COORDINADOR ELÉCTRICO NACIONAL

ESTÁNDAR DE CIBERSEGURIDAD PARA EL SECTOR ELÉCTRICO

Julio 2020

1. INTRODUCCIÓN

La creciente interconectividad y la dependencia de las plataformas y servicios basados en Internet han aumentado considerablemente la exposición al riesgo de los gobiernos, las empresas y las personas, a una gran variedad de actos relacionados con la delincuencia, el espionaje y la ciberseguridad. Los gobiernos y las empresas reconocen la necesidad de tener políticas y estrategias nacionales de ciberseguridad, cultura en ciberseguridad, educación, formación y competencias en seguridad, marcos jurídicos, reglamentos, normativas y estándares, así como contar con la cooperación e intercambio de información.

Los incidentes que han ocurrido en los últimos años han ocasionado que tanto los gobiernos, como las instituciones y organizaciones sean más conscientes de la necesidad de adoptar medidas para controlar los riesgos de ciberseguridad. En la medida que la industria se desarrolla e incrementa sus niveles de transformación, la ciberseguridad toma mayor relevancia.

El Coordinador Eléctrico Nacional, en adelante el Coordinador, de acuerdo a lo instruido por los oficios N°3377 del 25 de junio de 2018 y N°11508 del 3 de Junio de 2019 emitidos por la Superintendencia de Electricidad y Combustible (SEC), ha trabajado en establecer los requisitos mínimos de resguardo de la seguridad cibernética o ciberseguridad aplicables al Sector Eléctrico que permitan prevenir y/o mitigar potenciales ciber amenazas que pongan en riesgo la seguridad y continuidad del servicio de energía eléctrica.

Luego de un exhaustivo análisis de las diferentes normativas en materia de ciberseguridad para infraestructura crítica en el sector eléctrico, y junto al apoyo especializado de CAISO (California Independent System Operator), el Coordinador ha definido adoptar la Normativa CIP (Critical Infrastructure Protection) de NERC (North American Electric Reliability Corporation), en adelante NERC-CIP, como estándar de ciberseguridad a ser adoptado por los agentes participantes en el sector eléctrico nacional, debido a que esta norma contiene aspectos fundamentales para la seguridad de la información e infraestructuras tecnológica y de operación críticas de sistemas eléctricos.

2. DEFINICIONES

Las siguientes definiciones aplican para el cumplimiento del presente estándar:

- **Acceso Remoto Interactivo (ARI):** Acceso de usuario iniciado por una persona empleando un acceso remoto cliente u otra tecnología de acceso remoto que utilice un Protocolo Enrutable. El acceso remoto se origina desde un Ciber Activo que no es un Sistema Intermedio y no está localizado dentro del Perímetro de Seguridad Electrónica (PSE) de alguna Entidad Responsable o en un Punto de Acceso Electrónico (PAE) definido. Un acceso remoto puede ser iniciado desde i) un Ciber Activo utilizado por, o de propiedad de, una Entidad Responsable, ii) un Ciber Activo utilizado por, o de propiedad de, un empleado de la Entidad Responsable, y iii) un Ciber Activo utilizado por, o de

propiedad de, un tercero proveedor, contratista, o consultor de la Entidad Responsable. Un Acceso Remoto Interactivo no incluye procesos de comunicación entre sistemas.

- **Amenaza:** Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un Incidente de Ciberseguridad.

- **Autenticación:** Procedimiento para comprobar que alguien es quién dice ser cuando accede a un ordenador o a un servicio online. Este proceso constituye una funcionalidad característica para una comunicación segura.

- **Centro de Control (CC):** Instalación principal, o de respaldo, nacional o regional, dotada de un sistema SCADA y destinada a la supervisión, control y operación en tiempo real de las instalaciones eléctricas pertenecientes a los Coordinados.

- **Centro de Despacho y Control (CDC):** Instalación principal, o de respaldo, nacional o regional, dotada de un sistema SCADA y destinada a la coordinación de la operación en tiempo real del SEN por parte del Coordinador.

- **Ciber Activo SEN:** Ciber Activo que, en caso de fallar, ser degradado, mal utilizado o quedar indisponible, dentro de un intervalo de 15 minutos medidos desde el momento de ser requerido en tiempo real, desde tener que cumplir el programa operacional, desde su falla o desde su indisponibilidad, pudiese impactar adversamente una o más instalaciones, sistemas, o equipos los cuales, de ser destruidos, degradados, o volverse indisponibles cuando se requieran, afectaría la operación segura y confiable del SEN. La redundancia de las instalaciones, sistemas o equipos afectados, no se deberá considerar al momento de determinar el impacto adverso. Cada Ciber Activo SEN debe estar incluido en uno o más Ciber Sistemas SEN.

- **Ciber Activo Transitorio:** Un Ciber Activo que i) es capaz de transmitir o transferir código ejecutable, ii) no está incluido en un Ciber Sistema SEN, iii) no es un Ciber Activo Protegido (CAP) asociado a un Ciber Sistema SEN de Impacto Alto o Medio, y iv) está directamente conectado (usando por ejemplo comunicación serial, ethernet, USB, Wireless o Bluetooth) por 30 días calendario consecutivos o menos a un Ciber Activo SEN, una red dentro de un Perímetro de Seguridad Electrónica (PSE) que contenga Ciber Sistemas SEN de Impacto Alto o Medio, o un Ciber Activo Protegido (CAP) asociado con Ciber Sistemas SEN de Impacto Alto o Medio.

- **Ciber Activos o Activos Cibernéticos:** Dispositivos electrónicos inteligentes o programables, incluyendo el hardware, software y los datos almacenados en dichos dispositivos. Ciber Activos pueden incluir controladores lógicos programables (PLCs), sistemas de control distribuido (DCSs), relés y dispositivos electrónicos inteligentes (IEDs),

interfaces hombre máquina a (HMI), estaciones de trabajo y servidores de aplicaciones, entre otros.

- **Ciber Activos Protegidos (CAP):** Uno o más Ciber Activos conectados vía un protocolo enrutable dentro o sobre un Perímetro de Seguridad Electrónica (PSE) que no son parte del Ciber Sistema SEN del más alto impacto dentro del mismo Perímetro de Seguridad Electrónica (PSE). La calificación de impacto de los Ciber Activos Protegidos (CAP) es igual a la más alta calificación de impacto del Ciber Sistema SEN en el mismo Perímetro de Seguridad Electrónica (PSE).

- **Ciber Activos Transitorios (CAT):** Ciber Activos para ser usados en funciones transitorias, entre ellas para transferir datos, evaluación de vulnerabilidades, mantenciones, o solución de problemas (troubleshooting).

- **Ciber Sistema SEN:** Uno o más Ciber Activos SEN agrupados lógicamente por una Entidad Responsable.

- **Circunstancias Excepcionales CIP:** Situación que involucra, o amenaza involucrar, una o más de las siguientes condiciones que impactan la seguridad o confiabilidad del SEN, entre las que destacan: i) riesgo de accidente o muerte, ii) desastre natural, iii) disturbios civiles, iv) una falla inminente de equipos, software o hardware, v) un incidente de ciberseguridad que requiera apoyo de emergencia, vi) la firma de un acuerdo de asistencia mutua, o vii) una indisponibilidad de fuerza laboral de gran escala.

- **Conectividad Enrutable Externa (CEE):** Capacidad de acceder a un Ciber Sistema SEN desde un Ciber Activo que se encuentra fuera de su correspondiente Perímetro de Seguridad Electrónica (PSE) vía un protocolo de conexión enrutable bidireccional.

- **Coordinado:** A efectos de la aplicación del presente estándar, se entenderá por Coordinado a todo propietario, arrendatario, usufructuario o quien opere o explote a cualquier título instalaciones que se encuentren interconectadas, según se establece en la NTSyCS.

- **Coordinador:** Coordinador Independiente del Sistema Eléctrico Nacional al que se refiere el Título VI BIS de la Ley General de Servicios Eléctricos (LGSE).

- **Criptografía o Encriptación:** Técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca el sistema mediante el cual ha sido cifrado. Existen dos tipos principales de criptografía, por un lado, la conocida como criptografía simétrica, más tradicional, y la criptografía asimétrica o de clave pública.

- **Encargado CIP:** Ejecutivo senior, oficial de seguridad informática, o representante oficial con autoridad y responsabilidad para liderar y gestionar la implementación y continuo cumplimento de los requerimientos establecidos en el presente estándar.

- **Entidad Responsable:** Se refiere a las empresas Coordinadas (o Coordinados), al Coordinador, y a todo otro organismo al cual le apliquen los requerimientos establecidos en el presente estándar.

- **Evaluación de riesgos:** Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

- **Factor de Riesgo por Incumplimiento Alto (FRIA):** Un requerimiento que, de ser incumplido o violado, podría causar directamente o contribuir a una inestabilidad, separación en islas, o a una secuencia en cascada de fallas en el SEN, o podría exponer al SEN a un riesgo inaceptable de inestabilidad, separación en islas, o a una secuencia en cascada de fallas; o un requerimiento en un horizonte de planificación que, de ser incumplido o violado, bajo condiciones normales, de alerta, de emergencia, o de recuperación, podría causar directamente o contribuir a una inestabilidad, separación en islas, o a una secuencia en cascada de fallas en el SEN, o podría exponer al SEN a un riesgo inaceptable de inestabilidad, separación en islas, o a una secuencia en cascada de fallas, o podría impedir la recuperación del SEN a una condición normal.

- **Factor de Riesgo por Incumplimiento Medio (FRIM):** Un requerimiento que, de ser incumplido o violado, podría afectar directamente el estado eléctrico del SEN, o la capacidad para controlar y monitorear el SEN de manera efectiva; o un requerimiento en un horizonte de panificación que, de ser incumplido o violado, bajo condiciones normales, de alerta, de emergencia, o de recuperación, podría afectar directamente y de manera adversa el estado eléctrico del SEN o la capacidad para controlar, monitorear y recuperar el SEN de manera efectiva.

- **Factor de Riesgo por Incumplimiento Bajo (FRIB):** Un requerimiento que es de naturaleza administrativa y un requerimiento que, de ser incumplido o violado, no se esperaría que afecte de manera adversa el estado eléctrico del SEN, o la capacidad para controlar y monitorear el SEN de manera efectiva; o un requerimiento que es de naturaleza administrativa y un requerimiento en un horizonte de planificación que, de ser incumplido o violado, bajo condiciones normales, de alerta, de emergencia, o de recuperación, no se esperaría que afecte de manera adversa la capacidad para controlar, monitorear y recuperar el SEN de manera efectiva.

- **Incidente de Ciberseguridad Reportable (ICR):** Incidente de Ciberseguridad que ha comprometido o interrumpido i) un Ciber Sistema SEN que desempeña una o más funciones asociadas a mantener la seguridad y confiabilidad del SEN por parte de las Entidades Responsables, ii) un Perímetro se Seguridad Electrónica (PSE) de un Ciber Sistema SEN de Impacto Alto o Medio, o iii) un Sistema de Monitoreo o Control de Acceso Electrónico (SMCAE) de un Ciber Sistema SEN de Impacto Alto o Medio.

- **Incidente de Ciberseguridad**: Un acto malicioso o evento sospechoso que i) para un Ciber Sistema SEN de Impacto Alto o Medio, comprometa, o haga un intento de comprometer, un Perímetro de Seguridad Electrónica (PSE), un Perímetro de Seguridad Física (PSF) o un Sistema de Monitoreo o Control de Acceso Electrónico (SMCAE), o que ii) interrumpa, o intente interrumpir la operación de un Ciber Sistema SEN.

- **Información de Ciber Sistema SEN:** Información sobre un Ciber Sistema SEN que podría ser utilizada para obtener acceso no autorizado o plantear una amenaza de seguridad al Ciber Sistema SEN. Dicha información no incluye información individual aislada que, por sí misma, no plantee una amenaza o no pueda ser utilizada para obtener acceso no autorizado a un Ciber Sistema SEN, tal como, pero no limitada a, nombres de dispositivos, direcciones IP individuales sin contexto, nombres de Perímetros de Seguridad Electrónica (PSEs), o declaración de políticas. Ejemplos de Información de Ciber Sistema SEN pueden incluir, pero no está limitado a, registros de direcciones de redes, topología de redes del Ciber Sistema SEN, procedimientos de seguridad o información de seguridad de Ciber Sistemas SEN, Sistemas de Control de Acceso Físico (SCAF), y Sistemas de Monitoreo o Control de Acceso Electrónico (SMCAE) que no sea de acceso público y que podría utilizarse para permitir acceso no autorizado o distribución no autorizada.

- **Lista blanca (whitelisting):** Listado de elementos aprobados previamente para su uso, ejecución u operación.

- **Malware:** Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información.

- **Medios Removibles (MR):** Medios de almacenamiento que i) no son Ciber Activos, ii) son capaces de transferir código ejecutable, iii) pueden ser utilizados para almacenar, copiar, mover o acceder a datos, y iv) están directamente conectados, por 30 días calendario consecutivos o menos, a un Ciber Activo SEN, a una red dentro de un Perímetro de Seguridad Electrónica (PSE) que contenga Ciber Sistemas SEN de Impacto Alto o Medio, o a un Ciber Activo Protegido (CAP) asociado con Ciber Sistemas SEN de Impacto Alto o Medio. Ejemplos de Medios Removibles incluyen, pero no están limitados a, discos compactos o flexibles (floppy disks), dispositivos de memoria USB, discos duros externos, y otros dispositivos o tarjetas que contengan memoria no volátil.

- **Norma Técnica de Seguridad y Calidad de Servicio (NTSyCS)**: Establece las exigencias de seguridad y calidad de servicio de los sistemas interconectados, según lo establecido en la Ley General de Servicios Eléctricos (LGSE) y sus reglamentos.

- **Parche de Seguridad:** Un parche de seguridad es un conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos. Generalmente los parches de seguridad son desarrollados por el fabricante del software tras la detección de una vulnerabilidad en el software y pueden instalarse de forma automática o manual por parte del usuario.

- **Perímetro de Seguridad Electrónica (PSE):** Borde o limite lógico alrededor de una red a la cual los Ciber Sistemas SEN están conectados utilizando un protocolo enrutable.

- **Perímetro de Seguridad Física (PSF):** Borde o limite físico alrededor de espacios en donde residen Ciber Activos SEN, Ciber Sistemas SEN, o Sistemas de Monitoreo o Control de Acceso Electrónico (SMCAE), y en los cuales el acceso es controlado.

- **Plan:** El término Plan puede ser utilizado en el presente estándar en lugar de Proceso Documentado. Cuando se trata de un proceso que describe una respuesta o acción es referido generalmente como un Plan. Por ejemplo, un Plan de Seguridad puede describir un enfoque que involucre múltiples procedimientos para abordar un tema más amplio. En cualquier caso, el término Plan no implica un requerimiento adicional más allá de lo establecido en el presente estándar.

- **Política:** Para los efectos del presente estándar, el término Política se refiere a un, o una colección de, documento(s) que son utilizados por las Empresas Responsables para comunicar sus objetivos de estratégicos, metas de gestión y expectativas sobre como dichas entidades protegerán sus Ciber Sistemas SEN. El uso de Políticas también establece una base de gobernanza general para crear una cultura de seguridad y cumplimiento de leyes, regulaciones y estándares.

- **Proceso Documentado:** Para los efectos del presente estándar, el término Proceso Documentado se refiere a un conjunto de instrucciones requeridas específica para la Entidad Responsable y para alcanzar un resultado específico. El término no implica una estructura de nombres o aprobaciones que vaya más allá de lo establecido en los requerimientos. La Entidad Responsable deberá incluir en el Proceso Documentado tanto como crea necesario, pero deberá abordar el requerimiento aplicable.

- **Programa:** El término Programa también puede ser utilizado en el presente estándar en lugar de Proceso Documentado. Un Programa se puede referir a la implementación global en la organización de sus Políticas, Planes y procedimientos involucrando un tema específico. Ejemplos de Programas son el Programa de Evaluación de Riesgo del Personal y el Programa de Capacitación del Personal. En cualquier caso, el término Plan no implica un requerimiento adicional más allá de lo establecido en el presente estándar.

- **Protocolo Enrutable:** Los protocolos enrutables o enrutados establecen las direcciones para identificar a las computadoras y las redes individuales dentro de cada red. Son capaces de dar soporte a la capa de red (OSI) o internet (TCP/IP). Un protocolo enrutable debe ser capaz de asignar un número de red y un número de equipo a cada dispositivo de la red. Estos protocolos son los encargados de incluir la información suficiente para que un router pueda enviar los mensajes de un punto a otro de la red.

- **Punto de Acceso Electrónico (PAE):** Interfaz de un Ciber Activo en un Perímetro de Seguridad Electrónica (PSE) que permite comunicación enrutable entre Ciber Activos dentro y fuera de un Perímetro de Seguridad Electrónica (PSE).

- **Ransomware:** Ataque de ciberseguridad consistente en la toma control del equipo infectado secuestrando la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos.

- **Reforzamiento (Hardening) de Sistemas:** Conjunto de actividades que son llevadas a cabo por el administrador de un sistema para reforzar al máximo posible la seguridad.

- **Sistema de Monitoreo o Control de Acceso Electrónico (SMCAE):** Ciber Activo que desempeña el control o monitoreo del acceso electrónico de los Perímetros de Seguridad Electrónica (PSEs) o de los Ciber Sistemas SEN. Esto incluye los Sistemas Intermedios.

- **Sistema Eléctrico Nacional (SEN):** Sistema eléctrico interconectado cuya capacidad instalada de generación sea igual o superior a 200 megawatts.

- **Sistema Interconectado (SI):** Conjunto de instalaciones de un sistema eléctrico incluyendo: las centrales eléctricas; líneas de transmisión a nivel troncal, subtransmisión y adicionales; enlaces HVDC, equipos de compensación de energía activa, subestaciones eléctricas, incluidas las subestaciones primarias de distribución, y barras de consumo de clientes libres abastecidos directamente desde instalaciones de un sistema de transmisión o a través de alimentadores de uso exclusivo; que operan interconectadas entre sí, con el objeto de generar, transportar y distribuir energía eléctrica en dicho sistema eléctrico.

- **Sistema Intermedio:** Un Ciber Activo, o conjunto de Ciber Activos, desempeñando control de acceso para restringir Acceso Remoto Interactivo solo a usuarios autorizados. El Sistema Intermedio no debe estar localizado dentro del Perímetro de Seguridad Electrónica (PSE).

- **Sistema SCADA:** Sistema de Control y Adquisición de Datos destinado a supervisar monitorear, controlar y operar las instalaciones del SEN.

- **Sistemas de Control de Acceso Físico (SCAF):** Ciber Activos que controlan, alertan, u otorgan acceso a Perímetros de Seguridad Física (PSFs), excluyendo el hardware instalado localmente o dispositivos en el Perímetro de Seguridad Física (PSF) tales como sensores de movimiento, mecanismos de control de seguro electrónico y lectores de tarjetas de acceso.

- **Vulnerabilidad:** Fallos o deficiencias de un sistema, red, equipo, programa o software que pueden permitir que un usuario no legítimo realice acciones no autorizadas, o acceda de forma no autorizada a información manera local o remota.

- **Workflow:** Secuencia de los pasos que forman un determinado proceso ya sea industrial, administrativo, o de otro tipo.

