

Lineamientos De Ciberseguridad

Versión:	4
Código	TEC-N-1
Fecha de aprobación:	15/11/2022
Proceso responsable:	Tecnología
Aprobado por:	Comité Directivo

Lineamientos de la Política de Ciberseguridad

Contenido

1. Objetivo	3
2. Alcance	3
3. Descripción de los Lineamientos	3
3.1 ORGANIZACIÓN PARA LA CIBERSEGURIDAD	3
3.1.1 Responsable de ciberseguridad	3
3.1.2 Evaluación y planes para personal	3
3.1.2.1 Evaluación personal	4
3.1.2.2 Programa de conciencia de seguridad	4
3.1.2.3 Programa de entrenamiento y capacitación	4
3.2 CLASIFICACIÓN Y CONTROL DE CIBER ACTIVOS	4
3.2.1 Activos críticos	4
3.2.2 Ciberactivos críticos	5
3.3 TRATAMIENTO Y GESTIÓN DEL CIBER RIESGO	5
3.4 SEGURIDAD FÍSICA Y DEL ENTORNO	5
3.4.1 Plan de seguridad física	5
3.4.2 Restricción de acceso físico	6
3.4.3 Control de visitantes	6
3.4.4 Listas de acceso	6
3.4.5 Mantenimiento y pruebas de control de acceso	7
3.4.6 Monitoreo y registro de acceso	7
3.5 CONTROL DE ACCESO A LOS CIBER ACTIVOS	7
3.5.1 Gestión acceso a la información	7
3.5.2 Perímetros de seguridad electrónica	7
3.5.3 Procedimiento organizacional y técnico de puntos de acceso	7
3.5.4 Administración de accesos	7
3.5.5 Verificación de cuentas y privilegios de acceso	7
3.5.6 Revocación de accesos	8
3.5.7 Autenticación, autorización y registro	8
3.5.8 Monitoreo y registro de acceso	9
3.5.9 Validación de cambios	9
3.5.9 Procedimiento para habilitar los puntos de acceso	9
3.5.10 Listas de acceso	9
3.5.11 Administración de conexiones temporales	9
3.5.12 Sistema de control intermedio	9
3.6 GESTIÓN DE LA SEGURIDAD DE CIBERACTIVOS CRÍTICOS	10
3.6.1 Procedimiento información	10
3.6.2 Medidas para garantizar información	10
3.6.3 Control de cambios y gestión	10
3.6.4 Herramientas de prevención	10

3.6.5 Evaluación de vulnerabilidades	11
3.6.6 Control ciberactivos transitorios y medios extraíbles	11
3.6.7 Actualizaciones y parches de seguridad	11
3.6.8 Identificar y monitorear eventos	12
3.7 GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD	12
3.7.1 Respuesta a incidentes de ciberseguridad	12
3.7.2 Pruebas o simulacros.....	12
3.7.3 Registro de cambios del procedimiento de respuesta a incidentes	12
3.8 PLAN DE RECUPERACIÓN DE CIBERACTIVOS CRÍTICOS	13
3.8.1 Recuperación de desastres.....	13
3.8.2 Pruebas o simulacros.....	13
4. Excepciones.....	13
5. Definiciones.....	13
6. Anexos	15
Control de cambios.....	20

1. Objetivo

Definir los detalles de cómo se debe implementar la Política de ciberseguridad de CELSIA, que se consiguen con la aplicación de estos controles de ciberseguridad, para gestionar un nivel de ciber riesgo aceptable.

2. Alcance

Estos lineamientos son aplicables a todos los colaboradores, proveedores, contratistas, terceras partes, que ingresen física o remotamente a los perímetros de seguridad y accedan a ciber activos críticos propiedad de CELSIA y sus filiales.

Los lineamientos deben ser revisados como mínimo una vez al año o cuando sea necesario.

