COORDINADOR
ELÉCTRICO NACIONAL

Política de Seguridad Integral

ACTUALIZACIÓN - NOVIEMBRE 2025

Contenido | *Content*

1.	Introducción	2	*1.*	*Introduction*	*2*
2.	Objetivo	3	*2.*	*Objective*	*3*
3.	Alcance	4	*3.*	*Scope*	*4*
4.	Definiciones	5	*4.*	*Definitions*	*5*
5.	Principios Básicos	12	*5.*	*Basic Principles*	*12*
6.	Gobierno de Seguridad, Roles y Responsabilidades	16	*6.*	*Security Governance, Roles and Responsibilities*	*16*
7.	Modelo de Seguridad Integral	22	*7.*	*Integrated Security Model*	*22*
8.	Lineamientos de la Política de Seguridad Integral	24	*8.*	*Integrated Security Policy Guidelines*	*24*
9.	Evaluación y Seguimiento de la Política	28	*9.*	*Policy Evaluation and Monitoring*	*28*
10.	Difusión y Comunicación	29	*10.*	*Dissemination and Communication*	*29*
11.	Cumplimiento y Sanciones	30	*11.*	*Compliance and Sanctions*	*30*
12.	Vigencia y Aprobación	32	*12.*	*Validity and Approval*	*32*

Introducción | *Introduction*

La Ley 20.936 estableció un nuevo sistema de transmisión eléctrica y creó al CEN como organismo coordinador independiente del Sistema Eléctrico Nacional. Esta ley le otorgó autonomía y la responsabilidad de garantizar la operación segura, económica y confiable del sistema, además de asegurar acceso abierto a las redes de transmisión.

Se establece en la Ley Marco de Ciberseguridad N.º 21.663, artículo 4º, inciso segundo, que el Coordinador Eléctrico Nacional", es un servicio esencial.

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 considerando especialmente el rol del Coordinador en la operación del Sistema Eléctrico Nacional (SEN), resulta indispensable asegurar la continuidad operacional de todos sus procesos. Para ello, es fundamental crear, mantener y promover una cultura de protección, tanto de las personas como de los activos y recursos de información, frente a las diversas amenazas que puedan comprometer la seguridad, disponibilidad e integridad de sus instalaciones, plataformas y herramientas. Del mismo modo, esta protección debe extenderse a los activos de datos e información que el Coordinador utiliza para cumplir las funciones que le asigna la Ley General de Servicios Eléctricos (LGSE).

Law No. 20.936 established a new electrical transmission system and created the National Electric Coordinator (Coordinador Eléctrico Nacional, CEN) as the independent coordinating body of the National Electric System (Sistema Eléctrico Nacional, SEN). This law granted the CEN the autonomy and responsibility to guarantee the safe, economical and reliable operation of the system, as well as to ensure open access to the transmission networks.

Furthermore, the Cybersecurity Framework Law No. 21.663, article 4, second paragraph, establishes that the National Electric Coordinator is an essential service.

As an autonomous, technical and independent public body, the National Electric Coordinator, hereinafter the coordinator, must ensure the safe and economical operation of all the electric system facilities that operate in an interconnected manner with each other, thus enabling Chile and its inhabitants to be supplied with energy.

In this context, and especially considering the role of the coordinator in the operation of the National Electric System, it is essential to ensure the operational continuity of all its processes. To achieve this, it is necessary to create, maintain and promote a culture of protection – both for people and for information assets and resources – against the various threats that could compromise the security, availability and integrity of its facilities, platforms and tools. Furthermore, this protection must extend to the data and information assets that the coordinator uses to fulfill the functions assigned to it by the General Electric Services Law (Ley General de Servicios Eléctricos, LGSE).

Objetivo | *Objective*

La presente Política de Seguridad Integral, en adelante la Política, establece el marco de referencia para todas las actividades y acciones que se desarrollan en el Coordinador en materia de seguridad de la información, ciberseguridad, seguridad física e infraestructura crítica.

Sus principios fundamentales se encuentran definidos en el Estándar de Ciberseguridad para el Sector Eléctrico en Chile (en adelante el Estándar), el cual regula el uso, administración y protección frente a ataques físicos y cibernéticos, tanto de la información de la organización como de los activos asociados a su tratamiento, resguardo y preservación de su valor.

Se entiende por infraestructura crítica del Coordinador al conjunto de activos que incluyen a las personas, edificios, instalaciones, sistemas de información, centros de datos, centros de despacho, sistemas de telecomunicaciones, así como todos los datos e información alojados en dichos sistemas, ya sea en hardware o software.

Finalmente, esta Política define los lineamientos, normativa interna y procedimientos específicos en materia de seguridad de la información, ciberseguridad e infraestructura crítica aplicables al Coordinador.

This Integrated Security Policy, hereinafter the policy, establishes the framework for all activities and actions carried out by the coordinator in the areas of information security, cybersecurity, physical security and critical infrastructure.

Its fundamental principles are defined in the Cybersecurity Standard for the Electricity Sector in Chile (Estándar de Ciberseguridad para el Sector Eléctrico en Chile), hereinafter the standard, which regulates the use, management and protection against physical and cyberattacks of both the organization's information and the assets associated with the processing, safeguarding and preservation of its value.

The coordinator's critical infrastructure is understood to be the set of assets that include people, buildings, facilities, information systems, data centers, dispatch centers and telecommunications systems, as well as all data and information hosted on said systems, whether hardware or software.

Finally, this policy defines the guidelines, internal regulations and specific procedures regarding information security, cybersecurity and critical infrastructure applicable to the coordinator.



Alcance | *Scope*



Esta Política de Seguridad Integral aplica a toda la organización, siendo responsabilidad del Consejo Directivo, la Dirección Ejecutiva, las Gerencias y cada colaborador velar por su cumplimiento. Su alcance incluye todos los activos de información y datos (creación, monitoreo, procesamiento y almacenamiento), así como la infraestructura crítica del Coordinador.