3. APLICABILIDAD GENERAL

Los requerimientos establecidos en el presente estándar son aplicables a las siguientes Entidades Responsables:

a) Coordinador Eléctrico Nacional, y
b) Empresas Coordinadas

Si bien el presente estándar es de aplicación general en la industria eléctrica nacional, su aplicabilidad específica está asociada con las instalaciones o activos que caen dentro de las categorías de calificación de impacto definidas en la parte 6 del presente documento. A las Entidades Responsables que posean instalaciones que no estén contempladas dentro de alguna de las categorías de impacto Ato, Medio, o Bajo, no les será aplicable el presente estándar.

4. CUMPLIMIENTO Y MONITOREO

Los requerimientos establecidos en el presente estándar deberán ser implementados por las Entidades Responsables de forma obligatoria en los plazos señalados y según corresponda dada la calificación de impacto de sus instalaciones y las excepciones específicas.

Las Entidades Responsables deberán monitorear e informar a la SEC, con una frecuencia anual dentro del primer trimestre de cada año y en el formateo que esta defina, el nivel de cumplimiento de las medidas de control para cada requerimiento. Los reportes con el nivel de cumplimiento enviados a la SEC deberán ser revisados y aprobados por el Encargado CIP de cada Entidad Responsable.

Todo Incidente de Ciberseguridad Reportable (ICR) deberá ser notificado, a través del Encargado CIP, al Coordinador y a la SEC dentro de una hora de ser detectado por parte de la Entidad Responsable. El formato y contenido mínimo a incluir en la notificación de los ICR será definido por la SEC.

Las Entidades Responsable deberán mantener registros de evidencias y medidas de control por un periodo de al menos 3 años, plazo que se podría extender según lo requiera la SEC por existir una investigación en curso como resultado de una auditoría.

La SEC podrá instruir auditorias de cumplimiento y/o certificaciones por parte de terceros especializados en materias de ciberseguridad a fin de verificar el cumplimiento del presente estándar.

Las excepciones de aplicabilidad, dado en nivel de impacto de las instalaciones de las Entidades Responsables, se indican dentro de cada estándar CIP y para cada requerimiento según corresponda.

5. RESERVA Y CONFIDENCIALIDAD

Con el fin de proteger la información relacionada con la ciberseguridad en las instalaciones de las Entidades Responsables y la integridad y seguridad del SEN, todos los documentos y reportes que emitan las Entidades Responsables como resultado de implementar los requerimientos y las medidas de control establecidos en el presente estándar, así como los informes de cumplimiento entregados a la SEC, en adelante la "Información Reservada", deberán ser tratados con el carácter de reservado debiendo cada Entidad Responsable implementar los procedimientos necesarios para que las personas vinculadas a ella, sus socios, consejeros, asociados, y demás trabajadores o consultores internos o externos, sea que participen o no en el análisis de la Información Reservada, cumplan con dicha obligación.

En caso de que el cumplimiento de este estándar requiera interactuar con un organismo no relacionado, como es el caso de lo dispuesto en el numeral 7.13.3, cada Entidad Responsable deberá implementar los procedimientos necesarios para preservar el carácter de reservado de la Información Reservada, debiendo firmar el o los acuerdos de confidencialidad necesarios.

6. CRITERIOS PARA CALIFICACIÓN DE IMPACTO

A continuación, se presentan los criterios para la calificación de Ciber Sistemas SEN en niveles de Impacto Alto, Medio y Bajo, según las instalaciones en las cuales están localizados o con las cuales interactúan.

6.1. Impacto Alto

Califican como de Impacto Alto todos y cada uno de los Ciber Sistemas SEN utilizados por, o localizados en alguna de las siguientes instalaciones:

6.1.1. Centros de Despacho y Control, principal o de respaldo, nacional o regional, utilizados por el Coordinador para la realización de su función coordinación de la operación en tiempo real del SEN.

6.1.2. Centros Control, principal o de respaldo, nacional o regional, utilizados por las Empresas Coordinadas para la supervisión, control y operación en tiempo real de uno o más activos o instalaciones eléctricas de su propiedad que operan en el SEN, que cumplen con los criterios de Impacto Medio definidos en los puntos 6.2.1 al 6.2.8.

6.2. Impacto Medio

Califican como de Impacto Medio todos y cada uno de los Ciber Sistemas SEN no incluidos en 6.1 y que sean utilizados por, o localizados en alguna de las siguientes instalaciones:

6.2.1. Instalaciones de generación, agrupadas por unidades generadoras localizadas en una sola planta o central eléctrica, con una capacidad de potencia activa neta agregada, registrada en los últimos 12 meses, igual o superior a 300 MW en un sistema interconectado. Para cada grupo de unidades generadoras, los únicos Ciber Sistemas SEN que reúnen este criterio son aquellos Ciber Sistemas SEN compartidos que pudiesen, dentro de un intervalo de tiempo de 15 minutos, impactar adversamente la operación confiable de cualquier combinación de unidades que, de forma agregada, iguale o exceda los 300 MW.

6.2.2. Recursos de potencia reactiva o grupo de recursos reactivos en una única localización (excluyendo las instalaciones de generación) con una capacidad de potencia reactiva instalada agregada máxima, registrada en los últimos 12 meses, igual o superior a 100 MVAr. Los únicos Ciber Sistemas SEN que reúnen este criterio son aquellos Ciber Sistemas SEN compartidos que pudiesen, dentro de un intervalo de tiempo de 15 minutos, impactar adversamente la operación confiable de cualquier combinación de recursos que, de forma agregada, iguale o exceda los 100 MVAr.

6.2.3. Instalaciones de generación que el Coordinador identifique como necesarias a fin de evitar un impacto adverso en la seguridad y confiabilidad del SEN en un horizonte de planificación mayor un año.

6.2.4. Instalaciones de transmisión pertenecientes al sistema de transmisión nacional. En el caso de subestaciones que contengan instalaciones pertenecientes a este segmento, se incluye todo el perímetro electrónico o físico dentro de dichas subestaciones, independiente de su nivel de tensión.

6.2.5. Instalaciones de transmisión pertenecientes a sistemas de transmisión dedicados o zonales, con niveles de tensión igual o superior a 220 kV, que se conectan directamente al sistema de transmisión nacional. Adicionalmente, incluye subestaciones no conectadas directamente al sistema de transmisión nacional, cuyo nivel de tensión más alto es igual o superior a 220 kV y en donde confluya (se inyecte o retire) un flujo máximo de potencia activa, registrado en los últimos 12 meses, de a lo menos 300 MW.

6.2.6. Instalaciones de generación o transmisión que el Coordinador identifique como necesarias para no violar los límites de transmisión durante contingencias, definidos en el capítulo 5 de la Norma Técnica de Seguridad y Calidad Servicio (NTSyCS), pudiendo poner en riesgo la seguridad y confiabilidad del SEN.

6.2.7. Sistemas y equipos incluidos en los Planes de Defensa contra Contingencias Extremas (PDCE) y automatismos especiales que operen en el SEN, lo cuales, en caso de ser destruidos, degradados, mal utilizados o dejados indisponibles, causaría una violación de los límites de transmisión definidos en la NTSyCS, por no operar según fueron diseñados, pudiendo poner en riesgo la seguridad y confiabilidad del SEN.

6.2.8. Sistemas y equipos pertenecientes a esquemas de desconexión automática de carga (EDAC) y generación (EDAG), y a esquemas de reducción automática de generación (ERAG), bajo un sistema de control común y sin intervención humada para su activación, destinados a controlar frecuencia o tensión en el SEN.

6.2.9. Centros de Control, principal o de respaldo, nacional o regional, no incluidos en instalaciones de Impacto Alto definidas en 6.1, y que supervisen, monitoreen u operen instalaciones en el SEN.

6.3. Impacto Bajo

Califican como de Impacto Bajo todos y cada uno de los Ciber Sistemas SEN no incluidos en 6.1 o 6.2 que sean utilizados por, localizados en, o asociados con alguna de las siguientes instalaciones:

6.3.1. Instalaciones de generación y transmisión del SEN.

6.3.2. Instalaciones destinadas la recuperación de servicio y formación de islas incluidos en los Planes de Recuperación de Servicio (PRS) del SEN.

6.3.3. Sistemas especiales de protecciones destinados a la operación confiable y segura de SEN.

6.3.4. Instalaciones pertenecientes a empresas Distribuidoras destinadas a la protección y recuperación del SEN.

7. ESTÁNDAR DE CIBERSEGURIDAD

A continuación, se presentan los estándares NERC-CIP exigibles para el sector eléctrico. Cada estándar incluye la referencia al estándar original NERC-CIP, el propósito del estándar, sus requerimientos (R) y correspondientes medidas de control (M), aplicabilidad específica y/o excepciones, y entrada en vigor.

7.1. CIP-002: Ciber Seguridad - Categorización de Ciber Sistemas SEN

7.1.1. Propósito

Identificar y categorizar los Ciber Sistemas SEN y sus correspondientes Ciber Activos para la aplicación de requerimientos de ciberseguridad acordes con el impacto adverso que podría ocasionar, en la operación segura y confiable del SEN, la pérdida, compromiso, o mal uso de dichos Ciber Sistemas SEN. La identificación y categorización de Ciber Sistemas SEN servirá de apoyo para la adecuada protección contra eventos que afecten o comprometan instalaciones pudiendo conducir a una mala operación o inestabilidad del SEN.

7.1.2. Aplicabilidad Específica y Excepciones

No existe aplicabilidad específica adicional a lo definido en el punto 3 para el estándar CIP-002.

Se exceptúan los Ciber Activos asociados con redes de comunicaciones y enlaces de comunicaciones de datos entre Perímetros de Seguridad Electrónica (PSE) independientes.

7.1.3. Requerimientos (R) y Medidas de Control (M)

R1. Cada Entidad Responsable deberá implementar, para cada uno de los siguientes activos: i) Centros de Control principal y de respaldo, ii) subestaciones de transmisión y distribución, iii) recursos o plantas de generación y recursos de reactivos, iv) sistemas e instalaciones críticas para los Planes de Recuperación de Servicio (PRS), v) PDCE y sistemas especiales de protecciones para apoyar la operación segura y confiable del SEN, y vi) sistemas de protecciones de empresas Distribuidoras destinados a la protección y recuperación del SEN, un proceso con el propósito de:

a) Identificar, si existen, todos y cada uno de los Ciber Sistemas SEN de Impacto Alto según lo establecido en 6.1, en cada activo;

b) Identificar, si existen, todos y cada uno de los Ciber Sistemas SEN de Impacto Medio según lo establecido en 6.2, en cada activo; e
c) Identificar, si existen, todos y cada uno de los activos que contienen Ciber Sistemas SEN de Impacto Bajo según lo establecido en 6.3. No se requiere un listado detallado de los Ciber Sistemas SEN de Impacto Bajo.

R1 es calificado con Factor de Riesgo por Incumplimiento Alto (FRIA).

M1. Medida de control o evidencia aceptable incluye, pero no está limitada a, listados físicos o electrónicos fechados para las partes a) y b) del requerimiento R1.

R2. Cada Entidad Responsable deberá:

a) Revisar los ítems identificados en R1 y sus partes, y actualizarlos si hay cambios, al menos una vez cada 15 meses calendario, aun cuando no se haya identificado ningún ítem en R1, y
b) Contar con la aprobación, por parte del Encargado CIP, de las identificaciones en requerimiento R1, al menos una vez cada 15 meses calendario, aun cuando no se haya identificado ningún ítem en R1.

R2 es calificado con Factor de Riesgo por Incumplimiento Bajo (FRIB).

M2. Medida de control o evidencia aceptable incluye, pero no está limitada a, registros físicos o electrónicos fechados que demuestren que la Entidad Responsable ha revisado y actualizado, donde sea necesario, las identificaciones en R1 y sus partes, y que ha contado con la aprobación por parte del Encargado CIP de las identificaciones en R1 y sus partes, al menos una vez cada 15 meses calendario, aun cuando no se haya identificado ningún ítem en R1 y sus partes, según requerimiento R2.

7.1.4. Entrada en Vigor

El presente estándar CIP-002 entrará en vigor al momento de su aprobación por parte de la SEC y posterior publicación en la página web del Coordinador. Las Entidades Responsables tendrán un periodo de marcha blanca para implementar cada uno de los requerimientos en el estándar CIP-002 de acuerdo con los plazos máximos especificados en ANEXO 1, columna Marcha Blanca.

7.2. CIP-003: Ciber Seguridad – Controles de Gestión de la Seguridad

7.2.1. Propósito

Especificar controles de gestión de la seguridad consistentes y sostenibles que establezcan la responsabilidad para proteger Ciber Sistemas SEN contra eventos que afecten o comprometan instalaciones pudiendo conducir una mala operación o inestabilidad del SEN.

7.2.2. Aplicabilidad Especifica y Excepciones

No existe aplicabilidad específica adicional a lo definido en el punto 3 para el estándar CIP-003.

Se exceptúan los Ciber Activos asociados con redes de comunicaciones y enlaces de comunicaciones de datos entre Perímetros de Seguridad Electrónica (PSE) independientes.

7.2.3. Requerimientos (R) y Medidas de Control (M)

R1. Cada Entidad Responsable deberá revisar y obtener aprobación del Encargado CIP, al menos una vez cada 15 meses calendario, de una o más políticas de ciberseguridad documentadas que en su conjunto aborden los siguientes aspectos:

a) Para Ciber Sistemas SEN de Impacto Alto y Medio:

- Personal y capacitación (CIP-004);
- Perímetro(s) de Seguridad Electrónica (CIP-005), incluyendo Acceso Remoto Interactivo;
- Seguridad Física de Ciber Sistemas SEN Críticos (CIP-006);
- Gestión de Seguridad del Sistema (CIP-007);
- Reportes de Incidentes y Planes de Respuesta (CIP-008);
- Planes de Recuperación para Ciber Sistemas Críticos (CIP-009);
- Gestión de Cambio de Configuraciones y Evaluación de Vulnerabilidades (CIP-010);
- Protección de la Información (CIP-011);
- Seguridad Física (CIP-014); y
- Declaración y respuesta a Circunstancias Excepcionales CIP

b) Para sus activos identificados en CIP-002 que contengan Ciber Sistemas SEN de Impacto Bajo, si existen:

- Conciencia de ciberseguridad;

- Controles de seguridad física;
- Control de acceso electrónico;
- Respuesta a incidentes de ciberseguridad;
- Mitigación de riesgos de código malicioso en Ciber Activos Transitorios y Medios Removibles; y
- Declaración y respuesta a Circunstancias Excepcionales CIP

R1 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M1. Medidas de control o evidencia aceptable incluyen, pero no están limitadas a, documentos de políticas de ciberseguridad, revisión histórica, registros de revisión, o evidencia de workflow de un sistema de gestión de documentos que demuestre revisión de cada política de ciberseguridad al menos una vez cada 15 meses calendario; documentación de aprobación de cada política de ciberseguridad por parte del Encargado CIP.

R2. Cada Entidad Responsable con al menos un activo identificado en CIP-002 conteniendo Ciber Sistemas SEN de Impacto Bajo deberá implementar uno o más planes de ciberseguridad documentados para sus Ciber Sistemas SEN de Impacto Bajo que incluyan las secciones descritas en 7.2.4. No se requiere un inventario, listado, o identificación discreta (individualizada) de Ciber Sistemas SEN o sus Ciber Activos SEN, tampoco se requiere una lista de usuarios autorizados.

R2 es calificado con Factor de Riesgo por Incumplimiento Bajo (FRIB).

M2. Medida de control o evidencia deberá incluir cada uno de los planes de ciberseguridad documentados que en su conjunto incluyan cada una de las secciones en 7.2.4, junto con evidencia adicional para demostrar la implementación de los planes de ciberseguridad.

R3. Cada Entidad Responsable deberá identificar un Encargado CIP por su nombre y documentar por escrito cualquier modificación al respecto dentro de 30 días calendario de ocurrido el cambio.

R3 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M3. Medida de control o evidencia podrá incluir, pero no está limitada a, documentación fechada y aprobada por un alto ejecutivo con el nombre de la persona designada como Encargado CIP.

R4. Cada Entidad Responsable deberá implementar un proceso documentado para delegar autoridad, a menos que no se usen delegaciones. Según se indique en el presente estándar, el Encargado CIP, podrá delegar autoridad para acciones específicas a uno o más delegados. Dichas delegaciones deben estar documentadas incluyendo el nombre y título del delegado, las acciones específicas delegadas, y la fecha de delegación. Las delegaciones deberán ser aprobadas por el Encargado CIP y

actualizadas dentro de 30 días en caso de ser modificadas. Los cambios de delegación no necesitan ser modificados con un cambio en quien delega.

R4 es calificado con Factor de Riesgo por Incumplimiento Bajo (FRIB).

M4. Medida de control o evidencia podrá incluir, pero no está limitada a, un documento fechado aprobado por el Encargado CIP, listando las personas (por nombre o cargo) a quienes se les delega autoridad para aprobar o autorizar ítems específicos identificados.

7.2.4. Planes de Ciberseguridad para Ciber Sistemas SEN de Impacto Bajo

Las Entidades Responsables deberán incluir las secciones descritas a continuación en sus planes de ciberseguridad requeridos en CIP-003 R2.

Las Entidades Responsables con Ciber Sistemas SEN en múltiples calificaciones de impacto podrán utilizar políticas, procedimientos y procesos para sus Ciber Sistemas SEN de Impacto Alto y Medio para completar las distintas secciones en el desarrollo de sus planes de seguridad para Ciber Sistemas SEN de Impacto Bajo. Cada Entidad Responsable podrá desarrollar planes de ciberseguridad para, ya sea activos individuales como para grupos de activos.

Sección 1. Conciencia de Ciberseguridad

Cada Entidad Responsable deberá reforzar, al menos una vez cada 15 meses calendario, sus prácticas de ciberseguridad, las que podrán incluir sus asociadas prácticas de seguridad física.

Sección 2. Controles de Seguridad Física

Cada Entidad Responsable deberá controlar el acceso físico, en base a las necesidades definidas por la Entidad Responsable, para i) el activo o donde se ubiquen Ciber Sistemas SEN de Impacto Bajo dentro de dicho activo, y ii) los Ciber Activos, de existir y según lo especifique la Entidad Responsable, que provean control de acceso electrónico implementados según se indica en la Sección 3. parte 3.1.

Sección 3. Control de Acceso Electrónico

Para cada activo que contenga Ciber Sistemas SEN de Impacto Bajo según lo identificado de acuerdo con CIP-002 R1, la Entidad Responsable deberá implementar controles de acceso electrónico para:

3.1 Permitir solo el acceso electrónico entrante y saliente necesario, según lo defina la Entidad Responsable, para las comunicaciones:

i) entre un(os) Ciber Sistema(s) SEN de Impacto Bajo y un(os) Ciber Activo(s) fuera del activo conteniendo el(los) Ciber Sistema(s) SEN de Impacto Bajo.

ii) que utilicen un protocolo enrutable al entrar o salir del activo conteniendo el Ciber Sistema SEN de Impacto Bajo, y

iii) no utilizadas para protecciones tiempo-sensibles o funciones de control entre Dispositivos Electrónicos Inteligentes (DEI), como por ejemplo comunicaciones que usen protocolos IEC TR-61850-90-5 R-GOOSE.