3. Descripción de los Lineamientos

3.1 Organización para la Ciberseguridad

3.1.1 Responsable de ciberseguridad

Talento Humano y Soluciones Organizacionales debe asignar un responsable de Ciberseguridad formalmente y notificarlo al CNO, en caso de modificación se debe contemplar:

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

En caso de delegación se debe contemplar:

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

Registros

- Documento formal enviado al CNO donde se evidencie la asignación del responsable o de ciberseguridad, y las novedades frente a esta asignación.
- Documento con el procedimiento de delegación de la autoridad.

3.1.2 Evaluación y planes para personal

El personal que tiene acceso lógico autorizado o acceso físico no escoltado a ciberactivos críticos, incluyendo contratistas y prestadores de servicios deben tener una evaluación de riesgos de personal que cumplan con planes de concientización, capacitación y entrenamiento.

Registros

- Evidencia documentada de la evaluación de riesgo de personal.

3.1.2.1 Evaluación personal

Talento Humano y Soluciones Organizacionales debe realizar la evaluación de riesgos del personal propio, externo y la cadena de suministro para otorgar y conservar el acceso físico autorizado y lógico a los ciber activos críticos.

- La evaluación de riesgos del personal debe incluir:
- Confirmar la identidad de las personas.

Estudio de seguridad incluyendo validación de antecedentes al inicio y con una revisión periódica no superior a cinco (5) años

Registros

- Documento procedimiento de evaluación y confirmación de identidad.
- Estudio de seguridad incluyendo validación de antecedentes.

3.1.2.2 Programa de conciencia de seguridad

Tecnología debe contar con un programa de conciencia de seguridad, se debe realizar concientización anual para todos los empleados y terceros que tienen acceso a los ciberactivos críticos.

Registros

- Documento programa de concientización y evidencia que se realizó el plan de concientización.

3.1.2.3 Programa de entrenamiento y capacitación

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

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

Registros

- Documento programa de concientización y evidencia que se realizó el plan de concientización.

3.2 Clasificación y control de ciber activos

3.2.1 Activos críticos

Generación, Transmisión y Distribución y Talento Humano y Soluciones Organizacionales implementará y realizará el inventario de los activos críticos basado en los criterios que se encuentran en la definición activo crítico y la metodología de identificación de activos críticos.

Registros

- Lista de activos críticos.

3.2.2 Ciberactivos críticos

Generación, Transmisión y Distribución y Talento Humano y Soluciones Organizacionales será responsable de identificar y priorizar los ciber activos críticos de acuerdo con los ciber riesgos y exposiciones de ciberseguridad en un inventario actualizado aplicando la metodología de identificación de activos críticos según el requisito anterior; con el objetivo de evitar pérdidas financieras, operativas y/o de imagen para la organización.

Registros

- Lista de ciberactivos críticos

3.3 Tratamiento y Gestión del ciber riesgo

Generación, Transmisión y Distribución, Talento Humano y Soluciones Organizacionales son responsables de analizar, priorizar y realizar el tratamiento de los ciber riesgos con base en los objetivos de negocio y alineados con la política de gestión de riesgos.

En los proyectos o nuevas adquisiciones se debe realizar la identificación de los activos críticos y ciber activos críticos, los riesgos, vulnerabilidades y el nivel de gestión de ciberseguridad en la operación para establecer un plan de ciberseguridad.

Periódicamente se debe realizar una valoración del riesgo para contemplar los cambios en los requisitos de ciberseguridad y la situación de riesgo, tales como cambio en los activos críticos y ciber activos críticos, las amenazas, las vulnerabilidades y los impactos. Se debe decidir cuándo un riesgo es aceptable, ya sea por motivos de objetivos de negocio o por costes no rentables.

Los posibles tratamientos a los riesgos identificados incluyen:

- Evitar el riesgo.
- Disminuir la probabilidad de ocurrencia.
- Disminuir el impacto.
- Transferir los riesgos.
- Retener los riesgos.

