Procedimiento Normativo de Elaboración de NT de Ciberseguridad y Seguridad de la Información
Sesión 4

Departamento Eléctrico
Enero 2022

COMISIÓN NACIONAL DE ENERGÍA

Energía Abierta

Agenda

- Comité Consultivo Especial.
- Calendario
- Gobernanza
- Gestión de Riesgos
- Reporte de incidentes

Comité Consultivo Especial (Res Exta CNE N°524/2021)

N°	Nombre	Empresa/Institución
1	Félix Canales	Comisión Nacional de Energía
2	Jaime García	Comisión Nacional de Energía
3	Sandra Castro	Comisión Nacional de Energía
4	Daniel Charlín	Ministerio de Energía
5	Roxana Varela	Superintendencia de Electricidad
6	Hernán Espinoza	Ministerio del Interior
7	Sebastián Vargas	Coordinador Independiente del S
8	Paula Reyes	Coordinador Independiente del S
9	Laura Santos	Enel Generación Chile S.A.
10	Sebastián Celis	Colbún S.A.
11	Claudio Villalobos	Engie Energía Chile S.A.
12	Manuel Osses	Prime Energía SpA
13	Óscar Guarda	Acciona Energía SpA
14	Viviana Delgado	Sonnedix Chile Holding SPA
15	Fulvio Faletto	Enel Distribución Chile S.A.
16	Fernando Muñoz	Sociedad Austral de Electricidad S
17	Doris Herrera	Chilquinta Servicios S.A.
18	Daniel Soto	CGE S.A
19	Roberto Arriagada	Transelec S.A
20	Ricardo Javier Bustos	Experto Técnico
21	Francisco Muñoz	Experto Técnico
22	Freddy Macho	Experto Técnico
23	Eduardo Morales	Experto Técnico
24	Cristóbal Hammersley	Experto Técnico

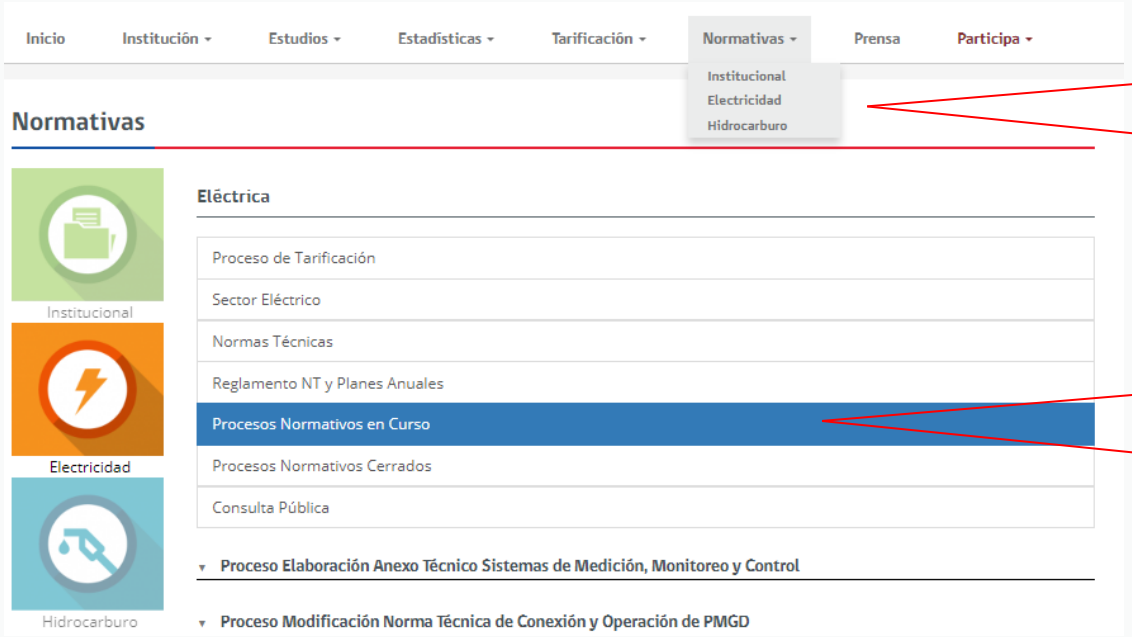
Presidente: Félix Canales
Secretaria de Actas: Sandra Castro

