Consejo Nacional de Operación

GUÍA DE CIBERSEGURIDAD

Historia

Version	Fecha	Tipo de Emisión	Cambios
0	10.12.2018	Versión para Comité Tecnológico	
0.1	14.02.2019	Versión actualizada según comentarios con anexo para comité.	Se complementa introducción, revisiones generales y nuevo anexo de cumplimiento
0.2	18.06.2019	Versión para publicar para comentaros. Recoge observaciones del Comité de Ciberseguridad y la mesa sectorial de infraestructura crítica.	Se modifica principalmente el capítulo de recuperación y Gestión de incidentes, se revisan tiempos de cumplimiento.

Consejo Nacional de Operación

TABLA DE CONTENIDO

1. CIBERSEGURIDAD

El Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética del Sector Electricidad Colombiano estableció los lineamientos que deben adoptar los diversos agentes del Sector electricidad y operadores de las infraestructuras críticas con el propósito de coordinar acciones eficientes e integrales que permitan prevenir y/o mitigar potenciales amenazas cibernéticas que pongan en riesgo la disponibilidad y continuidad del servicio de energía eléctrica por amenazas ciberneticas.

Ante la modernización tecnológica de la infraestructura del sector eléctrico en Colombia, la automatización de los procesos y de sus centros de operación local y remota, en el entorno de un mundo globalizado y convergente en tecnología IP se tiene que los riesgos asociados a la seguridad de la operación deben ser cubiertos mediante reglas y normas que determinen las buenas prácticas y que, actualmente, son de aplicación permanente en gran parte del mundo.

1.1 Introducción y Antecedentes

Casos como los apagones registrados en ucrania en 2015 y 2016 producidos por ciberataques, así como los ataques a infraestructuras eléctricas del Reino Unido, Irlanda, Estados Unidos entre otros han demostrado que los ataques cibernéticos a éstas son parte activa del panorama de riesgos actual.

Conscientes de su rol en la sociedad colombiana y de que el sector eléctrico se ha venido modernizando con tecnologías de operación que son susceptibles a ciberataques; el sector ha desarrollado acciones de concientización y protección desde el año 2011 a través del Consejo Nacional de Operación (CNO), primero publicando una guía de ciberseguridad para sus agentes con base en las Normas NERC-CIP v4, luego formalizándola a través de la adopción de la misma por acuerdo sectorial en 2015 todo acompañado de jornadas y talleres de ciberseguridad que han fortalecido las capacidades de los agentes para responder ante estas nuevas amenazas.

Esta guía recopila las medidas que deben establecer las empresas del Sector para prepararse, detectar, contener, responder, coordinar la reacción, recuperarse y aprender de incidentes cibernéticos que puedan afectar al Sistema Interconectado Nacional para consolidar un nivel de madurez adecuado en las capacidades de ciberseguridad y ciberdefensa del sector contribuyendo a la operación confiable, segura y resiliente del mismo.

En ese contexto, el sector eléctrico requiere de la implementación de normativa asociada a la ciberseguridad y de la apropiación de conocimiento de dicho entorno para garantizar la prestación eficiente del servicio de energía eléctrica.

Para la elaboración de esta guía se utilizó principalmente como referente la normativa publicada por la NERC (*North American Electric Reliability Corporation*) y compuesta por los estándares CIP (*Critical Infrastructure Protection*), CIP-002 a CIP-014, de los cuales se extractaron y adaptaron aspectos aplicables al caso colombiano que fueron revisados por expertos de diferentes empresas del sector asignados a la comisión de ciberseguridad y el comité de supervisión y ciberseguridad (antes comité tecnológico) del CNO.

Las normas NERC CIP-002 a la CIP-014, tratan:

CIP-002-5.1a	Categorización de ciberactivos críticos
CIP-003-7	Gestión de controles de seguridad
CIP-004-6	Personal y entrenamiento
CIP-005-6	Perímetro(s) de seguridad electrónica
CIP-006-6	Seguridad física de ciberactivos críticos
CIP-007-6	Gestión de seguridad del sistema
CIP-008-5	Reporte de incidentes planes de respuesta
CIP-009-6	Planes de recuperación de ciberactivos críticos
CIP-010-3	Gestión de la configuración, cambios y evaluación de vulnerabilidades
CIP-011-2	Protección de la información
CIP-013-1	Ciberseguridad cadena de suministro
CIP-014-2	Seguridad física

De acuerdo con lo anterior se recomienda la adopción de los requerimientos mínimos de seguridad para la protección de los activos del Sistema Interconectado Nacional (SIN) que son considerados críticos para la operación confiable del sistema eléctrico, en este sentido es necesario identificar los activos críticos, los ciberactivos críticos, los perímetros de seguridad electrónica y seguridad física y aplicar los criterios establecidos en esta guía que deberá ser revisada por lo menos cada dos años para mantener su vigencia y actualización.

1.2 Glosario

Activo crítico: Instalaciones, sistemas o equipos eléctricos que de ser destruidos, degradados o puestos indisponibles, afecten la confiablidad (suficiencia y seguridad), operatividad o que comprometan la seguridad de la operación del SIN.

Auditoría: Es la actividad mediante la cual un ente de control revisa y valida los registros y reportes de un procedimiento, con el fin de garantizar la calidad del mismo. En consecuencia, se generan acciones y los planes de mejoramiento.

