Revisión	Fecha	Descripción
0	10-12-2018	Versión para Comité Tecnológico
1	14-02-209	Versión actualizada según comentarios con anexo para comité. Se complementa introducción, revisiones generales y nuevo anexo de cumplimiento.
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.
3	29-07-2019	Versión con respuesta a solicitudes y comentarios. Cambios asociados a las solicitudes y comentarios.
4	28-08-2019	Versión con inclusión de comentarios faltantes. Se agrega capítulo de cadena de suministros y se explicita la resiliencia.
5	9-09-2020	Versión con actualización de plazos y aclaraciones. Se actualizan las fechas contadas a partir de la fecha de expedición del Acuerdo 1241.
6	13-10-2021	Actualización de las fechas de algunas actividades de la Guía de Ciberseguridad
7	1-12-2021	Modificación del numeral 4.3 del Anexo 2 de la Guía de Ciberseguridad se modifica el artículo 8 se incluyó el plazo de cumplimiento de la Guía de Ciberseguridad de los agentes nuevos y de los agentes existentes con nuevos activos, y se amplían los plazos de las siguientes actividades a partir del 3 de octubre de 2019, fecha de expedición del Acuerdo 1241.
8	3-11-2025	Se recomendó actualizar la Guía de Ciberseguridad y algunos plazos.

Contenido

1. CIBERSEGURIDAD

El Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética del Sector Electricidad Colombiano establece los lineamientos que deben adoptar los diversos agentes del sector eléctrico y los operadores de infraestructuras críticas con el propósito de coordinar acciones eficientes e integrales para prevenir y mitigar potenciales amenazas cibernéticas que puedan comprometer la disponibilidad y continuidad del servicio de energía eléctrica.

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 globalizado y convergente en tecnología IP, es necesario mitigar y adaptarse a los riesgos asociados a la seguridad de la operación mediante reglas y normas que determinen las buenas prácticas, las cuales son actualmente, de aplicación permanente en gran parte del mundo.

1.1. Introducción y Antecedentes

Casos como los apagones registrados en Ucrania en 2015, 2016, 2022 y 2024 producidos por ciberataques, así como los ataques a infraestructuras eléctricas del Reino Unido, Irlanda, Estados Unidos, Israel, India, entre otros han demostrado que los ataques cibernéticos a estas infraestructuras son una parte activa del panorama de riesgos actual y futuro. Conscientes de su rol en la sociedad colombiana y de que el sector eléctrico se ha venido modernizando con tecnologías de operación 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 basados en las Normas NERC-CIP v4, luego formalizada mediante la adopción por el Acuerdo 788 de 2015, todo ello 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 mínimas que deben establecer los agentes del Sector Eléctrico Colombiano para prepararse, detectar, contener, responder, coordinar la reacción y la recuperación. Así como la identificación de las lecciones aprendidas y las mejores prácticas para la gestión de los incidentes cibernéticos que puedan afectar al Sistema Interconectado Nacional. El objetivo es consolidar un nivel de madurez adecuado en las capacidades de ciberseguridad y ciberdefensa del sector, contribuyendo a la operación confiable, segura y resiliente de este.

En ese contexto, el sector eléctrico necesita implementar normativas asociadas con la ciberseguridad y apropiarse del conocimiento en este ámbito 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 estos estándares, se seleccionaron y adaptaron aspectos aplicables al caso colombiano que fueron revisados por expertos de diferentes empresas del sector asignados al Comité de Ciberseguridad del CNO.

