P40 - PROTECCION DE EQUIPOS UTILIZADOS FUERA DE LAS OFICINAS

Aplicación exclusiva a los centros de datos NGX Networks y ASSETEL / CloudSIDE

Evidencia documental de cumplimiento

1. Requisito de cumplimiento

Punto 40 del Anexo 10 de la RMF 2026: Documentación que describa el procedimiento para proteger los equipos que sean utilizados para actividades relacionadas con el monedero electrónico y que se encuentren fuera de las oficinas de la persona moral.

2. Objetivo y alcance específico

El presente expediente documenta la aplicación del procedimiento PR-SF-020 a los equipos que son trasladados, conectados, utilizados o custodiados durante intervenciones en los centros de datos de terceros utilizados por SENDERO FUEL: NGX Networks como centro de datos principal y ASSETEL / CloudSIDE como centro de datos secundario.

El alcance comprende equipos corporativos, equipos de proveedores autorizados, medios removibles, tokens, herramientas de diagnóstico y cualquier activo tecnológico utilizado para instalación, mantenimiento, soporte, recuperación, configuración, respaldo o atención de incidentes en dichos sitios. No comprende equipos que permanezcan instalados de forma permanente dentro de los racks, los cuales se controlan mediante el inventario de activos y los procedimientos de mantenimiento correspondientes.

3. Base documental

Código / evidencia	Documento	Identificación	Función dentro del control
PR-SF-020	Procedimiento para la protección de equipos utilizados fuera de las oficinas	Versión 1. Emisión 27/05/2026; revisión 25/06/2026.	Evidencia principal del punto 40. Define autorización, preparación técnica, custodia, uso, monitoreo, incidentes y retorno.
PR-SF-017	Procedimiento de acceso al centro de datos	Versión 1.	Complementa el control de ingreso a NGX y ASSETEL, la coordinación con terceros y la conservación de evidencia de la visita.
FO-SF-72	Solicitud y autorización de acceso al centro de datos	Registros disponibles para intervenciones en NGX.	Acredita necesidad, persona, sitio, fecha, actividad y autorización de acceso.
FO-SF-74	Bitácora de acceso al centro de datos	Registros disponibles para NGX y ASSETEL.	Acredita entrada, salida, actividad, acompañamiento e incidencias de la visita.
FO-SF-103 a FO-SF-107	Formatos relacionados con equipos fuera de oficinas	Definidos en PR-SF-020.	Solicitud, checklist técnico, responsiva, revisión periódica y reporte de incidente.

4. Centros de datos y escenarios cubiertos

Centro de datos	Función	Actividades cubiertas	Condición de uso del equipo
NGX Networks	Principal	Instalación, configuración, mantenimiento, soporte, respaldo, recuperación y atención de incidentes en infraestructura de producción.	Equipo corporativo o de proveedor previamente autorizado, registrado y validado.
ASSETEL / CloudSIDE	Secundario	Instalación, configuración, mantenimiento, pruebas de continuidad, recuperación y soporte del sitio alterno.	Equipo corporativo o de proveedor previamente autorizado, registrado y validado.

4.1 Evidencia histórica de intervenciones

Sitio	Fecha	Actividad documentada	Evidencia
NGX Networks	21 y 22/09/2023	Instalación inicial de clúster VMware y red.	FO-SF-72 y FO-SF-74.
NGX Networks	29/02/2024	Instalación de HPE StoreOnce para respaldos.	FO-SF-72 y FO-SF-74.
ASSETEL / CloudSIDE	28/05/2024	Instalación de servidores y equipo de red del sitio secundario.	FO-SF-74.