3.2 Autenticar toda comunicación telefónica (dial-up), de existir, que provea acceso a Ciber Sistema(s) SEN, según capacidad del Ciber Activo.

Sección 4. Respuesta a Incidentes de Ciberseguridad

Cada Entidad Responsable deberá contar con uno o más planes de respuesta a incidentes de ciberseguridad, ya sea por activo o grupo de activos, los que deberán incluir:

4.1 Identificación, clasificación y respuesta a incidentes de ciberseguridad;

4.2 Determinación si un incidente de ciberseguridad es un Incidente de Ciberseguridad Reportable y la subsecuente notificación;

4.3 Identificación de roles y responsabilidades para respuesta a incidentes de ciberseguridad, por grupo o individuos;

4.4 Gestión de incidentes frente a incidentes de ciberseguridad;

4.5 Testeo de planes de respuesta a incidentes de ciberseguridad al menos una vez cada 36 meses, ya sea i) respondiendo a un Incidente de Ciberseguridad Reportable real, ii) usando un ejercicio o ensayo (drill) de un Incidente Ciberseguridad Reportable, o iii) usando un ejercicio operacional de un Incidente de Ciberseguridad Reportable; y

4.6 Actualización de planes de respuesta a incidentes de ciberseguridad, se ser necesario, dentro de 180 días calendario luego de completada una prueba de los planes de respuesta a incidentes de ciberseguridad u ocurrido un Incidente de Ciberseguridad Reportable real.

Sección 5. Mitigación de Riesgos de Código Malicioso en Ciber Activos Transitorios y Medios Removibles

Cada Entidad Responsable deberá implementar, excepto bajo Condiciones Excepcionales CIP, uno o más planes para lograr los objetivos de mitigación de riesgo de introducción de código malicioso a Ciber Sistemas SEN de Impacto Bajo a través del uso de Ciber Activos Transitorios y Medios Removibles. El plan, o planes, deberá(n) incluir:

5.1 Para Ciber Activos Transitorios gestionados por Entidades Responsables, si existen, el uso de uno o una combinación de los siguientes métodos, de manera continua o por demanda (según capacidad del Ciber Activo Transitorio):

i) Software antivirus, incluyendo actualización manual o administrada de firmas o patrones;

ii) Aplicación de lista blanca; u

ii) Otro(s) método(s) para mitigar la introducción de código malicioso.

5.2 Para Ciber Activos Transitorios gestionados por terceros distintos a las Entidades Responsables, si existen:

i) Uso de uno o una combinación de los siguientes métodos previo a conectar Ciber Activos Transitorios a un Ciber Sistema SEN de Impacto Bajo (según capacidad del Ciber Activo Transitorio):

- Revisión del nivel de actualización del antivirus;
- Revisión del proceso de actualización del antivirus utilizado por terceros;
- Revisión de la aplicación de lista blanca utilizada por terceros;
- Revisión del uso de sistemas operativos vivos (Live OS) y software ejecutable solo desde medios de lectura (read-only);
- Revisión del reforzamiento (Hardening) de sistemas utilizado por terceros; u
- Otros métodos para mitigar la introducción de código malicioso

ii) Para cualquier método utilizado conforme a i), las Entidades Responsables deberán determinar si se necesitan acciones de mitigación adicionales e implementarlas previo a conectar Ciber Activos Transitorios.

5.3 Para Medios Removibles, el uso de los siguientes métodos:

i) Método(s) para detectar código malicioso en Medios Removibles usando Ciber Activos distintos a un Ciber Sistema SEN; y

ii) Mitigación de amenazas de código malicioso detectadas en Medios Removibles previo conectar dichos Medios en un Ciber Sistema SEN de Impacto Bajo.

7.2.5. Entrada en Vigor

El presente estándar CIP-003 entrará en vigor al momento de su aprobación por parte de la SEC y posterior publicación en la página web del Coordinador. Las Entidades Responsables tendrán un periodo de marcha blanca para implementar cada uno de los requerimientos en el estándar CIP-003 de acuerdo con los plazos máximos especificados en ANEXO 1, columna Marcha Blanca.

7.3. CIP-004: Ciber Seguridad – Personal y Capacitación

7.3.1. Propósito

Minimizar riesgos contra actos de individuos que accedan a Ciber Sistemas SEN, que podrían conducir a una mala operación o inestabilidad del SEN, exigiendo un adecuado nivel de Evaluación de Riesgos, conciencia de seguridad y capacitación del personal, como medidas apoyo para la protección de Ciber Sistemas SEN.

7.3.2. Aplicabilidad Específica y Excepciones

No existe aplicabilidad específica adicional a lo definido en el punto 3 para el estándar CIP-004.

Se exceptúan los Ciber Activos asociados con redes de comunicaciones y enlaces de comunicaciones de datos entre Perímetros de Seguridad Electrónica (PSE) independientes.

7.3.3. Requerimientos (R) y Medidas de Control (M)

R1. Cada Entidad Responsable deberá implementar uno o más Procesos Documentados que en su conjunto incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-004 R1 – Programa de Conciencia de Seguridad.

R1 es calificado con Factor de Riesgo por Incumplimiento Bajo (FRIB).

M1. Medida de control o evidencia aceptable debe incluir cada uno de los Procesos Documentados aplicables que en su conjunto incluyan cada uno de los requerimientos aplicables en Tabla CIP-004 R1 – Programa de Conciencia de Seguridad, y evidencia adicional para demostrar su implementación según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-004 R1 – Programa de Conciencia de Seguridad			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
1.1	✓ Ciber Sistemas SEN de Impacto Alto; y ✓ Ciber Sistemas SEN de Impacto Medio.	Conciencia de seguridad que, al menos trimestralmente, refuerce las prácticas de ciberseguridad (lo cual puede incluir las prácticas de seguridad física asociadas) para el personal de la Entidad Responsable que tenga acceso electrónico autorizado o acceso físico (no escoltado) a Ciber Sistemas SEN.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación validando que el reforzamiento trimestral se realizó. Ejemplos de evidencia del reforzamiento pueden incluir, pero no estar limitado a, copias fechadas de la información utilizada para reforzar la conciencia de seguridad, así como evidencia de la distribución de esta, tal como: • Comunicaciones directas (Ej.: e-mails, memos o capacitación e-learning); o • Comunicaciones indirectas (Ej.: posters, intranet o brochures); o • Apoyo gerencial y reforzamiento presencial (Ej.: reuniones o presentaciones).

R2. Cada Entidad Responsable deberá implementar uno o más Programas de capacitación en ciberseguridad sobre roles, funciones o responsabilidades de los individuos los cuales conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en Tabla CIP-004 R2 – Programa de Capacitación en Ciberseguridad.

R2 es calificado con Factor de Riesgo por Incumplimiento Bajo (FRIB).

M2. Medida de control o evidencia aceptable debe incluir el Programa de capacitación que incluya cada uno de los requerimientos aplicables en Tabla CIP-004 R2 – Programa de Capacitación en Ciberseguridad, y evidencia adicional para demostrar la implementación del(los) Programa(s).

Tabla CIP-004 R2 – Programa de Capacitación en Ciberseguridad			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
2.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Capacitación conteniendo las siguientes materias: 2.1.1 Políticas de ciberseguridad. 2.1.2 Control de acceso físico. 2.1.3 Control de acceso. electrónico. 2.1.4 Programa de control de visitas. 2.1.5 Manipulación y almacenamiento de información de Ciber Sistemas SEN. 2.1.6 Identificación de un Incidente de Ciberseguridad y notificación inicial de acuerdo con el Plan de respuesta a incidentes de la Entidad. 2.1.7 Plan de Recuperación para Ciber Sistemas SEN. 2.1.8 Respuesta a Incidentes de Ciberseguridad. 2.1.9 Riesgos de ciberseguridad asociados con interconectividad electrónica e interoperabilidad de Ciber Sistemas SEN con otros Ciber Activos, incluyendo CAT y MR.	Medida de control o evidencia puede incluir, pero no está limitada a, material de la capacitación tal como presentaciones PowerPoint, apuntes del instructor, apuntes de los alumnos, folletos, u otro material de la capacitación.

Tabla CIP-004 R2 – Programa de Capacitación en Ciberseguridad			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
2.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Se requiere completar la capacitación en ítem 2.1 previo a otorgar la autorización de acceso electrónico y la autorización de acceso físico no escoltado para el Ciber Activo que corresponda, excepto durante Circunstancias Excepcionales CIP.	Medida de control o evidencia puede incluir, pero no está limitada a, registro de las capacitaciones y documentación de cuando se invocaron Circunstancias Excepcionales CIP.
2.3	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Se requiere completar la capacitación en ítem 2.1 al menos una vez cada 15 meses calendario.	Medida de control o evidencia puede incluir, pero no está limitada a, registros individuales fechados de las capacitaciones.

R3. Cada Entidad Responsable deberá implementar uno o más Programas documentados de evaluación de riesgos del personal para obtener y retener acceso electrónico autorizado o acceso físico no escoltado autorizado a Ciber Sistemas SEN, los cuales conjuntamente incluyan cada uno de los requerimientos (columna Ítem) en la Tabla CIP-004 R3 – Programa de Evaluación de Riegos del Personal.

R3 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M3. Medida de control o evidencia aceptable debe incluir el(los) Programa(s) documentado(s) de evaluación de riesgos del personal que en su conjunto incluyan cada uno de los requerimientos aplicables en CIP-004 R3 – Programa de Evaluación de Riegos del Personal, y evidencia adicional para demostrar la implementación del(los) Programa(s).

Tabla CIP-004 R3 – Programa de Evaluación de Riegos del Personal			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
3.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Proceso para confirmar identidad.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación del proceso de la Entidad Responsable para confirmar identidad.

Tabla CIP-004 R3 – Programa de Evaluación de Riegos del Personal			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
3.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Proceso para realizar una verificación de antecedentes penales de los últimos 7 años, como parte de la evaluación de riesgos de cada persona, que incluya: 3.2.1 Residencia actual, independiente de la duración; y 3.2.2 Otras residencias donde, previo a los últimos 7 años a la fecha de realizada la verificación de antecedentes penales, la persona ha residido por 6 meses consecutivos o más. Si no es posible realizar la verificación de antecedentes por los 7 años, realizar la verificación para tanto años de historia de antecedentes como sea posible y documentar las razones por las cuales no fue posible realizar la verificación por los 7 años.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación del Proceso de la Entidad Responsable para para realizar una verificación de antecedentes penales por 7 hasta años de historia.

Tabla CIP-004 R3 – Programa de Evaluación de Riegos del Personal			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
3.3	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Criterios o Proceso para evaluar la verificación de antecedentes penales a fin de otorgar la autorización de accesos.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación del Proceso de la Entidad Responsable para evaluar verificación de antecedentes penales.
3.4	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Criterios o Proceso para verificar que la evaluación de riesgos del personal realizado para terceros contratistas o proveedores de servicio son conducidos de acuerdo con lo especificado en ítems 3.1 a 3.3.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación de criterios o Proceso de la Entidad Responsable para la verificación de evaluaciones de riesgos del personal de terceros contratistas y proveedores de servicios.
3.5	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Proceso para asegurar que individuos con acceso electrónico autorizado o acceso físico no escoltado autorizado han completado una evaluación de riesgos del personal de acuerdo con lo especificado en ítems 3.1 a 3.4, dentro de los ultimo 7 años.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación del Proceso para asegurar que individuos con acceso electrónico autorizado o acceso físico no escoltado autorizado han completado una evaluación de riesgos del personal dentro de los últimos 7 años.

R4. Cada Entidad Responsable deberá implementar uno o más Programas de administración de accesos los cuales conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en Tabla CIP-004 R4 – Programa de Administración de Accesos.

R4 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M4. Medida de control o evidencia aceptable debe incluir el Programa Documentado el cual incluya cada uno de los requerimientos aplicables en Tabla CIP-004 R4 – Programa de Administración de Accesos, y evidencia adicional para demostrar que el

Programa fue implementado según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-004 R4 – Programa de Administración de Accesos			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
4.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Proceso para autorizar, según lo requiera la Entidad Responsable, excepto para Circunstancias Excepcionales CIP: 4.1.1 Acceso electrónico; 4.1.2 Acceso físico no escoltado a un Perímetro de Seguridad Física (PSF); y 4.1.3 Acceso a localizaciones de almacenamiento designados, sean electrónicos o físicos, de información de Ciber Sistemas SEN.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación fechada del Proceso para autorizar acceso electrónico, acceso físico no escoltado a un Perímetro de Seguridad Física (PSF) y acceso a localizaciones de almacenamiento designados, sean electrónicos o físicos, de información de Ciber Sistemas SEN.
4.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Verificar, al menos trimestralmente, que individuos que cuentan con acceso electrónico o acceso físico no escoltado activo, tienen registros de autorización.	Medida de control o evidencia puede incluir, pero no está limitada a: • Documentación fechada de la verificación entre la lista generada por sistema de individuos que han sido autorizados por sistema (base de datos de workflow), y una lista generada por sistema del personal que tiene acceso (listado de cuenta de usuarios), o • Documentación fechada de la verificación entre la lista de individuos que han sido autorizados por acceso (formularios de autorización), y una lista de individuos provistos de acceso (formularios de provisión o listado de cuentas compartidas).

Tabla CIP-004 R4 – Programa de Administración de Accesos			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
4.3	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Para acceso electrónico, verificar al menos una vez cada 15 meses calendario, que todas las cuentas de usuario, grupos de cuentas de usuarios o categorías de rol de usuario, y sus privilegios específicos asociados, son correctos y son aquellos que la Entidad Responsable determina son necesarios.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación de la revisión que incluya todo lo siguiente: • Una lista fechada de todas las cuentas, grupos de cuentas, o roles dentro del sistema; • Una descripción resumida de los privilegios asociados con cada grupo o rol; • Cuentas asignadas al grupo o rol; y • Evidencia fechada verificando que los privilegios para el grupo son autorizados y adecuados para la función del trabajo realizado por las personas asignadas a cada cuenta.
4.4	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Verificar, al menos una vez cada 15 meses calendario, que el acceso a localizaciones designadas para el almacenamiento de información de Ciber Sistemas SEN, sea físico o electrónico, son correctos y son aquellos que la Entidad Responsable determina son necesarios.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación de la revisión que incluya todo lo siguiente: • Listado fechado de autorizaciones para acceder a información de Ciber Sistemas SEN; • Cualquier privilegio(s) asociado(s) con las autorizaciones; y • Evidencia fechada verificando que las autorizaciones y privilegios fueron confirmados como correctos y que son mínimos necesarios para realizar las funciones del trabajo asignado.

R5. Cada Entidad Responsable deberá implementar uno o más Programas Documentados de revocación (o eliminación) de accesos los cuales conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en Tabla CIP-004 R5 – Revocación de Accesos.

R5 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M5. Medida de control o evidencia aceptable debe incluir el Programa Documentado que incluya cada uno de los requerimientos (columna Ítems) aplicables en Tabla CIP-004 R5 – Revocación de Accesos, y evidencia adicional para demostrar su implementación según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-004 R5 – Revocación de Accesos			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
5.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Un Proceso para iniciar la eliminación (revocación) de la capacidad de un individuo para el acceso físico no escoltado y el acceso remoto interactivo una vez terminada una acción, y una eliminación completa dentro de 24 horas de terminada la acción. Revocar o eliminar la capacidad de acceso puede ser diferente a eliminar, deshabilitar, revocar o remover todos los derechos de acceso.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación que incluya todo lo siguiente: • Workflow fechado o formulario término de contrato de término de contrato verificando revocación de acceso asociado al término de la acción; y • Logs u otra prueba que demuestre que dicha persona ya no tiene acceso.

Tabla CIP-004 R5 – Revocación de Accesos			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
5.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Para reasignaciones o transferencias, revocar el acceso electrónico autorizado o el acceso físico no escoltado autorizado a individuos, que la Entidad Responsable defina no son necesarios, al final del día calendario siguiente a la fecha que la Entidad determine que el individuo no requiere más dicho acceso.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación que incluya todo lo siguiente: • Workflow fechado o formulario término de contrato verificando una revisión de acceso físico y lógico; y • Logs u otra prueba que demuestre que dicha persona no tiene ningún acceso que la Entidad Responsable defina no es necesario.
5.3	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Para acciones de término, revocar acceso de individuos a localizaciones designadas para el almacenamiento de información de Ciber Sistemas SEN, sea físico o electrónico (a menos que ya haya sido revocado de acuerdo con requerimiento R5.1) al final del día calendario siguiente a la fecha efectiva de término de la acción.	Medida de control o evidencia puede incluir, pero no está limitada a, formularios workflow o término de contrato verificando revocación de acceso a áreas físicas designadas o ciber sistemas conteniendo información de Ciber Sistemas SEN asociados a acciones de término fechadas dentro del día calendario siguiente al término de la acción.
5.4	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE.	Para acciones de término, revocar cuentas de usuarios no compartidas de individuos dentro de 30 días calendario de la fecha efectiva de término de la acción.	Medida de control o evidencia puede incluir, pero no está limitada a, formularios workflow o término de contrato verificando revocación de acceso para cualquier Ciber Activo individual y aplicaciones de software definidas como necesarias para completar la revocación de acceso y fechadas dentro de 30 días calendario del término de la acción.

Tabla CIP-004 R5 – Revocación de Accesos			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
5.5	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE.	Para acciones de término, cambiar contraseñas para cuentas compartidas conocidas por los usuarios dentro de 30 días calendario de terminada de acción. Para reasignaciones y transferencias, cambiar contraseñas para cuentas compartidas conocidas por los usuarios dentro de 30 días calendario seguidos a la fecha en que la Entidad Responsable determine que el individuo no requiere más conservar el acceso. Si la Entidad Responsable determina y documenta que por circunstancias operativas extenuantes se requiere un periodo más largo, cambiar las passwords dentro de 10 días calendario seguido al fin de las circunstancias operativas.	Medida de control o evidencia puede incluir, pero no está limitada a: • Formulario workflow o término de contrato demostrando reseteo de contraseñas dentro de 30 días calendario del término; • Formulario workflow o término de contrato demostrando reseteo de contraseñas dentro de 30 días calendario de la reasignación o transferencia; o • Documentación de las circunstancias operativas extenuantes o formulario workflow o término de contrato demostrando reseteo de contraseñas dentro de 10 días calendario seguido al fin de la circunstancia operativa.

7.3.4. Entrada en Vigor

El presente estándar CIP-004 entrará en vigor al momento de su aprobación por parte de la SEC y posterior publicación en la página web del Coordinador. Las Entidades Responsables tendrán un periodo de marcha blanca para implementar cada uno de los requerimientos en el estándar CIP-004 de acuerdo con los plazos máximos especificados en ANEXO 1, columna Marcha Blanca.

7.4. CIP-005: Ciber Seguridad – Perímetro de Seguridad Electrónica (PSE)

7.4.1. Propósito

Administrar el acceso electrónico a Ciber Sistemas SEN especificando un Perímetro de Seguridad Electrónica (PSE) controlado en apoyo a la protección de Ciber Sistemas SEN contra eventos o actos que podrían conducir a una mala operación o inestabilidad del SEN.

