de la Información.
- El Coordinador se encargará de monitorear los planes de acción de los Coordinados en materias de seguridad de la información, de acuerdo con los requerimientos establecidos en el Estándar, así como de verificar que

se tomen las medidas de protección necesarias para asegurar la continuidad y seguridad de la operación, con el objeto de resguardar la continuidad operacional del Coordinador.

- El Coordinador adherirá, en lo relativo a las funciones de Coordinación de la operación del sistema eléctrico nacional, al estándar NERC CIP para la protección de su infraestructura crítica.
- El Coordinador se compromete a fomentar la Seguridad de la Información y proporcionar toda su colaboración, además de proporcionar los recursos necesarios para implementar la normativa interna de Seguridad de la Información e iniciativas que hayan sido aprobadas por el Comité de Seguridad de Información, Ciberseguridad e Infraestructura Crítica.

Adicionalmente a lo anterior, el Coordinador definirá toda la normativa interna necesaria para cumplir con la actual política y la normativa aplicable en materia de ciberseguridad e infraestructura critica.

9. Evaluación y Seguimiento de la Política

La Unidad de Ciberseguridad e Infraestructura Crítica dependiente del Consejo Directivo, en conjunto con la Dirección Ejecutiva ejercerá el rol de monitoreo de cumplimiento continuo de esta Política Integral de Seguridad.

10. Difusión y Comunicación

La Unidad de Ciberseguridad e Infraestructura Crítica debe propender a que esta Política Integral de Seguridad y sus actualizaciones sean oportunamente difundidas.

11. Cumplimiento y Sanciones

El incumplimiento de esta política será sancionado de acuerdo con lo establecido en el Reglamento Interno de Orden, Higiene y Seguridad (RIOHS), Política de Prevención de Delitos, Código de Ética y Política Conflicto de Interés del Coordinador Eléctrico Nacional, sin perjuicio de las sanciones establecidas en la Ley N° 21.459 de Delitos Informáticos y demás normativa vigente.

12. Vigencia y Aprobación

La presente política tiene vigencia a partir de 17 de agosto de 2022. Todas las modificaciones que sean efectuadas a este documento deberán constar por escrito y entrarán en vigor una vez aprobadas por el Consejo Directivo.