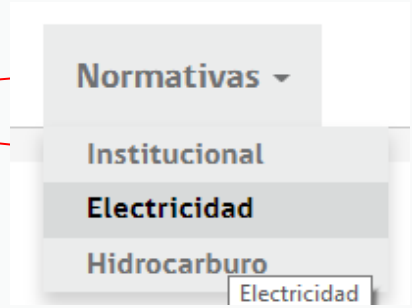
Objetivo del Comité Consultivo

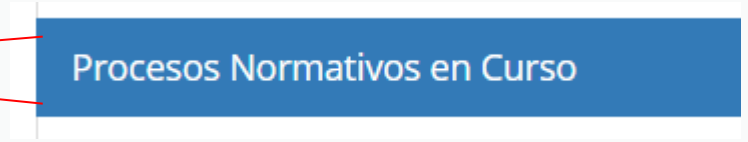
Artículo 17. DS 11/2017- "Para cada Procedimiento Normativo se deberá constituir un Comité Consultivo con el objeto de discutir, analizar y dar su opinión a la Comisión sobre la Norma Técnica de que se trate o de la correspondiente modificación de una ya existente."

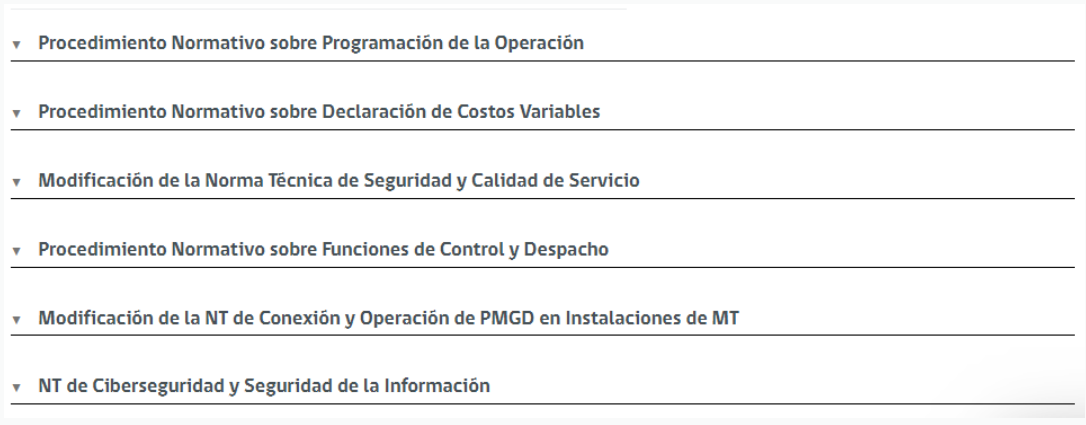
Trabajo próximas sesiones

Portal Normativo









Programación Sesiones de Comité

diciembre 2021						
Lun	Mar	Mié	Jue	Vie	Sáb	Dom
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

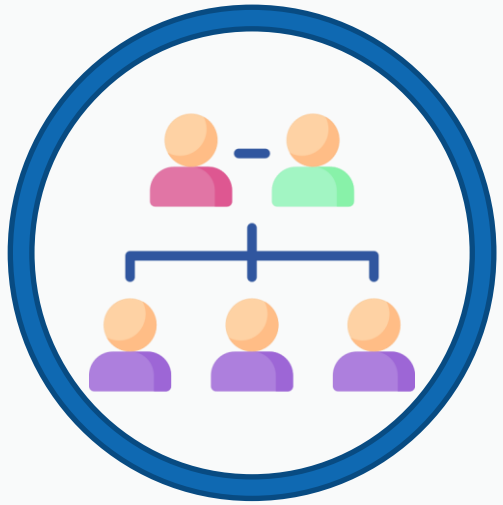
enero 2022						
Lun	Mar	Mié	Jue	Vie	Sáb	Dom
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Sesión	Temas	Fecha
1	Introducción Planificación Contenidos	07-12-2021
2	Presentaciones integrantes Comité	20-12-2021
3	Contenidos Norma Parte I	27-12-2021
4	Contenidos Norma Parte II	17-01-2022