7.4.2. Aplicabilidad Específica y Excepciones

No existe aplicabilidad específica adicional a lo definido en el punto 3 para el estándar CIP-005.

Se exceptúan los Ciber Activos asociados con redes de comunicaciones y enlaces de comunicaciones de datos entre Perímetros de Seguridad Electrónica (PSE) independientes.

7.4.3. Requerimientos (R) y Medidas de Control (M)

R1. Cada Entidad Responsable deberá implementar uno o más Procesos Documentados los cuales conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-005 R1 – Perímetro de Seguridad Electrónica (PSE).

R1 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M1. Medida de control o evidencia aceptable debe incluir cada uno de los Procesos Documentados aplicables que en su conjunto incluyan cada uno de los requerimientos aplicables en la Tabla CIP-005 R1 – Perímetro de Seguridad Electrónica (PSE), y evidencia adicional para demostrar su implementación según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-005 R1 – Perímetro de Seguridad Electrónica (PSE)			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
1.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados CAP.	Todos los Ciber Sistemas aplicables conectados a una red vía un protocolo enrutable deberán residir dentro de un PSE definido.	Medida de control o evidencia puede incluir, pero no está limitada a, una lista con todos lo PSEs incluyendo todos sus Ciber Activos identificables de manera única aplicables conectados vía un protocolo enrutable dentro de un PSE.

Tabla CIP-005 R1 – Perímetro de Seguridad Electrónica (PSE)			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
1.2	✓ Ciber Sistemas SEN de Impacto Alto con CEE y sus asociados CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Toda CEE debe ser a través de un PAE definido.	Medida de control o evidencia puede incluir, pero no está limitada a, diagramas de redes que muestren todas las vías de comunicación enrutable externa y PAEs identificados.
1.3	✓ PAEs para Ciber Sistemas SEN de Impacto Alto; y ✓ PAEs para Ciber Sistemas SEN de Impacto Medio.	Requiere permiso de acceso entrante y saliente, incluyendo las razones para otorgar el acceso, y denegación de todos los otros accesos por defecto.	Medida de control o evidencia puede incluir, pero no está limitada a, una lista de reglas (firewalls, lista de control de acceso, etc.) que demuestre que solo acceso autorizado es permitido y que cada regla de acceso tiene una razón documentada.
1.4	✓ Ciber Sistemas SEN de Impacto Alto con conectividad telefónica (dial-up) y sus asociados CAP; y	Donde sea factible, realizar autenticación cuando se establezca conectividad telefónica (dial-up) con Ciber Activos aplicables.	Medida de control o evidencia puede incluir, pero no está limitada a, un Proceso Documentado que describa como la Entidad Responsable provee acceso autenticado a través de

	✓ Ciber Sistemas SEN de Impacto Medio con conectividad telefónica (dial-up) y sus asociados CAP.		cada conexión telefónica (dial-up).
1.5	✓ PAEs para Ciber Sistemas SEN de Impacto Alto; y ✓ PAEs para Ciber Sistemas SEN de Impacto Medio en CDCs y CCs.	Contar con uno o más métodos para detectar comunicaciones maliciosas conocidas o sospechosas para comunicaciones entrantes y salientes.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación que demuestre la implementación de métodos para detectar comunicaciones maliciosas (Ej.: sistemas de detección de intrusos, firewall para capa de aplicaciones, etc.)

R2. Cada Entidad Responsable que permita Acceso Remoto Interactivo (ARI) a Ciber Activos SEN deberá implementar uno o más Procesos Documentados los cuales conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables, donde sea técnicamente factible, en la Tabla CIP-005 R2 – Administración de Acceso Remoto Interactivo (ARI).

R2 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M2. Medida de control o evidencia aceptable debe incluir el Proceso Documentado que aborde cada uno de los requerimientos aplicables en la Tabla CIP-005 R2 – Administración de Acceso Remoto Interactivo (ARI), y evidencia adicional para demostrar su implementación según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-005 R2 – Administración de Acceso Remoto Interactivo (ARI)			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
2.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados CAP.	Utilizar un Sistema Intermedio de modo que el Ciber Activo iniciando ARI no acceda directamente a un aplicable Ciber Activo.	Medidas de control o evidencia pueden incluir, pero no están limitadas a, diagramas de redes o documentos de arquitectura.
2.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados CAP.	Para todas las sesiones de ARI, utilizar encriptación que termine en un Sistema Intermedio.	Medida de control o evidencia puede incluir, pero no está limitada a, documentos de arquitectura detallando donde inicia y termina la encriptación.
2.3	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados CAP.	Requiere autenticación multi-factor para todas las sesiones ARI.	Medida de control o evidencia puede incluir, pero no está limitada a, documentos de arquitectura detallando los factores de autenticación utilizados. Ejemplo de autenticación, puede incluir, pero no está limitado a: • Algo que los individuos conozcan tales como contraseñas o PINs (Número de Identificación Personal), esto no incluye ID de usuario; • Algo que los individuos tienen tales como tokens, certificados digitales, tarjetas inteligentes (smart cards); o • Algo del individuo tal como huellas digitales, escaneo de iris o retina, u otras características biométricas.

7.4.4. Entrada en Vigor

El presente estándar CIP-005 entrará en vigor al momento de su aprobación por parte de la SEC y posterior publicación en la página web del Coordinador. Las Entidades Responsables tendrán un periodo de marcha blanca para implementar cada uno de los requerimientos en el estándar CIP-005 de acuerdo con los plazos máximos especificados en ANEXO 1, columna Marcha Blanca.

7.5. CIP-006: Ciber Seguridad – Seguridad Física de Ciber Sistemas SEN

7.5.1. Propósito

Administrar el acceso físico a Ciber Sistemas SEN especificando un Plan de seguridad física en apoyo a la protección de Ciber Sistemas SEN contra eventos o actos que podrían conducir a una mala operación o inestabilidad del SEN.

7.5.2. Aplicabilidad Específica y Excepciones

No existe aplicabilidad específica adicional a lo definido en el punto 3 para el estándar CIP-006.

Se exceptúan los Ciber Activos asociados con redes de comunicaciones y enlaces de comunicaciones de datos entre Perímetros de Seguridad Electrónica (PSE) independientes.

7.5.3. Requerimientos (R) y Medidas de Control (M)

R1. Cada Entidad Responsable deberá implementar uno o más Planes de seguridad física documentados los cuales conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-006 R1 – Plan de Seguridad Física.

R1 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M1. Medida de control o evidencia aceptable debe incluir cada uno de los Planes de seguridad física que en su conjunto incluyan cada uno de los requerimientos aplicables en la Tabla CIP-006 R1 – Plan de Seguridad Física, y evidencia adicional para demostrar la implementación del plan (o planes) según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-006 R1 – Plan de Seguridad Física			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
1.1	✓ Ciber Sistemas SEN de Impacto Medio sin CEE; y ✓ Sistemas de Control de Acceso Físico (SCAF) asociados con: • Ciber Sistemas SEN de Impacto Alto; o • Ciber Sistemas SEN de Impacto Medio con CEE.	Definir controles operacionales o procedimentales para restringir acceso físico.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación demostrando que los controles operacionales o procedimentales existen.
1.2	✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Utilizar al menos un control de acceso físico para permitir acceso físico no escoltado a cada Perímetro de seguridad física (PSF) aplicable a solo aquellos individuos que tienen acceso físico no escoltado autorizado.	Medida de control o evidencia puede incluir, pero no está limitada a, una sección en el Plan de seguridad física que describa cada PSF y como el acceso físico no escoltado es controlado por uno o más métodos distintos y prueba de que el acceso físico no escoltado es restringido solo a individuos autorizados, como por ejemplo una lista de individuos autorizados acompañada de sus logs o registros de acceso.
1.3	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP.	Donde sea técnicamente factible, utilizar dos o más controles de acceso físico distinto (esto no requiere dos sistemas de control de acceso físico completamente independientes) para, de manera colectiva, permitir acceso físico no escoltado a PSFs a solo aquellos individuos que tienen acceso físico no escoltado autorizado.	Medida de control o evidencia puede incluir, pero no está limitada a, una sección en el Plan de seguridad física que describa cada PSF y como el acceso físico no escoltado es controlado por dos o más métodos distintos y prueba de que el acceso físico no escoltado es restringido solo a individuos autorizados, como por ejemplo una lista de individuos autorizados acompañada de sus logs o registros de acceso.

Tabla CIP-006 R1 – Plan de Seguridad Física			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
1.4	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y PAC; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Monitorear acceso no autorizado a través de un punto de acceso físico en un PSF.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación de controles que monitorean acceso no autorizado a través de un punto de acceso físico en un PSF.
1.5	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y PAC; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Emitir una alarma o alerta en respuesta a un acceso no autorizado detectado a través de un punto de acceso físico en un PSF, al personal identificado en el Plan de respuesta a incidentes de ciberseguridad del SEN, dentro de 15 minutos de ser detectada.	Medida de control o evidencia puede incluir, pero no está limitada a, una sección en el Plan de seguridad física que describa la emisión de una alarma o alerta en respuesta a un acceso no autorizado detectado a través de un punto de acceso físico en un PSF, y evidencia adicional de que la alarma o alerta fue emitida y comunicada según lo identificado en el Plan de respuesta a incidentes de ciberseguridad del SEN, tales como una alarma manual o electrónica o logs de alertas, logs en teléfono celular o en papel, u otra evidencia donde se documente que la alarma o alerta fue generada y comunicada.
1.6	✓ Sistemas de Control de Acceso Físico (SCAF) asociados con: • Ciber Sistemas SEN de Impacto Alto; o • Ciber Sistemas SEN de Impacto Medio con CEE.	Monitorear cada Sistema de Control de Acceso Físico (SCAF) por acceso no autorizado a un SCAF.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación de controles que monitorean acceso no autorizado a un SCAF.

Tabla CIP-006 R1 – Plan de Seguridad Física			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
1.7	✓ Sistemas de Control de Acceso Físico (SCAF) asociados con: • Ciber Sistemas SEN de Impacto Alto; o • Ciber Sistemas SEN de Impacto Medio con CEE.	Emitir una alarma o alerta en respuesta a un acceso físico no autorizado detectado a un SCAF, al personal identificado en el Plan de respuesta a incidentes de ciberseguridad del SEN, dentro de 15 minutos de ser detectada.	Medida de control o evidencia puede incluir, pero no está limitada a, una sección en el Plan de seguridad física que describa la emisión de una alarma o alerta en respuesta a un acceso no autorizado a un SCAF, y evidencia adicional de que la alarma o alerta fue emitida y comunicada según lo identificado en el Plan de respuesta a incidentes de ciberseguridad del SEN, tales como logs de alarmas o alertas, logs en teléfono celular o en papel, u otra evidencia donde se documente que la alarma o alerta fue generada y comunicada
1.8	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y PAC; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Log o registro de entrada (a través de medios automáticos o del personal que controla la entrada) de cada individuo con acceso físico no escoltado a cada PSF, con información para identificar al individuo y la fecha y hora de entrada.	Medida de control o evidencia puede incluir, pero no está limitada a, una sección en el Plan de seguridad física que describa el registro y grabación de entrada física a cada PSF, y evidencia adicional para demostrar que este registro ha sido implementado, tal como registros de acceso físico a PSFs que muestren al individuo y la fecha y hora de entrada al PSF.
1.9	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y PAC; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Retener logs de entrada de acceso físico de individuos con acceso físico no escoltado autorizado a cada PSF, por al menos 90 días calendario.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación fechada como logs de acceso a PSFs que muestren la fecha y hora de entrada al PSF.

Tabla CIP-006 R1 – Plan de Seguridad Física			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
1.10	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados PAC; y ✓ Ciber Sistemas SEN de Impacto Medio en CDCs y CCs y sus asociados CAP.	Restringir acceso físico a cables y otros componentes de comunicación no programable utilizados para conexiones entre Ciber Activos aplicables dentro de un mismo PSE en aquellas instancias cuando dichos cables y componentes están localizadas fuera de un PSF. Donde las restricciones de acceso físico a dichos cables y componentes no son implementadas, la Entidad Responsable deberá documentar e implementar una o más de las siguientes medidas: • Encriptación de los datos que transitan en dichos cables y componentes; o • Monitoreo del estado de enlaces de comunicaciones compuestos por dichos cables y componentes, y emisión de una alarma o alerta en respuesta a fallas de comunicación detectadas, al personal identificado en el Plan de respuesta a incidentes de ciberseguridad del SEN, dentro de 15 minutos de ser detectada. • Una protección lógica igualmente efectiva.	Medida de control o evidencia puede incluir, pero no está limitada a, registros de la implementación, por parte de la Entidad Responsable, de las restricciones de acceso físico (Ej.: cables y componentes protegidos por ductos o bandejas para cables), encriptación, monitoreo, o protecciones lógicas igualmente efectivas.

R2. Cada Entidad Responsable deberá implementar uno o más Programas Documentados de control de visitas que incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-006 R2 – Programa de Control de Visitas.

R2 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M2. Medida de control o evidencia aceptable debe incluir uno o más Programas de control de visitas documentados los cuales conjuntamente incluyan cada uno de los requerimientos aplicables en la Tabla CIP-006 R2 – Programa de Control de Visitas, y evidencia adicional para demostrar su implementación según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-006 R2 – Programa de Control de Visitas			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
2.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y PAC; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Requiere acceso escoltado continuo de visitas (individuos que están provistos de acceso, pero que están autorizados para acceso físico no escoltado) dentro de cada PSF, excepto durante Condiciones Excepcionales CIP.	Medida de control o evidencia puede incluir, pero no está limitada a, una sección en el Programa de Control de Visitas que requiere acceso escoltado continuo de visitas dentro de PSFs, y evidencia adicional para demostrar que el proceso fue implementado, como logs o registros de visitas.
2.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y PAC; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Requiere registro manual o automático de entrada y salida de visitas en un PSF que incluya fecha y hora de la entrada inicial y última salida, el nombre del visitante, y el nombre de una persona de contacto responsable de la visita, excepto durante Condiciones Excepcionales CIP.	Medida de control o evidencia puede incluir, pero no está limitada a, una sección en el Programa de Control de Visitas que requiere acceso escoltado continuo de visitas dentro de PSFs, y evidencia adicional para demostrar que el proceso fue implementado, como registros de visitas fechados que incluyan la información requerida.
2.3	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y PAC; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE y CAP.	Retener o guardar registros del visitante por al menos 90 días calendario.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación que muestre que los registros han sido guardados o retenidos por al menos 90 días calendario.

R3. Cada Entidad Responsable deberá implementar uno o más Programas de prueba y mantenimiento de Sistemas de Control de Acceso Físico (SCAF) documentados que en su conjunto incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-006 R3 – Programas de Prueba y Mantenimiento de SCAF.

R3 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M3. Medida de control o evidencia aceptable debe incluir cada uno de los Programas de prueba y mantenimiento de Sistemas de Control de Acceso Físico (SCAF) documentados los cuales conjuntamente incluyan cada uno de los requerimientos aplicables en la Tabla CIP-006 R3 – Programa de Prueba y Mantenimiento de SCAF, y evidencia adicional para demostrar su implementación según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-006 R3 – Programa de Prueba y Mantenimiento de SCAF			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
3.1	✓ Sistemas de Control de Acceso Físico (SCAF) asociados con: • Ciber Sistemas SEN de Impacto Alto; o • Ciber Sistemas SEN de Impacto Medio con CEE ✓ Hardware o dispositivos montados localmente en PSF asociados con: • Ciber Sistemas SEN de Impacto Alto; o • Ciber Sistemas SEN de Impacto Medio con CEE.	Realizar mantenimiento y pruebas de cada SCAF y hardware o dispositivos montados localmente en PSFs, al menos una vez cada 24 meses calendario para asegurar su correcto funcionamiento.	Medida de control o evidencia puede incluir, pero no está limitada a, programas de mantenimiento y pruebas provistos para testear cada SCAF y hardware o dispositivos montados localmente asociados con PSFs, al menos una vez cada 24 meses calendario, y evidencia adicional para demostrar que las pruebas fueron realizadas, tal como registros de mantenimiento fechados, u otra documentación que demuestre que el mantenimiento y pruebas han sido realizados en cada dispositivo o sistema aplicable al menos una vez cada 24 meses calendario.

7.5.4. Entrada en Vigor

El presente estándar CIP-006 entrará en vigor al momento de su aprobación por parte de la SEC y posterior publicación en la página web del Coordinador. Las Entidades Responsables tendrán un periodo de marcha blanca para implementar cada uno de los requerimientos en el estándar CIP-006 de acuerdo con los plazos máximos especificados en ANEXO 1, columna Marcha Blanca.

7.6. CIP-007: Ciber Seguridad – Gestión de la Seguridad de Sistemas

7.6.1. Propósito

Gestionar la seguridad de sistemas especificando un conjunto selecto de requerimientos técnicos, operacionales y procedimentales en apoyo a la protección de Ciber Sistemas SEN contra eventos o actos que podrían conducir a una mala operación o inestabilidad del SEN.

7.6.2. Aplicabilidad Específica y Excepciones

No existe aplicabilidad específica adicional a lo definido en el punto 3 para el estándar CIP-007.

Se exceptúan los Ciber Activos asociados con redes de comunicaciones y enlaces de comunicaciones de datos entre Perímetros de Seguridad Electrónica (PSE) independientes.

7.6.3. Requerimientos (R) y Medidas de Control (M)

R1. Cada Entidad Responsable deberá implementar uno o más Procesos Documentados los cuales conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-007 R1 – Puertos y Servicios.

R1 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M1. Medida de control o evidencia aceptable debe incluir los Procesos Documentados que en su conjunto incluyan cada uno de los requerimientos aplicables en la Tabla CIP-007 R1 – Puertos y Servicios, y evidencia adicional para demostrar su implementación según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-007 R1 – Puertos y Servicios			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
1.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE, SCAF, y CAP.	Donde sea técnicamente factible, habilitar solo puertos de acceso lógicos de redes que hayan sido definidos necesarios por la Entidad Responsable, incluyendo servicios o rangos de puertos requeridos para manipular puertos dinámicos. Si un dispositivo no tiene provisión para deshabilitar o restringir puertos lógicos entonces los puertos que están abiertos son considerados necesarios.	Medidas de control o evidencias pueden incluir, pero no están limitadas a: • Documentación de la necesidad de todos los puertos habilitados en todos los Ciber Activos aplicables y puntos de acceso electrónico, individualmente o por grupo; • Listado de puertos en modo escucha en Ciber Activos, individualmente o por grupo, ya sea de los archivos de configuración del dispositivo, de la salida de comando (como netstat), o escaneo de red de puertos abiertos; o • Archivos de configuración de cortafuegos (firewalls) host-based u otro mecanismo a nivel de dispositivo que solo permita dispositivos necesarios y rechace o niegue todos los otros.
1.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados CAP y componentes de comunicación no programable localizados dentro de un PSE y un PSF; y ✓ Ciber Sistemas SEN de Impacto Medio en CDCs y CCs y sus asociados CAP y componentes de comunicación no programables localizados dentro de un PSE y un PSF.	Proteger contra el uso de puertos físicos de entrada/salida innecesarios utilizados para conectividad de red, comandos de consola, o Medios Removibles.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación mostrando los tipos de protección de puertos físicos de entrada/salida, sea lógicamente a través de configuración de sistemas, o físicamente usando un candado (lock) de puerto o señalización.