Registros

- Matriz de evaluación de riesgos para los proyectos.
- Riesgos de la operación consignados en la herramienta corporativa para la gestión del riesgo.

3.4 Seguridad Física y del Entorno

3.4.1 Plan de seguridad física

Protección de Recursos debe tener un plan de seguridad física documentando la implementación, revisión y actualización del control, monitoreo, registro y mantenimiento y pruebas del acceso físico y de los sistemas de seguridad.

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

- Identificar de todos los puntos de acceso físico para cada perímetro de seguridad física y las medidas para controlar el acceso a esos puntos.
- Definir los procedimientos y herramientas para monitorear el acceso físico a los perímetros.
- Definir la emisión de alertas o alarmas en respuesta al acceso no autorizado, al personal de respuesta a incidentes de ciberseguridad.

Documentar e implementar las operaciones y procedimientos de control para manejar y registrar el acceso físico a todos los puntos de acceso del perímetro(s) de seguridad física.

Registros

- Documento con el plan de seguridad física cumpliendo los requisitos.

3.4.2 Restricción de acceso físico

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

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

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

Registros

- Evidencia de los controles implementados para protección física del cableado y otros componentes de comunicación.
- Alarma o alerta en respuesta a fallas de comunicación detectadas.

3.4.3 Control de visitantes

Protección de Recursos deberá implementar y documentar un procedimiento de control de visitantes que incluyan los requisitos aplicables al acceso de los visitantes en cada perímetro de seguridad física.

Protección de Recursos implementará un procedimiento de mantenimiento y pruebas para garantizar que los sistemas de seguridad física funcionan adecuadamente.

Registros

- Documento procedimiento control de visitantes.

3.4.4 Listas de acceso

Protección de Recursos mantendrá lista(s) del personal con acceso físico a los ciberactivos críticos, revisará semestralmente la lista y la actualizará en siete (7) días calendario ante cualquier cambio.

Registros

- Bitácora con registro de acceso del personal y Evidencias documentales de la verificación.

3.4.5 Mantenimiento y pruebas de control de acceso

Protección de Recursos tendrá un procedimiento de mantenimiento y pruebas del sistema de control de acceso.

Registros

- *Documento procedimiento de mantenimiento y pruebas periódicas a los sistemas de control relacionados a la seguridad física*
Evidencia mantenimiento

3.4.6 Monitoreo y registro de acceso

Protección de Recursos implementará y documentará un procedimiento para el monitoreo y registro de accesos físicos permitidos y denegados en puntos de acceso al (los) perímetro(s) de seguridad electrónica veinticuatro (24) horas al día, siete (7) días por semana.

Registros

- *Documento con procedimientos para el monitoreo y registro de accesos físicos lógicos.*

3.5 Control de acceso a los ciber activos

3.5.1 Gestión acceso a la información

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

Registros

- *Procedimiento para gestión de acceso a la información de ciberactivos críticos.*

3.5.2 Perímetros de seguridad electrónica

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

Registros

- *Documento con los perímetros de seguridad y requisitos de accesos.*

3.5.3 Procedimiento organizacional y técnico de puntos de acceso

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

Registros

- *Procedimiento organizacional y técnico de puntos de acceso.*

3.5.4 Administración de accesos

Tecnología deberá implementar actividades de administración de acceso lógico y físico.