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

CIP-002-5.1a Categorización de ciberactivos críticos
CIP-003-9 Gestión de controles de seguridad
CIP-004-7 Personal y entrenamiento
CIP-005-7 Perímetro(s) de seguridad electrónica
CIP-006-6 Seguridad física de ciberactivos críticos
CIP-007-6 Gestión de seguridad del sistema
CIP-008-6 Reporte de incidentes planes de respuesta
CIP-009-6 Planes de recuperación de ciberactivos críticos
CIP-010-4 Gestión de la configuración, cambios y evaluación de vulnerabilidades
CIP-011-3 Protección de la información
CIP-012-1 Comunicación entre centros de control
CIP-013-2 Ciberseguridad cadena de suministro
CIP-014-3 Seguridad física

Asimismo, los agentes tendrán la libertad de usar diferentes marcos de referencia (ISO, IEC, IEEE, NIST, ENISA, otros) para la elaboración de los procedimientos de acuerdo con los criterios definidos por sus equipos de ciberseguridad, siempre que el resultado cumpla con los requerimientos de la guía y sus anexos.

En este sentido, 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. Es necesario, identificar los activos críticos, los ciberactivos críticos, los perímetros de seguridad lógica y seguridad física, y aplicar los criterios establecidos en esta guía, la cual deberá ser revisada por lo menos cada dos años para mantener su vigencia y actualización.

1.2. Glosario

A continuación, se describen las definiciones de los principales conceptos asociados a la gestión de la ciberseguridad.

Acceso remoto: Acceso iniciado por el usuario empleando un software cliente u otra tecnología que utilice protocolos enrutables para obtener acceso remoto. El acceso remoto se origina desde un Ciberactivo que no es un Sistema intermedio y no está ubicado dentro del perímetro de seguridad de los Sistemas lógicos en el agente del SIN o entidades operativas del sector eléctrico. El acceso remoto puede ser iniciado a partir de:

- Ciberactivos utilizados o propiedad de la Entidad Responsable,
- Ciberactivos utilizados o propiedad de empleados, y
- Ciberactivos utilizados o propiedad de proveedores, contratistas o consultores. El acceso remoto interactivo no incluye el proceso de sistema a sistema.

Activo crítico: Instalaciones con sistemas o equipos eléctricos que, si son destruidos, degradados o puestos fuera de servicio, afectarían la confiabilidad (suficiencia y seguridad), operatividad, o comprometerían la seguridad de la operación del SIN, según lo establecido en el Anexo "Criterios de activos críticos" **(Anexo 2)** de este Acuerdo.

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

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

Ciberespacio: Dominio global dentro del entorno de la información conformado por redes interdependientes de infraestructuras de sistemas de información que incluyen: internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores integrados.

Ciberseguridad: Es la práctica para la prevención de daños, uso no autorizado, explotación y, si es necesario, la restauración de los sistemas electrónicos de información, comunicaciones, y la información que contienen, con el fin de fortalecer la confidencialidad, integridad y disponibilidad de estos sistemas.

Control compensatorio: Un control de gestión, operativo y/o técnico (salvaguarda o contramedida) empleado por una organización como reemplazo o complemento de otro control de seguridad recomendado y que proporciona una protección equivalente o comparable.

Entidad Responsable: Hace referencia a los agentes generadores, transmisores, distribuidores y el operador del Sistema Interconectado Nacional responsables de activos y ciberactivos críticos que deben dar cumplimiento al 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).

Gestión de vulnerabilidades: Capacidad del monitoreo continuo de la ciberseguridad por la cual se identifican vulnerabilidades (vulnerabilidades y exposiciones comunes - CVE) en dispositivos que podrían ser explotados por atacantes, para comprometer un dispositivo y usarlo como una plataforma desde la cual extender el compromiso a la red.

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

Medios extraíbles: Medios de almacenamiento que:

1) No son ciberactivos,
2) Son capaces de transferir código ejecutable,
3) Pueden usarse para almacenar, copiar, mover o acceder a datos, y
4) Están conectados directamente a:
   - Ciberactivos críticos,
   - La red dentro de un Perímetro de Seguridad lógica de los ciberactivos críticos o
   - Ciberactivos protegidos asociados a los ciberactivos críticos.

Ejemplos de medios extraíbles incluyen, entre otros, disquetes, discos compactos, unidades flash USB, discos duros externos y otras tarjetas/unidades de memoria flash.

Perímetro de Seguridad lógica: Es la frontera lógica, que rodea, aísla y protege la red donde se conectan los ciberactivos críticos de las conexiones de otras redes.