5. Equipos y medios comprendidos

Equipo / medio	Uso permitido	Riesgos principales	Controles mínimos
Laptop corporativa de soporte	Consola de administración, diagnóstico y ejecución de cambios autorizados.	Robo, pérdida, malware, conexión no autorizada, extracción de información.	Inventario, cifrado de disco, EDR, firewall, parches, bloqueo automático, MFA, VPN, privilegio mínimo y registro de actividad.
Laptop de proveedor autorizado	Soporte especializado o mantenimiento de fabricante.	Configuración desconocida, software no aprobado, extracción de información.	Autorización previa, validación técnica, cuenta temporal, supervisión, acceso limitado y revisión posterior.
Token o factor de autenticación	Acceso individual a VPN, consola o plataforma autorizada.	Uso indebido o pérdida de credenciales.	Asignación individual, MFA, custodia, prohibición de préstamo y revocación inmediata ante pérdida.
Medio removible autorizado	Carga controlada de firmware, drivers, respaldos o evidencias.	Malware, fuga de información, copia no autorizada.	Uso excepcional, cifrado, identificación, análisis antimalware, registro de entrada/salida y sanitización posterior.
Teléfono o tableta	Comunicación, autenticación o documentación autorizada.	Fotografías no autorizadas, exposición de datos, conexión inalámbrica.	Uso limitado; fotografía y grabación prohibidas salvo autorización expresa del proveedor y SENDERO FUEL.
Herramienta de diagnóstico con almacenamiento	Captura de logs, pruebas de red o diagnóstico de hardware.	Retención de datos, captura excesiva o manipulación.	Alcance aprobado, almacenamiento cifrado, custodia y eliminación segura de datos temporales.
Refacciones o equipo temporal	Sustitución, pruebas o contingencia.	Pérdida de trazabilidad, incorporación de equipo no validado.	Registro de serie, cadena de custodia, aprobación de cambio, verificación previa y actualización del inventario.

6. Línea base técnica obligatoria

Antes de autorizar el ingreso o uso de un equipo en cualquiera de los centros de datos, TI / ENERFUEL TECH deberá verificar y documentar, como mínimo, los siguientes controles:

- Equipo registrado en el inventario de activos, con propietario, custodio, marca, modelo, número de serie y etiqueta de identificación.
- Cifrado completo de disco o cifrado equivalente para toda información almacenada localmente.
- EDR o antimalware activo, actualizado y sin alertas críticas abiertas.
- Sistema operativo, aplicaciones y firmware con actualizaciones de seguridad vigentes.
- Firewall local habilitado y servicios de red innecesarios desactivados.
- Arranque seguro, protección de BIOS/UEFI y bloqueo de arranque desde medios no autorizados, cuando técnicamente sea viable.
- Bloqueo automático de pantalla en un máximo de cinco minutos y autenticación robusta.
- Cuenta individual, MFA y privilegios administrativos limitados al tiempo estrictamente necesario.
- Conexión a los sistemas de SENDERO FUEL únicamente mediante VPN, canal cifrado, consola segura o mecanismo aprobado.
- Prohibición de almacenar datos de contribuyentes localmente; cuando sea indispensable, se utilizará almacenamiento temporal cifrado y se eliminará al cierre de la actividad.
- Puertos USB y medios removibles restringidos; sólo se habilitarán para medios corporativos autorizados y registrados.
- Respaldo previo de configuraciones o información que pudiera verse afectada por la intervención.
- Sincronización horaria y registro de eventos suficientes para reconstruir la actividad ejecutada.
- Prueba de conectividad y validación de que el equipo no se conecta automáticamente a redes inalámbricas públicas o no autorizadas.

7. Procedimiento operativo específico para centros de datos

Fase	Actividad obligatoria	Evidencia esperada
1. Solicitud y planificación	El responsable de la actividad genera la solicitud de uso fuera de oficinas y la solicitud de acceso al centro de datos. Debe indicar persona, equipo, series, motivo, fecha, ventana, sistemas involucrados, cambio o ticket asociado y sitio a visitar.	FO-SF-103, FO-SF-72, ticket de cambio o mantenimiento.
2. Validación previa	TI / ENERFUEL TECH aplica el checklist técnico, confirma inventario, cifrado, EDR, parches, MFA, VPN, respaldo, cuentas autorizadas y ausencia de datos locales innecesarios.	FO-SF-104 y evidencia técnica.
3. Autorización y coordinación	Control Interno / Seguridad valida el riesgo y autoriza. Se coordina el acceso con NGX o ASSETEL, incluyendo lista de personas y equipos que ingresarán, horario y acompañamiento.	Autorización interna y confirmación del proveedor.
4. Preparación y entrega	El custodio recibe el equipo y firma responsiva. El equipo se transporta apagado o bloqueado, en estuche cerrado, bajo custodia personal y sin permanecer desatendido en vehículos o espacios públicos.	FO-SF-105 e inventario actualizado.
5. Registro de ingreso	En el filtro del centro de datos se registra la persona y, cuando el proveedor lo permita, marca, modelo, serie, accesorios y medios removibles. No ingresan equipos personales no autorizados.	FO-SF-74, registro o pase del proveedor.