El conocimiento del personal, en función de su rol organizacional, también se reconoce como un activo de información sujeto a esta política. Asimismo, las normas, procedimientos y directrices vigentes y las que se emitan en el marco de esta política serán exigibles tanto al personal interno como a terceros que interactúen con el Coordinador, ya sea de forma presencial o remota, en relación con los activos de información y la infraestructura crítica.

This Integrated Security Policy applies to the entire organization, and the board of directors, executive management, management and each employee are responsible for ensuring compliance. Its scope includes all information and data assets (creation, monitoring, processing and storage), as well as the coordinator's critical infrastructure.

Staff knowledge, based on their role within the organization, is also recognized as an information asset subject to this policy. Furthermore, the current regulations, procedures and guidelines, as well as those issued within the framework of this policy, will be applicable to both internal personnel and third parties who interact with the coordinator, whether in person or remotely, in relation to information assets and critical infrastructure.



Definiciones | *Definitions*

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.

For the purposes of this policy, the terms adopted shall be used in the sense of the definitions set forth below:

- ***Information:***
  Organized set of data that has meaning.

- ***Information Security:***
  Corresponds to ensuring the confidentiality, integrity and availability of information, with the goal of guaranteeing operational continuity and minimizing the consequences of information security incidents.

- ***Cybersecurity:***
  The condition of being protected against physical, digital or other consequences resulting from failure, damage, error, accident, harm or any other event in cyberspace that may be considered undesirable.

- **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.

- **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:

  i. **Sensible:** Información restringida con el más alto grado de sensibilidad y confidencialidad. El acceso a esta información se considera altamente restringido y se aplica el máximo grado de protección, seguridad, recelo y cuidado debido a posibles efectos adversos en un individuo, organización, seguridad nacional o seguridad pública.

  ii. **Confidencial:** De grado medio de sensibilidad, cuya divulgación, aún al interior del negocio, puede causar daño a la organización. Usarla,

- ***Critical Infrastructure:***
  Fundamental, indispensable assets whose operation is essential and does not allow for alternative solutions. Their disruption or destruction would therefore have a serious impact on the processes and services essential for the fulfillment of the coordinator's functions.

- ***Information System:***
  Set of elements aimed at managing data and information (sending and receiving, processing, storage and administration) in an organized manner and ready to be used to cover a defined need or objective.

- ***Information Classification:***
  The process by which the importance of each piece of data or information to the coordinator is identified, based on the potential harm it could cause to the coordinator if it is misused or disclosed without authorization. Four categories are recognized:

  i. ***Sensitive:*** *Restricted information with the highest degree of sensitivity and confidentiality. Access to this information is considered highly restricted, and the highest level of protection, security, confidentiality and caution is applied due to potential adverse effects on an individual, organization, national security or public safety.*

  ii. ***Confidential:*** *Medium-sensitivity, the disclosure of which, even within the business, could cause harm to the organization. Using, sharing and*

compartirla, y almacenarla requiere autorización del propietario y medidas de control de seguridad.

iii. **Uso Interno:** De menor grado de sensibilidad, aunque restringida solo a colaboradores de la organización. La divulgación a externos debe ser autorizada.

iv. **Pública:** Puede ser conocida al exterior de la organización sin que ello represente daño.

- **Datos personales:**
  Según la Ley de Protección de Datos Personales N.º 21.719, establece una clasificación, considerando su nivel de sensibilidad y el riesgo para los derechos fundamentales de las personas, estos son:

  - **Dato Personal:** Información que identifica o puede identificar a una persona natural.
  - **Dato Personal Sensible:** Información íntima o de alto riesgo para la persona, como salud, orientación sexual, religión.
  - **Dato de Fuente de Acceso Público:** Información obtenida de registros legalmente accesibles por cualquier persona.
  - **Dato Anonimizado:** Información que ya no permite identificar a una persona (proceso irreversible).
  - **Dato Seudonimizado:** Información con identidad oculta que puede ser revertida bajo medidas de seguridad.

storing this information requires authorization from the owner, in addition to security control measures.

iii. ***Internal Use:*** *Less sensitive, but restricted to employees of the organization. Disclosure of this information to external stakeholders must be authorized.*

iv. ***Public:*** *Can be shared outside the organization without causing harm.*

- ***Personal Data:***
  The Personal Data Protection Act No. 21.719 classifies personal data according to their level of sensitivity and the risk to individuals' fundamental rights:

  - ***Personal Data:*** *Information that identifies or may identify a natural person.*
  - ***Sensitive Personal Data:*** *A person's intimate or high-risk information, such as that related to health, sexual orientation and religion.*
  - ***Publicly Accessible Source Data:*** *Information obtained from records legally accessible to anyone.*
  - ***Anonymized Data:*** *Information that no longer allows a person to be identified (irreversible process).*
  - ***Pseudonymized Data:*** *Information with a person's identity hidden, which can be reversed under security measures.*



- **Política de seguridad:**
  Declaración documentada que establece los lineamientos y el modelo de gobierno de la organización en materia de seguridad, abordando de forma integral la seguridad de la información, la ciberseguridad y la protección de infraestructura crítica. Define principios desde el diseño, planificación y gestión hasta la implementación, control, monitoreo y mejora continua de la estrategia de seguridad y su nivel de madurez.

- **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.

- **Activo de Información:**
  Corresponde a las instalaciones físicas y a todo elemento, equipo, red, aplicación, plataforma o tecnología que sustente los procesos del Coordinador. Su afectación, degradación, interrupción o destrucción podría comprometer la continuidad y seguridad operativa del sistema

- ***Security Policy:***
  A documented statement that establishes the organization's governance model and guidelines on security, addressing in an integrated manner information security, cybersecurity, and critical infrastructure protection. It defines principles from design, planning, and management to implementation, control, monitoring, and continuous improvement of the security strategy and its maturity level.