Ciberactivo crítico: Dispositivo para la operación confiable de activos críticos que cumple los atributos descritos en el numeral 4.2.2.

Ciberactivo: Dispositivo electrónico programable y elementos de las redes de comunicaciones incluyendo hardware, software, datos e información. Así como aquellos elementos con protocolos de comunicación enrutables, que permitan el acceso al mismo de forma local o remota.

Ciberactivo transitorio: Puede ser uno de los muchos tipos de dispositivos que son especialmente diseñados para dar soporte o mantenimiento a los ciberactivos existentes, que puede ejecutarse desde un computador portátil o una tableta y que además puede interactuar o ejecutar aplicaciones compatibles con los ciberactivos existentes o con la red en donde éstos se encuentran conectados.

Entidad Responsable: Hacen referencia a cada uno de los agentes del sector que dará cumplimiento del acuerdo CNO.

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias, puede ocurrir una o varias veces en sistemas o servicios y puede tener múltiples causas, puede ser algo que no ha sucedido y algunas veces se puede referir a "incidente" o "accidente". (ISO/IEC 27000:2016, 2.25).

Incidente de Ciberseguridad: Cualquier acto malicioso o evento sospechoso que compromete o intenta comprometer, la seguridad física o electrónica de un ciberactivo crítico o su perímetro.

Medios extraíbles: Pueden ser en forma de disquetes, discos compactos, unidades flash *USB*, discos duros externos y otras tarjetas o unidades de memoria flash que contienen memoria no volátil.

NERC – CIP: *North American Electric Reliability Corporation.* Es la Corporación de Confiabilidad Eléctrica de Norteamérica. CIP. *Critical Infrastructure Protection*. Protección de la infraestructura crítica, incluye un conjunto de normas numeradas del 002 al 0014.

Perímetro de Seguridad Electrónica: Es la frontera lógica, con acceso controlado, que rodea una red aislada o con conectividad enrutable a otras redes dentro de la cual están conectados los ciberactivos críticos.

Perímetro de Seguridad Física: Es la frontera física, con acceso controlado, completamente contenida (“seis paredes”) que rodea cuartos de control, cuartos de comunicaciones, centros de operación y otros sitios que alojan ciberactivos críticos.

Pista de auditoría: Es la evidencia o resultado de la actividad de registrar y generar reportes durante la ejecución de un procedimiento.

Programa: Es un conjunto de iniciativas, planes o proyectos desarrollados para el logro de objetivos comunes y concretos.

Puntos de acceso al (los) Perímetro(s) de Seguridad Electrónica: primera capa de defensa que controla el tráfico de red entrante y saliente de un perímetro de seguridad electrónica y entre otras zonas externas.

Responsable de Ciberseguridad: Persona con la autoridad para dirigir la implementación de la guía de ciberseguridad.

Riesgo: Amenaza evaluada en términos de impacto y probabilidad, conforme a la política de riesgos de cada entidad, con el fin de minimizar posibles impactos en la operación confiable (suficiencia y seguridad) del SIN.

Seguridad de la información: Es la preservación de las siguientes características:

- **Confidencialidad**: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.
- **Disponibilidad**: Se garantiza que los usuarios autorizados tengan acceso y puedan usar la información y los recursos relacionados con ella cada vez que se requiera.
- **Integridad**: Se salvaguarda la exactitud y completitud de la información y los métodos de procesamiento.
- **No-repudio:** Se previene la negación de la autoría de una acción que tuvo lugar o reclamar la autoría de una acción que no se llevó a cabo.

2. APLICACIÓN

Los criterios y requisitos establecidos en esta guía son aplicables a las siguientes entidades operativas:

a) Operador del sistema.

b) Generadores.

c) Transportadores.

d) Distribuidores.

3. CUMPLIMIENTO

La entidad responsable deberá revisar, actualizar y conservar toda la documentación de soporte del cumplimiento de las acciones de la guía, basado en el anexo de cumplimiento por un mínimo de tres (3) años calendario.

4. IDENTIFICACIÓN DE ACTIVOS CRÍTICOS.

Este capítulo define un marco de referencia y/o actuación de ciberseguridad para la identificación de ciberactivos críticos que soportan la operación confiable del Sistema Interconectado Nacional.

4.1 Propósito

Identificar y documentar los ciberactivos críticos asociados con los activos críticos que soportan la operación confiable del Sistema Interconectado Nacional. Estos activos críticos deben ser identificados por medio de la aplicación de los elementos dados en el anexo 1 “Criterios de Activos Críticos”.

4.2 Criterios y Requisitos

4.2.1 Activos críticos

Cada entidad responsable identificará y documentará sus activos críticos basada en los criterios del Anexo 1: Criterios de activos críticos.

4.2.2 Ciberactivos críticos

Usando la lista de activos críticos desarrollada según el requisito anterior, cada entidad responsable identificará y documentará sus ciberactivos críticos, esenciales para la operación de los activos críticos. Los ciberactivos críticos son calificados como aquellos que tienen al menos una de las siguientes características:

- El ciberactivo usa un protocolo enrutable para comunicarse afuera del perímetro de seguridad electrónica, o,
- El ciberactivo usa un protocolo enrutable con un centro de control, o,
- El ciberactivo es accesible por marcación.

