CONSEJO NACIONAL DE OPERACIÓN
CNO

ACUERDO No. 788
Septiembre 3 de 2015

Por el cual se aprueba la Guía de Ciberseguridad

El Consejo Nacional de Operación en uso de sus facultades legales, en especial las conferidas en el Artículo 36 de la Ley 143 de 1994, el Anexo general de la Resolución CREG 025 de 1995 y su Reglamento Interno y según lo definido en la reunión No. 441 del 3 de septiembre de 2015, y

CONSIDERANDO

1. Que el documento CONPES 3701 del 14 de Julio de 2011 establece los lineamientos de política para la ciberseguridad y ciberdefensa, orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que puedan afectar significativamente al país.

2. Que el documento CONPES 3701, implica un compromiso del Gobierno Nacional por garantizar la seguridad de la información y busca sentar las bases de política para los tópicos de ciberseguridad y ciberdefensa, y las entidades públicas y privadas involucradas tendrán la responsabilidad de desarrollar estas bases y generar mecanismos que permitan garantizar la seguridad de la información a nivel nacional, teniendo en cuenta las normas técnicas y los estándares nacionales e internacionales, así como iniciativas internacionales sobre protección de infraestructura crítica y ciberseguridad.

3. Que el Grupo Tecnológico, hoy Comité Tecnológico del Consejo Nacional de Operación realizó un estudio de las normas aplicables a la industria eléctrica para mitigar los riesgos de ciberseguridad en el sector y en el Sistema Interconectado Nacional y concluyó que la mejor referencia de aplicación, es la Norma NERC CIP para tecnologías de activos críticos y con base en esta norma, se elaboró la guía de Ciberseguridad orientada a la protección de los activos del SIN.

4. Que en septiembre de 2011 el CNO envió a los agentes del sector eléctrico un cuestionario cuyo objetivo fue la realización del levantamiento de información que permita identificar los activos críticos, los riesgos y vulnerabilidades y el nivel de gestión de ciberseguridad en la operación de las empresas del sector eléctrico.

5. Que teniendo en cuenta los resultados de la encuesta se elaboró un diagnóstico, se formularon las recomendaciones generales de Ciberseguridad y una hoja de ruta para la implementación de Ciberseguridad por parte de los agentes del SIN.

6. Que el Comité Tecnológico en la reunión 34 del 8 de julio de 2015 recomendó la expedición del presente Acuerdo.

ACUERDA:

PRIMERO: Se aprueba la Guía de Ciberseguridad que se encuentra en el Anexo del presente Acuerdo, el cual hace parte integral del mismo.

SEGUNDO: En un plazo máximo de (6) seis meses contados a partir de la fecha de expedición del presente Acuerdo los agentes generadores, transmisores y distribuidores del Sistema Interconectado Nacional deberán designar la persona responsable de dirigir y administrar la implementación de la Guía de Ciberseguridad.

TERCERO: El CNO definirá y estructurará un plan de trabajo que incluya actividades de sensibilización, comunicación, entrenamiento y socialización de la Guía de Ciberseguridad del CNO y de los procesos de seguridad cibernética que incluyan como mínimo aspectos como:

- Identificación y documentación de la situación actual.
- Establecimiento de procesos
- Diseño de arquitecturas detalladas
- Definición e implantación de controles mínimos legales, técnicos, organizativos y físicos
- Implementación de un ciclo de mejora permanente del proceso.

CUARTO: El operador del Sistema y los agentes generadores, transmisores y distribuidores del Sistema Interconectado Nacional, deben realizar la identificación de los activos críticos y ciber activos críticos, los riesgos y vulnerabilidades y el nivel de gestión de ciberseguridad en la operación de sus empresas en un plazo máximo de (1) un año contado a partir de la fecha de expedición del presente Acuerdo.

QUINTO: El presente Acuerdo rige a partir de la fecha de su expedición.