3.5.5 Verificación de cuentas y privilegios de acceso

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

Registros

- *Evidencias documentadas de la verificación periódica.*

3.5.6 Revocación de accesos

Tecnología deberá implementar un procedimiento de revocación de acceso documentado los cuales incluyan los siguientes escenarios:

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

Registros

- *Documento procedimiento para revocación de acceso:*
 - *Bloqueo (terminación laboral)*
 - *Revocación (eliminar o inhabilitar)*
 - *Cambio de contraseñas (terminación laboral)*
 - *Cambio de contraseñas (reasignaciones o transferencias)*

3.5.7 Autenticación, autorización y registro

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

Las cuentas del colaborador, de herramientas o dispositivos deberán considerar los siguientes aspectos:

- *La longitud de la contraseña no debe ser inferior a once (11) caracteres.*
- *Las contraseñas deben contar con una mezcla de caracteres alfabéticos (donde se combinen las mayúsculas y las minúsculas), dígitos e incluso caracteres especiales (@, j, +, &).*
- *No almacenar las contraseñas en un lugar público y al alcance de los demás.*
- *La contraseña no debe contener el nombre de usuario de red, o cualquier otra información personal fácil de averiguar, tampoco una serie de letras dispuestas adyacentemente en el teclado (qwerty) o siguiendo un orden alfabético o numérico (123456, abcde, etc.)*
- *Las cuentas del colaborador, de herramientas o dispositivos que vengan por omisión se deben deshabilitar inmediatamente después de la instalación de los sistemas o software.*
- *Las contraseñas predeterminadas por el proveedor se deben cambiar inmediatamente después de la instalación de los sistemas, software o dispositivos.*

- No compartir las contraseñas, son personales e intransferibles.

Registros

- Procedimiento de autenticación, autorización y registro.

3.5.8 Monitoreo y registro de acceso

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

Registros

- Documento procedimiento para el monitoreo y registro de accesos físicos y lógicos.

3.5.9 Validación de cambios

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

Registros

- Documento procedimiento de control de cambios.
- Evidencia documental de los cambios realizados.

3.5.9 Procedimiento para habilitar los puntos de acceso

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

Registros

- Documento de línea base para equipos de punto de acceso al perímetro.

3.5.10 Listas de acceso

Tecnología revisará la lista de su personal con acceso lógico a ciberactivos críticos semestralmente y actualizará la lista en siete (7) días calendario ante cualquier cambio.

Registros

- Lista del personal con acceso físico no escoltado o acceso lógico a los ciberactivos críticos.
- Evidencia documental de los cambios realizados.

3.5.11 Administración de conexiones temporales

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

Registros

- Documento procedimiento de administración de conexiones temporales.

3.5.12 Sistema de control intermedio

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

Registros

- Documento de inventario.
- Evidencia de la revisión periódica del control implementado.

3.6 Gestión de la seguridad de ciberactivos críticos**3.6.1 Procedimiento información**

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

Registros

- Procedimiento para identificar, clasificar y proteger la información asociada con los ciberactivos críticos.

3.6.2 Medidas para garantizar información

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

Registros

- Evidencia documentada de que se realizan pruebas de respaldo y su resultado.

3.6.3 Control de cambios y gestión

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

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

Registros

- Documento procedimiento gestión de cambios y gestión de configuración.
- Evidencias con los cambios realizados.

3.6.4 Herramientas de prevención

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

Registros

- Evidencia de implementación de herramientas de prevención de software malicioso.

3.6.5 Evaluación de vulnerabilidades

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

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

Tecnología deberá realizar una evaluación de vulnerabilidad antes de adicionar un nuevo ciber activo al entorno de producción, y también cuando se realicen reemplazos programados de ciberactivos existentes.

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

Registros

- Evidencia de evaluación periódica de vulnerabilidades.
- Evidencia de vulnerabilidades sobre nuevos activos.
- Plan de acción del resultado de análisis de vulnerabilidad.

3.6.6 Control ciberactivos transitorios y medios extraíbles

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

Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se monitorea el uso de dispositivos USB, medios removibles; la autorización de uso de los medios removibles debe ser autorizada a través del líder del proceso y se debe llevar un registro de los medios autorizados.

Todas las estaciones de trabajo que soportan las tecnologías de la operación deben tener los puertos USB deshabilitados.

Tecnología establecerá y documentará un procedimiento para control de ciberactivos transitorios y medios extraíbles tales como USB, discos removibles, entre otros.