4.3 Acciones

4.3.1 Activos críticos

Realizar el inventario de activos críticos.

4.3.2 Ciberactivos críticos

Realizar el inventario ciberactivos críticos.

5. GOBIERNO Y GESTIÓN DEL PERSONAL

Este capítulo define un marco de referencia y/o actuación de ciberseguridad para la definición de gobierno, roles y responsabilidades.

5.1 Propósito

Requerir al personal que tiene acceso lógico autorizado o acceso físico no escoltado a ciberactivos críticos, incluyendo contratistas y prestadores de servicios, una evaluación del nivel de riesgo de personal, entrenamiento y sensibilización en seguridad, así como las pautas para la protección de la información.

5.2 Criterios y Requisito

5.2.1 Política y lineamiento de ciberseguridad

La entidad responsable documentará e implementará una política o lineamiento de ciberseguridad que represente el compromiso y la habilidad de la entidad para proteger sus ciberactivos críticos.

5.2.2 Responsable de ciberseguridad

La entidad responsable debe identificar y nombrar un responsable de ciberseguridad.

5.2.3 Evaluación y planes para personal

Esta guía requiere que el personal que tienen acceso lógico autorizado o acceso físico no escoltado a ciberactivos críticos, incluyendo contratistas y prestadores de servicios tengan evaluación de riesgos de personal, cumplan con planes de concientización, capacitación y entrenamiento.

5.2.4 Procedimiento información

La entidad responsable implementará y documentará el procedimiento para identificar, clasificar y proteger la información asociada con los ciberactivos críticos.

5.2.5 Medidas para garantizar información

La entidad responsable debe adoptar medidas que garanticen que la información no pueda ser recuperada sin autorización, cuando se presenten cambios, reutilización, reemplazos, retiros de hardware o software de los ciberactivos críticos.

5.2.6 Procedimiento gestión acceso a la información

La entidad responsable documentará e implementará un procedimiento para gestión de acceso a la información de ciberactivos críticos.

5.2.7 Procedimiento organizacional y técnico de puntos de acceso

Cada entidad responsable implementará y documentará los procedimientos organizacionales y técnicos para todos los puntos de acceso electrónico a los perímetros de seguridad electrónica.

5.3 Acciones

5.3.1 Política y lineamiento de ciberseguridad

Definir una política o lineamiento de ciberseguridad donde se establezcan los compromisos de la empresa y recursos para cumplir con la guía de ciberseguridad y aprobarla al nivel organizacional que garantice su cumplimiento.

5.3.2 Responsable de ciberseguridad

Asignar un Responsable de Ciberseguridad formalmente y notificarlo al CNO, en caso de modificación se debe contemplar:

- Reportar el cambio del responsable con máximo treinta (30) días hábiles de anterioridad al CNO, en caso de desvinculación del responsable, esta se debe notificar en un plazo máximo cinco (5) días hábiles después de la misma, indicando su reemplazo.

En caso de delegación se debe contemplar:

- Implementar y documentar el procedimiento de delegación de la autoridad.
- El responsable de ciberseguridad puede delegar la autoridad para acciones específicas. Esta delegación debe estar documentada, incluyendo el nombre del titular del delegado, las acciones específicas a delegar y la fecha de la delegación; aprobado por el responsable de ciberseguridad y actualizado máximo a treinta (30) días de cualquier cambio de delegación.

5.3.3 Evaluación personal

Cada entidad responsable realizara la evaluación de riesgos del personal propio, externo y la cadena de suministro para otorgar y conservar el acceso físico autorizado y lógico a los ciberactivo críticos.

La evaluación de riesgos del personal debe incluir:

- Confirmar la identidad de las personas.
- Estudio de seguridad incluyendo validación de antecedentes al inicio y con una revisión periódica no superior a cinco (5) años.

5.3.4 Programa de conciencia de seguridad

Toda entidad responsable debe contar con uno o varios programas de conciencia de seguridad, Se debe realizar concientización anual para todos los empleados y terceros que tienen acceso con los ciberactivos críticos.

5.3.5 Programa de entrenamiento y capacitación

Toda entidad debe contar con un programa de entrenamiento y capacitación según el rol desempeñado y su criticidad, este debe contener los siguientes elementos:

- Políticas o lineamiento de ciberseguridad.
- Controles de acceso físico y control de visitantes.
- Controles de acceso electrónicos.
- Manejo de ciberactivos críticos, Información y su almacenamiento.
- Gestión de incidente de ciberseguridad, notificaciones iniciales de acuerdo con el procedimiento de respuesta a incidentes de la entidad y respuesta a incidentes de seguridad.
- Procedimiento de recuperación para ciberactivos críticos.
- Riesgos de ciberseguridad asociados con la interconectividad e interoperabilidad con ciberactivos críticos.

5.3.6 Administración de accesos

Cada entidad responsable deberá implementar actividades de administración de acceso lógico y físico.

5.3.7 Verificación de los registros de autorización

Cada entidad responsable deberá verificar al menos una (1) vez cada semestre calendario que las personas con acceso electrónico activo o acceso físico sin escolta tengan registros de autorización.