Presidente,

DIANA M. JIMÉNEZ RODRÍGUEZ

Secretario Técnico,

ALBERTO OLARTE AGUIRRE

Consejo Nacional de Operación

CONSEJO NACIONAL DE OPERACIÓN – C N O

CIBERSEGURIDAD

Historia

Versión	Fecha	Tipo de Emisión	Cambios
0	21.10.2010	Preliminar para revisión	
1	03.11.2010	Versión para C N O	
2	17.05.2011	Versión para C N O revisada con versión 4 de CIP	
3	20.06.2011	Versión con comentarios de reunión del Grupo Tecnológico	Se cambia Norma por Guía
4	14.08.2011	Versión con revisión del anexo 1 revisado por SEE.	
5	23.08.2011	Versión con comentarios de ISAGEN	
6	06 06 2013	Version con comentarios expertos de las empresas	

TABLA DE CONTENIDO

CIBERSEGURIDAD

Introducción y antecedentes

Ante la inminente modernización tecnológica de la infraestructura del sector eléctrico en Colombia, la automatización de los procesos y de sus centros de gestión de energía local y remota, bajo un mundo globalizado sobre 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. Se requiere la estructuración de lineamientos y procedimientos que conlleven a las empresas del sector eléctrico colombiano a la aplicación de requerimientos mínimos de ciberseguridad, reduciendo riesgos de ciber terrorismo y guerra electrónica debido a que este sector es estratégico y crítico para la seguridad y estabilidad nacional, pues el riesgo para la industria eléctrica está asociado tanto a la red de comunicaciones como a cualquier equipo electrónico que gestione equipos de potencia. Debido a la evolución continua en las tecnologías y los protocolos de comunicación, es necesario estar revisando y actualizando las normas de ciber seguridad de acuerdo con los cambios tecnológicos que impacten el sector eléctrico colombiano.

El enfoque en la industria eléctrica ha sido orientado a la implementación de equipos que garanticen la confiabilidad del sistema de potencia. Este desarrollo ha estado acompañado de la incorporación de técnicas de automatización, las cuales están soportadas en una infraestructura electrónica con arquitecturas de comunicaciones abiertas que involucran comunicaciones sobre TCP/IP, comunicaciones inalámbricas, satelitales, electrónica de potencia, sistemas de gestión de operaciones, internet, etc., lo que aumenta el riesgo de posibles amenazas a la confidencialidad, integridad, disponibilidad y no-repudio. Un ejemplo de esta vulnerabilidad está en los protocolos de comunicación orientados a TCP/IP, los cuales son cada vez más usados en este sector mediante normas y estándares que sugieren su implementación, por ejemplo IEC60870-5-104, DNP3.0, Norma IEC61850, ,entre otros; lo que implica que la especialización o "Seguridad por oscuridad" tradicionalmente empleada, deja de ser válida.

Para la elaboración de este documento se utilizó 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-009, de los cuales se extractaron aspectos aplicables al caso colombiano.
Las normas NERC CIP-002 a la CIP-009, tratan:
CIP-002: Definición de ciber activos críticos
CIP-003: Controles en la gestión de seguridad e información
CIP-004: Personal y entrenamiento
CIP-005: Perímetros de seguridad electrónica
CIP-006: Seguridad física
CIP-007: Gestión del sistema de seguridad
CIP-008: Reporte de incidentes y planes de respuestas
CIP-009: Planes de recuperación para ciber activos críticos.

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

GLOSARIO.

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

Activo crítico. Instalaciones, sistemas o equipo eléctrico que si es destruido, degradado o puesto indisponible, afecte la confiablidad u operatividad del sistema eléctrico. Acorde con las recomendaciones del Comité Tecnológico del CNO para la definición de activos críticos que comprometan la seguridad de operación del SIN.

Ciber activo. 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.

Ciber activo crítico. Dispositivo para la operación confiable de activos críticos que cumple los atributos descritos en el numeral 2.2.3.

Entidad Responsable. Hacen referencia a las entidades operativas definidas en cada numeral.

Incidente de ciber seguridad: Cualquier acto malicioso o evento sospechoso que compromete o intenta comprometer, la seguridad física o electrónica de un Ciber Activo Crítico o su Perímetro.

NERC – CIP: North American Electric Reliability Corporation. Es la Corporación de Confiabilidad Eléctrica de Norteamerica. CIP. Critical Infrastructure Protection. Protección de la infraestructura crítica, incluye un conjunto de normas numeradas del 002 al 009.

Perímetro de Seguridad Electrónica – Es la frontera lógica con acceso controlado, que rodea una red dentro de la cual están conectados los Ciber Activos 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 Ciber Activos Críticos.

Puntos de acceso al (los) Perímetro(s) de Seguridad Electrónica: Incluye todos los terminales de comunicación externamente conectados (por ejemplo: módems de marcación) que conecten con cualquier dispositivo dentro del Perímetro de Seguridad Electrónica.