Temas	Fecha
CCE	Dic 21 - Ene 22
Consulta Pública	Feb-Mar 2022

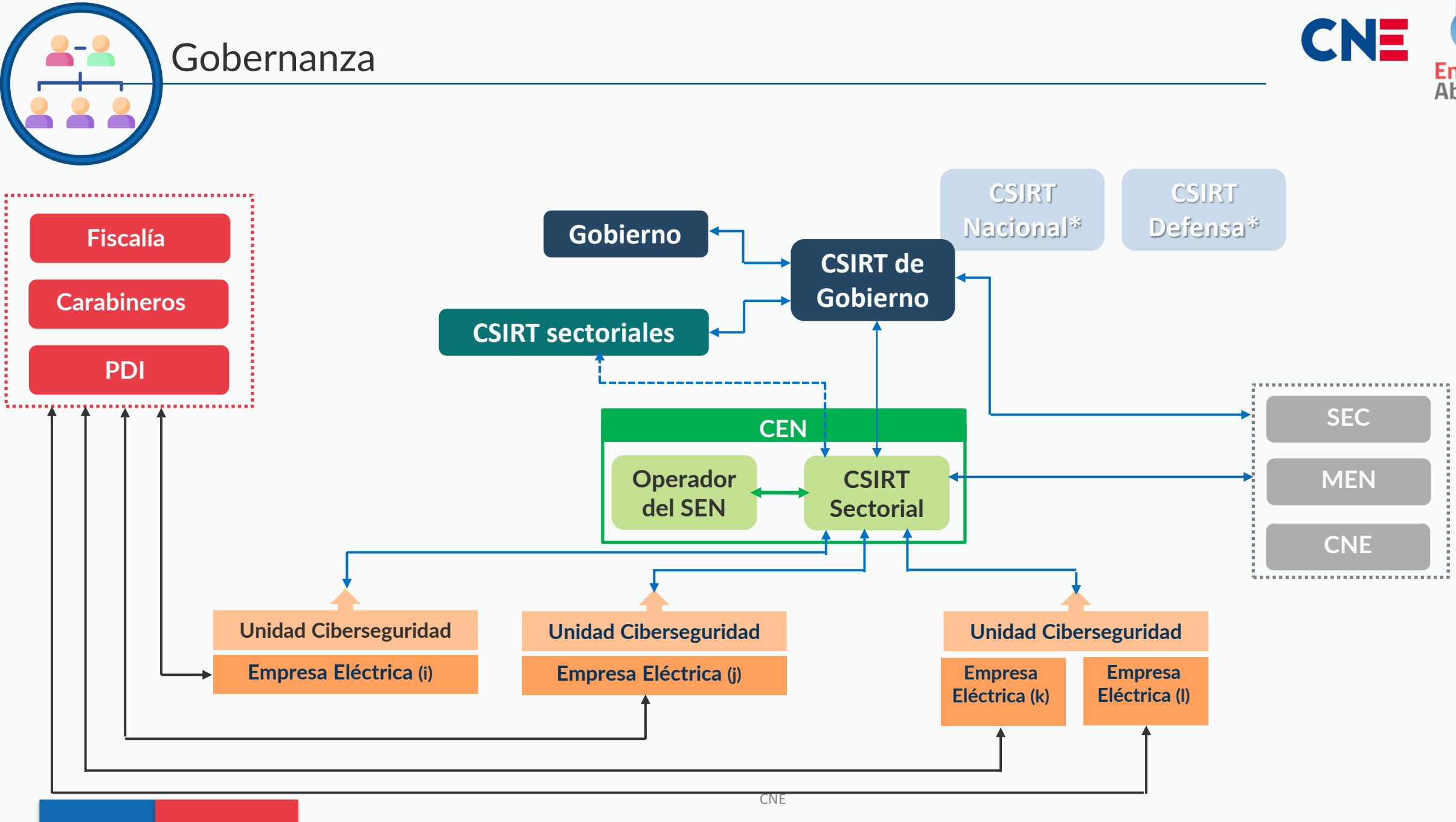
Gobernanza

Gobernanza

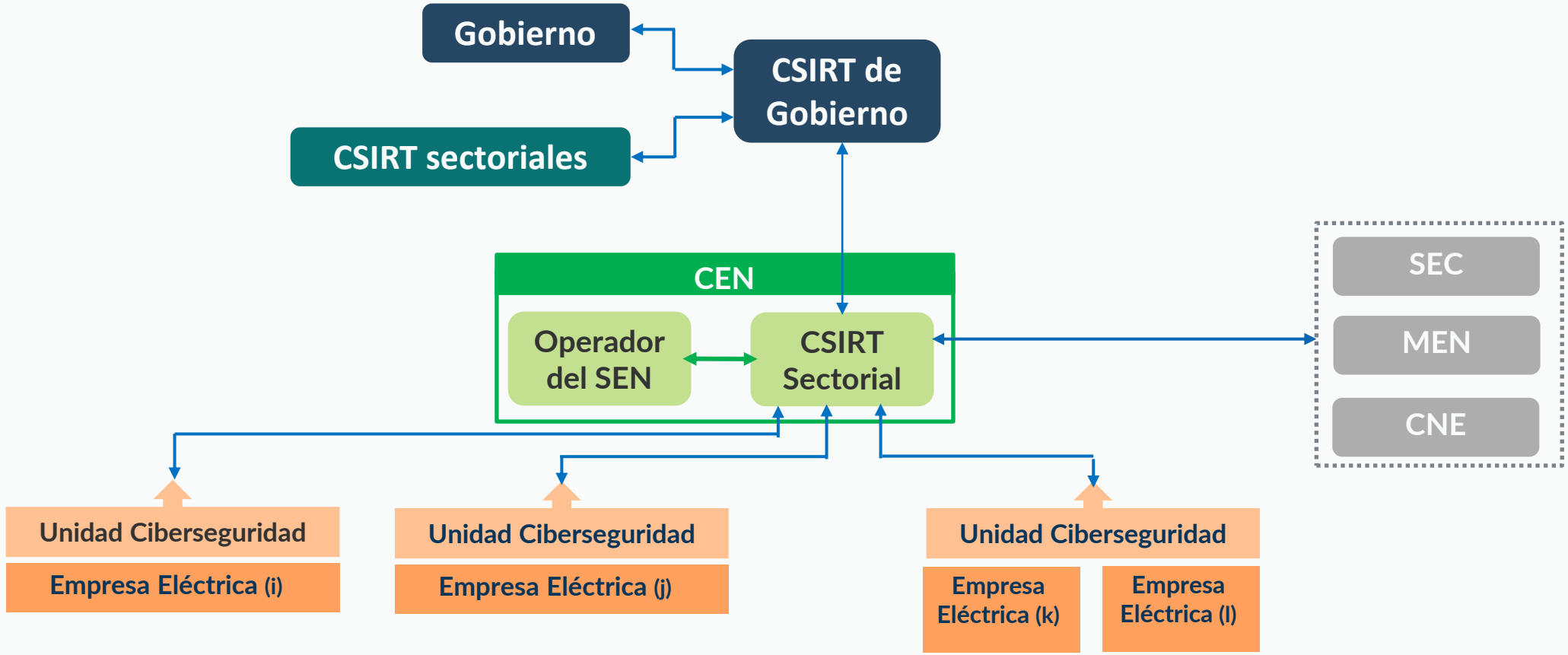


- La gobernanza propuesta considera todas las eventuales interacciones entre los distintos agentes.
- Incluye interacciones obligatorias y opcionales.
- La NTCySI se enfocará en las exigencias respecto a los reportes de incidentes a nivel Empresas Eléctricas y CSIRT sectorial eléctrico.