5.3.8 Verificación de cuentas y privilegios de acceso

Cada entidad responsable deberá verificar al menos una (1) vez cada año que el acceso electrónico y/o físico para todas las cuentas de usuario, grupos de cuentas de usuario o categorías de roles de usuario, y sus privilegios asociados específicos sean correctos y que sean los que la entidad responsable determine que sean necesarios.

5.3.9 Procedimiento de revocación de accesos

Cada entidad responsable implementará uno o más procedimiento de revocación de acceso documentados los cuales incluyan los siguientes escenarios:

- Un procedimiento en caso de terminación laboral con un bloqueo de cuenta para los accesos físicos y remotos dentro de las veinte cuatro (24) horas de acción de la terminación.
- Un procedimiento de revocación (eliminar o inhabilitar) de cuentas bloqueadas en un tiempo máximo de treinta (30) días calendario posteriores a la acción de terminación.
- Para las acciones de terminación laboral, cambie las contraseñas de las cuentas compartidas conocidas por el usuario dentro de los treinta (30) días calendario posteriores a la acción de terminación.
- Para reasignaciones o transferencias, cambie las contraseñas de cuentas compartidas conocidas por el usuario dentro de los treinta (30) días calendario siguientes a la fecha en que la entidad responsable determine que la persona ya no requiere de ese acceso.
- En caso de un impedimento técnico para el bloqueo o revocación éste deberá documentarse con su respectivo análisis de riesgos y controles compensatorios que los mitiguen.

6. PERÍMETRO

Este capítulo define un marco de referencia para la definición de perímetros.

6.1 Propósito

Identificar y proteger los perímetros de seguridad electrónica dentro de los cuales residen los ciberactivos críticos, al igual que todos los puntos de acceso al perímetro.

6.2 Criterios y Requisitos

6.2.1 Procedimiento gestión de acceso

La entidad responsable documentará e implementará un procedimiento para gestión de acceso a la información protegida de ciberactivos críticos.

6.2.2 Procedimiento control de acceso

Cada entidad responsable implementará y documentará los procedimientos organizacionales y los mecanismos técnicos para el control de acceso en todos los puntos de acceso electrónico al perímetro de seguridad electrónica.

6.2.3 Procedimiento de autenticación, autorización y registro

La entidad responsable establecerá, implementará y documentará los controles técnicos y procedimentales que apliquen para la autenticación de acceso, autorización y registros que permitan la asignación de responsabilidad por toda actividad de los usuarios, y que minimice el riesgo de acceso o uso no autorizado de ciberactivos críticos.

6.3 Acciones

6.3.1 Perímetros de seguridad electrónica

La entidad responsable deberá identificar y documentar perímetros de seguridad electrónica, los puntos y requisitos de acceso a los mismos, asegurando que cada ciberactivo crítico resida dentro de un perímetro de seguridad electrónica.

6.3.2 Listas de acceso

La entidad responsable mantendrá lista(s) del personal con acceso físico no escoltado o acceso lógico a los ciberactivos críticos. Cada entidad responsable revisará la lista de su personal con acceso físico y/o lógico a ciberactivos críticos semestralmente y actualizará la lista en siete (7) días calendario ante cualquier cambio.

6.3.3 Procedimiento de monitoreo y registro de acceso

La entidad responsable implementará y documentará procedimientos para el monitoreo y registro de accesos lógicos permitidos y denegados en puntos de acceso al (los) perímetro(s) de seguridad electrónica veinticuatro (24) horas al día, siete (7) días por semana.

6.3.4 Validación de cambios

Cada entidad responsable deberá asegurar que nuevos ciberactivos y cambios en ciberactivos existentes dentro del perímetro de seguridad electrónica, no afecten adversamente los controles de ciberseguridad existentes.

6.3.5 Procedimiento para habilitar los puntos de acceso

La entidad responsable establecerá, documentará e implementará un procedimiento para garantizar que solamente aquellos puertos y servicios requeridos para las operaciones normales y de emergencia sean habilitados en cada punto de acceso de los perímetros de seguridad electrónica.

6.3.6 Procedimiento para la administración de conexiones temporales

La entidad responsable establecerá, documentará e implementará procedimientos de administración de conexiones temporales dentro del perímetro de seguridad electrónica.

6.3.7 Sistema de control intermedio

La entidad responsable debe implementar un sistema de control intermedio para todas las conexiones remotas interactivas que permita monitorear, cifrar y controlar la autorización con controles de doble factor de autenticación.

7. GESTIÓN DE LA SEGURIDAD DE CIBERACTIVOS CRÍTICOS

Este capítulo define un marco de referencia para la gestión de la seguridad de ciberactivos críticos.

7.1 Propósito

Definir procedimientos e implementación de controles tecnológicos sobre los ciberactivos con el fin te tener un estándar mínimo de gestión de seguridad que permita disminuir el nivel de riesgo y mejorar la resiliencia de cada una de la compañías y homologar los criterios de protección.

7.2 Criterios y Requisitos

7.2.1 Procedimiento de control de cambios y gestión de configuraciones

La entidad responsable establecerá y documentará un procedimiento de control de cambios y gestión de configuraciones para adiciones, modificaciones, reemplazos o retiros de hardware o software de ciberactivos críticos.