Seguridad de la información: Es la preservación de las siguientes características (ISO 27000):

- **Confidencialidad**: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.
- **Integridad**: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad**: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella cada vez que se requiera.
- **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.

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 segura y confiable del SIN.

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

IDENTIFICACIÓN DE ACTIVOS CRÍTICOS.

Propósito

Esta guía define un marco de referencia y/o actuación de ciberseguridad para la identificación y protección de ciber activos críticos que soportan la operación confiable del sistema eléctrico.

Se reconocen los diferentes roles de cada entidad en la operación del sistema eléctrico, la criticidad y vulnerabilidad de los activos que se deben gestionar para garantizar la confiablidad del sistema eléctrico y los riesgos a los cuales están expuestos.
Esta guía requiere la identificación y documentación de los ciber activos críticos asociados con los activos críticos que soportan la operación confiable del sistema eléctrico. Estos activos críticos deben ser identificados por medio de la aplicación de los elementos dados en el anexo 1 "Criterios de Activos Criticos".
Aplicación: La aplicación de los criterios y procedimientos establecidos en esta sección corresponde a las siguientes entidades operativas:

a) Consejo Nacional de Operación
b) Operador del Sistema
c) Generadores
d) Transportadores
e) Distribuidores

Criterios y Requisitos

Método de identificación de activos críticos. Cada entidad responsable identificará y documentará sus activos críticos basada en los criterios de éste documento (Anexo 1: Criterios de activos críticos).

Cada entidad responsable mantendrá documentación que describa sus procedimientos y criterios de evaluación de sus activos críticos.

Identificación de activos críticos. Cada entidad responsable desarrollará una lista de sus activos críticos de acuerdo con lo descrito en 2.2.1. La entidad responsable revisará esta lista al menos anualmente y la actualizará si es necesario.

Identificación de ciber activos críticos. Usando la lista de activos críticos desarrollada según el requisito 2.2.1, la entidad responsable elaborará

una lista de los ciber activos críticos asociados, esenciales para la operación de los activos críticos. La entidad responsable revisará esta lista al menos cada dos años y la actualizará si es necesario. Los ciber activos críticos son calificados como aquellos que tienen al menos una de las siguientes características:
2.2.3.1 El ciber activo usa un protocolo enrutable para comunicarse afuera del perímetro de seguridad electrónica, o,
2.2.3.2 El ciber activo usa un protocolo enrutable con un centro de control, o,
2.2.3.3 El ciber activo es accesible por marcación.

Acciones
La entidad responsable tendrá disponible la documentación de:

La lista de activos críticos
La lista de ciber activos críticos

Cumplimiento
Aprobación: El responsable de cada entidad aprobará periódicamente las listas de activos y ciber activos críticos.

Cada entidad responsable certificará por medio de reportes de auditoría que el inventario de activos y ciber activos críticos se mantiene actualizado y acorde con la metodología definida para su selección.
2.4.3 El CNO definirá cómo y cuándo se realizará el seguimiento del cumplimiento de los requisitos establecidos en esta guía.

GESTIÓN DE LA SEGURIDAD DE CIBER ACTIVOS CRITICOS

Propósito
El cumplimiento de esta guía requiere que las entidades responsables tengan controles de gestión de la seguridad para proteger los ciber activos críticos.

Esta guía requiere que personal que tiene acceso lógico autorizado o acceso físico no escoltado a ciber activos críticos, incluyendo contratistas y prestadores de servicios, tengan una evaluación del nivel de riesgo de personal, entrenamiento y sensibilización en seguridad.
Esta guía requiere la identificación y protección de los Perímetros de Seguridad Electrónica dentro de los cuales residen los Ciber Activos Críticos, al igual que todos los puntos de acceso al perímetro.
Esta guía requiere la identificación, clasificación, respuesta y reporte de incidentes de ciber seguridad relacionados con Ciber Activos críticos.

Aplicación
La aplicación de los criterios y procedimientos establecidos en esta sección corresponde a las siguientes entidades operativas:

a) Consejo Nacional de Operación
b) Operador del Sistema y
c) Generadores
d) Transportadores
e) Distribuidores

Criterios y Requisitos
Política de Ciber Seguridad. La entidad responsable documentará e implementará una política de Ciber Seguridad que represente el compromiso y la habilidad de la entidad para proteger sus ciber activos críticos.