Registros

- Documento procedimiento control transitorio y medios extraíbles.
- Evidencias de control periódico.

3.6.7 Actualizaciones y parches de seguridad

Tecnología deberá implementar y mantener un procedimiento de actualizaciones y parches de seguridad, donde sea técnicamente factible.

Registros

- Documento procedimiento de actualización e implementación de parches.
- Evidencias de los ciclos de parchado.

3.6.8 Identificar y monitorear eventos

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

Registros

- Documento procedimiento de monitoreo.
- Evidencia de controles implementados.

3.7 Gestión de incidentes de ciberseguridad

3.7.1 Respuesta a incidentes de ciberseguridad

Tecnología debe disponer de procedimientos de gestión y respuesta a incidentes documentados.

Se debe tener y revisar con periodicidad anual los planes de respuesta a incidentes para los ciberactivos críticos, este debe considerar como mínimo:

- Identificar, clasificar y especificar las acciones y procedimientos requeridos en respuesta a eventos.

El reporte de incidentes se hará en cumplimiento con los acuerdos y procedimientos definidos para el CNO, y se publicará a los entes de control una vez sea verificada la veracidad y naturaleza del evento.

Registros

- Documento plan de recuperación y respuesta a incidentes y los procedimientos asociados.

3.7.2 Pruebas o simulacros

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

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

Tecnología debe disponer de registros documentales de las pruebas o simulacros que se realicen periódicamente y las acciones de mejora como resultados de las pruebas, así como, documentación de la divulgación de los mismos. Estos deben reflejarse máximo noventa (90) días después de realizadas las pruebas y/o simulacros.

Registros

- Evidencia de pruebas o simulacros, y acciones de mejora de estos.

3.7.3 Registro de cambios del procedimiento de respuesta a incidentes

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

Registros

- Evidencia de los cambios realizados a los procedimientos.

3.8 Plan de recuperación de ciberactivos críticos

3.8.1 Recuperación de desastres

Tecnología debe disponer de procedimientos de recuperación de desastres documentados.

Se debe tener y revisar con periodicidad anual los planes de recuperación de desastres para los ciberactivos críticos, este debe considerar como mínimo:

- *Las condiciones que podrían activar los planes de recuperación, escalamiento a nivel interno y externo.*
- *Definir los roles y responsabilidades de los recursos asignados.*
- *Incluir los procedimientos para el respaldo y almacenamiento de la información necesaria para la recuperación efectiva de los ciberactivos críticos.*
- *Procedimientos de verificación de respaldos que confirmen que estos se realicen de manera satisfactoria y asegurar que la información sea íntegra y esté disponible.*

Registros

- *Documento plan de recuperación y los procedimientos asociados.*

3.8.2 Pruebas o simulacros

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

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

Tecnología debe disponer de registros documentales de las pruebas o simulacros que se realicen periódicamente y las acciones de mejora como resultados de las pruebas, así como, documentación de la divulgación de los mismos. Estos deben reflejarse máximo noventa (90) días después de realizadas las pruebas y/o simulacros.

Tecnología debe disponer de registros documentales sobre las pruebas de los respaldos.

Registros

- *Evidencia que se realizan pruebas de respaldo y su resultado.*

4. Excepciones

Las excepciones a cualquiera de los lineamientos de ciberseguridad deben ser aprobados por Tecnología, la cual puede requerir autorización del Líder de CELSIA y del Líder de Gestión Humana Administrativa y Tecnología. Todas las excepciones a la política deben ser formalmente documentadas, registradas y revisadas.

5. Definiciones

Para los propósitos de este documento, se definen los siguientes conceptos:

- **Activo crítico:** *Instalaciones, sistemas o equipo eléctrico que, si es destruido, degradado o puesto indisponible, afecta la confiabilidad u operatividad del sistema eléctrico. Acorde con*

las recomendaciones del Comité Tecnológico del CNO para la definición de activos críticos que comprometan la seguridad de operación del SIN.