7.2.2 Herramientas de prevención

La entidad responsable deberá utilizar herramientas de prevención contra software malicioso (“malware”), donde sea técnicamente factible, para detectar, prevenir, disuadir y mitigar la introducción, exposición y propagación de malware a todos los ciberactivos dentro del (los) perímetro(s) de seguridad electrónica.

7.2.3 Procedimiento de evaluación de vulnerabilidades

La entidad responsable establecerá y documentará un procedimiento de evaluación de vulnerabilidades para garantizar periódicamente la implementación adecuada de los controles de seguridad electrónica en ciberactivos críticos y perímetros de seguridad electrónica.

7.2.4 Procedimiento de control ciberactivos transitorios y medios extraíbles

La entidad responsable establecerá y documentará un procedimiento para control de ciberactivos transitorios y medios extraíbles los cuales son usados temporalmente.

7.2.5 Procedimiento de actualizaciones y parches de seguridad

La entidad responsable deberá implementar y mantener un procedimiento de actualizaciones y parches de seguridad donde sea técnicamente factible.

7.2.6 Procedimiento para identificar y monitorear eventos

La entidad responsable, donde sea técnicamente factible, establecerá un procedimiento para identificar y monitorear eventos del sistema relacionados con ciberactivos.

7.3 Acciones

7.3.1 Procedimiento de control de cambios y gestión de configuraciones

La entidad responsable deberá documentar los cambios y la gestión de la configuración sobre los ciberactivos críticos y la evaluación del riesgo e impacto sobre ciberseguridad, Se deberá asegurar que nuevos ciberactivos y cambios en ciberactivos existentes dentro del perímetro de seguridad electrónica, no afecten adversamente los controles de ciberseguridad existentes.

7.3.2 Herramientas de prevención de malware

La entidad responsable deberá implementar herramientas de prevención de software malicioso donde sea técnicamente posible.

7.3.3 Procedimiento de evaluación de vulnerabilidades

Cada entidad responsable deberá efectuar una evaluación de vulnerabilidad de los ciberactivos y de todos los puntos electrónicos de acceso al (los) perímetro(s) de seguridad electrónica como máximo cada dos (2) años.

La entidad responsable deberá realizar una evaluación de vulnerabilidad antes de adicionar un nuevo ciberactivo al entorno de producción, y también cuando se realicen reemplazos programados de ciberactivos existentes.

La entidad responsable debe documentar el resultado de las evaluaciones de vulnerabilidad realizadas y los planes de acción para remediar o mitigar los hallazgos identificados, incluidas las fechas planificadas para completar cada plan de acción y los estados de ejecución.

7.3.4 Procedimiento de control ciberactivos transitorios y medios extraíbles

Cada entidad responsable deberá tomar medidas para mitigar los riesgos asociados al uso de ciberactivos transitorios y medios extraíbles, con el fin de prevenir el acceso no autorizado a la red e información y la propagación de malware a los ciberactivos existentes.

7.3.5 Procedimiento de actualizaciones y parches de seguridad

La entidad responsable deberá realizar la instalación de actualizaciones y parches de seguridad de manera periódica según el procedimiento definido.

7.3.6 Procedimiento para identificar y monitorear eventos

La entidad responsable se asegurará que todos los ciberactivos dentro del perímetro de seguridad electrónica, donde sea técnicamente factible, cuenten con herramientas automatizadas o controles organizacionales de procedimiento para monitorear eventos del sistema.

8. PLAN DE RECUPERACIÓN DE CIBERACTIVOS CRÍTICOS

Este capítulo define un marco de referencia para la implementación del plan de recuperación de ciberactivos críticos.

8.1 Propósito

Implementar el plan de recuperación para ciberactivos críticos con sus procedimientos asociados que correspondan a las técnicas y prácticas establecidas para la continuidad del negocio.

8.2 Criterios y Requisitos

8.2.1 Plan de recuperación

La entidad responsable debe disponer de un plan con sus procedimientos de recuperación

8.2.2 Pruebas o simulacros

Los procedimientos de recuperación deben probarse mínimo una (1) vez al año. Una prueba o simulacro del procedimiento de recuperación puede comprender desde una prueba de escritorio a un ejercicio operativo completo que simule un incidente real.

Los procedimientos de recuperación deben revisarse, actualizarse y comunicarse para reflejar los cambios, procedimientos de mejoramiento y lecciones aprendidas de la ejecución de los mismos.

8.3 Acciones

8.3.1 Plan de recuperación

La entidad responsable debe tener y revisar con periodicidad anual el plan de recuperación para los ciberactivos críticos, este debe considerar como mínimo:

- Definir los roles y responsabilidades de los recursos asignados.
- Incluir los procedimientos para el respaldo y almacenamiento de la información necesaria para la recuperación efectiva de los ciberactivos críticos.
- Procedimientos de verificación de respaldos que confirmen que estos se realicen de manera satisfactoria y asegurar que la información sea integra y esté disponible.

8.3.2 Documentación de pruebas o simulacros

La entidad responsable debe disponer de registros documentales de las pruebas o simulacros que se realicen periódicamente y las acciones de mejora como resultados de las pruebas.

