Protocolo de Notificación de Incidentes de Ciberseguridad para el Sector Eléctrico

Diciembre 2021

Coordinador Eléctrico Nacional

www.coordinador.cl

Contenido

1. Comunicación de Incidentes

De acuerdo con lo establecido en el estándar de ciberseguridad para el sector eléctrico, basado en el estándar NERC-CIP, emitido por el Coordinador Eléctrico Nacional (el Coordinador), las empresas Coordinadas deberán comunicar al Coordinador Eléctrico Nacional CEN y este a la Superintendencia de Electricidad y Combustibles SEC, y a otras autoridades que defina la SEC, los incidentes y amenazas de ciberseguridad que afecten o intenten poner en riesgo la seguridad y confiabilidad del Sistema Eléctrico Nacional. La Entidad Responsable (Empresa Coordinada o el Coordinador) será asimismoresponsable de mantener informados tanto al Coordinador como a la SEC de la evolución y desarrollo de las medidas o acciones de detección, respuesta y recuperación de los incidentes reportados según se indica en el presente protocolo.

2. Aplicabilidad

El presente protocolo aplica a todas las Entidades Responsables, tal como se especifica en el estándar de ciberseguridad para el sector eléctrico, para los siguientes incidentes:

a) Incidentes de Ciberseguridad Reportables (ICR): Corresponden a aquellos Incidentes de Ciberseguridad que han 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, sean de impacto alto, medio o bajo.
   - Un Perímetro se Seguridad Electrónica (PSE) de un Ciber Sistema SEN de Impacto Alto o Medio, o
   - 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 clientes del SEN, con la periodicidad y tiempos indicados en el punto 3 para ICR.

b) Incidentes de Ciberseguridad (IC): Corresponden a aquellos actos maliciosos o eventos que:

   - 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
   - Amenacen o intenten interrumpir la operación de un Ciber Sistema SEN, sea calificado como de impacto alto, medio o bajo.

Los incidentes que amenacen comprometer o interrumpan Ciber Sistemas o perímetros de seguridad según se indica en los puntos anteriores, se deberán reportar con la periodicidad y tiempos indicados en el punto 3 para IC.

3. Periodicidad de Reportes

Los reportes deberán ser entregados a más tardar dentro de los tiempos y frecuencia indicados en la siguiente tabla:

Tipo de Incidente	Reporte Inicial	Reportes Intermedios	Reporte final
Incidente de Ciberseguridad Reportable (ICR)	60 minutos	2 reportes 6 horas / 24 horas	Máximo 10 días
Incidente de Ciberseguridad (IC)	24 horas	1 reporte 48 horas	Máximo 10 días

Los días indicados en la tabla anterior corresponde a días corridos y los plazos se consideran como máximos contados desde el momento en que la Entidad Responsable detecta el Incidente de Ciberseguridad.

4. Notificación de Incidentes

El reporte de notificación inicial, intermedio(s) y final deberá incluir, a lo menos, la información especificada en el siguiente formulario:

Ítem	Descripción	Campos Obligatorios por reporte		
		Inicial	Intermedio	Final
1. Nombre de la Entidad Afectada:	Nombre de la empresa Coordinada afectada	✓	✓	✓
2. Fecha y Hora del presente reporte	Indicar Fecha y hora del reporte en formato AAAAMMDD HH:MM Ejemplo: 20201103 18:35	✓	✓	✓
3. Calificación de Incidente: • Incidente Ciberseguridad Reportable (ICR) • Incidente de Ciberseguridad (IC)	ICR/IC	✓	✓	✓
4. Código único identificador del incidente:	Tipo + RUT Entidad + fecha + hora	✓	✓	✓