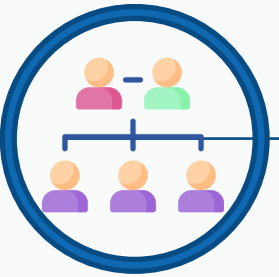
Gobernanza


Fiscalía
Carabineros
PDI
Gobierno
CSIRT sectoriales
CSIRT de Gobierno
CSIRT Nacional*
CSIRT Defensa*
CEN
Operador del SEN
CSIRT Sectorial
SEC
MEN
CNE
Unidad Ciberseguridad
Empresa Eléctrica (i)
Unidad Ciberseguridad
Empresa Eléctrica (j)
Unidad Ciberseguridad
Empresa Eléctrica (k)
Empresa Eléctrica (l)

Gobernanza: Reporte de incidentes



Gobernanza: Reporte Incidentes - Posible delito



Fiscalía

Carabineros

PDI

CSIRT de Gobierno

CEN

Operador del SEN

CSIRT Sectorial

SEC

MEN

CNE

Unidad Ciberseguridad

Empresa Eléctrica (i)

Unidad Ciberseguridad

Empresa Eléctrica (j)

Unidad Ciberseguridad

Empresa Eléctrica (k)

Empresa Eléctrica (l)

Gestión de Riesgos

Todas las Empresas Eléctricas deberán identificar y mantener actualizado el **inventario de activos de información.**

Tipo de activo de información

- Personas
- Soportes de la información (TI y TO)
- Información misma

El inventario de activos debería considerar, al menos la siguiente información: Identificación del activo de información, ubicación, identificación de quienes lo utilizan, responsable y/o propietario del activo.

Gestión de Riesgos

Una vez definido el inventario de activos de información, las Empresas Eléctricas deberán realizar un **Análisis de Criticidad** para determinar los activos sujetos a una evaluación de riesgos de la seguridad de la información y ciberseguridad.

El análisis de criticidad deberá considerar al menos los siguientes criterios:

- Disponibilidad
- Integridad
- Confidencialidad

Gestión de Riesgos: Ejemplo Análisis de Criticidad

Atributo asociado a criticidad	Valor	Descripción
Confidencialidad	Público	El activo no tiene restricciones de acceso
	Reservado	Activo de información cuyo acceso no autorizado tiene impacto para la empresa o terceros.
Integridad	Bajo	Activo de Información cuya modificación no deseada tiene consecuencias con impacto leve para la empresa o terceros.
	Medio	Activo de Información cuya modificación no deseada tiene consecuencias con impacto significativo para la empresa o terceros.
	Alto	Activo de Información cuya modificación no deseada tiene consecuencias con impacto grave para la empresa o terceros.
Disponibilidad	Bajo	Activo de Información cuya inaccesibilidad, tiene impacto leve para la empresa o terceros.
	Medio	Activo de Información cuya inaccesibilidad, tiene impacto significativo para la empresa o terceros.
	Alto	Activo de Información cuya inaccesibilidad, tiene impacto grave para la empresa o terceros.

Gestión de Riesgos

Las Empresas Eléctricas deberán realizar un análisis y evaluación de riesgos de seguridad de la información y ciberseguridad a todos los activos clasificados con criticidad “Alta y Media”.

Gestión de Riesgos: Análisis y Evaluación de Riesgos

Cada empresa deberá identificar las **amenazas, vulnerabilidades y los posibles riesgos**, tanto internos como externos, a los que están expuestos los activos de información con mayor criticidad (clasificados con criticidad "Alta y Media") .

Se deberá efectuar un análisis de riesgos para determinar su nivel de gravedad, considerando la probabilidad de ocurrencia y su impacto.