R2. Cada Entidad Responsable deberá implementar uno o más Procesos Documentados los cuales conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-007 R2 – Administración de Parches de Seguridad.

R2 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M2. Medida de control o evidencia aceptable debe incluir los Procesos Documentados que en su conjunto incluyan cada uno de los requerimientos aplicables en la Tabla CIP-007 R2 – Administración de Parches de Seguridad, y evidencia adicional para demostrar su implementación según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-007 R2 – Administración de Parches de Seguridad			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
2.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF, y CAP.	Un proceso de administración de parches para rastrear o dar trazabilidad, evaluar, e instalar parches de ciberseguridad para los Ciber Activos aplicables. La parte de rastreo deberá incluir la identificación de una fuente de origen (o fuentes) de donde la Entidad Responsable pueda rastrear la liberación de parches de ciberseguridad para Ciber Activos aplicables que son actualizables y para los cuales existe una fuente de origen de parches.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación del proceso de administración de parches y documentación o lista de fuentes de origen que son monitoreadas, ya sea a nivel individual de Ciber Sistema SEN o Ciber Activo.
2.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF, y CAP.	Al menos una vez cada 35 días calendario, evaluar los parches de seguridad aplicables que hayan sido lanzados desde la última evaluación desde la(s) fuente(s) identificada(s) en el ítem 2.1.	Medida de control o evidencia puede incluir, pero no está limitada a, una evaluación conducida por, referenciada por, o en representación de una Entidad Responsable de los parches de seguridad lanzados por las fuentes documentadas al menos una vez cada 35 días calendario.

Tabla CIP-007 R2 – Administración de Parches de Seguridad			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
2.3	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF, y CAP.	Para los parches aplicables identificados en ítems 2.2, y dentro de los 35 días calendario de completada la evaluación, tomar una de las siguientes acciones: • Aplicar los parches aplicables; o • Crear Plan de mitigación fechado; o • Revisar un Plan de mitigación existente. Los Planes de mitigación deberán incluir las acciones planificadas por las Entidades Responsables para mitigar las vulnerabilidades abordadas por cada parche de seguridad y un cronograma para completar dichas mitigaciones.	Medidas de control o evidencias pueden incluir, pero no están limitadas a: • Registro de instalación de parches (Ej.: exportaciones de herramientas de administración automática de parches que provean las fechas de instalación, verificación de revisión de componentes de software de Ciber Activos SEN, o exportación de registros que muestren que el software ha sido instalado); o • Un Plan fechado mostrando cuándo y cómo la vulnerabilidad será abordada, que incluya documentación de las acciones a ser tomadas por parte de las Entidades Responsables para mitigar las vulnerabilidades abordadas por cada parche de seguridad y un cronograma para completar dichas mitigaciones.
2.4	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF, y CAP.	Cada Plan de mitigación creado o revisado según ítem 2.3, se debe ser implementado dentro de los plazos especificados para dicho Plan, a menos que una revisión o extensión de los plazos el cronograma indicado en el ítem 2.3, sea aprobado por el Encargado CIP.	Medida de control o evidencia puede incluir, pero no está limitada a, registros de la implementación de las mitigaciones.

R3. Cada Entidad Responsable deberá implementar uno o más Procesos Documentados los cuales conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-007 R3 – Prevención de Código Malicioso.

R3 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M3. Medida de control o evidencia aceptable debe incluir los Procesos Documentados que en su conjunto incluyan cada uno de los requerimientos aplicables en la Tabla CIP-007 R3 – Prevención de Código Malicioso, y evidencia adicional para demostrar su implementación según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-007 R3 – Previsión de Código Malicioso			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
3.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF, y CAP.	Implementar mecanismos o métodos para disuadir, detectar o prevenir código malicioso.	Medidas de control o evidencias pueden incluir, pero no están limitadas a, registros de la Entidad Responsable sobre el desempeño de estos procesos o mecanismos (Ej.: a través de antivirus tradicionales, reforzamiento (hardening) de sistemas, políticas, etc.).
3.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF, y CAP.	Mitigar las amenazas frente a códigos maliciosos detectados.	Medida de control o evidencia puede incluir, pero no está limitada a: • Registros de procesos de respuesta frente a detección de código maliciosos; o • Registro de desempeño de estos procesos cuando código malicioso es detectado.
3.3	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF, y CAP.	Para aquellos métodos identificados en ítem 3.1, que utilizan firmas o patrones, contar con un proceso de actualización de firmas y patrones. El proceso debe abordar la instalación y prueba de las firmas y patrones.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación que muestre los procesos utilizados para la actualización de firmas y patrones.

R4. Cada Entidad Responsable deberá implementar uno o más Procesos Documentados los cuales conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-007 R4 – Monitoreo de Eventos de Seguridad.

R4 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M4. Medida de control o evidencia aceptable debe incluir los Procesos Documentados que en su conjunto incluyan cada uno de los requerimientos aplicables en la Tabla CIP-007 R4 – Monitoreo de Eventos de Seguridad, y evidencia adicional para demostrar su implementación según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-007 R4 – Monitoreo de Eventos de Seguridad			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
4.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF, y CAP.	Registrar eventos a nivel de Ciber Sistema SEN (según capacidad del Ciber Sistema SEN) o Ciber Activo para la identificación de, e investigaciones expost de, incidentes de ciberseguridad que incluyan como mínimo cada uno de los siguientes tipos de eventos: 4.1.1 Intentos exitosos de inicio de sesión (login) detectados; 4.1.2 Intentos fallados de acceso e intentos fallados de inicio de sesión (login); 4.1.3 Código malicioso detectado.	Medidas de control o evidencias pueden incluir, pero no están limitadas a, listados de tipos de eventos generados por sistema o en papel los cuales el Ciber Sistema SEN es capaz de detectar y, para eventos generados, está configurado para iniciar sesión. Dicho listado debe incluir los tipos de eventos requeridos.
4.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE, SCAF, y CAP.	Generar alertas para eventos de seguridad que la Empresa Responsable determine necesitan de una alerta. Como mínimo, cada uno de los siguientes tipos de eventos (según la capacidad de los Ciber Activos o Ciber Sistemas SEN) 4.2.1 Código malicioso detectado en ítem 4.1; y 4.2.2 Fallas detectadas para eventos de inicio de sesión en ítem 4.1.	Medidas de control o evidencias pueden incluir, pero no están limitadas a, listados de tipos de eventos generados por sistema o en papel que la Entidad Responsable determine necesitan alertas, incluyendo lista generada por sistema o en papel mostrando cómo las alertas son configuradas.

Tabla CIP-007 R4 – Monitoreo de Eventos de Seguridad			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
4.3	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio en CDCs y CCs, y sus asociados SMCAE, SCAF, y CAP.	Donde sea técnicamente factible, retener o guardar registros de eventos aplicables identificados en ítem 4.1 por al menos los últimos 90 días calendario consecutivos, excepto bajo Circunstancias Excepcionales CIP.	Medidas de control o evidencias pueden incluir, pero no están limitadas a, documentación del proceso de retención de registros de eventos y reportes generados por sistema o en papel mostrando la configuración de retención de registros establecida para 90 días o más.
4.4	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP.	Revisar un resumen o muestra de eventos de inicio de sesión según lo determine la Entidad Responsable, en intervalos no mayores a 15 días calendario, para identificar incidentes de ciberseguridad no detectados.	Medidas de control o evidencias pueden incluir, pero no están limitadas a, documentación describiendo la revisión, hallazgos de la revisión (de existir), y documentación fechada mostrando la revisión realizada.

R5. Cada Entidad Responsable deberá implementar uno o más Procesos Documentados los cuales conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-007 R5 – Controles de Acceso a Sistemas.

R5 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M5. Medida de control o evidencia aceptable debe incluir los Procesos Documentados que en su conjunto incluyan cada uno de los requerimientos aplicables en la Tabla CIP-007 R5 – Controles de Acceso a Sistemas, y evidencia adicional para demostrar su implementación según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-007 R5 – Controles de Acceso a Sistemas			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
5.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio en CDCs y CCs, y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE, SCAF, y CAP.	Contar con un método para forzar la autenticación de acceso de usuario interactivo donde sea técnicamente factible	Medida de control o evidencia puede incluir, pero no está limitada a, documentación describiendo como el acceso es autenticado.
5.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF, y CAP.	Identificar y contar con un inventario de todos los tipos de cuentas habilitadas por defecto y otras genéricas, ya sea por sistemas, por grupos de sistemas, por ubicación, o por tipos de sistemas.	Medida de control o evidencia puede incluir, pero no está limitada a, listado de cuentas, por tipo de cuentas, mostrando los tipos de cuentas habilitadas o genéricas en uso por Ciber Sistemas SEN.
5.3	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus asociados SMCAE, SCAF, y CAP.	Identificar individuos que tengan acceso autorizado para compartir cuentas.	Medida de control o evidencia puede incluir, pero no está limitada a, listado de cuentas compartidas y de los individuos que tengan acceso autorizado a cada cuenta compartida.

Tabla CIP-007 R5 – Controles de Acceso a Sistemas			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
5.4	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF, y CAP.	Cambiar contraseñas por defecto conocidas, según capacidad del Ciber Activo.	Medidas de control o evidencias pueden incluir, pero no están limitadas a: • Registros de un procedimiento que muestre las contraseñas son cambiadas cuando los nuevos dispositivos están en producción; o • Documentación en manuales de sistema u otros documentos de fabricantes mostrando que las contraseñas por defecto de fabricantes fueron generadas de forma pseudo aleatoria y son, por lo tanto, únicas para el dispositivo.
5.5	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF, y CAP.	Para autenticación, solo mediante contraseña, de usuarios de acceso interactivo, ya sea técnica o procedimentalmente, forzar los siguientes parámetros de contraseñas: 5.5.1 Largo de contraseña que sea de, al menos, el menor valor entre 8 caracteres o el máximo largo soportado por el Ciber Activo; y 5.5.2 Complejidad de contraseña mínima que sea la menor entre tres o más tipos de caracteres distintos o de la máxima complejidad soportada por el Ciber Activo.	Medidas de control o evidencias puede incluir, pero no están limitadas a: • Reportes generados por sistema o pantallazos de los parámetros de contraseña forzados por sistema, incluyendo largo y complejidad; y • Certificación que incluya referencia a los procedimientos documentados seguidos.
5.6	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio con CEE y sus	Donde sea técnicamente factible, para autenticación, solo mediante contraseña, de usuarios de acceso interactivo, ya sea técnica o procedimentalmente, forzar cambios de contraseña o una obligación a cambiar las	Medidas de control o evidencias pueden incluir, pero no están limitadas a: • Reportes generados por sistema o pantallazos de la periodicidad de cambio de contraseña forzado por sistema; o

	asociados SMCAE, SCAF, y CAP.	contraseñas al menos una vez cada 15 meses calendario.	• Certificación que incluya referencia a los procedimientos documentados seguidos.

Tabla CIP-007 R5 – Controles de Acceso a Sistemas			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
5.7	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF, y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio en CDCs y CC, y sus asociados SMCAE, SCAF, y CAP.	Donde sea técnicamente factible: • Limite el número de intentos de autenticación fallidos; o • Genera alertas luego de un límite de intentos de autenticación fallidos.	Medidas de control o evidencias pueden incluir, pero no están limitadas a: • Documentación de parámetros de bloqueo de cuentas; o • Reglas en la configuración de alertas mostrando como el sistema notificó individuos luego de un determinado número de intentos fallidos de inicio de sesión.

7.6.4. Entrada en Vigor

El presente estándar CIP-007 entrará en vigor al momento de su aprobación por parte de la SEC y posterior publicación en la página web del Coordinador. Las Entidades Responsables tendrán un periodo de marcha blanca para implementar cada uno de los requerimientos en el estándar CIP-007 de acuerdo con los plazos máximos especificados en ANEXO 1, columna Marcha Blanca.

7.7. CIP-008: Ciber Seguridad – Reporte de Incidentes y Planes de Respuesta

7.7.1. Propósito

Mitigar los riesgos en la operación segura y confiable del SEN como resultado de un incidente de ciberseguridad, especificando requerimientos de respuesta a incidentes.

7.7.2. Aplicabilidad Específica y Excepciones

No existe aplicabilidad específica adicional a lo definido en el punto 3 para el estándar CIP-008.

Se exceptúan los Ciber Activos asociados con redes de comunicaciones y enlaces de comunicaciones de datos entre Perímetros de Seguridad Electrónica (PSE) independientes.

7.7.3. Requerimientos (R) y Medidas de Control (M)

R1. Cada Entidad Responsable deberá documentar uno o más Planes de respuesta a incidentes de ciberseguridad los cuales conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-008 R1 – Especificaciones del Plan de Respuesta a Incidentes de Ciberseguridad.

R1 es calificado con Factor de Riesgo por Incumplimiento Bajo (FRIB).

M1. Medida de control o evidencia aceptable debe incluir cada uno de los Planes que en su conjunto incluyan cada uno de los requerimientos aplicables en la Tabla CIP-008 R1 – Especificaciones del Plan de Respuesta a Incidentes de Ciberseguridad.

Tabla CIP-008 R1 – Especificaciones del Plan de Respuesta a Incidentes de Ciberseguridad			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
1.1	✓ Ciber Sistemas SEN de Impacto Alto; y ✓ Ciber Sistemas SEN de Impacto Medio.	Uno o más procesos para identificar, clasificar, y responder a incidentes de ciberseguridad.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación fechada de Planes de respuesta a incidentes de ciberseguridad que incluyan el proceso para identificar, clasificar, y responder a incidentes de ciberseguridad.
1.2	✓ Ciber Sistemas SEN de Impacto Alto; y ✓ Ciber Sistemas SEN de Impacto Medio.	Uno o más procesos para determinar si un incidente de ciberseguridad identificado es un Incidente de Ciberseguridad Reportable y notificarlo según lo especificado en la parte 4 del presente documento. La notificación inicial, no debe exceder una hora desde la identificación y determinación del Incidente de Ciberseguridad Reportable.	Medidas de control o evidencias pueden incluir, pero no están limitadas a, documentación fechada de Planes de respuesta a incidentes de ciberseguridad que entreguen lineamientos, orientación y definan umbrales para determinar cuáles incidentes de ciberseguridad son Incidentes de Ciberseguridad Reportables, y documentación de notificación inicial.
1.3	✓ Ciber Sistemas SEN de Impacto Alto; y ✓ Ciber Sistemas SEN de Impacto Medio.	Los roles y responsabilidades de individuos o grupos de respuesta a incidentes de ciberseguridad.	Medida de control o evidencia puede incluir, pero no está limitada a, procesos o procedimientos de respuesta a incidentes de ciberseguridad fechados, que definan los roles y responsabilidades (Ej.: monitoreo, reportabilidad, iniciación, documentación, etc.), de individuos o grupos de respuesta a incidentes de ciberseguridad.
1.4	✓ Ciber Sistemas SEN de Impacto Alto; y ✓ Ciber Sistemas SEN de Impacto Medio.	Procedimiento de manejo de incidentes para incidentes de ciberseguridad.	Medida de control o evidencia puede incluir, pero no está limitada a, procesos o procedimientos de respuesta a incidentes de ciberseguridad fechados, que aborden el manejo de incidentes (Ej.: contención, erradicación, recuperación /resolución de incidentes, etc.).

R2. Cada Entidad Responsable deberá implementar cada uno de sus Planes de respuesta a incidentes de ciberseguridad los cuales conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-008 R2 – Implementación y Prueba del Plan de Respuesta a Incidentes de Ciberseguridad.

R2 es calificado con Factor de Riesgo por Incumplimiento Bajo (FRIB).

M2. Medida de control o evidencia aceptable debe incluir, pero no está limitada a, documentación que en su conjunto demuestre la implementación de cada uno de los requerimientos aplicables en la Tabla CIP-008 R2 – Implementación y Prueba del Plan de Respuesta a Incidentes de Ciberseguridad.

Tabla CIP-008 R2 – Implementación y Prueba del Plan de Respuesta a Incidentes de Ciberseguridad			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
2.1	✓ Ciber Sistemas SEN de Impacto Alto; y ✓ Ciber Sistemas SEN de Impacto Medio.	Probar cada Plan de respuesta a incidentes de ciberseguridad, al menos una vez cada 15 meses calendario: • Respondiendo a un Incidente de Ciberseguridad Reportable real; • Con una simulación o ejercicio table top (drill) de un Incidente de Ciberseguridad Reportable; o • Con un ejercicio operacional de un Incidente de Ciberseguridad Reportable.	Medidas de control o evidencias pueden incluir, pero no están limitadas a, evidencia fechada de un reporte de lecciones aprendidas que incluya un resumen de las pruebas o un compilado de notas, registros, y comunicaciones que resulten de las pruebas. Tipos de ejercicios pueden incluir discusiones o ejercicios en base a operaciones.
2.2	✓ Ciber Sistemas SEN de Impacto Alto; y ✓ Ciber Sistemas SEN de Impacto Medio.	Utilizar el Plan de respuesta a incidentes de ciberseguridad en requerimiento R1 en respuesta a un Incidente de Ciberseguridad Reportable o al realizar un ejercicio de un Incidente de Ciberseguridad Reportable. Documentar las desviaciones respecto del Plan levantadas durante la respuesta al incidente o el ejercicio.	Medidas de control o evidencias pueden incluir, pero no están limitadas a, notas, registros y reportes de incidentes que fueron mantenidos durante el proceso de respuesta al incidente, y documentación de seguimiento que describa desviaciones levantadas durante la respuesta al incidente o el ejercicio.

Tabla CIP-008 R2 – Implementación y Prueba del Plan de Respuesta a Incidentes de Ciberseguridad			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
2.3	✓ Ciber Sistemas SEN de Impacto Alto; y ✓ Ciber Sistemas SEN de Impacto Medio.	Retener o guardar registros relacionados con los Incidente de Ciberseguridad Reportables.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación fechada tal como registros de seguridad, políticas, e-mails, checklists o formularios de respuesta, resultados de análisis forenses, registros de restauración, y notas de revisiones post incidentes relacionados con los Incidente de Ciberseguridad Reportables.

R3. Cada Entidad Responsable deberá mantener cada uno de sus en concordancia con cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-008 R3 – Revisión, Actualización y Comunicación del Plan de Respuesta a Incidentes de Ciberseguridad.

R3 es calificado con Factor de Riesgo por Incumplimiento Bajo (FRIB).

M3. Medida de control o evidencia aceptable debe incluir, pero no está limitada a, documentación que en su conjunto demuestre mantención de cada Plan de respuesta a incidentes de ciberseguridad en concordancia con los requerimientos aplicables en la Tabla CIP-008 R3 – Revisión, Actualización y Comunicación del Plan de Respuesta a Incidentes de Ciberseguridad.