- Cada grupo de unidades de generación en una localización de planta simple con capacidad efectiva neta mayor o igual 20 MW.
 - Cada recurso o grupo de recursos de potencia reactiva (excepto generadores) instalados desde el Nivel IV hasta el STN.
 - Todas las subestaciones con sus respectivas bahías, en aquellas subestaciones con nivel de tensión IV y superior que a criterio del operador del sistema se consideren.
 - Flexible AC Transmisión Systems (FACTS), que, a criterio del operador del sistema, pertenezcan a cortes críticos desde el punto de vista de confiabilidad.
 - Esquemas especiales de protección como los esquemas suplementarios, que operan de tal manera que garantizan la confiabilidad del sistema.
 - Cada sistema que ejecuta desconexión automática de carga por bajo voltaje o baja frecuencia.
 - Cada centro de control o centro de control de respaldo usado para ejecutar las obligaciones funcionales del operador del sistema, Generador, Transmisor o Distribuidor.
 - Cualquier activo adicional que soporte la operación confiable de interconexiones internacionales.
 - Cualquier activo adicional que soporte la operación confiable del SIN que la entidad responsable estime adecuado incluir en su evaluación.
- **Ciberactivo:** Dispositivo electrónico programable y elementos de las redes de comunicaciones incluyendo hardware, software, datos e información. Así como aquellos elementos con protocolos de comunicación enrutables, que permitan el acceso al mismo de forma local o remota.
 - **Ciberactivo crítico:** Dispositivo para la operación confiable de activos críticos que cumple los siguientes atributos:
 - El ciber activo usa un protocolo enrutable para comunicarse afuera del perímetro de seguridad electrónica, o,
 - El ciber activo usa un protocolo enrutable con un centro de control, o,
 - El ciber activo es accesible por marcación.
 - **Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
 - **Desastre o contingencia:** interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras u otros medios necesarios para la operación normal de un negocio.
 - **Disponibilidad:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
 - **Evento de ciberseguridad:** presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de ciberseguridad o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
 - **Lineamientos de ciberseguridad:** son productos, procedimientos y métricas aprobadas, que definen en detalle como las políticas de seguridad serán implementadas para un ambiente en particular, teniendo en cuenta las fortalezas y debilidades de las características

de seguridad disponibles. Deben estar reflejadas en un documento que describe la implantación de una guía para un componente específico de hardware, software o infraestructura.

- **Integridad:** propiedad de salvaguardar la exactitud y el estado completo de los activos.
- **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información, además puede involucrar otras propiedades tales como: autenticidad, trazabilidad (accountability), no repudio y fiabilidad.
- **Vulnerabilidad:** debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas.

6. Anexos

- TEC-I-25_Metodología Identificación activos críticos
- TEC-P-34_Plan de respuesta ante incidentes
- Lista de cumplimiento de la política de Ciberseguridad.

Cap.	#	Acción	Actividad / Soporte / Evidencia *	Periodo de revisión (meses)	SI/NO
cumplimiento	3	Cumplimiento	Reportes de auditorías internas	24	
IDENTIFICACIÓN DE ACTIVOS CRÍTICOS	4.3	Identificación activos críticos	Aprobar por parte del responsable la lista de activos y ciberactivos críticos	Cada vez que se actualice	
			Certificar que el inventario de activos y ciberactivos críticos esta actualizado (reporte de auditoría)	24	
	4.3.1	Activos críticos	Realizar lista de activos críticos	12	
	4.3.2	Ciberactivos críticos	Realizar lista de ciberactivos críticos	24	
GOBIERNO Y GESTIÓN DEL PERSONAL	5.3.1	Política y lineamiento de ciberseguridad	Documento política o lineamiento de ciberseguridad	Cada vez que se requiera	
	5.3.2	Responsable de ciberseguridad	Documento formal enviado al CNO donde se evidencie la asignación del responsable o de ciberseguridad, y las novedades frente a esta asignación (reportar el cambio de responsable con máximo 30 días hábiles de antelación y por desvinculación en máximo 5 días hábiles)	Cada vez que se actualice	
			Documento procedimiento de delegación de la autoridad	Un (1) mes, cualquier cambio de delegación	
	5.3.3	Evaluación personal y riesgos	Documento procedimiento de evaluación y confirmación de identidad	24	
Cap.	#	Acción	Actividad / Soporte / Evidencia *	Periodo de revisión (meses)	SI/NO
cumplimiento	3	Cumplimiento	Reportes de auditorías internas	24	
			Estudio de seguridad incluyendo validación de antecedentes	Al inicio y antes de 60 meses	