La entidad asignará un responsable con toda la autoridad para dirigir y administrar la implementación y adherencia a esta guía.
La entidad debe mantener un programa de entrenamiento y sensibilización que refuerce los conocimientos y buenas prácticas en seguridad para todo el personal que tiene acceso a los ciber activos críticos.

Excepciones. Los casos en los cuales la entidad responsable no pueda cumplir con su política de ciber seguridad, deben ser documentados como excepciones y autorizados por el responsable.

Las excepciones documentadas a la política de ciber seguridad deben incluir una explicación de la necesidad de la excepción y de la medida alterna aplicada.

Protección de información. La entidad responsable implementará y documentará un programa para identificar, clasificar y proteger la información asociada con los ciber activos críticos.
La entidad responsable clasificará la información a ser protegida bajo éste programa, basado en la sensibilidad de la información del ciber activo crítico.

Control de acceso a la información. La entidad responsable documentará e implementará un programa para gestión de acceso a la información protegida de ciber activos críticos.
Controles de Acceso Electrónico – Cada entidad responsable implementará y documentará los procesos organizacionales y los

mecanismos técnicos y procedimentales para el control de acceso en todos los puntos de acceso electrónico al perímetro de seguridad electrónica.

Control de cambios y gestión de configuraciones. La entidad responsable establecerá y documentará un proceso de control de cambios y gestión de configuraciones para adiciones, modificaciones, reemplazos o retiros de hardware o software de ciber activos críticos.

Prevención de Software Malicioso – La Entidad Responsable deberá utilizar anti-virus y herramientas de prevención contra otro software malicioso ("malware"), donde sea técnicamente factible, para detectar, prevenir, disuadir y mitigar la introducción, exposición y propagación de malware a todos los Ciber Activos dentro del (los) Perímetro(s) de Seguridad Electrónica.

Administración de Cuentas - La Entidad Responsable establecerá, implementará y documentará los controles técnicos y procedimentales que apliquen la autenticación de acceso y responsabilidad por toda actividad de usuarios, y que minimice el riesgo de acceso no – autorizado al sistema.

Plan de respuesta de incidentes de Ciber Seguridad – La entidad responsable debe desarrollar, implementar y mantener un plan de respuesta a incidentes de Ciber Seguridad.

Acciones

La entidad responsable deberá identificar y documentar Perímetros de Seguridad Electrónica, los puntos y requisitos de acceso a los mismos asegurando que cada ciber activo crítico resida dentro de un perímetro de seguridad electrónica
Acceso: La entidad responsable mantendrá lista(s) del personal con acceso físico no escoltado o acceso lógico a los ciber activos críticos, incluyendo sus derechos de acceso físico y electrónico específicos de acuerdo con su rol.

Cada entidad responsable revisará la lista de su personal con acceso a ciber activos críticos trimestralmente y actualizará la lista en (7) siete días calendario ante cualquier cambio de personal con acceso a los ciber activos críticos o cualquier cambio en los derechos de acceso de tal

personal. La entidad responsable asegurará que la lista de acceso de contratistas o prestadores de servicios, se mantiene vigente.

La entidad responsable revocará los accesos a ciber activos críticos en 24 horas para el personal desvinculado de la empresa y en siete días calendario para personal que ya no requiere acceso a los ciber activos críticos.

Monitoreo de Acceso Electrónico – La Entidad Responsable implementará y documentará proceso(s) manuales ó electrónicos para el monitoreo y registro de accesos en puntos de acceso al (los) Perímetro(s) de Seguridad Electrónica veinticuatro horas al día, siete días por semana.
Evaluación de Ciber Vulnerabilidad – Cada entidad responsable deberá efectuar una evaluación de vulnerabilidad de todos los puntos electrónicos de acceso al (los) Perímetro(s) de Seguridad Electrónica como máximo cada dos años.

Procedimientos de Prueba – Cada Entidad Responsable deberá asegurar que nuevos Ciber Activos y cambios significativos a Ciber Activos existentes dentro del Perímetro de Seguridad Electrónica, no afecten adversamente los controles de Ciber seguridad existentes.

Puertos y Servicios – La entidad responsable establecerá, documentará e implementará un proceso para garantizar que solamente aquellos puertos y servicios requeridos para las operaciones normales y de emergencia sean habilitados.