- ***Cyberspace:***
  A complex environment resulting from the interaction of people, software and services on the Internet through the devices and technology networks connected to it, which do not exist physically.

- ***Process:***
  A set of interrelated or interacting activities that transform input elements into output elements.

- ***Information Asset:***
  Corresponds to the physical facilities and any element, equipment, network, application, platform or technology that support the coordinator's processes. Their impact, degradation, interruption or destruction could compromise the continuity and operational security of the electric system, as well



eléctrico, así como el cumplimiento de su rol como operador de red y de mercado eléctrico.

- **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 estándar NERC-CIP, ISO 27001 y las recomendaciones Zero Trust.

- **Ciberataque:**
  Intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático, según la definición de la Ley Marco de Ciberseguridad en Chile N° 21.663.

as the fulfillment of its role as a grid and electricity market operator.

- ***Availability:***
  Property of information consisting of it being accessible and usable when required by an authorized entity.

- ***Integrity:***
  Property of information with regard to its accuracy and completeness.

- ***Confidentiality:***
  Property of information consisting of it not being made available or revealed to unauthorized individuals, entities or processes.

- ***Responsible Entity:***
  Refers to the coordinated companies, coordinator and any other body to which the requirements established in the NERC-CIP, ISO 27001 standards and the Zero Trust recommendations apply.

- ***Cyberattack:***
  An attempt to destroy, expose, alter, disable, exfiltrate or gain unauthorized access to or use of an IT asset, as defined by Chile's Cybersecurity Framework Law No. 21.663.

- **Incidente de Ciberseguridad Reportable (ICR):**
  Incidente de Ciberseguridad que ha comprometido o interrumpido, según lo establecido en el Estándar de Ciberseguridad para el Sector Eléctrico (CIP-008), o interrumpan Ciber Sistemas o perímetros de seguridad, 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.

- **Incidente de seguridad (IC):**
  Corresponden a aquellos actos maliciosos o eventos que:
  i. Amenacen o intenten comprometer, 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, o
  ii. 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.

- **BCM (Business Continuity Management):**
  Proceso integral para asegurar la resiliencia organizacional frente a eventos disruptivos.

- ***Reportable Cybersecurity Incident (RCI):***
  Any cybersecurity incident that has compromised or interrupted cyber systems or security perimeters – as established in the Cybersecurity Standard for the Electricity Sector (CIP-008) – must be reported as an RCI, whether or not it causes interruption to the SEN coordinators, within the times defined in the Cybersecurity Incident Notification Protocol for the Electricity Sector (Protocolo de Notificación de Incidentes de Ciberseguridad para el Sector Eléctrico).

- ***Security Incident (SI):***
  Corresponds to malicious acts or events that:
  i. Threaten or attempt to compromise an Electronic Security Perimeter (Perímetro de Seguridad Electrónica, PSE), a Physical Security Perimeter (Perímetro de Seguridad Física, PSF) or an Electronic Access Monitoring or Control System (Sistema de Monitoreo o Control de Acceso Electrónico, SMCAE) for a high or medium impact SEN cyber system, or
  ii. Threaten or attempt to disrupt the operation of a SEN cyber system, whether it is classified as high, medium or low impact.

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

- ***CSIRT:***
  Computer Security Incident Response Team.

- ***BCM (Business Continuity Management):***
  Integrated process to ensure organizational resilience to disruptive events.



- **BCP (Business Continuity Plan):**
  Plan documentado que establece los procedimientos de respuesta, recuperación y restablecimiento de operaciones críticas.

- **TI:**
  Tecnología de la Información.

- **TO:**
  Tecnología de Operación.

- **IA:**
  Inteligencia Artificial.

- **PDSI:**
  Programa Director de Seguridad Integral.

- **DPD:**
  Delegado de Protección de Datos Personales.

- **Zero Trust:**
  Enfoque de seguridad basado en el principio de "nunca confiar, siempre verificar", limitando el acceso según identidad, contexto y necesidad mínima.

- ***BCP (Business Continuity Plan):***
  Documented plan that establishes the procedures for the response, recovery and restoration of critical operations.

- ***IT:***
  Information technology.

- ***OT:***
  Operation technology.

- ***AI:***
  Artificial Intelligence.

- ***ISPD:***
  Integrated Security Program Director.

- ***DPO:***
  Data Protection Officer

- ***Zero Trust:***
  A security approach based on the principle of "never trust, always verify", limiting access based on identity, context and minimum need.

Principios Básicos | *Basic Principles*

El Coordinador enfrenta riesgos inherentes a sus actividades que pueden afectar el cumplimiento de sus objetivos y estrategias. La gestión de riesgos cibernéticos, de seguridad de la información y de infraestructura crítica se regirá por los siguientes principios:

The coordinator faces risks inherent to its activities that may affect the fulfillment of its goals and strategies. Cyber, information security and critical infrastructure risk management will be governed by the following principles:

PRINCIPIOS ESTRATÉGICOS

STRATEGIC PRINCIPLES

- **Protección integral y resiliencia:**
  La seguridad es un pilar estratégico para garantizar la operación continua, confiable y segura del SEN.

- ***Integrated protection and resilience:***
  Security is a strategic focus to ensure the continuous, reliable and safe operation of the SEN.

- **Confianza pública:**
  La seguridad de la información y de la infraestructura crítica es esencial para mantener la legitimidad y credibilidad del Coordinador.

- ***Public trust:***
  The security of information and critical infrastructure is essential to maintaining the legitimacy and credibility of the Coordinator.

- **Continuidad operacional:**
  Es un elemento clave para asegurar la disponibilidad de los procesos y servicios bajo responsabilidad del Coordinador.