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.

Plantas menores: Plantas de generación de energía con capacidad mayor a 5MW y menor a 20 MW. Para efectos del cumplimiento del presente acuerdo, se tendrá en cuenta la definición “Generación con plantas menores” del artículo 1 Definiciones de la resolución CREG 086 de 1996[1] o aquella que la modifique o sustituya.

Procedimiento operativo: Un documento que identifica los pasos generales para lograr una meta operativa genérica. Un proceso operativo incluye pasos con opciones que pueden seleccionarse dependiendo de las condiciones en tiempo real (por ejemplo, una guía para controlar el alto voltaje se puede considerar como un proceso operativo).

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

Perímetro de Seguridad lógica: Es la frontera lógica, que rodea, aísla y protege la red donde se conectan los ciberactivos críticos de las conexiones de otras redes.

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 características descritas a continuación.

- **Confidencialidad**: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.

[1] https://gestornormativo.creg.gov.co/gestor/entorno/docs/resolucion_creg_0086_1996.htm

- **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.

Sistema de control intermedio: Un Ciberactivo o grupo de ciberactivos que realizan control de acceso para restringir las actividades de Acceso remoto solo a usuarios autorizados. El Sistema Intermedio no debe ubicarse dentro el Perímetro de Seguridad lógica.

2. ÁMBITO DE APLICACIÓN

Los criterios y requisitos establecidos en esta guía son aplicables a los siguientes agentes prestadores del servicio público de energía eléctrica y al operador del Sistema Interconectado Nacional, que cumplen con el Anexo "Criterios de activos críticos" (**Anexo 2)**.

a) Operador del sistema.
b) Generadores.
c) Transportadores.
d) Distribuidores.

Para efecto de este documento, se entiende que las anteriores empresas de servicios públicos domiciliarios son entidades responsables.

En el Anexo "Lista de cumplimiento" **(Anexo 3)** del presente Acuerdo, se indican los numerales de esta Guía con los requisitos mínimos de ciberseguridad que aplican a los agentes generadores con plantas menores.

3. CUMPLIMIENTO

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

Todo nuevo ciberactivo crítico deberá considerar la implementación de todos los aspectos de ciberseguridad solicitados en esta Guía. Para los ciberactivos críticos existentes, donde técnicamente no sea factible implementar algún control, esto deberá estar debidamente documentado. Además, deberán documentarse e implementarse controles compensatorios y de monitoreo, que disminuyan el riesgo de explotación de las vulnerabilidades, e incluirlo en el plan de modernización, si aplica.

3.1. Auditorías

Cada entidad responsable debe contar con un programa de auditoría que incluya la verificación de los requisitos previstos en esta guía. La auditoría debe realizarse cada 2 años.

Cada entidad responsable debe revisar, actualizar y conservar toda la documentación de soporte del cumplimiento de las acciones de la guía, basándose en el Anexo "Lista de cumplimiento" **(Anexo 3)** Lista de cumplimiento, por un mínimo de tres (3) años calendario.

4. IDENTIFICACIÓN DE ACTIVOS CRÍTICOS

En este numeral se define un marco de referencia y actuación en ciberseguridad para la identificación de ciberactivos críticos que soportan la operación confiable del Sistema Interconectado Nacional.

Su propósito es identificar y documentar los ciberactivos críticos asociados con los activos críticos que garantizan la operación confiable del Sistema Interconectado Nacional. Estos activos críticos deben ser identificados mediante la aplicación de los elementos establecidos en el Anexo "Criterios de Activos Críticos" **(Anexo 2).**

4.1. Activos críticos

Cada entidad responsable debe identificar, documentar e inventariar sus activos críticos basada en los criterios del Anexo "Criterios de activos críticos" **(Anexo 2).**

4.2. 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 usan un protocolo enrutable o de comunicación para comunicarse afuera o dentro del perímetro de seguridad lógica.