8.3.3 Registro de cambios del procedimiento de recuperación

La entidad responsable debe disponer de los registros de cambios efectuados a los procedimientos de recuperación, así como, documentación de la divulgación de los mismos. Estos deben reflejarse máximo noventa (90) días después de realizadas las pruebas y/o simulacros.

8.3.4 Respaldos y almacenamiento de información

La entidad responsable debe realizar respaldos y almacenamientos de información necesaria para el restablecimiento de la operación de los ciberactivos críticos.

8.3.5 Pruebas a los respaldos

La entidad responsable debe realizar pruebas funcionales a una muestra significativa de los respaldos realizados.

9. PLAN DE RESPUESTA ANTE INCIDENTES EN CIBERACTIVOS CRÍTICOS

Este capítulo define un marco de referencia para la implementación del plan de respuesta a incidentes de ciberactivos críticos.

9.1 Propósito

Implementar el plan de respuesta a incidentes con sus procedimientos asociados que correspondan a las técnicas y prácticas establecidas.

9.2 Criterios y Requisitos

9.2.1 Plan de respuesta a incidentes

La entidad responsable debe disponer de un plan con sus procedimientos de respuesta a incidentes documentados.

9.2.2 Pruebas o simulacros

Los procedimientos de respuesta a incidentes deben probarse mínimo una (1) vez al año. Una prueba o simulacro del procedimiento de incidentes puede comprender desde una prueba de escritorio a un ejercicio operativo completo que simule un incidente real.

Los procedimientos de respuesta a incidentes deben revisarse, actualizarse y comunicarse para reflejar los cambios, procedimientos de mejoramiento y lecciones aprendidas de la ejecución de los mismos.

9.3 Acciones

9.3.1 Plan de respuesta a incidentes

La entidad responsable debe tener y revisar con periodicidad anual el plan de respuesta a incidentes para los ciberactivos críticos, este debe considerar como mínimo:

- Identificar, clasificar y especificar las acciones y procedimientos requeridos para la gestión oportuna de eventos, evento de seguridad, y alertas derivadas de los mismos o recibidas de los centros de respuesta a incidentes sectoriales o nacionales, así como la respuesta a los incidentes que se identifiquen.
- Las condiciones que podrían activar los planes de escalamiento a nivel interno y externo, las cuales deben ser coherentes con los requerimientos de los centros de respuesta a incidentes sectoriales y nacionales que hayan sido asignados para defender al sector eléctrico, si las hubiere.
- Definir los roles y responsabilidades de los recursos asignados.

- Especificar los recursos tecnológicos que apoyan estas labores para que los eventos de seguridad sean identificados y gestionados oportunamente.

9.3.2 Documentación de pruebas o simulacros

La entidad responsable debe disponer de registros documentales de las pruebas o simulacros que se realicen periódicamente y las acciones de mejora como resultados de las pruebas.

9.3.3 Registro de cambios del procedimiento de respuesta a incidentes

La entidad responsable debe disponer de los registros de cambios efectuados a los procedimientos de respuesta a incidentes, así como, documentación de la divulgación de los mismos. Estos deben reflejarse máximo noventa (90) días después de realizadas las pruebas y/o simulacros.

10. SEGURIDAD FÍSICA DE CIBERACTIVOS CRÍTICOS

Este capítulo define un marco de referencia para la seguridad física de ciberactivos críticos.

10.1 Propósito

Administrar el acceso físico a los ciberactivos del Sistema Interconectado Nacional (SIN) especificando un plan de seguridad física que soporte la protección de los ciberactivos críticos en contra de situaciones que puedan llevar a una mala operación o inestabilidad en el SIN.

10.2 Criterios y Requisitos

10.2.1 Plan de seguridad física

La entidad responsable deberá documentar, implementar y mantener uno o más plan(es) de seguridad física, aprobado por el responsable de seguridad física.

10.2.2 Restricción de acceso físico

La entidad responsable deberá restringir el acceso físico al cableado y otros componentes de comunicación no programables utilizados para la conexión entre activos cibernéticos aplicables dentro del mismo perímetro de seguridad electrónica.

10.2.3 Procedimiento de control de visitantes

Cada entidad responsable implementará uno o más procedimiento de control de visitantes documentados que incluyan los requisitos aplicables al acceso de los visitantes en cada perímetro de seguridad físico.

El responsable de la entidad implementará uno o más procedimientos de mantenimiento y pruebas para garantizar que los sistemas de seguridad física funcionan adecuadamente.

10.3 Acciones

10.3.1 Plan de seguridad física

La entidad responsable tendrá un plan de seguridad física documentando la implementación, revisión y actualización del control, monitoreo, registro, mantenimiento y pruebas del acceso físico y de los sistemas de seguridad asociados. Este plan deberá considerar, como mínimo, lo siguiente:

- Todos los ciberactivos definidos en un perímetro de seguridad electrónico deberán residir dentro de un perímetro de seguridad física. En los casos para los cuales un límite (“6 paredes”) no pueda ser establecido, el responsable de la entidad deberá documentarlo como excepción e implementar medidas alternativas para controlar el acceso físico a dichos ciberactivos.