	Donde: Tipo: IC o ICR RUT Coordinado: 99888777 (sin puntos, guion ni dígito verificador fecha: AAAAMMDD Hora en formato 24 horas: HHMM Ejemplo: ICR99999999202011032333			
5. Incidentes previos relacionados:	Ingresar el Código único identificador del incidente si existiera un incidente anterior	✓	✓	✓
6. Estado de Notificación: Inicial/Intermedia/Final	Declarar si es notificación inicial, intermedia o final.	✓	✓	✓
7. Estado de Incidente:	Declarar estado del incidente (Abierto/Cerrado): • Abierto: en curso de remediación o investigación • Cerrado: incidente remediado o resuelto	✓	✓	✓
8. Fecha y hora de inicio o detección del incidente UTC Chile:	Fecha AAAAMMDD y hora del tipo HH:MM Ejemplo: 20201103 18:35	✓	✓	✓
9. Fecha y hora de cierre o resolución del incidente UTC Chile (si aplica):	Fecha AAAAMMDD y hora del tipo HH:MM Ejemplo: 20201103 18:35	✓	✓	✓
10. Descripción técnica del incidente:	Origen o causa, Aspectos técnicos de la detección, identificación, categorización del incidente que puedan aportar a la industria a prevenirlo.		✓	✓
11. Tipo de Incidente y vector de ataque	Ciber ataque, phishing, malware, acceso electrónico, acceso físico, daño por terceros, etc.		✓	✓
12. Afectación	Afectación en el Incidente			
• Ciber Activos, o Ciber Activos SEN:	Listado de Ciber activos o Ciber sistemas involucrados	✓	✓	✓
• Instalaciones y Calificación de Impacto (Alto, Medio, Bajo):	Ubicación física donde se generó el incidente y calificación de impacto de la instalación	✓	✓	✓

• Capacidad:	Cantidad de MW afectados o interrumpidos	✓	✓	✓
• Transmisión:	Líneas o subestaciones afectadas	✓	✓	✓
• Cantidad de clientes:	Número total de clientes afectados o interrumpidos		✓	✓
13. Proveedores involucrados:				
• Nombre y RUT de la empresa (si aplica):	Nombre y RUT de la empresa proveedora involucrada en el incidente (si aplica)			✓
14. Medidas adoptadas y en curso	Descripción técnica de las medidas adoptadas para contener, mitigar y/o recuperar el(los) sistema(s) afectado(s).	✓	✓	✓
15. Datos del Ataque				
• IP/PUERTO/HOST/URL/ DOMINIOS/EMAIL/HASH	Identificadores del origen del ataque (ejemplo: IP de origen de una conexión fraudulenta, Puerto utilizado para iniciar una conexión a una dirección IP o dominio que actúe como centro de comando y control de un ataque, dirección de email desde donde se envía el archivo malicioso, HASH del archivo ejecutable del malware, entre otros)		✓	✓
• Indicadores del ataque	Elementos que permitan indicar la ocurrencia del ataque. (actividades o hechos previos identificados que pueden ser indicios del ataque, email, phishing, llamadas sospechosas, entre otros.)		✓	✓
• Otros	Otros antecedentes de valor del incidente			✓
16. Plan de acción	Nombre del documento o informe de cierre que contiene plan de trabajo que incluya las acciones futuras para evitar que el incidente se repita.			✓
17. Nombre y Firma Encargado CIP:		✓	✓	✓

5. Informe de Cierre del Incidente

Una vez cerrado el incidente, y dentro de 5 días corridos de la emisión del reporte de notificación final, la Entidad Responsable deberá emitir un informe de cierre de incidente, que incluya la información contenida en el reporte de notificación final más toda la información que respalde los planes recuperación y de acción correctivos llevados a cabo o planificados en cumplimiento con lo establecido en el estándar de ciberseguridad del sector eléctrico. La Entidad Responsable deberá identificar e indicar en dicho informe qué acciones de mitigación se ejecutaron y/o ejecutarán para evitar que el incidente reportado se repita.

Adicionalmente, en los casos que el Coordinador o la SEC lo estime necesario, podrá requerir informes complementarios a la Entidad Responsable (por ejemplo, informes forenses informáticos).

6. Envío de la Información

Los reportes de notificación de incidentes de ciberseguridad, así como los informes de cierre, deberán ser enviados mediante correo electrónico a la casilla ciberincidenteSEN@coordinador.clen cualquier horario, sean días hábiles, fines de semana o festivos, dentro del plazo máximo estipulado en los puntos 3 y 5 del presente protocolo.

Para estos efectos, el Encargado CIP o su delegado, deberá revisar, firmar y enviar la información según lo indicado en el presente protocolo. El no contar con toda la información solicitada al momento de cada notificación, no deberá ser impedimento para el envío de la comunicación dentro de los plazos estipulados.

Finalmente, con los antecedentes del ciber incidente reportados desde las empresas coordinadas a CEN, este comunicará según lo establecido en los puntos 3 y 5 a la SEC oportunamente y con el contenido definido en este protocolo.