Administración de Conexiones Provisionales de Seguridad – La entidad responsable, bien sea de forma separada ó como un componente del proceso, establecerá, documentará e implementará un programa de administración de conexiones temporales dentro del Perímetro de Seguridad Electrónica.

La entidad responsable deberá mantener la documentación y registros del desarrollo del plan de sensibilización y entrenamiento.
La entidad responsable debe tener disponibles sus planes de respuesta a incidentes de Ciber Seguridad y la documentación actualizada relacionada con la gestión de incidentes.

entidad La entidad responsable deberá usar software de antivirus y herramientas de prevención de software malicioso donde sea técnicamente posible.

La responsable deberá implementar y mantener una política de actualizaciones y parches de seguridad.

Cumplimiento

Monitoreo de Condición de Seguridad - La entidad responsable se asegurará que todos los Ciber Activos dentro del Perímetro de Seguridad Electrónica, según sea técnicamente factible, cuenten con herramientas automatizadas ó controles organizacionales de proceso para monitorear eventos del sistema relacionados con ciber seguridad.
Evaluación de Ciber Vulnerabilidad – La entidad responsable deberá efectuar una evaluación de vulnerabilidad de todos los Ciber Activos dentro del Perímetro de Seguridad Electrónica como máximo cada dos años.

Revisión y Conservación de Documentación – La entidad responsable deberá revisar, actualizar y conservar toda la documentación de soporte del cumplimiento de los requisitos de la guía y de los incidentes presentados, del año calendario anterior.

SEGURIDAD FÍSICA DE CIBER ACTIVOS CRÍTICOS

Propósito

Esta guía requiere que la entidad responsable implemente un programa de seguridad física para la protección de Ciber activos críticos.

Aplicación

La aplicación de los criterios y procedimientos establecidos en esta sección corresponde a las siguientes entidades operativas:

a) Consejo Nacional de Operación
b) Operador del Sistema y
c) Generadores
d) Transportadores
e) Distribuidores

Criterios y Requisitos

Plan de Seguridad física – La entidad responsable deberá documentar, implementar y mantener un plan de seguridad física, aprobado por el representante legal o su delegado que deberá considerar, como mínimo, lo siguiente:

Todos los ciber activos 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 activos.

Identificación de todos los puntos de acceso físico para cada perímetro de seguridad física y las medidas para controlar el acceso a esos puntos. Procesos, herramientas y procedimientos para monitorear el acceso físico a los perímetros.

Control de Acceso Físico – El responsable de la entidad deberá documentar e implementar las operaciones y procedimientos de control para manejar el acceso físico a todos los puntos de acceso del perímetro(s) de seguridad física. El responsable de la entidad deberá implementar mecanismos tales como Tarjetas de Acceso, Cerraduras especiales, Personal de seguridad y Otros dispositivos de autenticación (biométricos, teclados, etc.).

Monitoreo del Acceso físico – La entidad responsable deberá documentar e implementar los controles técnicos y de procedimiento para el control de acceso físico a todos los puntos de acceso al perímetro de seguridad física.

Registro de Acceso Físico –El responsable de la entidad documentará e implementará los mecanismos procedimentales y técnicos para registrar las entradas en todos los puntos de acceso al perímetro de seguridad física.

Mantenimientos y pruebas – El responsable de la entidad implementará un programa de mantenimiento y pruebas para garantizar que los sistemas de seguridad física funcionan adecuadamente.

Acciones

La entidad responsable tendrá un Plan de Seguridad Física documentando la implementación, revisión y actualización del control, monitoreo, registro y mantenimiento y pruebas del acceso físico y de los sistemas de seguridad asociados.

Cumplimiento

La entidad responsable definirá los mecanismos que estime conveniente para controlar el cumplimiento de esta guía incluyendo revisiones periódicas a las seguridades de acceso, a los controles y registros establecidos por el Plan de Seguridad Física.

El cumplimiento del Plan de Seguridad Física dentro de cada entidad debe ser asignado a un nivel gerencial adecuado para asegurar su cumplimiento y visibilidad. Esa gerencia será responsable de autorizar desviaciones temporales y excepciones prácticas a los criterios y guías que apliquen en su entidad.