- Identificar las medidas para controlar el acceso a todos los puntos de acceso físico de cada perímetro de seguridad física.
- Definir los procedimientos y herramientas para monitorear el acceso físico a los perímetros.
- Definir la emisión de alertas o alarmas en respuesta el acceso no autorizado, las cuales deben ser notificadas al personal de respuesta a incidentes de ciberactivos críticos.
- Documentar e implementar las operaciones y procedimientos de control para manejar y registrar el acceso físico a todos los puntos de acceso del perímetro(s) de seguridad física.

10.3.2 Restricción de acceso físico

La entidad responsable deberá restringir el acceso físico al cableado y otros componentes de comunicación no programables utilizados para la conexión entre ciberactivos aplicables dentro del mismo perímetro de seguridad electrónica, en aquellos casos en que dicho cableado y componentes estén ubicados fuera de un perímetro de seguridad física.

En caso de que no se implementen restricciones de acceso físico a dicho cableado y componentes, la entidad responsable deberá documentar e implementar uno o más de los siguientes:

- Encriptación de datos que transitan por los cables y componentes.
- Monitorear el estado del enlace de comunicación compuesto de dicho cableado y componentes y emitir una alarma o alerta en respuesta a fallas de comunicación detectadas al personal identificado en procedimiento de respuesta al incidente de ciberseguridad de ciberactivos críticos dentro de los quince (15) minutos posteriores a la detección.
- Protección lógica igualmente efectiva.

10.3.3 Procedimiento de control de visitantes

La entidad tendrá uno o más procedimientos de control de visitantes.

10.3.4 Procedimiento de mantenimiento y pruebas

La entidad tendrá uno o más procedimientos de mantenimientos y pruebas periódicas del sistema de control relacionados a la seguridad física.

Anexo 1 - Criterios de activos críticos

Los siguientes son considerados activos críticos:

1.1. Cada grupo de unidades de generación en una localización de planta simple con capacidad efectiva neta mayor o igual 20 MW.

1.2. Cada recurso o grupo de recursos de potencia reactiva (excepto generadores) instalados desde el Nivel IV hasta el STN.

1.3. Todas las subestaciones con sus respectivas bahías, en aquellas subestaciones con nivel de tensión IV y superior que a criterio del operador del sistema se consideren.

1.4. Flexible AC Transmisión Systems (FACTS), que, a criterio del operador del sistema, pertenezcan a cortes críticos desde el punto de vista de confiabilidad.

1.5. Esquemas especiales de protección como los esquemas suplementarios, que operan de tal manera que garantizan la confiabilidad del sistema.

1.6. Cada sistema que ejecuta desconexión automática de carga por bajo voltaje o baja frecuencia.

1.7. Cada centro de control o centro de control de respaldo usado para ejecutar las obligaciones funcionales del operador del sistema, Generador, Transmisor o Distribuidor.

1.8. Cualquier activo adicional que soporte la operación confiable de interconexiones internacionales.

1.9. Cualquier activo adicional que soporte la operación confiable del SIN que la entidad responsable estime adecuado incluir en su evaluación.

Consejo Nacional de Operación

Anexo 2 – Lista de cumplimiento periódico de la guía de ciberseguridad

Cap.	#	Acción	Actividad	Periodo de revisión (meses)	SI/NO
IDENTIFICACIÓN DE ACTIVOS CRÍTICOS	4.3	Identificación activos críticos	Aprobar por parte del responsable la lista de activos y ciberactivos críticos	Cada vez que se actualice	
			Certificar que el inventario de activos y ciberactivos críticos esta actualizado (reporte de auditoría)	24	
	4.3.1	Activos críticos	Realizar lista de activos críticos	12	
	4.3.2	Ciberactivos críticos	Realizar lista de ciberactivos críticos	24	
GOBIERNO Y GESTIÓN DEL PERSONAL	5.3.1	Política y lineamiento de ciberseguridad	Documento política o lineamiento de ciberseguridad	Cada vez que se requiera	
	5.3.2	Responsable de ciberseguridad	Documento formal enviado al CNO donde se evidencie la asignación del responsable o de ciberseguridad, y las novedades frente a esta asignación (reportar el cambio de responsable con máximo 30 días hábiles de antelación y por desvinculación en máximo 5 días hábiles)	Cada vez que se actualice	
			Documento procedimiento de delegación de la autoridad	Un (1) mes, cualquier cambio de delegación	
	5.3.3	Evaluación personal	Documento procedimiento de evaluación y confirmación de identidad	24	
			Estudio de seguridad incluyendo validación de antecedentes	Al inicio y antes de 60 meses	
	5.3.4	Programa de conciencia de seguridad	Documento programa de concientización y evidencia que se realizó el plan de concientización	24	
	5.3.5	Programa de entrenamiento y capacitación	Documento programa entrenamiento y capacitación según el rol desempeñado y su criticidad	24	
	5.3.6	Administración de accesos	Documento procedimiento para gestión de accesos lógicos y físicos	24	