Tabla CIP-008 R3 – Revisión, Actualización y Comunicación del Plan de Respuesta a Incidentes de Ciberseguridad			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
3.1	✓ Ciber Sistemas SEN de Impacto Alto; y ✓ Ciber Sistemas SEN de Impacto Medio.	No más allá de 90 días calendario de terminada la prueba de un Plan de respuesta a incidentes de ciberseguridad o la respuesta a un Incidentes de Ciberseguridad Reportable real: 3.1.1 Documentar la existencia o ausencia de cualquier lección aprendida; 3.1.2 Actualizar el Plan de respuesta a incidentes de ciberseguridad en base a las lecciones aprendidas documentadas asociadas con el plan; y 3.1.3 Notificar a cada persona o equipo con un rol definido en el Plan de respuesta a incidentes de ciberseguridad de las actualizaciones del Plan en base a las lecciones aprendidas.	Medida de control o evidencia puede incluir, pero no está limitada a, todas las siguientes: • Documentación fechada de reuniones de revisión post incidentes o reportes de seguimiento mostrando las lecciones aprendidas asociadas con la prueba del Plan de respuesta a incidentes de ciberseguridad o la respuesta a un Incidentes de Ciberseguridad Reportable real, o documentación fechada que establezca no hubo lecciones aprendidas; • Plan de respuesta a incidentes de ciberseguridad fechado y revisado mostrando cualquier cambio en base a las lecciones aprendidas; y • Evidencia de la distribución y comunicación del Plan actualizado incluyendo, pero no limitado a: e-mails, correo u otro servicio, sistema de distribución electrónica, o planillas de registro en capacitaciones.
3.2	✓ Ciber Sistemas SEN de Impacto Alto; y ✓ Ciber Sistemas SEN de Impacto Medio.	No más allá de 60 días calendario de un cambio ya sea a los roles o responsabilidades, los individuos o equipos de respuesta a incidentes de ciberseguridad, o la tecnología que la Entidad Responsable Determine impactaría la capacidad de ejecutar el Plan:	Medida de control o evidencia puede incluir, pero no está limitada a: • Plan de respuesta a incidentes de ciberseguridad fechado y revisado con cambios a los roles o responsabilidades, equipos de respuesta o tecnología; y • Evidencia de la distribución y comunicación del Plan actualizado incluyendo, pero

		3.2.1 Actualizar el Plan de respuesta a incidentes de ciberseguridad; y 3.2.2 Notificar las actualizaciones a cada persona o equipo con un rol definido en el Plan de respuesta a incidentes de ciberseguridad.	no limitado a: e-mails, correo u otro servicio, sistema de distribución electrónica, o planillas de registro en capacitaciones.

7.7.4. Entrada en Vigor

El presente estándar CIP-008 entrará en vigor al momento de su aprobación por parte de la SEC y posterior publicación en la página web del Coordinador. Las Entidades Responsables tendrán un periodo de marcha blanca para implementar cada uno de los requerimientos en el estándar CIP-008 de acuerdo con los plazos máximos especificados en ANEXO 1, columna Marcha Blanca.

7.8. CIP-009: Ciber Seguridad – Planes de Recuperación para Ciber Sistemas SEN

7.8.1. Propósito

Recuperar la confiabilidad de las funciones realizadas por los Ciber Sistemas SEN especificando requerimientos en los planes de recuperación en apoyo a la continua estabilidad, operabilidad y confiabilidad del SEN.

7.8.2. Aplicabilidad Específica y Excepciones

No existe aplicabilidad específica adicional a lo definido en el punto 3 para el estándar CIP-009.

Se exceptúan los Ciber Activos asociados con redes de comunicaciones y enlaces de comunicaciones de datos entre Perímetros de Seguridad Electrónica (PSE) independientes.

7.8.3. Requerimientos (R) y Medidas de Control (M)

R1. Cada Entidad Responsable deberá contar con uno o más Planes de recuperación documentados los cuales conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-009 R1 – Especificaciones del Plan de Recuperación.

R1 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M1. Medida de control o evidencia aceptable debe incluir los Planes de recuperación documentados que en su conjunto incluyan cada uno de los requerimientos aplicables en la Tabla CIP-009 R1 – Especificaciones del Plan de Recuperación.

Tabla CIP-009 R1 – Especificaciones del Plan de Recuperación			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
1.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y SCAF; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE y SCAF.	Condiciones para la activación del Plan (o planes) de recuperación.	Medida de control o evidencia puede incluir, pero no está limitada a, uno o más planes que incluyan una sección identificando las condiciones para la activación del plan (o planes) de recuperación.
1.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y SCAF; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE y SCAF.	Roles y responsabilidades de los equipos de respuesta.	Medida de control o evidencia puede incluir, pero no está limitada a, uno o más planes de recuperación que incluyan una sección identificando los roles y responsabilidades de los equipos de respuesta.
1.3	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y SCAF; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE y SCAF.	Uno o más procesos para el respaldo y almacenamiento de información requeridos para recuperar la funcionalidad de los Ciber Sistemas SEN.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación de procesos específicos para el respaldo y almacenamiento de información requeridos para recuperar la funcionalidad de los Ciber Sistemas SEN.
1.4	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y SCAF; y ✓ Ciber Sistemas SEN de Impacto Medio en CDCs y CCS, y sus asociados SMCAE y SCAF.	Uno o más procesos para verificar que se completaron exitosamente los procesos de respaldo en ítem 1.3, y los procesos para abordar cualquier falla de respaldo.	Medida de control o evidencia puede incluir, pero no está limitada a, registros, workflow u otra documentación confirmando que se completaron exitosamente los procesos de respaldo, y las fallas de respaldo, de existir, fueron abordadas.

Tabla CIP-009 R1 – Especificaciones del Plan de Recuperación			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
1.5	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y SCAF; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE y SCAF.	Uno o más procesos para preservar datos, según capacidad del Ciber Activo, para determinar las causas de un incidente de ciberseguridad que gatille la activación del Plan (o planes) de recuperación. La preservación de datos no debe impedir o restringir la recuperación.	Medida de control o evidencia puede incluir, pero no está limitada a, procedimiento para recuperar datos tales como discos corruptos o realizando un espejo de datos del sistema antes de proceder con la recuperación.

R2. Cada Entidad Responsable deberá implementar sus Planes de recuperación documentados los cuales conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-009 R2 – Implementación y Prueba del Plan de Recuperación.

R2 es calificado con Factor de Riesgo por Incumplimiento Bajo (FRIB).

M2. Medida de control o evidencia aceptable debe incluir documentación que en su conjunto demuestre implementación de cada uno de los requerimientos aplicables en la Tabla CIP-009 R2 – Implementación y Prueba del Plan de Recuperación.

Tabla CIP-009 R2 – Implementación y Prueba del Plan de Recuperación			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
2.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y SCAF; y ✓ Ciber Sistemas SEN de Impacto Medio en CDCs y CCS, y sus asociados SMCAE y SCAF.	Probar o testear cada uno de los Planes de recuperación referenciados en requerimiento R1, al menos una cada 15 meses calendario: • Recuperándose de un incidente real; • Con un ejercicio table top o ensayo (drill) en papel; o • Con un ejercicio operacional.	Medida de control o evidencia puede incluir, pero no está limitada a, evidencia fechada de una prueba (recuperándose de un incidente real, o con un ejercicio table top o ensayo (drill) en papel, o con un ejercicio operacional) del Plan de recuperación al menos una vez cada 15 meses. Para el ejercicio, o ensayo en papel, o el ejercicio operacional, la evidencia puede incluir notas de reuniones, minutas, u otros registros de hallazgos en los ejercicios.

Tabla CIP-009 R2 – Implementación y Prueba del Plan de Recuperación			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
2.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y SCAF; y ✓ Ciber Sistemas SEN de Impacto Medio en CDCs y CCS, y sus asociados SMCAE y SCAF.	Probar una muestra de información representativa utilizada para recuperar la funcionalidad un Ciber Sistema SEN, al menos una vez cada 15 meses calendario, para asegurar que la información es utilizable y es compatible con las configuraciones actuales. Una recuperación real que incorpora la información usada para recuperar la funcionalidad un Ciber Sistema SEN es sustituto para esta prueba.	Medida de control o evidencia puede incluir, pero no está limitada a, registros operacionales o resultados de pruebas con criterios para aprobar la usabilidad (Ej.: pruebas de carga de respaldo de información) y compatibilidad con configuraciones de que sistemas actuales (Ej.: Checkpoints de comparación, manuales o automáticos, entre contenido de medios de respaldo y configuración actual).
2.3	✓ Ciber Sistemas SEN de Impacto Alto.	Probar cada uno de los Planes de recuperación referenciados en requerimiento R1, al menos una vez cada 36 meses calendario, a través de un ejercicio operacional del Plan de recuperación en un ambiente representativo de un ambiente de producción. Una respuesta de recuperando real puede sustituir un ejercicio operacional.	Medidas de control o evidencias pueden incluir, pero no están limitadas a, documentación fechada de: • Un ejercicio operacional, al menos una vez cada 36 meses calendario, entre ejercicios que demuestren recuperación en un ambiente representativo; o • Una respuesta de recuperación real ocurrida dentro de del periodo de 36 meses calendario de ejercitados los planes de recuperación.

R3. Cada Entidad Responsable deberá mantener cada uno de sus Planes de recuperación en concordancia cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-009 R3 – Revisión, Actualización y Comunicación del Plan de Recuperación.

R3 es calificado con Factor de Riesgo por Incumplimiento Bajo (FRIB).

M3. Medida de control o evidencia aceptable debe incluir cada uno de los requerimientos aplicables en la Tabla CIP-009 R3 – Revisión, Actualización y Comunicación del Plan de Recuperación.

Tabla CIP-009 R3 – Revisión, Actualización y Comunicación del Plan de Recuperación			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
3.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y SCAF; y ✓ Ciber Sistemas SEN de Impacto Medio en CDCs y CCS, y sus asociados SMCAE y SCAF.	No más allá de 90 días calendario de completada la prueba del plan de recuperación o una recuperación real: 3.1.1 Documentar toda lección aprendida asociada con la prueba del Plan de recuperación o recuperación real, o documentar la ausencia de lecciones aprendidas si fuese el caso; 3.1.2 Actualizar el Plan de recuperación en base a cualquier lección aprendida documentada asociada con el Plan; y 3.1.3 Notificar a cada persona o equipo con un rol definido en el Plan de recuperación, de las actualizaciones del Plan de recuperación en base a cualquier lección aprendida documentada.	Medida de control o evidencia puede incluir, pero no está limitada a, todas las siguientes: • Documentación fechada de deficiencias identificadas o lecciones aprendidas para cada prueba del Plan de recuperación o recuperación de un incidente real, o documentación fechada estableciendo que no hubo lecciones aprendidas; • Plan de recuperación revisado y fechado mostrando cualquier cambio basado en lecciones aprendidas; y • Evidencia de la distribución de la actualización del Plan incluyendo, pero no limitado a: e-mails, correo u otros servicios de envío, sistema de distribución electrónica, u planillas de registro en capacitaciones.
3.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y SCAF; y ✓ Ciber Sistemas SEN de Impacto Medio en CDCs y CCS, y sus asociados SMCAE y SCAF.	No más allá de 90 días calendario de un cambio a los roles o responsabilidades, en el equipo de respuesta, o en la tecnología que la Entidad Responsable determine impactaría la capacidad de ejecutar el Plan de recuperación: 3.2.1 Actualizar el Plan de recuperación; y 3.2.2 Notificar a cada persona o grupo con un rol definido en el Plan de recuperación, de dichas actualizaciones.	Medida de control o evidencia puede incluir, pero no está limitada a, todas las siguientes: • Planes de recuperación fechados y revisados con los cambios a los roles o responsabilidades, al equipo de respuesta, o la tecnología; y • Evidencia de la distribución de la actualización del Plan incluyendo, pero no limitado a: e-mails, correo u otros servicios de envío, sistema de distribución electrónica, u planillas de registro en capacitaciones.

7.8.4. Entrada en Vigor

El presente estándar CIP-009 entrará en vigor al momento de su aprobación por parte de la SEC y posterior publicación en la página web del Coordinador. Las Entidades Responsables tendrán un periodo de marcha blanca para implementar cada uno de los requerimientos en el estándar CIP-009 de acuerdo con los plazos máximos especificados en ANEXO 1, columna Marcha Blanca.

7.9. CIP-010: Ciber Seguridad – Gestión de Cambio de Configuración y Evaluación de Vulnerabilidades

7.9.1. Propósito

Prevenir y detectar cambios no autorizados a Ciber Sistemas SEN especificando requerimientos para la gestión de cambio de configuración y evaluación de vulnerabilidades, en apoyo a la protección de Ciber Sistemas SEN, frente a eventos o actos que podrían conducir a una mala operación o inestabilidad del SEN.

7.9.2. Aplicabilidad Específica y Excepciones

No existe aplicabilidad específica adicional a lo definido en el punto 3 para el estándar CIP-010.

Se exceptúan los Ciber Activos asociados con redes de comunicaciones y enlaces de comunicaciones de datos entre Perímetros de Seguridad Electrónica (PSE) independientes.

7.9.3. Requerimientos (R) y Medidas de Control (M)

R1. Cada Entidad Responsable deberá contar con uno o más Procesos Documentados los que conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-010 R1 – Gestión de Cambio de Configuración.

R1 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M1. Medida de control o evidencia aceptable debe incluir cada uno de los Procesos Documentados aplicables que en su conjunto incluyan cada uno de los requerimientos aplicables en la Tabla CIP-010 R1 – Gestión de Cambio de Configuración, y evidencia adicional para demostrar su implementación según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-010 R1 – Gestión de Cambio de Configuración			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
1.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF y CAP.	Desarrollar una línea base de configuración, individualmente o por grupo, la que deberá incluir los siguientes ítems: 1.1.1 Sistemas operativos (incluyendo versión) o firmware donde no exista un sistema operativo independiente; 1.1.2 Cualquier software de aplicación de código abierto (open-source) disponible (incluyendo versión), instalado intencionalmente; 1.1.3 Cualquier software personalizado instalado; 1.1.4 Cualquier puerto lógico de red accesible; y 1.1.5 Cualquier parche de seguridad aplicado.	Medidas de control o evidencias pueden incluir, pero no están limitadas a: • Una hoja de cálculo identificando los ítems requeridos en la línea base de configuración para cada Ciber Activo, individualmente o por grupo; • Un registro en un sistema de gestión de activos que identifique los ítems requeridos en la línea base de configuración para cada Ciber Activo, individualmente o por grupo.
1.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF y CAP.	Autorizar y documentar cambios que se desvíen de la línea base de configuración existente.	Medidas de control o evidencias pueden incluir, pero no están limitadas a: • Un registro de requerimiento de cambio y autorización electrónica asociada (realizada por un individuo o grupo con autoridad para autorizar cambios), para cada cambio, en un sistema de gestión de cambio; o • Documentación mostrando que el cambio fue realizado de acuerdo con el requerimiento.

Tabla CIP-010 R1 – Gestión de Cambio de Configuración			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
1.3	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF y CAP.	Para un cambio que se desvíe de la línea base de configuración existente, actualizar dicha línea base de configuración según sea necesario dentro de 30 días calendario de completado el cambio.	Medida de control o evidencia puede incluir, pero no está limitada a, documentación de la línea base actualizada con una fecha que está dentro de los 30 días calendario a la fecha de completado el cambio.
1.4	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF y CAP.	Para un cambio que se desvíe de la línea base de configuración existente: 1.4.1 Previo al cambio, determine los controles de ciberseguridad requeridos en CIP-005 y CIP-007 que podrían ser impactado por el cambio; 1.4.2 A continuación al cambio, verificar que los controles de ciberseguridad requeridos determinados en 1.4.1 no son afectados adversamente; y 1.4.3 Documentar los resultados de la verificación.	Medida de control o evidencia puede incluir, pero no está limitada a, una lista de controles de ciberseguridad verificados o probados, junto con los resultados fechados de las pruebas.

Tabla CIP-010 R1 – Gestión de Cambio de Configuración			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
1.5	✓ Ciber Sistemas SEN de Impacto Alto.	Donde sea técnicamente factible, para cada cambio que se desvíe de la línea base de configuración existente: 1.5.1 Previo a implementar cualquier cambio en el ambiente de producción, probar los cambios en un ambiente de prueba, o probar los cambios en un ambiente de producción en donde la prueba sea realizada de una manera que minimice los efectos adversos, que modele la línea base de configuración para asegurar que los controles de ciberseguridad en CIP-005 y CIP-007 no sean afectados de forma adversa; y 1.5.2 Documentar los resultados de las pruebas y, si se utilizó un ambiente de prueba, las diferencias entre el ambiente de prueba y el ambiente de producción, incluyendo una descripción de las medidas utilizadas para contabilizar cualquier diferencia en la operación entre los ambientes de prueba y producción.	Medida de control o evidencia puede incluir, pero no está limitada a, una lista de controles de ciberseguridad probados, junto con resultados de pruebas exitosas y una lista de diferencias entre ambientes de prueba y producción, con descripciones de cómo fueron contabilizadas las diferencias, incluyendo la fecha de la prueba.

R2. Cada Entidad Responsable deberá contar con uno o más Procesos Documentados los que conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-010 R2 – Monitoreo de Configuración.

R2 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M2. Medida de control o evidencia aceptable debe incluir cada uno de los Procesos Documentados aplicables que en su conjunto incluyan cada uno de los requerimientos aplicables en la Tabla CIP-010 R2 – Monitoreo de Configuración, y evidencia adicional para demostrar su implementación según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-010 R2 – Monitoreo de Configuración			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
2.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP.	Monitorear al menos una vez cada 35 días calendario por cambios en la línea base de configuración, según lo descrito en requerimiento R1, ítem 1.1). Documentar e investigar cambios no autorizados detectados.	Medida de control o evidencia puede incluir, pero no está limitada a, registros de un sistema que monitoree la configuración junto con registros de investigación de cualquier cambio(s) no autorizado(s) que fuera(n) detectado(s).

R3. Cada Entidad Responsable deberá contar con uno o más Procesos Documentados los que conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-010 R3 – Evaluación de Vulnerabilidades.

R3 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M3. Medida de control o evidencia aceptable debe incluir cada uno de los Procesos Documentados aplicables que en su conjunto incluyan cada uno de los requerimientos aplicables en la Tabla CIP-010 R3 – Evaluación de Vulnerabilidades, y evidencia adicional para demostrar su implementación según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-010 R3 – Evaluación de Vulnerabilidades			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
3.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF y CAP.	Al menos una vez cada 15 meses calendario, conducir una evaluación de vulnerabilidad activa o en papel.	Medidas de control o evidencias pueden incluir, pero no están limitadas a: • Un documento listando la fecha de la evaluación (realizado al menos una vez cada 15 meses calendario), los controles evaluados para cada Ciber Activo SEN junto con el método de evaluación; o • Un documento listando la fecha de la evaluación y resultados o salidas de las herramientas utilizadas para la evaluación.