La información del inventario de ciberactivos críticos debe contener la información que permita la identificación del ciberactivo de manera única en la red y el activo crítico al que pertenece.

5. GOBIERNO Y GESTIÓN DEL PERSONAL

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

Tiene como propósito requerir al personal que tiene acceso lógico o acceso físico no escoltado a ciberactivos críticos, una evaluación del nivel de riesgo de personal, entrenamiento y sensibilización en seguridad, así como las pautas para la protección de la información.

5.1. Política y lineamiento de ciberseguridad

La entidad responsable debe definir y documentar una política o lineamiento de ciberseguridad que establezca los compromisos de la empresa y la asignación de recursos para cumplir con la guía de ciberseguridad. Esta política debe ser aprobada a nivel organizacional para garantizar su cumplimiento.

5.2. Responsable de ciberseguridad

La entidad responsable debe identificar y nombrar un responsable de ciberseguridad y notificarlo al CNO, mediante comunicación escrita dirigida al correo **info@cno.org.co**. En caso de modificación, el cambio del responsable debe ser reportado en un plazo máximo de veinte (20) días calendario.

5.3. Evaluación de riesgos para el personal

Cada entidad responsable debe realizar la evaluación de riesgos del personal que tendrá acceso lógico o físico a los ciberactivos críticos. La evaluación de riesgos del personal debe incluir al menos alguno de las siguientes revisiones:

- Confirmar la identidad de las personas.
- Estudio de seguridad de acuerdo con la normativa de cada agente.
- Estudio de riesgos incluyendo validación de antecedentes.

En el caso de personal de proveedores y contratistas, se deberá solicitar la certificación de la realización de esta evaluación de riesgos.

5.4. Programa de conciencia y entrenamiento en ciberseguridad

Toda entidad responsable debe contar con un programa de concienciación y entrenamiento que mitigue los riesgos que puedan impactar al SIN, con alcance al personal de la entidad que tenga acceso a los activos críticos y ciber activos críticos, según los criterios definidos en la política de seguridad de cada entidad y al presente acuerdo de ciberseguridad. Este programa debe abarcar al menos los siguientes temas:

- Políticas, guías o procedimientos de ciberseguridad.
- Tratamiento de riesgos que puedan afectar al SIN.
- Controles de ciberseguridad implementados.
- Roles y responsabilidades.

5.5. Administración de accesos

La entidad responsable debe documentar e implementar un procedimiento para gestión de acceso lógico y físico a la información de ciberactivos críticos.

Todas las conexiones remotas deben de tener mecanismos que permitan el doble factor de autenticación, el monitoreo, el cifrado y controlar la autorización.

5.6. Verificación de registros de autorización

Cada entidad responsable deberá verificar al menos una (1) vez cada año el nivel de acceso a todas las cuentas de usuario, grupos de cuentas de usuario o categorías de roles de usuario, y sus privilegios asociados específicos.

5.7. Verificación de cuentas y privilegios de acceso

Cada entidad responsable deber verificar al menos una (1) vez cada año que el acceso lógico 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.

5.8. Procedimiento de revocación de accesos

Cada entidad responsable debe implementar uno o más procedimientos 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 cambio de roles, reasignaciones o transferencias, se debe cambiar 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 de las cuentas compartidas deberá documentarse con su respectivo análisis de riesgos y controles compensatorios que los mitiguen.

6. PERÍMETRO

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

Tiene como propósito identificar y proteger los perímetros de seguridad lógica dentro de los cuales residen los ciberactivos críticos, al igual que todos los puntos de acceso al perímetro.

6.1. Perímetros de seguridad lógica

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

6.2. Listas de acceso

La entidad responsable mantendrá actualizada la (s) lista(s) del personal con acceso lógico a los ciberactivos críticos. Cada entidad responsable revisará la lista de su personal con acceso lógico a ciberactivos críticos al menos cada seis meses.

6.3. 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 físico y lógico veinticuatro (24) horas al día, siete (7) días por semana.