Una vez establecido el nivel de gravedad del riesgo, cada empresa deberá aplicar uno o más marcos referenciales de controles específicos para implementar medidas de prevención y mitigación.

Gestión de Riesgos

- Las empresas deberán contar con planes documentados de gestión de riesgos de Seguridad de la Información.
  →La documentación y antecedentes disponibles para cualquier solicitud de la SEC.
  →Actualizado anualmente.

- Objetivo:
  - ❖ Anticipar consecuencias derivadas de amenazas tales como ciberataques y ciberincidentes no hostiles.
  - ❖ Evitar o reducir la ocurrencia de contingencias y mitigar sus eventuales efectos.
  - ❖ Indicar acciones inmediatas y medidas progresivas de mejoras (con sus respectivos indicadores, controles y documentación).

- Dichos planes deberán considerar la realización de pruebas de seguridad a la infraestructura tecnológica
  - – Resultados, oportunidades de mejora y plan de acción informados a la SEC
  - ➢ Empresas Categoría Alta y Crítica: Anual
  - ➢ Empresas categoría Media y Baja: Bianual

Reporte de incidentes

Reporte de incidentes

- Todas las Empresas Eléctricas tienen la obligación de reportar sus incidentes a CSIRT sectorial, de acuerdo con lo establecido en la NTCySI.

- La Unidad de ciberseguridad de cada empresa es la encargada de comunicarse con el CSIRT sectorial, quien informará a CSIRT de gobierno y autoridades respectivas.

➢ Niveles de incidentes (peligrosidad e impacto)

➢ Plazos de respuesta

➢ Contenidos mínimos

Reporte de incidentes: Niveles de Peligrosidad (TI y TO)

Nivel	Clasificación	Tipo de incidente
Crítico	Otros	Amenaza Avanzada Persistente
Muy alto	Código dañino	-Distribución de malware -Configuración de malware
	Intrusión	-Robo -Sabotaje (TI y TO)
	Pérdida de disponibilidad	Interrupciones
Alto	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado
	Código Dañino	-Sistema infectado -Servidor C&C (Mando y Control)
	Intrusión	-Compromiso de aplicaciones o dispositivos -Compromiso de cuentas con privilegios
	-Intento de Intrusión -Pérdida de disponibilidad -Compromiso de la información -Fraude	-Ataque desconocido -DoS (Denegación de servicio) -DDoS (Denegación distribuida de servicio) -Acceso no autorizado a información
		Modificación no autorizada de información
		-Pérdida de datos -Phishing

Fuente: ENISA

Reporte de incidentes: Niveles de Peligrosidad (TI y TO)

Nivel	Clasificación	Tipo de incidente
Medio	Contenido abusivo	Discurso de odio
	Obtención de información	Ingeniería social Explotación de vulnerabilidades conocidas
	Intrusión	Intento de acceso con vulneración de credenciales Compromiso de cuentas sin privilegios
	Pérdida de disponibilidad	Mala configuración Uso no autorizado de recursos
	Fraude	Derechos de autor Suplantación
	Vulnerable	Criptografía débil Amplificador DDoS
		Servicios con acceso potencial no deseado
		Revelación de información Sistema vulnerable
Bajo	-Contenido abusivo -Obtención de información -Otros	Spam Escaneo de redes
		Análisis de paquetes (sniffing) Otros

Solicitud de opinión 1: Proponer propuesta de criterios.

Reporte de incidentes: Niveles de Impacto (TI y TO)