- ***Operational continuity:***
  This is a key element to ensure the availability of the processes and services under the responsibility of the Coordinator.

- **Cumplimiento normativo:**
  Todas las acciones se enmarcan en la Ley Marco de Ciberseguridad N° 21.663, la Ley de Protección de Datos Personales N° 21.719, el Estándar SEN (NERC-CIP) y la ISO 22301.

- ***Regulatory compliance:***
  All actions are in compliance with the Cybersecurity Framework Law No. 21.663, the Personal Data Protection Law No. 21.719 the SEN Standard (NERC-CIP) and ISO 22301.

- **Alineación estratégica:**
  La gestión de la seguridad se ajusta a los objetivos, prioridades y buenas prácticas de la industria, asegurando coherencia con las metas institucionales.

- ***Strategic alignment:***
  Security management is aligned with industry objectives, priorities and best practices, ensuring consistency with institutional goals.



PRINCIPIOS DE GESTIÓN DE RIESGOS

- **Confidencialidad, Integridad y Disponibilidad (CID):**
  La protección de los activos de información se centra en salvaguardar estos tres atributos fundamentales.

- **Gestión permanente de riesgos:**
  La identificación temprana de amenazas, vulnerabilidades y riesgos es esencial para reducir impactos, justificando costos en función de las medidas de mitigación y los beneficios esperados.

- **Uso adecuado de controles:**
  Se deben emplear de manera correcta las herramientas de control de ciberseguridad y registrar sus resultados de forma trazable.

- **Zero Trust por diseño:**
  Ningún usuario, sistema o dispositivo es confiable por defecto; todo acceso debe validarse y auditarse.

PRINCIPIOS ORGANIZACIONALES

- **Responsabilidad compartida:**
  La seguridad es responsabilidad de todos los trabajadores, proveedores y entidades coordinadas; debe ser gestionada en cada proceso.

- **Transparencia:**
  Los riesgos y medidas adoptadas deben comunicarse con claridad al Consejo Directivo, manteniendo canales efectivos de información.

RISK MANAGEMENT PRINCIPLES

- ***Confidentiality, integrity and availability (CIA):***
  The protection of information assets focuses on safeguarding these three fundamental attributes.

- ***Ongoing risk management:***
  Early identification of threats, vulnerabilities and risks is essential to reducing impacts and justifying costs based on mitigation measures and expected benefits.

- ***Proper use of controls:***
  Cybersecurity control tools must be used correctly and their results recorded in a traceable manner.

- ***Zero Trust by design:***
  No user, system or device is trusted by default; all access must be validated and audited.

ORGANIZATIONAL PRINCIPLES

- ***Shared responsibility:***
  Security is the responsibility of all employees, suppliers and coordinated entities; it must be managed in every process.

- ***Transparency:***
  Risks and measures taken must be clearly communicated to the board of directors, maintaining effective information channels.

- **Capacitación y cultura de seguridad:**
  Se fomenta la sensibilización, formación y entrenamiento constante del personal para fortalecer la cultura organizacional.

- **Mejora continua:**
  La política de seguridad es dinámica y evoluciona según cambios regulatorios, tecnológicos y operativos, asegurando la actualización constante de políticas, procedimientos y sistemas.

- ***Training and security culture:***
  Awareness, capacity building and ongoing training of staff are encouraged to strengthen the organizational culture.

- ***Continuous improvement:***
  The security policy is dynamic and evolves according to regulatory, technological and operational changes, ensuring the constant updating of policies, procedures and systems.



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:

- **Comité Directivo de Seguridad Integral**
  - **Objetivo:** Monitorear, verificar e informar el cumplimiento del Programa Director de Seguridad Integral, con periodicidad bimensual.
  - **Participantes:** Unidad de Ciberseguridad e Infraestructura Crítica, Dirección Ejecutiva, Unidades y Gerencias que reportan a la Dirección Ejecutiva.

- **Reuniones bimensuales de la Unidad de Ciberseguridad e Infraestructura Crítica con el consejo Directivo:**
  - **Objetivo:** Monitoreo bimensual de la Estrategia de Seguridad Integral y del cumplimiento del Estándar de Ciberseguridad para el Sector Eléctrico a nivel Sectorial.
  - **Participantes:** Unidad de Ciberseguridad e Infraestructura Crítica y el Consejo Directivo.

- **Unidad de Ciberseguridad e Infraestructura Crítica y Oficial de Seguridad**
  Responsable del monitoreo del cumplimiento e informe a la SEC, según corresponda, del Estándar

Security Governance, Roles and Responsibilities

The National Electric Coordinator's information security, cybersecurity and critical infrastructure governance is exercised by the board of directors through the Cybersecurity and Critical Infrastructure Unit. Its scope ranges from the design of policies on these matters to the ongoing monitoring of compliance throughout the organization and third parties associated with this policy.

The formal bodies through which the coordinator exercises governance over information security, cybersecurity and critical infrastructure are as follows:

- ***Integrated Security Steering Committee***
  - ***Objective:*** *To monitor, verify and report on compliance with the Integrated Security Policy Program on a bimonthly basis.*
  - ***Participants:*** *Cybersecurity and Critical Infrastructure Unit and executive management, as well as the units and management that report to executive management.*

- ***Bimonthly meetings between the Cybersecurity and Critical Infrastructure Unit and the board of directors:***
  - ***Objective:*** *Bimonthly monitoring of the Integrated Security Strategy and compliance with the Cybersecurity Standard for the Electricity Sector at the sectoral level.*
  - ***Participants:*** *Cybersecurity and Critical Infrastructure Unit and the board of directors.*

- ***Cybersecurity and Critical Infrastructure Unit and Security Officer***
  Responsible for monitoring compliance and reporting to the SEC, as appropriate, of the standard and other standards defined by the authority in


COORDINADOR
III CONFERENCIA INTERNACIONAL
DE CIBERSEGURIDAD E INFRAESTRUCTURA
CRÍTICA ELÉCTRICA
COORDINADO
ELÉCTRICO NACIONA



y otros definidos por la autoridad en materia de ciberseguridad, tanto para el Coordinador como para las empresas Coordinadas.