6.4. Validación de cambios

Cada entidad responsable deberá asegurar que nuevos ciberactivos críticos y cambios en ciberactivos críticos existentes dentro del perímetro de seguridad lógica, no afecten adversamente los controles de ciberseguridad existentes, esto debe incluir la aprobación de cambio por el responsable de ciberseguridad o su delegado.

6.5. Procedimiento para habilitar los puntos de acceso

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

6.6. 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 lógica.

6.7. Sistema de control intermedio

La entidad responsable debe implementar un sistema de control intermedio para restringir el acceso remoto hacia los ciberactivos críticos.

7. GESTIÓN DE LA SEGURIDAD DE CIBERACTIVOS CRÍTICOS

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

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

7.1. Procedimiento de control de cambios y gestión de configuraciones

La entidad responsable debe establecer y documentar el (los) procedimiento(s) de control de cambios y gestión de configuraciones para adiciones, modificaciones, reemplazos o retiros de hardware o software de ciberactivos críticos.

La entidad responsable debe 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 críticos y cambios en ciberactivos críticos existentes dentro del perímetro de seguridad lógica, no afecten adversamente los controles de ciberseguridad existentes.

7.2. Herramientas de prevención de programas malignos “malware”

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

Donde no sea técnicamente factible se deben implementar controles compensatorios que mitiguen el riesgo.

7.3. Procedimiento de evaluación de vulnerabilidades

Cada entidad responsable debe establecer, documentar y realizar una evaluación de vulnerabilidades técnicas de los ciberactivos críticos y de todos los puntos de acceso al (los) perímetro(s) de seguridad lógica como máximo cada dos (2) años. La entidad responsable deberá realizar una evaluación de vulnerabilidad antes de adicionar un nuevo ciberactivo crítico al entorno de producción, y también cuando se realicen reemplazos programados de ciberactivos críticos 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.

Donde el escaneo de vulnerabilidades no se pueda realizar se deben implementar controles compensatorios que mitiguen el riesgo.

7.4. Procedimiento de control ciberactivos críticos transitorios y medios extraíbles

La entidad responsable debe establecer y documentar un procedimiento para control de ciberactivos críticos transitorios y medios extraíbles, los cuales son usados temporalmente.

Así mismo, debe tomar medidas para mitigar los riesgos asociados al uso de ciberactivos críticos 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 críticos existentes.

7.5. Procedimiento de actualizaciones y parches de seguridad

La entidad responsable debe documentar e implementar procedimientos de actualizaciones y parches. Así mismo La entidad responsable debe realizar la instalación de actualizaciones y parches de seguridad de manera periódica según el procedimiento definido. Donde no sea técnicamente factible la actualización o instalación del parche, se deben implementar controles compensatorios para mitigar el riesgo.

7.6. Procedimiento para identificar y monitorear eventos

La entidad responsable debe establecer procedimientos para identificar y monitorear eventos del sistema, así mismo se asegurará que todos los ciberactivos críticos dentro del perímetro de seguridad lógica, donde sea técnicamente factible, cuenten con herramientas tecnológicas o controles organizacionales de procedimiento para monitorear eventos del sistema.

8. PLAN DE RECUPERACIÓN DE CIBERACTIVOS CRÍTICOS

Este numeral define un marco de referencia para la implementación del plan de recuperación que este enfocado en la resiliencia del servicio prestado soportado por los ciberactivos críticos. Tiene como propósito Implementar el plan de recuperación y resiliencia para ciberactivos críticos con sus procedimientos asociados que correspondan a las técnicas y prácticas establecidas para la continuidad del negocio.

8.1. Plan de recuperación y resiliencia

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.
- Procedimientos de contingencia y continuidad que faciliten la resiliencia del proceso.
- Documentación de lecciones aprendidas y planes de acción.

8.2. Ejecución y documentación de pruebas o simulacros

La entidad responsable debe probar los procedimientos de recuperación 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 de ciberseguridad probable. Los procedimientos de resiliencia y recuperación deben revisarse, actualizarse y comunicarse para reflejar los cambios, procedimientos de mejoramiento y lecciones aprendidas de la ejecución de estos.