Tabla CIP-010 R3 – Evaluación de Vulnerabilidades			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
3.2	✓ Ciber Sistemas SEN de Impacto Alto.	Donde sea técnicamente factible, al menos una vez cada 36 meses calendario: 3.2.1 Realizar una evaluación de vulnerabilidad activa en un ambiente de prueba, o realizar una evaluación de vulnerabilidad activa en un ambiente de producción donde la prueba sea realizada de manera que minimicen efectos adversos, que modele la línea base de configuración de Ciber Sistemas SEN en un ambiente de producción; y 3.2.2 Documentar los resultados de las pruebas y, si se utilizó un ambiente de pruebas, las diferencias entre los ambientes de prueba y producción,	Medida de control o evidencia puede incluir, pero no está limitada a, un documento listando la fecha de las evaluaciones (realizadas al menos una vez cada 36 meses calendario), resultados o salidas de las herramientas utilizadas para realizar la evaluación, y una lista de las diferencias entre los ambientes de prueba y producción con descripciones de cómo las diferencias fueron contabilizadas al realizar la evaluación.

		incluyendo una descripción de las medidas utilizadas para contabilizar cualquier diferencia en operación entre los ambientes de prueba y producción.	
3.3	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP.	Previo a agregar nuevos Ciber Activos aplicables a un ambiente de producción, realizar una evaluación de vulnerabilidades activa del nuevo Ciber Activo, excepto para Circunstancias Excepcionales CIP, y como reemplazo del mismo tipo de Ciber Activo con una línea base de configuración que modele una línea base de configuración existente del Ciber Activo previo, u otro existente.	Medida de control o evidencia puede incluir, pero no está limitada a, un documento listando la fecha de las evaluaciones (realizadas previo a la puesta en servicio del nuevo Ciber Activo) y los resultados o salidas de las herramientas utilizadas para realizar la evaluación.

Tabla CIP-010 R3 – Evaluación de Vulnerabilidades			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
3.4	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF y CAP.	Documentar los resultados de las evaluaciones conducidas de acuerdo con ítems 3.1, 3.2 y 3.3, y el plan de acción para remediar o mitigar vulnerabilidades identificadas en la evaluación, incluyendo fecha planificada para completar el plan de acción y el estado de la ejecución de todas las acciones de remediación y mitigación.	Medida de control o evidencia puede incluir, pero no está limitada a, un documento listando los resultados, revisión o evaluación, una lista de planes de acción, fechas propuestas documentadas para completar los planes de acción, y registros del estado de los planes de acción (tales como minuta de reuniones de avance, actualizaciones en un sistema de órdenes de trabajo, o planillas con la trazabilidad de los planes de acción).

R4. Cada Entidad Responsable, para sus Ciber Sistemas SEN de impacto alto y sus asociados Ciber Activos Protegidos (CAP), deberá implementar, excepto bajo Circunstancias Excepcionales CIP, uno o más Planes documentados para Ciber Activos Transitorios y Medios Removibles, que incluyan las secciones descritas en 7.9.4.

R4 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M4. Medida de control o evidencia aceptable debe incluir cada uno de los Planes documentados para Ciber Activos Transitorios y Medios Removibles que colectivamente incluyan cada una de las secciones aplicables en 7.9.4, y evidencia adicional para demostrar la implementación de dichos Planes. Si la Entidad Responsable no utiliza Ciber Activos Transitorios o Medios Removibles, ejemplos de evidencia podrán incluir, pero no están limitados a, una declaración, política u otro documento en donde se declare que la Entidad Responsable no utiliza Ciber Activos Transitorios o Medios Removibles.

7.9.4. Planes para Ciber Activos Transitorios y Medios Removibles

Las Entidades Responsables deberán incluir cada una de las secciones descritas a continuación en sus Planes para Ciber Activos Transitorios y Medios Removibles requeridos en CIP-010 R4.

Sección 1. Ciber Activos Transitorios Gestionados por la Entidad Responsable

1.1. Gestión de Ciber Activos Transitorios (CAT): Las Entidades Responsables deberán gestionar CAT, individualmente o por grupos: (1) de manera continua para asegurar cumplimiento con los requerimientos aplicables todo el tiempo, (2) según demanda aplicando los requerimientos aplicables antes de conectarse a un Ciber Sistema SEN, o (3) una combinación de ambos (1) y (2) arriba.

1.2. Autorización de Ciber Activos Transitorios (CAT): Para cada CAT individual o grupo de CAT, cada Entidad Responsable deberá autorizar:

1.2.1. Usuarios, ya sea individualmente, o por grupo o rol;
1.2.2. Localizaciones, ya sea individualmente o por grupo; y
1.2.3. Usos, los que deben estar limitados a lo necesario para realizar las funciones del negocio.

1.3. Mitigación de Vulnerabilidades de Software: Usar uno, o una combinación, de los siguientes métodos para lograr el objetivo de mitigar riesgos de vulnerabilidades planteadas por software no parchado en CAT (según capacidad del CAT):

- Parches de seguridad, incluyendo actualizaciones manuales o administradas;
- Sistemas Operativos vivos (Live OS) y software ejecutable solo de medios de lectura (read-only);
- Reforzamiento de sistemas (system hardening); u
- Otros métodos para mitigar vulnerabilidades de software.

1.4. Mitigación de Introducción de Código Malicioso: Usar uno, o una combinación, de los siguientes métodos para lograr el objetivo de mitigar la Introducción de código malicioso (según capacidad del CAT):

- Software antivirus, incluyendo actualizaciones manuales o administradas de firmas o patrones;
- Aplicación de lista blanca (whitelisting); u
- Otros métodos para mitigar la introducción de código malicioso.

1.5. Mitigación de Uso No Autorizado: Usar uno, o una combinación, de los siguientes métodos para lograr el objetivo de mitigar los riesgos por uso no autorizado de CAT:

- Restringir acceso físico;
- Cifrado de disco completo (Full-disk) con autenticación;
- Autenticación multi-factor; u
- Otros métodos para mitigar los riesgos de uso no autorizado.

Sección 2. Ciber Activos Transitorios Gestionados por terceros, distintos a la Entidad Responsable

2.1. Mitigación de Vulnerabilidades de Software: Usar uno, o una combinación, de los siguientes métodos para lograr el objetivo de mitigar riesgos de vulnerabilidades planteadas por software no parchado en CAT (según capacidad del CAT):

- Revisión de los parches de seguridad instalados;
- Revisión de lo proceso de parches de seguridad usados por terceros;
- Revisión de otras medidas de mitigación de vulnerabilidades realizadas por terceros; u
- Otros métodos para mitigar vulnerabilidades de software.

2.2. Mitigación de Introducción de Código Malicioso: Usar uno, o una combinación, de los siguientes métodos para lograr el objetivo de mitigar la Introducción de código malicioso (según capacidad del CAT):

- Revisar nivel de actualización del antivirus;
- Revisar proceso de actualización del antivirus usado por terceros;
- Revisar la aplicación de lista blanca (whitelisting) usada por terceros;
- Revisar el uso de Sistemas Operativos vivos (Live OS) y software ejecutable solo de medios de Revisar lectura (read-only);
- Revisar el reforzamiento de sistema usado por terceros; u;
- Otros métodos para mitigar la introducción de código malicioso.

2.3. Para cualquier método utilizado para mitigar vulnerabilidades de software o código malicioso según o especificado en 2.1 y 2.2, las Entidades Responsables deberán determinar si acciones de mitigación adicionales son necesarias e implementar dichas acciones previo a conectar los CAT.

Sección 3. Medios Removibles

3.1. Autorización de Medios Removibles: Para cada Medio Removible individual o en grupo, cada Entidad Responsable deberá autorizar:

3.1.1. Usuarios, ya sea individualmente, o por grupo o rol; y

3.1.2. Localizaciones, ya sea individualmente o por grupo.

3.2. Mitigación de Código Malicioso: Para lograr el objetivo de mitigar amenazas de introducción de código malicioso en Ciber Sistemas SEN de impacto alto o medio, y sus asociados Ciber Activos Protegido (CAP), cada Entidad Responsable deberá:

3.2.1. Utilizar métodos para detectar código malicioso en Medios Removibles usando un Ciber Activo distinto al Ciber Sistema SEN o Ciber Activo Protegido; y

3.2.2. Mitigar las amenazas de código malicioso detectado en Medios Removibles previo a conectarlos en Ciber Sistemas SEN de impacto alto o medio o en sus asociados Ciber Activos Protegidos (CAP).

7.9.5. Entrada en Vigor

El presente estándar CIP-010 entrará en vigor al momento de su aprobación por parte de la SEC y posterior publicación en la página web del Coordinador. Las Entidades Responsables tendrán un periodo de marcha blanca para implementar cada uno de los requerimientos en el estándar CIP-010 de acuerdo con los plazos máximos especificados en ANEXO 1, columna Marcha Blanca.

7.10. CIP-011: Ciber Seguridad – Protección de Información

7.10.1. Propósito

Prevenir acceso no autorizado a información en Ciber Sistemas SEN especificando requerimientos de protección de información en apoyo a la protección de Ciber Sistemas SEN, frente a eventos o actos que podrían conducir a una mala operación o inestabilidad del SEN.

7.10.2. Aplicabilidad Específica y Excepciones

No existe aplicabilidad específica adicional a lo definido en el punto 3 para el estándar CIP-011.

Se exceptúan los Ciber Activos asociados con redes de comunicaciones y enlaces de comunicaciones de datos entre Perímetros de Seguridad Electrónica (PSE) independientes.

7.10.3. Requerimientos (R) y Medidas de Control (M)

R1. Cada Entidad Responsable deberá implementar uno o más Programas de protección de información documentados los que conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-011 R1 – Protección de Información.

R1 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M1. Medida de control o evidencia aceptable para el Programa de protección de información debe incluir los requerimientos aplicables en la Tabla CIP-011 R1 – Protección de Información, y evidencia adicional para demostrar su implementación según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-011 R1 – Protección de Información			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
1.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE y CAP.	Método(s) para identificar información que cumpla con la definición de Información de Ciber Sistema SEN.	Medidas de control o evidencias pueden incluir, pero no están limitadas a: • Método documentado para identificar la Información de Ciber Sistema SEN a partir del programa de protección de información de la Entidad; o • Indicaciones sobre la información (Ej.: etiquetas o clasificación)) que identifiquen Información de Ciber Sistema SEN según se consigne en el programa protección de información de la Entidad; o • Material de capacitación que provea al personal conocimiento suficiente para reconocer Información de Ciber Sistema SEN; o • Repositorio, o localización electrónica o física, designada a almacenar información de Ciber Sistema SEN en el programa de protección de información de la Entidad.
1.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE y CAP.	Procedimiento para proteger y manipular de forma segura Información de Ciber Sistemas SEN, incluyendo almacenamiento, tránsito, y uso.	Medidas de control o evidencias pueden incluir, pero no están limitadas a: • Procedimientos para proteger y manipular de forma segura, incluyendo tópicos como almacenamiento, seguridad durante tránsito, y uso de, Información de Ciber Sistemas SEN; o • Registros indicando que la Información de Ciber Sistemas SEN es manipulada de manera consistente con los procedimientos documentados de la Entidad.

R2. Cada Entidad Responsable deberá implementar uno o más Procesos Documentados los que conjuntamente incluyan cada uno de los requerimientos (columna Ítems) aplicables en la Tabla CIP-011 R2 – Reutilización y Eliminación de Ciber Activos SEN.

R2 es calificado con Factor de Riesgo por Incumplimiento Bajo (FRIB).

M2. Medida de control o evidencia debe incluir cada uno de los Procesos Documentados que en conjunto incluyan cada uno de los requerimientos aplicables en la Tabla CIP-011 R2 – Reutilización y Eliminación de Ciber Activos SEN, y evidencia adicional para demostrar su implementación según lo descrito en columna Medidas de la misma tabla.

Tabla CIP-011 R2 – Reutilización y Eliminación de Ciber Activos SEN			
Ítem	**Aplicación**	**Requerimientos**	**Medidas**
2.1	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados SMCAE, SCAF y CAP.	Previo a la liberación por reutilización de Ciber Activos aplicables que contengan Información de Ciber Sistemas SEN (excepto para reutilización dentro de otros sistemas identificados en la columna "Aplicación" de esta tabla), la Entidad Responsable deberá tomar acciones para prevenir la recuperación o rescate no autorizado de Información de Ciber Sistemas SEN desde el medio de almacenamiento de datos del Ciber Activo.	Medidas de control o evidencias pueden incluir, pero no están limitadas a: • Registros que permitan trazar acciones de sanitización tomadas para prevenir el rescate no autorizado de Información de Ciber Sistemas SEN, tales como limpieza, purificación, o destrucción; o • Registros que permitan trazar acciones, tales como encriptación, retención en Perímetros de Seguridad Física (PSF), u otros métodos utilizados para prevenir el rescate no autorizado de Información de Ciber Sistemas SEN.
2.2	✓ Ciber Sistemas SEN de Impacto Alto y sus asociados SMCAE, SCAF y CAP; y ✓ Ciber Sistemas SEN de Impacto Medio y sus asociados	Previo a la eliminación (disposal) de Ciber Activos aplicables que contengan Información de Ciber Sistemas SEN, la Entidad Responsable deberá tomar acciones para prevenir la recuperación o rescate no autorizado de Información de Ciber Sistemas SEN desde el Ciber	Medidas de control o evidencias pueden incluir, pero no están limitadas a: • Registros que indiquen que el medio de almacenamiento de datos fue destruido previo a la eliminación de un Ciber Activo aplicable; o

	SMCAE, SCAF y CAP.	Activo, o destruir el medio de almacenamiento de los datos.	• Registro de acciones tomadas para prevenir el rescate no autorizado de Información de Ciber Sistemas SEN previo a la eliminación de un Ciber Activo aplicable.

7.10.4. Entrada en Vigor

El presente estándar CIP-011 entrará en vigor al momento de su aprobación por parte de la SEC y posterior publicación en la página web del Coordinador. Las Entidades Responsables tendrán un periodo de marcha blanca para implementar cada uno de los requerimientos en el estándar CIP-011 de acuerdo con los plazos máximos especificados en ANEXO 1, columna Marcha Blanca.

7.11. CIP-012: Ciber Seguridad – Comunicaciones entre Centros de Control

7.11.1. Propósito

Proteger la confidencialidad e integridad de datos transmitidos entre Centros de Control para la evaluación y monitoreo en tiempo real del SEN.

7.11.2. Aplicabilidad Específica y Excepciones

El presente estándar sólo aplica a Entidades Responsables que operan Centros de Despacho y Control y/o Centros de Control destinados a operar Ciber Sistemas SEN en instalaciones de impacto alto según lo definido en 6.1.

7.11.3. Requerimientos (R) y Medidas de Control (M)

R1. Cada Entidad Responsable deberá implementar, excepto bajos Circunstancias Excepcionales CIP, uno o más Planes documentados para mitigar los riesgos de divulgación y modificación no autorizada de datos para la evaluación y monitoreo en tiempo real del SEN, cuando dichos datos sean transmitidos entre Centros de Control aplicables. No se requiere que la Entidad Responsable incluya la una estrategia comunicacional en su Plan. El Plan deberá incluir:

1.1. Identificación de la protección de seguridad utilizada para mitigar riesgos generados por la divulgación y modificación no autorizada de datos para la evaluación y monitoreo en tiempo real del SEN, cuando dichos datos sean transmitidos entre Centros de Control;

1.2. Identificación de donde la Entidad Responsable aplicó protección de seguridad para transmitir datos entre Centros de Control para la evaluación y monitoreo en tiempo real del SEN; y

1.3. Si los Centros de Control son de propiedad u operados por las Entidades Responsables, identificación de las responsabilidades de cada Entidad Responsable para aplicar protección de seguridad para transmitir datos entre Centros de Control para la evaluación y monitoreo en tiempo real del SEN.

R1 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M1. Medida de control o evidencia puede incluir, pero no está limitada a, Planes documentados que reúnan los objetivos de seguridad en requerimiento R1 y documentación demostrando la implementación de dichos Planes.

7.11.4. Entrada en Vigor

El presente estándar CIP-012 entrará en vigor al momento de su aprobación por parte de la SEC y posterior publicación en la página web del Coordinador. Las Entidades Responsables tendrán un periodo de marcha blanca para implementar cada uno de los requerimientos en el estándar CIP-012 de acuerdo con los plazos máximos especificados en ANEXO 1, columna Marcha Blanca.

7.12. CIP-013: Ciber Seguridad – Gestión de Riesgos en la Cadena de Suministros

7.12.1. Propósito

Mitigar riesgos de ciberseguridad para una operación segura y confiable del SEN, implementando controles de seguridad para la gestión de riesgos en la cadena de suministro de Ciber Sistemas SEN.

7.12.2. Aplicabilidad Específica y Excepciones

No existe aplicabilidad específica adicional a lo definido en el punto 3 para el estándar CIP-013.

Se exceptúan los Ciber Activos asociados con redes de comunicaciones y enlaces de comunicaciones de datos entre Perímetros de Seguridad Electrónica (PSE) independientes.

7.12.3. Requerimientos (R) y Medidas de Control (M)

R1. Cada Entidad Responsable deberá desarrollar uno o más Planes documentados de gestión de riesgos de ciberseguridad para la cadena de suministro de Ciber Sistemas SEN de Impacto Alto y Medio. El(los) Plan(es) deberá(n) incluir:

1.1. Uno o más procesos utilizados en la planificación de adquisiciones de Ciber Sistemas SEN para identificar y evaluar los riesgos de ciberseguridad para el SEN de productos de fabricantes o proveedores de servicios que resulten de: i) la compra e instalación de equipos y software de fabricantes; y ii) transiciones de un fabricante a otro fabricante.

1.2. Uno o más procesos utilizados en la adquisición o compra de Ciber Sistemas SEN, que aborden lo siguiente, según aplique:

1.2.1. Notificación del fabricante de incidentes, identificados por el fabricante, relativos a productos o servicios suministrados a la Entidad Responsable que generen un riesgo de ciberseguridad a la dicha Entidad;

1.2.2. Coordinación de respuestas a incidentes, identificados por el fabricante, relativos a productos o servicios suministrados a la Entidad Responsable que generen un riesgo de ciberseguridad a la dicha Entidad;

1.2.3. Notificación de los fabricantes cuando el acceso remoto o local (on-site) ya no se requiera para algún representante del fabricante;

1.2.4. Divulgación por parte del fabricante de vulnerabilidades conocidas relacionadas con productos o servicios provistos a la Entidad Responsable;

1.2.5. Verificación de la integridad y autenticidad de todo software y parches provistos por el fabricante para uso en Ciber Sistemas SEN; y

1.2.6. Coordinación de controles para: i) Acceso Remoto Interactivo iniciado por el fabricante, ii) Acceso remoto sistema-s-sistema con fabricantes.

R1 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M1. Medida de control o evidencia debe incluir uno o más Planes de gestión de riesgos de ciberseguridad de la cadena de suministro según se especifica en requerimiento R1.

R2. Cada Entidad Responsable deberá implementar su(s) Plan(es) de gestión riesgos de ciberseguridad de la cadena de suministro según se especifica en requerimiento R1. La implementación del Plan no requiere que la Entidad Responsable renegocio o derogue contratos existentes (incluyendo adendas a contratos maestros y órdenes de compra). Adicionalmente, los siguientes aspectos están fuera del alcance del requerimiento R2: (1) los términos y condiciones de un contrato de compra real; y (2) desempeño de un fabricante y adherencia o cumplimiento a un contrato.

R2 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M2. Medida de control o evidencia debe incluir documentación para demostrar implementación los Planes de gestión de riesgos de ciberseguridad de la cadena de suministro, la cual podría incluir, pero no está limitada a, correspondencia, políticas, o documentos de trabajo que demuestren el uso del Plan de gestión de riesgos de ciberseguridad de la cadena de suministro.