- **Oficial de Seguridad**
  es responsable de monitorear el cumplimiento de esta Política de Seguridad Integral dentro del Coordinador, así como verificar el cumplimiento del PDSI y medir la madurez de la Seguridad Integral en forma continua anual o bianualmente.

DIRECCIÓN EJECUTIVA:

- **Encargado CIP:** Responsable de liderar y gestionar la implementación y continuo cumplimento de los requerimientos establecidos en el Estándar de Ciberseguridad en el Coordinador Eléctrico Nacional.
- **Responsable PDSI:** Diseñar, ejecutar y realizar seguimiento del Programa Director de Seguridad Integral (Incorpora iniciativas de Seguridad de la Información, Ciberseguridad, Seguridad Física y Prevención de Riesgos).
- **Responsable BCM:** Responsable de liderar y gestionar el proceso de planes de continuidad Operativa en situaciones de crisis.
- **Delegado de Protección de Datos Personales (DPD):** Responsable de supervisar el cumplimiento de la Ley N.° 21.719 en la organización, velando por el tratamiento seguro y lícito de los datos personales. Actúa como enlace con la Agencia de Protección de Datos Personales, asesora internamente, gestiona incidentes y promueve el respeto a los derechos de los titulares. Coordina su función con las áreas de ciberseguridad y seguridad de la información.

cybersecurity matters, both for the coordinator and coordinated companies.

- ***Chief Security Officer***
  The security officer is responsible for monitoring compliance with this Integrated Security Policy with the coordinator, as well as verifying compliance with the ISPD and measuring Integrated Security levels of maturity on an ongoing annual or biannual basis.

EXECUTIVE MANAGEMENT:

- ***CIP Manager:*** *Responsible for leading and managing the implementation and ongoing compliance with the requirements established in the Cybersecurity Standard for the Electricity Sector.*
- ***ISPD Manager:*** *Responsible for designing, executing and monitoring the Integrated Security Policy Program, incorporating information security, cybersecurity, physical security and risk prevention initiatives.*
- ***BCM Manager:*** *Responsible for leading and managing the operational continuity planning process in crisis situations.*
- ***Data Protection Officer (DPO):*** *Responsible for overseeing compliance with Law No. 21.719 within the organization, ensuring the safe and lawful processing of personal data. The DPO acts as a liaison with the Personal Data Protection Agency, provides internal guidance, manages incidents and promotes respect for the rights of data subjects. They coordinate their function with the areas of cybersecurity and information security.*

- ***Technology and Systems Management |***

- **Gerencia de Tecnología y Sistemas | Departamento de Seguridad de la Información**
  - Encargado del cumplimiento y gestión operativa de la Política de Seguridad Integral. Además de la creación de: campañas de concientización, manuales, protocolos, y/o instructivos que implementen esta Política de Seguridad Integral.
  - 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.

- **Gerencia de Tecnología y Sistemas | Departamento de SCADA y SITR**
  - **Cumplir la normativa con enfoque Zero Trust:** Aplicar la Política de Seguridad Integral, el Estándar de Ciberseguridad para el Sector Eléctrico bajo el principio de "nunca confiar, siempre verificar", asegurando validación continua de identidades, accesos y dispositivos en todos los sistemas.
  - **Gestionar y proteger activos críticos con control estricto de acceso:** Mantener inventario actualizado de sistemas SCADA/ SITR, implementar controles segmentados, monitoreo constante, respaldo seguro y planes de continuidad, limitando el acceso solo a lo necesario (mínimo privilegio) y validando cada conexión como no confiable por defecto.
  - **Capacitar, reportar y auditar con verificación continua:** Formar al personal en ciberseguridad bajo criterios de Zero Trust, asegurando respuesta oportuna a incidentes, registro trazable de accesos y actividades, y participación activa en auditorías para garantizar la mejora continua y la resiliencia del entorno operativo.

Information Security Department

- *Responsible for compliance and operational management of the Integrated Security Policy, in addition to creating awareness campaigns, manuals, protocols and/or instructions to implement this policy.*
- *Responsible for the execution of tasks and activities, and the implementation of information security and cybersecurity policies, procedures and plans.*

- *Technology and Systems Management | SCADA and SITR Department*
  - ***Comply with regulations with a Zero Trust approach:*** *Implement the Integrated Security Policy, Cybersecurity Standard for the Electricity Sector under the principle of "never trust, always verify", ensuring continuous validation of identities, access and devices across all systems.*
  - ***Manage and protect critical assets with strict access control:*** *Maintain an up-to-date inventory of SCADA / SITR systems, and implement segmented controls, constant monitoring, secure backups and continuity plans, limiting access to only what is necessary (least privilege) and validating each connection as untrusted by default.*
  - ***Train, report and audit with continuous verification:*** *Train staff in cybersecurity using Zero Trust criteria, ensuring timely incident response, traceable logs of access and activities, and active participation in audits to guarantee the continuous improvement and resilience of the operating environment.*

- **Gerencia de Personas y Administración | Seguridad Física**

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

  El CEN, como una Corporación de Derecho Público, cumple con lo dispuesto en la Ley 21.659, en lo referente a Seguridad Privada y con toda la normativa jurídica aplicable, garantizando la idoneidad de su personal de seguridad, la implementación de sistemas tecnológicos y protocolos con estricto apego al respeto de los derechos individuales de las personas. Todo lo anterior en coordinación con autoridades civiles y policiales.