	5.3.4	Programa de conciencia de seguridad	Documento programa de concientización y evidencia que se realizó el plan de concientización	24	
	5.3.5	Programa de entrenamiento y capacitación	Documento programa de entrenamiento y capacitación según el rol desempeñado y su criticidad	24	
	5.3.6	Administración de accesos	Documento procedimiento para gestión de accesos lógicos y físicos	24	
	5.3.7	Verificación de los registros de autorización	Evidencias documentales de la verificación periódica	6	
	5.3.8	Verificación de cuentas y privilegios de acceso	Evidencias documentales de la verificación periódica	12	
	5.3.9	Procedimiento de revocación de accesos	Documento procedimiento para revocación de acceso	24	
			Bloqueo (terminación laboral)	24 horas	
			Revocación (eliminar o inhabilitar)	1	
			Cambio de contraseñas (terminación laboral)	1	
			Cambio de contraseñas (reasignaciones o transferencias)	1	
PERÍMETRO	6.3.1	Perímetros de seguridad electrónica	Documento con los perímetros de seguridad y requisitos de accesos	Cada vez que se actualice	
	6.3.2	Listas de acceso	Lista del personal con acceso físico no escoltado o acceso lógico a los ciberactivos críticos	6	
			Evidencia documental de los cambios realizados	7 días	

Cap.	#	Acción	Actividad / Soporte / Evidencia *	Periodo de revisión (meses)	SI/NO
cumplimiento	3	Cumplimiento	Reportes de auditorías internas	24	
	6.3.3	Procedimiento de monitoreo y registro de acceso	Documento procedimiento para el monitoreo y registro de accesos físicos y lógicos	Permanente (24/7)	
	6.3.4	Validación de cambios	Documento procedimiento de control de cambios	24	
			Evidencia documental de los cambios realizados	Cada vez que se realice	
	6.3.5	Procedimiento para habilitar los puntos de acceso	Documento de línea base para equipos de punto de acceso al perímetro	24	
	6.3.6	Procedimiento para la administración de conexiones temporales	Documento procedimiento de administración de conexiones temporales	24	
	6.3.7	Sistema de control intermedio	Documento de inventario	24	
			Evidencia de la revisión periódica del control implementado	Cada vez que se realice	
	7.3.1	Procedimiento de control de cambios y gestión de configuraciones	Documento procedimiento gestión de cambios y gestión de configuración	24	
			Evidencias con los cambios realizados	Cada vez que se realice	
	7.3.2	Herramientas de prevención de malware	Evidencia de implementación de herramientas de prevención de software malicioso	Cada vez que se realice	
GESTIÓN DE LA SEGURIDAD	7.3.3	Procedimiento de evaluación de vulnerabilidades	Documento procedimiento de evaluación de vulnerabilidades	24	
			Evidencia de evaluación periódica de vulnerabilidades	Cada vez que se realice	
			Evidencia de vulnerabilidades sobre nuevos activos	Cada vez que se realice	
			Plan de acción del resultado de análisis de vulnerabilidad	24	