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. Registro de cambios del procedimiento de recuperación y resiliencia

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

8.4. 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.

8.5. Pruebas a los respaldos y mecanismos de contingencia y continuidad

La entidad responsable debe realizar pruebas funcionales a una muestra significativa de los respaldos realizados y de los mecanismos de contingencia y continuidad establecidos para el ciberactivo crítico.

9. PLAN DE RESPUESTA ANTE INCIDENTES EN CIBERACTIVOS CRÍTICOS

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

Tiene como propósito implementar el plan de respuesta a incidentes con sus procedimientos asociados que correspondan a las técnicas y prácticas establecidas.

9.1. Plan de respuesta a incidentes de ciberseguridad

La entidad responsable debe establecer, mantener y revisar como mínimo de manera anual un plan o planes de respuesta a incidentes, que puedan afectar la prestación de los servicios de los activos críticos, este debe considerar como mínimo, lo siguiente:

- El establecimiento y aplicación de las acciones de gestión (identificación, análisis, detección, contención, erradicación y recuperación) requeridas para la gestión oportuna de eventos que amenacen la operación del servicio (Disponibilidad, integridad y confidencialidad) de los activos críticos desde la perspectiva de ciberseguridad.
- La evaluación y clasificación de los incidentes.
- Identificación de Riesgos y escenarios probables de incidente de ciberseguridad.
- Fecha vigencia del plan.
- Roles y responsabilidades de la implementación, ejecución y mantenimiento del(los) plan(es).
- La documentación y gestión de las lecciones aprendidas.

9.2. Simulacros o pruebas a los planes de respuesta a incidentes de ciberseguridad

El (los) plan(es) 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 de ciberseguridad probable.
- Dejar registros documentales de las pruebas. Los ejercicios podrán ser realizados por cada entidad, en conjunto con otras entidades, con el operador del sistema o con participación de entidades de apoyo nacional.

9.3. Mantenimientos de los planes de respuesta a incidentes de ciberseguridad

El (los) plan(es) de respuesta a incidentes deben:

- Revisarse, actualizarse y comunicarse a sus interesados para reflejar los cambios, mejoras y lecciones aprendidas a las que haya lugar, mínimo una (1) vez al año.
- Mantener registros de cambios efectuados a la documentación del (los) Plan (es) de respuesta a incidentes de ciberseguridad, así como, documentación de la divulgación de estos a las partes interesadas.
- Los cambios a partir de los ejercicios deben reflejarse máximo noventa (90) días después de realizadas las pruebas y/o simulacros.

10. SEGURIDAD FÍSICA DE CIBERACTIVOS CRÍTICOS

Este numeral define un marco de referencia para la seguridad física de ciberactivos críticos, el cual tiene como propósito administrar el acceso físico a los ciberactivos críticos del Sistema Interconectado Nacional especificando un plan de seguridad física que soporte la protección de estos ciberactivos en contra de situaciones que puedan llevar a una situación que comprometa la operación segura y confiable del Sistema.

10.1. Plan de seguridad física

La entidad responsable debe tener 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 críticos definidos en un perímetro de seguridad lógica 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 críticos.

  Para los demás ciberactivos, deben residir dentro de un perímetro de seguridad física protegido.
- Identificar las medidas para controlar el acceso a todos los puntos de acceso físico de cada perímetro de seguridad física incluyendo, pero sin limitarse a, Tarjetas de control de acceso, controles de acceso biométricos, CCTV entre otros.
- Identificar activos y ciberactivos de terceros y otras compañías del sector que se encuentran en las instalaciones, así mismo, definir mecanismos de cooperación para identificar eventos sobre estos activos.
- Definir los procedimientos y herramientas para monitorear el acceso físico a los perímetros.
- Definir la emisión de alertas o alarmas en respuesta al 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.

10.2. Restricción de acceso físico

La entidad responsable debe restringir el acceso físico al cableado y otros componentes de comunicación no programables, utilizados para la conexión entre ciberactivos críticos.