- **Gerencia de Personas y Administración | Prevención de Riesgos**

  La organización se compromete a proteger la vida y salud de sus trabajadores y colaboradores, asegurando condiciones laborales seguras y cumplimiento normativo. Promueve una cultura preventiva basada en capacitación continua, participación y exigencia de ambientes seguros a contratistas y proveedores. Asimismo, mantiene un sistema de gestión estructurado orientado a la mejora continua en seguridad y salud ocupacional.

- ***People Management and Administration | Physical Security***

  Responsible for creating awareness campaigns, manuals, protocols and/or instructions that implement this Integrated Security Policy. They are also responsible for implementing protective measures regarding the physical security of the coordinator's critical infrastructure.

  The CEN, as a Public Law Corporation, complies with the provisions of Law 21.659 regarding Private Security, as well as all applicable legal regulations. It ensures the suitability of its security personnel and the implementation of technological systems and protocols in strict adherence to the respect for individuals' rights. All of this is carried out in coordination with civil and police authorities.

- ***People Management and Administration | Risk Prevention***

  The organization is committed to protecting the lives and health of its employees and collaborators, ensuring safe working conditions and regulatory compliance. It promotes a culture of prevention based on ongoing training, participation and ensuring safe environments for contractors and suppliers. It also maintains a structured management system aimed at continuous improvement in occupational health and safety.

Modelo de Seguridad Integral

Integrated Security Model

El modelo de gestión de seguridad integral se desarrolla en tres etapas del ciclo de vida de los riesgos que pueden afectar la continuidad operacional del Coordinador: prevención, respuesta y mitigación. Este enfoque permite gestionar y mejorar continuamente la seguridad antes, durante y después de que una amenaza se convierta en incidente. Esta Política de Seguridad Integral se fundamenta en la normativa vigente, principalmente en el Estándar de Ciberseguridad para el Sector Eléctrico de Chile. Asimismo, se consideran como referencias complementarias:

- **Normas ISO/IEC 27000,**
  que entregan las bases del Sistema de Gestión de Seguridad de la Información (SGSI).
- **ISO 22301, orientada al Sistema de Gestión de Continuidad del Negocio (SGCN),**
  para fortalecer la resiliencia del Coordinador.
- **Ley N° 21.663, Ley Marco de Ciberseguridad,**
  que establece los deberes legales, obligaciones de reporte y la institucionalidad de la ciberseguridad en Chile, para servicios esenciales y Operadores de Importancia Vital (OIV).
- **Ley N° 21.719, sobre Protección de Datos Personales,**
  que asegura el resguardo de la privacidad y tratamiento adecuado de la información.

The Integrated Security Management Model has been developed considering the three stages of the risk management lifecycle that may affect the coordinator's operational continuity: prevention, response and mitigation. This approach allows security to be managed and continuously improved before, during and after a threat becomes an incident. This Integrated Security Policy is based on current regulations, primarily the Cybersecurity Standard for the Electricity Sector in Chile. The following are also considered as complementary references:

- ***ISO/IEC 27000,***
  which provide the foundations for the Information Security Management System (Sistema de Gestión de Seguridad de la Información, SGSI).
- ***ISO 22301, oriented to the Business Continuity Management System (BCMS)***
  in order to strengthen the coordinator's resilience.
- ***Law No. 21.663, the Cybersecurity Framework Law,***
  which establishes the legal duties, reporting obligations and institutional framework for cybersecurity in Chile, for esential services and Vital Importance Operators (VIO).
- ***Law No. 21.719 on the protection of personal data,***
  which ensures the protection of privacy and the proper handling of information.



- **Modelo Zero Trust, bajo el principio de "nunca confiar, siempre verificar",**
  que implica que ningún usuario, sistema o dispositivo es confiable por defecto, requiriendo validación y auditoría de todo acceso.

De esta forma, el modelo integral articula marcos normativos, estándares internacionales y principios de seguridad avanzada, garantizando una gestión coherente, resiliente y gestión de mejora continua.

- ***Zero Trust Model, based on the principle of "never trust, always verify",***
  which implies that no user, system or device is trustworthy by default, requiring validation and auditing of all access.

In this way, the Integrated model articulates regulatory frameworks, international standards and advanced security principles, ensuring coherent, resilient and continuously improving management.

Lineamientos de la Política de Seguridad Integral

Guidelines of the Integrated Security Policy

- **Gestión de Activos**
  - Mantener un inventario actualizado y clasificado de activos e información, priorizando aquellos críticos para la continuidad operacional.
  - Proteger los activos frente a amenazas físicas, lógicas o humanas, asegurando su confidencialidad, integridad y disponibilidad.

- **Principio de Acceso Mínimo y Zero Trust**
  - El acceso a información y sistemas será estrictamente limitado según el rol y necesidad de cada colaborador, proveedor o tercero.
  - Bajo el modelo Zero Trust, ningún usuario, dispositivo o aplicación se considera confiable por defecto; todo acceso debe ser autenticado, validado y auditado.

- **Seguridad en el Ciclo de Vida**
  - La seguridad de la información será integrada desde el diseño en todo proceso, sistema, red o servicio, tanto internos como los provistos a terceros.
  - Se aplicarán controles de revisión y autorización en procesos sensibles para asegurar trazabilidad y responsabilidad clara.

- **Clasificación y Manejo de la Información**
  - Los datos serán clasificados (p. ej. Sensibles, Confidenciales, Uso Interno, Públicos) y gestionados según su criticidad.
  - Información sensible no podrá ser compartida externamente sin autorización formal y nunca podrá permanecer expuesta en soportes físicos o digitales no seguros.