PLAN DE RECUPERACIÓN (DE CIBER ACTIVOS CRÍTICOS)

Propósito

Esta guía requiere que la entidad responsable implemente planes de recuperación para ciber activos críticos y que esos planes correspondan a las técnicas y prácticas establecidas para la continuidad de negocios y los planes de recuperación.

Aplicación

La aplicación de los criterios y procedimientos establecidos en esta sección corresponde a las siguientes entidades operativas:

a) Consejo Nacional de Operación
b) Operador del Sistema
c) Generadores
d) Transportadores
e) Distribuidores

Criterios y Requisitos

Planes de recuperación: La entidad responsable debe crear y revisar con periodicidad anual los planes de recuperación para los ciber activos críticos. Los planes de recuperación deben considerar como mínimo:

Especificar las acciones requeridas en respuesta a eventos o condiciones de diversa duración y severidad que podrían activar los planes de recuperación.

Definir los roles y responsabilidades de los recursos asignados.

Pruebas (Simulacros): Los planes de recuperación deben probarse mínimo una vez al año. Una prueba o simulacro del plan de recuperación puede comprender desde una prueba de escritorio a un ejercicio operativo completo que simule un incidente real.

Control de cambios: Los planes de recuperación deben actualizarse para reflejar los cambios, planes de mejoramiento y lecciones aprendidas de las pruebas o simulacros o de las recuperaciones ante incidentes reales.
Respaldo y recuperación: Los planes de recuperación deben incluir los procesos y procedimientos para el respaldo y almacenamiento de la información necesaria para la recuperación efectiva de los ciber activos críticos. El respaldo debe incluir entre otros los equipos, componentes electrónicos para reposición, la documentación de parámetros de configuración, software y el respaldo de datos.

Pruebas a los medios de respaldo: La información esencial de recuperación que se almacene en medios de respaldo debe ser probada mínimo una vez al año para asegurar que la información sea integra y esté disponible.

Acciones
La entidad responsable debe disponer de planes de recuperación de acuerdo con la guía.

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 la pruebas.
La entidad responsable debe disponer de los registros de cambios efectuados a los planes de recuperación y documentación de todas las comunicaciones.

La entidad responsable debe disponer de los registros resultantes de los respaldos y almacenamientos de información.
La entidad responsable debe disponer de registros documentales sobre las pruebas de los medios de respaldo.

Cumplimiento
La entidad responsable definirá los mecanismos que estime convenientes para controlar el cumplimiento de esta guía de acuerdo con los procedimientos establecidos por los responsables del Plan de Recuperación de Activos Críticos.

El cumplimiento del Plan de Recuperación en cada entidad responsable debe ser asignado a un nivel gerencial adecuado para asegurar su cumplimiento y visibilidad. Ese nivel gerencial debe ser responsable por autorizaciones a desviaciones temporales y excepciones prácticas a los criterios y guías que apliquen en su entidad.

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 máxima de potencia real neta mayor o igual 100 MW.

1.2. Cada recurso o grupo de recursos de reactiva (excepto generadores) con una capacidad de en una localización simple mayor o igual a 100 Mvars.

1.3. Cada planta de generación que a criterio del operador del sistema, es considerada critica para garantizar la confiabilidad del sistema, considerado generación de seguridad.

1.4. Cada recurso identificado como importante por parte del operador del sistema en el plan de restauración desde Blackstart.

1.5. Instalaciones que se encuentran en sitios particulares y cumplen con los requerimientos de suicheo iniciales desde el Blackstart al primer punto de interconexión de las unidades de generación a ser arrancadas o llevadas al camino donde existen más de una alternativa y que es identificado como importante en el plan de recuperación.

1.6. Instalaciones de transmisión operadas a 220 KV o mayor, es decir, que pertenezcan al STN (Sistema de Transmisión Nacional).

1.7. Instalaciones de transmisión operadas a 110 kV o más y que contengan más de una instalación con otros niveles de tensión.

1.8. Instalaciones de transmisión que, a criterio del operador del sistema, pertenezcan a cortes críticos desde el punto de vista de confiabilidad.

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

1.10. Instalaciones de transmisión que conectan generación al sistema y que su indisponibilidad podría indisponer equipos de generación como los considerados en los ítems 1.1. y 1.3.

1.11. Esquemas especiales de protección como los Esquemas Suplementarios, que operan de tal manera que garantizan la confiabilidad del sistema.

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

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

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

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