Los componentes que estén ubicados fuera de un perímetro de seguridad física, que no implementen restricciones de acceso físico a dicho cableado y componentes, la entidad responsable deberá documentar e implementar uno o más de los siguientes controles compensatorios:

- Cifrado de datos que transitan por los medios de transmisión y componentes.
- Monitorear la disponibilidad 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.
- Protección lógica igualmente efectiva.

10.3. Procedimiento de control de visitantes

Cada entidad responsable debe definir, implementar y mantener un procedimiento de control de visitantes que incluyan los requisitos aplicables a cada perímetro de seguridad físico.

10.4. Procedimiento de mantenimiento y pruebas

El responsable de la entidad debe definir, implementar y mantener procedimiento de mantenimiento y pruebas, para garantizar que los sistemas de seguridad física funcionan adecuadamente.

11. GESTIÓN DE LA CADENA DE SUMINISTRO

Este numeral define un marco de referencia para la gestión de riesgos de la cadena de suministro.

Tiene como propósito mitigar los riesgos de ciberseguridad de la operación confiable de los ciber activos críticos, mediante la implementación de controles de seguridad para la gestión de riesgos de la cadena de suministro.

11.1. Plan de Gestión de riesgo de la cadena de suministro

La entidad responsable debe documentar, implementar y mantener un procedimiento de gestión de riesgos de la cadena de suministro para los contratistas y proveedores que suministren ciber activos críticos, o que requieran acceso a los ciber activos críticos, aprobado por el responsable de ciberseguridad y actualizado máximo cada veinticuatro (24) meses.

11.2. Plan de conciencia y entrenamiento en ciberseguridad de la cadena de suministro

La entidad responsable debe solicitar a sus proveedores y contratistas, que desarrollen un plan anual de conciencia y entrenamiento para sus empleados que tengan acceso a ciberactivos críticos.

12. GESTIÓN DE RIESGOS DE CIBERSEGURIDAD EN ACTIVOS CRÍTICOS

Este numeral define un marco de referencia para la gestión de riesgos en activos críticos.

Tiene como propósito establecer un marco sistemático para identificar, evaluar, tratar y monitorear los riesgos asociados con los activos críticos, ciberactivos críticos. Este proceso busca mejorar la resiliencia y la seguridad de la infraestructura crítica del sector eléctrico, permitiendo a las entidades responsables tomar decisiones informadas y proactivas para proteger sus activos contra ciber amenazas.

12.1. Evaluación de riesgos

Cada entidad responsable debe implementar y documentar un proceso de evaluación de riesgos que cubra los activos críticos y ciberactivos críticos inventariados. Este proceso debe:

- Identificar las amenazas potenciales y vulnerabilidades asociadas a los activos críticos, ciberactivos críticos y ciberactivos.
- Evaluar el impacto potencial de estas amenazas y vulnerabilidades en la operación segura y confiable.
- Determinar el nivel de riesgo asociado a cada amenaza y vulnerabilidad identificada.

12.2. Plan de tratamiento de riesgos

Con base en los resultados de la evaluación de riesgos, cada entidad responsable debe desarrollar e implementar un plan de tratamiento de riesgos que incluya:

- Medidas de mitigación para los riesgos identificados, priorizando aquellos de mayor impacto y probabilidad.
- Cronograma para la implementación de las medidas de mitigación.
- Asignación de responsabilidades para la ejecución de las medidas de mitigación.

12.3. Monitoreo y revisión

Cada entidad responsable debe:

- Monitorear continuamente la efectividad de las medidas de mitigación implementadas. Actualizando la evaluación de riesgos y el plan de tratamiento al menos una vez cada doce (12) meses o cuando se produzcan cambios significativos en el entorno de riesgo.
- Mantener registros de todas las actividades de gestión de riesgos.

Nota: En caso de no haber viabilidad de la implementación de alguno de controles de esta guía se deberá optar por la implementación de controles compensatorios