	5.3.7	Verificación de los registros de autorización	Evidencias documentales de la verificación periódica	6	
	5.3.8	Verificación de cuentas y privilegios de acceso	Evidencias documentales de la verificación periódica	12	
	5.3.9	Procedimiento de revocación de accesos	Documento procedimiento para revocación de acceso	24	
			Bloqueo (terminación laboral)	24 horas	
			Revocación (eliminar o inhabilitar)	1	
			Cambio de contraseñas (terminación laboral)	1	
			Cambio de contraseñas (reasignaciones o transferencias)	1	
PERÍMETRO	6.3.1	Perímetros de seguridad electrónica	Documento con los perímetros de seguridad y requisitos de accesos	Cada vez que se actualice	
	6.3.2	Listas de acceso	Lista del personal con acceso físico no escoltado o acceso lógico a los ciberactivos críticos	6	
			Evidencia documental de los cambios realizados	7 días	
	6.3.3	Procedimiento de monitoreo y registro de acceso	Documento procedimiento para el monitoreo y registro de accesos físicos y lógicos	Permanente (24/7)	
	6.3.4	Validación de cambios	Documento procedimiento de control de cambios	24	
			Evidencia documental de los cambios realizados	Cada vez que se realice	
	6.3.5	Procedimiento para habilitar los puntos de acceso	Documento de línea base para equipos de punto de acceso al perímetro	24	
	6.3.6	Procedimiento para la administración de conexiones temporales	Documento procedimiento de administración de conexiones temporales	24	
	6.3.7	Sistema de control intermedio	Documento de inventario	24	
			Evidencia de la revisión periódica del control implementado	Cada vez que se realice	
GESTIÓN DE LA SEGURIDAD	7.3.1	Procedimiento de control de cambios y gestión de configuraciones	Documento procedimiento gestión de cambios y gestión de configuración	24	
			Evidencias con los cambios realizados	Cada vez que se realice	
	7.3.2	Herramientas de prevención de malware	Evidencia de implementación de herramientas de prevención de software malicioso	Cada vez que se realice	
	7.3.3		Documento procedimiento de evaluación de vulnerabilidades	24	

		Procedimiento de evaluación de vulnerabilidades	Evidencia de evaluación periódica de vulnerabilidades	Cada vez que se realice	
			Evidencia de vulnerabilidades sobre nuevos activos	Cada vez que se realice	
			Plan de acción del resultado de análisis de vulnerabilidad	24	
	7.3.4	Procedimiento de control ciberactivos transitorios y medios extraíbles	Documento procedimiento control transitorio y medios extraíbles	24	
			Evidencias de control periódico	Cada vez que se realice	
	7.3.5	Procedimiento de actualizaciones y parches de seguridad	Documento procedimiento de actualización e implementación de parches	24	
			Evidencias de los ciclos de parchado	Cada vez que se realice	
	7.3.6	Procedimiento para identificar y monitorear eventos	Documento procedimiento de monitoreo	24	
			Evidencia de controles implementados	Cada vez que se realice	
PLAN DE RECUPERACIÓN	8.3.1	Plan de recuperación	Documento plan de recuperación y los procedimientos asociados	12	
	8.3.2	Plan de pruebas o simulacros	Evidencia de pruebas o simulacros, y acciones de mejora de estos	12	
	8.3.3	Registro de cambios del procedimiento de recuperación	Evidencia de los cambios realizados a los procedimientos	3	
	8.3.4	Respaldos y almacenamiento de información	Evidencia documentada de los respaldos realizados y almacenamiento de la información	Cada vez que se realice	
	8.3.5	Registro de pruebas a los respaldos	Evidencia documentada de que se realizan pruebas de respaldo y su resultado	Cada vez que se realice	
PLAN DE RESPUESTA ANTE INCIDENTES	9.3.1	Plan de respuesta ante incidentes	Documento con el plan de respuesta ante incidentes y los procedimientos asociados	12	
	9.3.2	Plan de pruebas o simulacros	Evidencia de pruebas o simulacros, y acciones de mejora de estos	12	
	9.3.3	Registro de cambios del procedimiento respuesta a incidentes	Evidencia de los cambios realizados a los procedimientos	3	
SEGURIDAD FÍSICA DE CIBERACTIVOS CRÍTICOS	10.3.1	Plan de seguridad física	Documento plan de seguridad física cumpliendo los requisitos	24	
	10.3.2	Restricción de acceso físico	Evidencia de los controles implementados para protección física del cableado y otros componentes de comunicación	Cada vez que se realice	
			Alarma o alerta en respuesta a fallas de comunicación detectadas	15 minutos	
	10.3.3	Procedimiento de control de visitantes	Documento procedimiento control de visitantes	24	
	10.3.4	Procedimiento de mantenimiento y pruebas	Documento procedimiento de mantenimiento y pruebas periódicas a los sistemas de control relacionados a la seguridad física	24	

			Evidencia mantenimiento y pruebas periódicas	Cada vez que se realice	

Consejo Nacional de Operación

AGRADECIMIENTOS

El Consejo Nacional de Operación hace un reconocimiento especial al Comité Tecnológico y a la Comisión Temporal de Ciberseguridad del CNO por su gestión y coordinación para la realización de las sesiones de trabajo, contribuyendo con ello al fortalecimiento de la Ciberseguridad y Ciberseguridad Nacional. Así como, a las organizaciones CELSIA-EPSA, ENEL-CODENSA, COLOMBIA INTELIGENTE, ELECTRICARIBE, EPM, GEB, INTERCOLOMBIA, INTERNEXA, ISAGEN, TERMOCANDELARIA y XM, por aportar su equipo de líderes para la construcción, análisis y discusión de la presente guía.