- ***Asset Management***
  - *To maintain an updated and classified inventory of assets and information, prioritizing those critical to operational continuity.*
  - *To protect assets from physical, logical or human threats, ensuring their confidentiality, integrity and availability.*

- ***Principle of Least Access and Zero Trust***
  - *Access to information and systems will be strictly limited according to the role and needs of each collaborator, supplier or third party.*
  - *Under the Zero Trust model, no user, device or application is considered trusted by default; all access must be authenticated, validated and audited.*

- ***Lifecycle Security***
  - *Information security will be integrated from the design stage into every process, system, network or service, both internal and those provided to third parties.*
  - *Review and authorization controls will be applied to sensitive processes to ensure clear traceability and accountability.*

- ***Classification and Management of Information***
  - *Data will be classified (e.g. sensitive, confidential, internal use, public) and managed according to its criticality.*
  - *Sensitive information may not be shared externally without formal authorization and may never remain exposed on unsecured physical or digital media.*

- **Continuidad y Resiliencia**
  - Se mantendrán planes de contingencia y continuidad de negocio (BCP/DRP) probados periódicamente, asegurando la recuperación y resiliencia frente a incidentes o desastres.
  - La gestión se alineará con ISO 22301, garantizando la continuidad de operaciones críticas.

GESTIÓN PROACTIVA DEL RIESGO Y TECNOLOGÍAS EMERGENTES

En concordancia con su rol como servicio esencial conforme a la Ley N° 21.663, el Coordinador Eléctrico Nacional incorpora dentro de su modelo de seguridad integral la prevención activa de riesgos emergentes que pudiesen comprometer la continuidad operacional del Sistema Eléctrico Nacional (SEN), la integridad de la infraestructura crítica y la protección de los datos personales y estratégicos.

- **Prevención de Riesgos Tecnológicos:**
  Se promoverá una cultura de prevención que anticipe eventos disruptivos tales como ciberataques, uso de software no autorizado, fallas críticas de infraestructura TI/TO, y fenómenos tecnológicos emergentes que puedan afectar el desempeño y disponibilidad de los procesos críticos definidos en la Política de Continuidad del Negocio (BCP/BCM).

- **Uso Responsable de Inteligencia Artificial (IA):**
  En atención a los principios de seguridad por diseño y proporcionalidad en la gestión de riesgos definidos por la Ley Marco de Ciberseguridad, queda estrictamente prohibido el uso de herramientas de inteligencia artificial generativa, modelos de lenguaje o algoritmos predictivos que no estén

- ***Continuity and Resilience***
  - *Business continuity and contingency plans (BCP/DRP) will be maintained and periodically tested, ensuring recovery and resilience in the event of incidents or disasters.*
  - *Management will be aligned with ISO 22301, ensuring the continuity of critical operations.*

PROACTIVE RISK MANAGEMENT AND EMERGING TECHNOLOGIES

In accordance with its role as an essential service under Law No. 21.663, the National Electric Coordinator incorporates into its Integrated Security model the active prevention of emerging risks that could compromise the operational continuity of the National Electric System (SEN), the integrity of critical infrastructure and the protection of personal and strategic data.

- ***Technological Risk Prevention:***
  A culture of prevention will be promoted to anticipate disruptive events such as cyberattacks, the use of unauthorized software, critical IT/OT infrastructure failures and emerging technological phenomena that could affect the performance and availability of critical processes defined in the Business Continuity Policy (BCP/BCM).

- ***Responsible Use of Artificial Intelligence (AI):***
  In accordance with the principles of security by design and proportionality in risk management defined by the Cybersecurity Framework Law, the use of generative artificial intelligence tools, language models or predictive algorithms that are not expressly authorized, licensed, auditable and

expresamente autorizados, licenciados, auditables y sujetos a evaluación de impacto de seguridad y protección de datos.

Cualquier uso de sistemas de IA en procesos críticos deberá:

- Ser aprobado por el Comité Directivo de Seguridad Integral.
- Estar sustentado en un análisis de riesgo que considere su impacto sobre la confidencialidad, integridad y disponibilidad de la información.
- Incluir medidas de control para evitar fugas de datos, manipulación algorítmica o resultados no verificables.
- Asegurar trazabilidad, supervisión humana y cumplimiento del principio de transparencia tecnológica y explicabilidad de decisiones automatizadas conforme a la Ley 21.719.

- **Control del Software No Licenciado:**
  Se establecerán mecanismos para prevenir, detectar y erradicar el uso de software, plataformas o servicios de IA que no cuenten con licencias válidas, estándares de ciberseguridad apropiados o resguardo adecuado de datos sensibles. Su uso constituye un riesgo crítico para la seguridad del SEN y podrá ser tipificado como incidente de ciberseguridad reportable según el Estándar de Ciberseguridad para el Sector Eléctrico.

CULTURA DE SEGURIDAD INTEGRAL Y RESPONSABILIDAD

- La seguridad es responsabilidad de todos: cada colaborador debe proteger los activos a los que accede.

subject to a security and data protection impact assessment is strictly prohibited.

Any use of AI systems in critical processes must:

- *Be approved by the Integrated Security Steering Committee.*
- *Be supported by a risk analysis that considers its impact on the confidentiality, integrity and availability of information.*
- *Include control measures to prevent data leaks, algorithmic manipulation or unverifiable results.*
- *Ensure traceability, human supervision and compliance with the principle of technological transparency and the explainability of automated decisions in accordance with Law 21.719.*

- ***Control of Unlicensed Software:***
  Mechanisms will be established to prevent, detect and eradicate the use of AI software, platforms or services that lack valid licenses, appropriate cybersecurity standards or the adequate protection of sensitive data. Their use constitutes a critical risk to the security of the SEN and may be classified as a reportable cybersecurity incident according to the Standard of Cibersecurity of Electric Sector.