Nivel	Descripción
Crítico	Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas.
	i)Afecta a elementos declarados como Infraestructura Crítica. ii)Desconexión intempestiva sobre el 75% de sus instalaciones eléctricas.
	Afecta a sistemas clasificados como confidenciales o que contengan información calificada como sensible de acuerdo a la ley.
	El incidente requiere más de 13 horas continuas del Equipo de Respuestas para su resolución.
Muy alto	i)Afecta a la seguridad ciudadana con potencial peligro para bienes materiales. ii)Afecta a un servicio esencial (No eléctrico).
	Desconexión intempestiva entre el 50% hasta el 75% de sus instalaciones eléctricas.
	Afecta a información clasificada como reservada o sensible.
	El incidente requiere más de 9 horas continuas del Equipo de Respuestas para su resolución.
Alto	Desconexión intempestiva entre el 25% hasta el 50% de sus instalaciones eléctricas.
	El incidente requiere más de 7 horas continuas del Equipo de Respuestas para su resolución.
Medio	Desconexión intempestiva entre el 10% hasta el 25% de sus instalaciones eléctricas.
	El incidente requiere más de 4 horas continuas del Equipo de Respuestas para su resolución.
Bajo	Afecta a los sistemas del regulado.
	El incidente requiere más de 2 horas continuas del Equipo de Respuestas para su resolución.
Sin Impacto	No hay ningún impacto apreciable.

Solicitud de opinión 2: Proponer propuesta de criterios.

Reporte de incidentes: Plazos de respuestas

La Empresa Eléctrica evaluará el Nivel de peligrosidad y Nivel de impacto a cada incidente, dando la categoría que sea la más alta entre ambas tablas.

Nivel de peligrosidad o impacto	Reporte inicial	Reporte intermedio	Reporte final
Crítico	30 minutos	6/ 12 / 24 horas	5 días
Muy alto	1 hora	6/24/ 48 horas	10 días
Alto	1 hora	24/ 72 horas	15 días
Medio	12 horas	72 horas	Mes siguiente
Bajo	24 horas	NA	Mes siguiente

CSISRT tiene plazo de 5 días hábiles para observar o solicitar correcciones

Solicitud de opinión 3: Proponer propuesta de criterios.

Reporte de incidentes: Contenidos mínimos

Formato y Medios serán definidos por el CSIRT sectorial

Contenidos adicionales por CSIRT sectorial, SEC o CSIRT de gobierno

Contenidos Mínimos (1 de 3):

- Resumen ejecutivo del ciberincidente.
- Identificación de la empresa eléctrica.
- Encargado de ciberseguridad en funciones.
- Fecha y hora precisas de ocurrencia del ciberincidente, si se conociera.
- Fecha y hora precisas de detección del ciberincidente.
- Descripción detallada de lo sucedido, señalando los activos de información y su atributo de criticidad afectado (confidencialidad/ integridad/ disponibilidad).
- Recursos tecnológicos afectados.

Reporte de incidentes: Contenidos mínimos

- Origen o causa identificable del ciberincidente. Esto incluye incidentes cuyo origen sea de un proveedor cuya red esté interconectada o tenga altos grados de interoperación.
- Taxonomía, es decir, clasificación y tipo de ciberincidente.
- Nivel de peligrosidad.
- Nivel de impacto.
- Impacto transfronterizo, si corresponde.
- Indicadores de compromiso: indicadores de compromiso de nivel IP, indicadores de compromiso de nivel de dominios y subdominios, indicadores de compromiso de correos, indicadores de compromiso a nivel HASH (MD5/SHA1/SHA256 o el que los reemplace), vulnerabilidades facilitadoras del incidente y posibles vectores de ingreso/egreso de los artefactos, y en general los datos técnicos del incidente, entre otros similares.

Reporte de incidentes: Contenidos mínimos

- Clasificación Traffic Light Protocol (TLP).
- Afectados actuales y potenciales.
- Impacto económico estimado, si procede y es conocido.
- Extensión geográfica, si se conoce.
- Daños reputacionales, aun cuando sean eventuales.
- Medios necesarios para la resolución calculados en horas persona.
- Medidas de mitigación y resolución.
- Las bitácoras generadas de forma automática por los sistemas.

Solicitud de opinión 4: Proponer propuesta de criterios.

Muchas Gracias

Comisión Nacional de Energía
Alameda 1449,, Torre 4, Piso 13
Tel. (2) 2797 2600
Fax. (2) 2797 2627
www.cne.cl

Santiago - Chile

CNE COMISIÓN NACIONAL DE ENERGÍA

Energía Abierta