R3. Cada Entidad Responsable deberá revisar y obtener la aprobación del Encargado CIP, o delegado, del(los) Plan(es) de gestión riesgos de ciberseguridad de la cadena de suministro especificado(s) en requerimiento R1, al menos una vez cada 15 meses calendario.

R3 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M3. Medida de control o evidencia debe incluir el o los Planes de gestión riesgos de ciberseguridad de la cadena de suministro fechados, aprobados por el Encargado CIP o delegado, y evidencia adicional para demostrar la revisión de dichos planes. Evidencia podrá incluir, pero no está limitada a, políticas, revisiones históricas, registro de revisiones, o evidencia de workflow de un sistema de gestión de documentos que indique revisión del Plan de gestión riesgos de ciberseguridad de la

cadena de suministro al menos una vez cada 15 meses calendario; y aprobación documentadas por parte del Encargado CIP o delegado.

7.12.4. Entrada en Vigor

El presente estándar CIP-013 entrará en vigor al momento de su aprobación por parte de la SEC y posterior publicación en la página web del Coordinador. Las Entidades Responsables tendrán un periodo de marcha blanca para implementar cada uno de los requerimientos en el estándar CIP-013 de acuerdo con los plazos máximos especificados en ANEXO 1, columna Marcha Blanca.

7.13. CIP-014: Ciber Seguridad – Seguridad Física

7.13.1. Propósito

Identificar y proteger instalaciones de generación y transmisión, y sus asociados CDCs o CCs principales, las cuales, de volverse inoperable, quedar indisponibles o dañarse como resultado de un ataque físico podría resultar en una inestabilidad, separación en islas no controlada, o falla en cascada en el SEN.

7.13.2. Aplicabilidad Específica y Excepciones

El presente estándar sólo aplica a los CDCs y CC principales (no de respaldo) especificados en 6.1.1 y 6.1.2, y a las instalaciones de generación y transmisión definidas en los puntos 6.2.1 a 6.2.6 del presente estándar.

7.13.3. Requerimientos (R) y Medidas de Control (M)

R1. Cada Entidad Responsable deberá realizar un análisis y evaluación de riesgo inicial (y subsiguientes) de sus instalaciones aplicables según 7.13.2, sean estas existentes o planificadas para entrar en servicio dentro de los próximos 24 meses. Dichas evaluaciones (inicial y subsiguientes) deberán contemplar uno o más análisis de transmisión diseñados para identificar las instalaciones que de ser dañadas, volverse inoperables o indisponibles, podría resultar en una inestabilidad, separación en islas no controlada, o falla en cascada en el SEN.

1.1. Las evaluaciones de riesgos subsiguientes deberán ser realizadas:

- Al menos una vez cada 30 meses calendario, por las Entidades Responsables que hayan identificado en su evaluación de riesgos previa (según lo verificado de acuerdo con requerimiento R2), una o más instalaciones que de ser dañadas, volverse inoperables o indisponibles, podría resultar en una inestabilidad, separación en islas no controlada, o falla en cascada en el SEN; o
- Al menos una vez cada 60 meses calendario, por las Entidades Responsables que no hayan identificado en su evaluación de riesgos previa (según lo verificado de acuerdo con requerimiento R2), ninguna instalación que, de ser dañada, volverse inoperable o indisponible, podría resultar en una inestabilidad, separación en islas no controlada, o falla en cascada en el SEN.

1.2. Las Entidades Responsables deberán identificar los CDCs y CCs primarios (o principales) que operacionalmente supervisan, monitorean y/o controlan las instalaciones identificadas en la evaluación de riesgos del requerimiento R1.

R1 es calificado con Factor de Riesgo por Incumplimiento Alto (FRIA).

M1. Medidas de control o evidencias aceptables pueden incluir, pero no están limitadas a, documentación por escrito (formato papel o electrónico) fechada de la evaluación de riesgos de instalaciones (existentes o planificadas para entrar en servicio dentro de los próximos 24 meses) que reúna los criterios de aplicabilidad según lo especificado requerimiento R1. Adicionalmente, evidencia aceptable podrá incluir, pero no está limitada a, documentación por escrito (formato papel o electrónico) fechada de la identificación de CDCs y CCs primarios (o principales) que operacionalmente supervisan, monitorean y/o controlan las instalaciones identificadas en la evaluación de riesgos del requerimiento R1, según lo especificado en R1, parte 1.2.

R2. Cada Entidad Responsable deberá realizar una verificación de la evaluación de riesgos realizada de acuerdo con requerimiento R1, a través de un tercero no relacionado con la Entidad Responsable. La verificación puede ser concurrente con o después de completada la evaluación de riesgos realizada según requerimiento R1.

2.1. Cada Entidad Responsable deberá seleccionar un organismo tercero (no relacionado) verificador que podrá ser:

- El Coordinador, quien cobrara por el servicio; o
- Un tercero especializado, o consultor independiente, con experiencia en estudios y análisis de planificación y operación de sistemas de transmisión.

2.2. El organismo no relacionado verificador deberá revisar la evaluación de riesgos realizada por parte de la Entidad Responsable según lo especificado en R1, revisión que podrá incluir recomendaciones para agregar o remover instalaciones. La Entidad Responsable deberá asegurar que la verificación es completada dentro de 90 días calendario seguidos al término de la evaluación de riesgos en requerimiento R1.

2.3. Si el organismo no relacionado verificador recomienda agregar o remover una instalación de la identificación realizada por la Entidad Responsable según requerimiento R1, la Entidad Responsable deberá, dentro de 60 días calendario de completada la verificación, y para cada instalación agregada o removida:

- Modificar la identificación realizada según requerimiento R1, en base a la recomendación; o
- Documentar las bases técnicas para no modificar la identificación según la recomendación.

2.4. Cada Entidad Responsable deberá implementar procedimientos, según lo establecido en la sección 5 sobre reserva y confidencialidad, para proteger información sensible o confidencial compartida con el organismo no relacionado verificador, y para proteger o eximir la divulgación publica de información sensible o confidencial desarrollada como parte del presente estándar.

R2 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M2. Medidas de control o evidencias aceptables pueden incluir, pero no están limitadas a, documentación por escrito (formato papel o electrónico) fechada que demuestre la realización, por parte de la Entidad Responsable, de una verificación del requerimiento R1 por parte de un tercero no relacionado, y satisfaciendo todas la recomendaciones según requerimiento R2, incluyendo, si aplicara, documentación de las bases técnicas para no modificar la identificación realizada según requerimiento R1 y especificado en la sección 2.3 de R2. Adicionalmente, evidencia aceptable podrá incluir, pero no está limitada a, documentación por escrito (formato papel o electrónico) fechada de procedimientos para proteger información según la sección 2.4 de R2.

R3. Para CDCs y CCs primarios (o principales) identificados por la Entidad Responsable propietaria de acuerdo con requerimiento R1, sección 1.2, que a) que operacionalmente supervisan, monitorean y/o controlan las instalaciones verificadas de acuerdo con requerimiento R2, y b) no está bajo el control operacional de dicha Entidad Responsable propietaria, esta última deberá, dentro de 7 días calendario de completado el requerimiento R2, notificar a la Entidad Responsable que tiene control operacional del CDC o CC primario de aquella identificación y la fecha en que se completó el requerimiento R2.

3.1. Si una instalación previamente identificada bajo requerimiento R1 y verificada de acuerdo con requerimiento R2, es removida de una identificación durante una subsecuente evaluación de riesgos realizada de acuerdo con requerimiento R1, o una verificación de acuerdo con requerimiento R2, entonces la Entidad Responsable propietaria deberá, dentro de 7 días calendario seguidos a la verificación o subsecuente evaluación de riesgos, notificar a la Entidad Responsable que tiene control operacional del CDC o CC primario, de dicha remoción.

R3 es calificado con Factor de Riesgo por Incumplimiento Bajo (FRIB).

M3. Medidas de control o evidencias aceptables pueden incluir, pero no están limitadas a, notificaciones o comunicaciones por escrito (formato papel o electrónico) fechadas que demuestren que la Entidad Responsable propietaria notificó a cada Entidad Responsable según aplica y de acuerdo con requerimiento R3.

R4. Cada Entidad Responsable que identifique instalaciones eléctricas, CDCs o CCs primarios en requerimiento R1 y verificadas de acuerdo con requerimiento R2, y cada

Entidad Responsable notificada por un Entidad Responsable propietaria de acuerdo con requerimiento R3, deberán conducir una evaluación de potenciales amenazas y vulnerabilidades de ataques físicos a cada una de sus respectivas instalaciones eléctricas, CDCs y CCs primarios identificados en requerimiento R1 y verificados de acuerdo con requerimiento R2. La evaluación deberá considerar lo siguiente:

4.1. Características únicas de las instalaciones eléctricas, CDCs y CCs primarios identificadas y verificadas;

4.2. Historial previo de ataques en instalaciones similares, tomando en cuenta la frecuencia, proximidad geográfica, y severidad de los eventos pasados relacionados con la seguridad física; y

4.3. Advertencias de amenazas o información de inteligencia recibida de parte de entidades encargadas de la seguridad pública como fuerzas especiales, policías locales, fuerzas armadas, policía de investigaciones, bomberos y otras entidades a cargo de la seguridad pública.

R4 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M4. Medidas de control o evidencias aceptables pueden incluir, pero no están limitadas a, documentación por escrito (formato papel o electrónico) fechadas que demuestren que la Entidad Responsable condujo una evaluación de potenciales amenazas y vulnerabilidades de ataques físicos a sus respectivas instalaciones eléctricas, CDCs y CCs primarios, según se especifica requerimiento R4.

R5. Cada Entidad Responsable que identifique instalaciones eléctricas, CDCs o CCs primarios en requerimiento R1 y verificadas de acuerdo con requerimiento R2, y cada Entidad Responsable notificada por un Entidad Responsable propietaria de acuerdo con requerimiento R3, deberán desarrollar e implementar Planes de seguridad física documentados que cubran sus respectivas instalaciones. El o los Planes de seguridad física deberán ser implementados dentro de 120 días calendario de completado el requerimiento R2 y ejecutado de acuerdo con el cronograma especificado en dicho Plan o Planes de seguridad física. El Plan o Planes de seguridad física deberán incluir los siguientes atributos:

5.1. Medidas de seguridad y resiliencia diseñadas conjuntamente para disuadir, detectar, retrasar, evaluar, comunicar, y responder a potenciales amenazas físicas y vulnerabilidades identificadas durante la evaluación conducida en requerimiento R4.

5.2. Información de contacto y coordinación de autoridades encargadas de la seguridad pública.

5.3. Un cronograma para la ejecución de las mejoras y modificaciones de seguridad físicas de instalaciones especificadas en el plan de seguridad física;

5.4. Consideraciones para evaluar la evolución de amenazas físicas a instalaciones, y sus correspondientes medidas de seguridad.

R5 es calificado con Factor de Riesgo por Incumplimiento Alto (FRIA).

M5. Medidas de control o evidencias aceptables pueden incluir, pero no están limitadas a, documentación por escrito (formato papel o electrónico) fechadas de los planes de seguridad física que cubran las respectivas instalaciones identificadas y verificadas según lo especificado en requerimiento R5, y evidencia adicional que demuestre la ejecución de los planes de seguridad física de acuerdo con los cronogramas definidos en dichos planes.

R6. Cada Entidad Responsable que identifique instalaciones eléctricas, CDCs o CCs primarios en requerimiento R1 y verificadas de acuerdo con requerimiento R2, y cada Entidad Responsable notificada por un Entidad Responsable propietaria de acuerdo con R3, deberán realizar una revisión de la evaluación realizada según requerimiento R4 y del plan de seguridad desarrollado según requerimiento 5, a través de un tercero no relacionado con la Entidad Responsable. La verificación puede ser concurrente con o después de completada la evaluación realizada según requerimiento R5.

6.1. Cada Entidad Responsable deberá seleccionar un organismo tercero (no relacionado) revisador entre los siguiente:

- Una entidad u organización con experiencia en seguridad física en la industria eléctrica y cuyo personal revisor tenga al menos un miembro que posea una Certificación de Protección Profesional (CPP), una Certificación Profesional de Seguridad Física (PSP), u otra certificación válida equivalente;
- Una entidad u organización aprobada por la SEC;
- Una agencia gubernamental con experiencia en seguridad física; o
- Una entidad u organización con experiencia demostrada en seguridad pública seguridad física militar o gubernamental.

6.2. La Entidad Responsable deberá asegurar que la revisión por parte del tercero no relacionado es completada dentro de 90 días calendario del término del Plan de seguridad desarrollado en requerimiento R5. La revisión por parte del tercero no relacionado podrá incluir cambios recomendados.

6.3. Si el organismo no relacionado revisor recomienda cambios a la evaluación realizada según requerimiento R4 o el Plan de seguridad desarrollado según requerimiento R5, la Entidad Responsable deberá, dentro de 60 días calendario de completada la revisión, para cada recomendación:

- Modificar su evaluación o Plan de seguridad consistentemente con la recomendación; o
- Documentar las razones para no modificar la evaluación o Plan de seguridad consistentemente con la recomendación.

6.4. Cada Entidad Responsable deberá implementar procedimientos, según lo establecido en la sección 5 sobre reserva y confidencialidad, para proteger información sensible o confidencial compartida con el organismo no relacionado revisor, y para proteger o eximir la divulgación publica de información sensible o confidencial desarrollada como parte del presente estándar.

R6 es calificado con Factor de Riesgo por Incumplimiento Medio (FRIM).

M6. Medidas de control o evidencias aceptables pueden incluir, pero no están limitadas a, documentación por escrito (formato papel o electrónico) fechada que demuestre la realización, por parte de la Entidad Responsable, de una revisión de la evaluación realizada según requerimiento R4 y el Plan de seguridad según requerimiento R5 por parte de un tercero no relacionado según lo especificado en requerimiento R6, incluyendo, si aplicara, documentación de las razones para no modificar la evaluación o Plan de seguridad de acuerdo con las recomendaciones según la sección 6.3 de R6. Adicionalmente, evidencia aceptable podrá incluir, pero no está limitada a, documentación por escrito (formato papel o electrónico) fechada de procedimientos para proteger información según la sección 6.4 de R6.

7.13.4. Entrada en Vigor

El presente estándar CIP-014 entrará en vigor al momento de su aprobación por parte de la SEC y posterior publicación en la página web del Coordinador. Las Entidades Responsables tendrán un periodo de marcha blanca para implementar cada uno de los requerimientos en el estándar CIP-014 de acuerdo con los plazos máximos especificados en ANEXO 1, columna Marcha Blanca.

ANEXO 1 – Tabla Resumen de Requerimientos y su Implementación

Estándar	Req.	Descripción	Impacto	FRI	Marcha Blanca
CIP-002 Categorización de Ciber Sistemas SEN	R1	Proceso de identificación de Ciber Sistemas SEN.	A-M-B	Alto	6 meses
	R2	Revisión y aprobación de R1.	A-M-B	Bajo	6 meses
CIP-003 Controles de Gestión de la Seguridad	R1	Políticas de ciberseguridad (Plazo para desarrollo de políticas)	A-M-B	Medio	4-12 meses
	R2	Planes de ciberseguridad. (Plazo para desarrollo de políticas)	B	Bajo	4-12 meses
	R3	Identificación de encargado CIP.	A-M-B	Medio	3 meses
	R4	Proceso de delegación.	A-M-B	Bajo	3 meses
CIP-004 Personal y Capacitación	R1	Programa de conciencia de seguridad.	A-M	Bajo	6 meses
	R2	Programa de capacitación en ciberseguridad.	A-M	Bajo	6 meses
	R3	Programa de evaluación de riegos del personal.	A-M	Medio	12 meses
	R4	Programa de administración de accesos.	A-M	Medio	12 meses
	R5	Programa de revocación de accesos.	A-M	Medio	6 meses
CIP-005 Perímetro de Seguridad Electrónica (PSE)	R1	Proceso para perímetro de seguridad electrónica.	A-M	Medio	12 meses
	R2	Proceso de administración de acceso remoto interactivo.	A-M	Medio	12 meses
CIP-006 Seguridad Física de Ciber Sistemas SEN	R1	Plan de seguridad 4ísica.	A-M	Medio	6 meses
	R2	Programa de control de visitas.	A-M	Medio	18 meses
	R3	Programas de prueba y mantenimiento de SCAF.	A-M	Medio	18 meses
CIP-007 Gestión de la Seguridad de Sistemas	R1	Proceso para puertos y servicios.	A-M	Medio	12 meses
	R2	Proceso para administración de parches de seguridad.	A-M	Medio	12 meses
	R3	Proceso para prevención de código malicioso.	A-M	Medio	12 meses
	R4	Proceso para el monitoreo de eventos de seguridad.	A-M	Medio	12 meses
	R5	Proceso para controles de acceso a sistemas.	A-M	Medio	12 meses

Estándar	Req.	Descripción	Impacto	FRI	Marcha Blanca
CIP-008 Reporte de Incidentes y Planes de Respuesta	R1	Plan de Respuesta a incidentes de ciberseguridad.	A-M	Bajo	6 meses
	R2	Implementación y prueba de plan en R1.	A-M	Bajo	12 meses
	R3	Revisión, actualización y comunicación de plan en R1.	A-M	Bajo	12 meses
CIP-009 Planes de Recuperación para Ciber Sistemas SEN	R1	Plan de Recuperación.	A-M	Medio	8 meses
	R2	Implementación y prueba de plan en R1.	A-M	Bajo	12 meses
	R3	Revisión, actualización y comunicación de plan en R1	A-M	Bajo	12 meses
CIP-010 Gestión de Cambio de Configuración y Evaluación de Vulnerabilidades	R1	Proceso de gestión de cambio de configuración.	A-M	Medio	10 meses
	R2	Proceso para Monitoreo de Configuración.	A	Medio	10 meses
	R3	Proceso para evaluación de vulnerabilidades.	A-M	Medio	10 meses
	R4	Plan para ciber activos transitorios.	A	Medio	10 meses
CIP-011 Protección de Información	R1	Programa de protección de información.	A-M	Medio	8 meses
	R2	Proceso para reutilización y eliminación de ciber activos SEN.	A-M	Bajo	8 meses
CIP-012 Comunicaciones entre Centros de Control	R1	Plan para mitigar riesgos de ciberseguridad sobre datos transmitidos entre centros de control.	A	Medio	18 meses
CIP-013 Gestión de Riesgos en la Cadena de Suministros	R1	Plan para gestión de riesgos de ciberseguridad en la cadena de suministro.	A-M	Medio	12 meses
	R2	Implementación de Plan en R1	A-M	Medio	24 meses
	R3	Aprobación de R1 por Encargado CIP	A-M	Medio	12 meses
CIP-014 Seguridad Física	R1	Evaluación de riesgos e identificación de instalaciones.	A-M	Alto	6 meses
	R2	Verificación de tercero de evaluación de riesgos en R1.	A-M	Medio	9 meses
	R3	Notificación a entidad responsable.	A	Bajo	9 meses
	R4	Evaluación de amenazas y vulnerabilidades.	A-M	Medio	12 meses
	R5	Desarrollo e implementación de plan de seguridad física.	A-M	Alto	18 meses
	R6	Revisión de tercero de R4 y R5.	A-M	Medio	24 meses