CULTURE OF INTEGRATED SECURITY AND RESPONSIBILITY

- *Security is the responsibility of everyone; every employee must protect the assets they access.*

- El Coordinador fomentará la capacitación, concientización y cultura de seguridad en forma permanente.
- Los incidentes de seguridad deberán ser reportados de inmediato a las instancias correspondientes, siguiendo protocolos establecidos.

MONITOREO Y CUMPLIMIENTO NORMATIVO

- La gestión de seguridad se regirá por estándares internacionales (ISO/IEC 27001, NERC-CIP) y marcos legales nacionales (Ley Marco de Ciberseguridad 21.663, Ley de Protección de Datos Personales 21.719).
- Se implementarán controles de cumplimiento, auditorías y revisiones periódicas para garantizar la mejora continua.
- Se exigirá a proveedores y terceros, medidas equivalentes para proteger la cadena de valor.

GOBERNANZA Y MEJORA CONTINUA

- La política será supervisada por el Comité Directivo de Seguridad Integral y el Oficial de Seguridad, quienes velarán por su actualización y cumplimiento.
- Se priorizará la mejora continua mediante métricas, reportes y revisiones periódicas, garantizando transparencia hacia el Consejo Directivo.

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 crítica (directrices y reglas).

- *The coordinator will promote ongoing training, awareness and a culture of security.*
- *Security incidents must be reported immediately to the appropriate authorities, following established protocols.*

MONITORING AND REGULATORY COMPLIANCE

- *Security management will be governed by international standards (ISO/IEC 27001, NERC-CIP) and Chile's legal frameworks (Cybersecurity Framework Law No. 21.663, Personal Data Protection Law No. 21.719).*
- *Compliance controls, audits and periodic reviews will be implemented to ensure continuous improvement.*
- *Suppliers and third parties will be required to take equivalent measures to protect the value chain.*

GOVERNANCE AND CONTINUOUS IMPROVEMENT

- *The policy will be overseen by the Integrated Security Steering Committee and the security officer, who will ensure it is updated and enforced.*
- *Continuous improvement will be prioritized through metrics, reports and periodic reviews, ensuring transparency for the board of directors.*

In addition to the above, the coordinator will define all internal regulations necessary to comply with the current policy and applicable regulations regarding cybersecurity and critical infrastructure (guidelines and rules).

Evaluación y Seguimiento de la Política

Policy Evaluation and Monitoring

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

The Cybersecurity and Critical Infrastructure Unit, under the board of directors and in conjunction with executive management, will be responsible for monitoring and managing ongoing compliance with this Integrated Security Policy.



Difusión y Comunicación

Dissemination and Communication



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

The Cybersecurity and Critical Infrastructure Unit must ensure that this Integrated Security Policy and its updates are promptly disseminated.

Cumplimiento y Sanciones

Compliance and Sanctions

El incumplimiento de la presente política será sancionado conforme a lo establecido en el Reglamento Interno de Orden, Higiene y Seguridad (RIOHS), la Política de Prevención de Delitos, el Código de Ética y la Política de Conflicto de Interés del Coordinador Eléctrico Nacional, sin perjuicio de las responsabilidades civiles, administrativas y penales que correspondan. Asimismo, serán aplicables las disposiciones y regímenes sancionatorios contemplados en la Ley N° 21.459 sobre Delitos Informáticos, la Ley N° 21.719 sobre Protección de Datos Personales y la Ley N° 21.663, Ley Marco de Ciberseguridad, atendida la condición del Coordinador Eléctrico Nacional como Servicio Esencial y Operador de Importancia Vital, de conformidad con la normativa vigente.

Failure to comply with this policy will be sanctioned in accordance with the Internal Regulations for Order, Hygiene and Security (Reglamento Interno de Orden, Higiene y Seguridad, RIOHS), the Crime Prevention Policy, the Code of Ethics and the Conflict-of-Interest Policy of the National Electric Coordinator, without prejudice to any applicable civil, administrative and criminal liabilities. Furthermore, the provisions and sanctioning regimes included in Law No. 21.459 on Computer Crimes, Law No. 21.719 on Personal Data Protection and Law No. 21.663, the Cybersecurity Framework Law, will be applicable, given the status of the National Electric Coordinator as an essential service and operator of vital importance, in accordance with current regulations.



Vigencia, Aprobación y Reemplazo

Validity, Approval and Replacement

La presente política tiene vigencia a partir de 03 de noviembre de 2025. Todas las modificaciones que sean efectuadas a este documento deberán constar por escrito y entrarán en vigor una vez aprobadas por el Consejo Directivo.

La presente política reemplaza íntegramente, desde la fecha de su entrada en vigencia, a la "Política Integral de Seguridad de la Información, Ciberseguridad e Infraestructura Crítica del Coordinador Eléctrico Nacional", aprobada por el Consejo Directivo en Sesión Ordinaria N°8, celebrada el 17 de agosto de 2022.

This policy is effective from November 3, 2025. All modifications made to this document must be in writing and will come into effect once approved by the board of directors.

This policy fully replaces, as of its effective date, the "Integrated Policy on Information Security, Cybersecurity and Critical Infrastructure of the National Electric Coordinator", approved by the board of directors at its 8th Ordinary Session held on August 17, 2022.

Disclaimer:
El idioma oficial para efectos de cumplimiento y aplicación de esta Política de Seguridad Integral es el español. La versión en inglés se pone a disposición exclusivamente para facilitar su comprensión por parte de personas, colaboradores, visitas, autoridades u otros que lo requieran y cuya lengua principal sea el inglés. En caso de discrepancias, prevalecerá siempre la versión en español.

Disclaimer.
The official language for the purposes of compliance and enforcement of this Integrated Security Policy is Spanish. An English version is provided solely to facilitate understanding for individuals, collaborators, visitors, authorities, or others who may require it and whose primary language is English. In the event of any discrepancies, the Spanish version shall prevail.



Elabora | Unidad de
Ciberseguridad e
Infraestructura Crítica