Cap.	#	Acción	Actividad / Soporte / Evidencia *	Periodo de revisión (meses)	SI/NO
cumplimiento	3	Cumplimiento	Reportes de auditorías internas	24	
	7.3.4	Procedimiento de control ciberactivos críticos transitorios y medios extraíbles	Documento procedimiento control transitorio y medios extraíbles	24	
			Evidencias de control periódico	Cada vez que se realice	
	7.3.5	Procedimiento de actualizaciones y parches de seguridad	Documento procedimiento de actualización e implementación de parches	24	
			Evidencias de los ciclos de parchado	Cada vez que se realice	
	7.3.6	Procedimiento para identificar y monitorear eventos	Documento procedimiento de monitoreo	24	
			Evidencia de controles implementados	Cada vez que se realice	
PLAN DE RECUPERACIÓN	8.3.1	Plan de recuperación	Documento plan de recuperación y los procedimientos asociados	12	
	8.3.2	Plan de pruebas o simulacros	Evidencia de pruebas o simulacros, y acciones de mejora de estos	12	
	8.3.3	Registro de cambios del procedimiento de recuperación	Evidencia de los cambios realizados a los procedimientos	3	
	8.3.4	Respalos y almacenamiento de información	Evidencia documentada de los respaldos realizados y almacenamiento de la información	Cada vez que se realice	
	8.3.5	Registro de pruebas a los respaldos	Evidencia documentada de que se realizan pruebas de respaldo y su resultado	Cada vez que se realice	
PLAN DE RESPUESTA ANTE INCIDENTES	9.3.1	Plan de respuesta ante incidentes	Documento con el plan de respuesta ante incidentes y los procedimientos asociados	12	
	9.3.2	Plan de pruebas o simulacros	Evidencia de pruebas o simulacros, y acciones de mejora de estos	12	
	9.3.3	Registro de cambios del procedimiento respuesta a incidentes	Evidencia de los cambios realizados a los procedimientos	3	

Cap.	#	Acción	Actividad / Soporte / Evidencia *	Periodo de revisión (meses)	SI/NO
cumplimiento	3	Cumplimiento	Reportes de auditorías internas	24	
SEGURIDAD FÍSICA DE CIBERACTIVOS CRÍTICOS	10.3.1	Plan de seguridad física	Documento plan de seguridad física cumpliendo los requisitos	24	
	10.3.2	Restricción de acceso físico	Evidencia de los controles implementados para protección física del cableado y otros componentes de comunicación	Cada vez que se realice	
			Alarma o alerta en respuesta a fallas de comunicación detectadas		
	10.3.3	Procedimiento de control de visitantes	Documento procedimiento control de visitantes	24	
	10.3.4	Procedimiento de mantenimiento y pruebas	Documento procedimiento de mantenimiento y pruebas periódicas a los sistemas de control relacionados a la seguridad física	24	
			Evidencia mantenimiento y pruebas periódicas	Cada vez que se realice	
GESTIÓN DE LA CADENA DE SUMINISTRO	11.3.1	Plan de Gestión de riesgo de la cadena de suministro	Documento y evidencia de la implementación del plan de gestión de riesgos de la cadena de suministro.	24	

Control de cambios

Versión	Fecha	Justificación de la versión
1	15/02/2019	Creación del documento.
2	18/12/2020	Se actualiza la norma de referencia; número del acuerdo 1241 por Guía de Ciberseguridad del Consejo Nacional de Operación.
3	11/11/2021	Se excluye las normas de referencia que fueron utilizadas como base para la política. Cambio de nombre de la vicepresidencia Gestión Humana Administrativa y Tecnología por Talento Humano y Soluciones Organizacionales. Cambio en el formato de documentación de las políticas.
4	15/11/2022	Se actualiza el lineamiento 3.5.7 donde se especifica la gestión de las contraseñas en las herramientas y dispositivos de la operación.