Fase	Actividad obligatoria	Evidencia esperada
6. Uso dentro del sitio	El equipo sólo se conecta a activos y puertos autorizados; se trabaja dentro de la ventana aprobada; se prohíben redes abiertas, fotografías, extracción de información, software no autorizado y conexión a infraestructura de otros clientes.	Ticket, bitácora de trabajo y registros técnicos.
7. Cierre y salida	Se valida el resultado, se recopilan logs, se eliminan archivos temporales, se desconectan sesiones, se registra la salida de equipos y medios, y se documentan incidencias o desviaciones.	FO-SF-74, evidencia de cierre y ticket.
8. Revisión posterior	TI revisa integridad, malware, registros, cambios de configuración y datos temporales; revoca accesos temporales y actualiza inventario. La devolución se formaliza con el acta de retorno.	FO-SF-105 y reporte de revisión.
9. Atención de incidentes	Ante pérdida, robo, manipulación, malware o acceso no autorizado: aislar, bloquear cuentas, revocar tokens, notificar al proveedor, preservar evidencia y activar el proceso de incidentes.	FO-SF-107 y ticket de incidente.

8. Reglas específicas durante la intervención

- El equipo permanecerá bajo custodia del usuario autorizado o de su acompañante designado durante toda la visita.
- No se permitirá el préstamo de credenciales, tokens, cuentas, cables de consola, medios removibles ni equipo de soporte.
- Las cuentas temporales deberán tener vigencia limitada a la ventana de trabajo y serán revocadas al cierre.
- Las conexiones de administración deberán realizarse mediante interfaces de gestión, jump server, VPN o consola previamente autorizada.
- Toda captura de pantalla, fotografía o video requerirá autorización expresa del centro de datos y deberá evitar información de otros clientes, credenciales, direcciones, números de serie o configuraciones sensibles.
- No se utilizarán nubes personales, correo personal, mensajería no autorizada ni medios externos para transferir archivos.
- Los archivos de firmware, drivers o utilidades deberán verificarse antes de la visita y mantenerse en repositorios o medios corporativos controlados.
- Los datos obtenidos durante diagnóstico se limitarán al mínimo necesario y se conservarán sólo durante el periodo autorizado.
- Cualquier desviación del alcance aprobado suspenderá la actividad hasta recibir autorización adicional.
- Al término de la intervención se realizará una conciliación de equipos, accesorios y medios ingresados contra los retirados.

9. Tratamiento de equipos de proveedores

Cuando el fabricante, integrador o proveedor requiera utilizar equipo propio dentro de NGX o ASSETEL, se aplicarán controles equivalentes o compensatorios:

Control	Aplicación al proveedor
Autorización	Solicitud previa con empresa, técnico, equipo, serie, actividad, fecha y sistemas a intervenir.
Validación técnica	Declaración o evidencia de sistema actualizado, antimalware/EDR, cifrado, firewall y ausencia de software no autorizado.

Control	Aplicación al proveedor
Acceso lógico	Cuenta temporal individual, privilegios mínimos, MFA cuando aplique y conexión únicamente a activos autorizados.
Supervisión	Acompañamiento por personal de SENDERO FUEL / ENERFUEL TECH o monitoreo de sesión.
Transferencia de archivos	Sólo mediante repositorio, canal o medio aprobado; prohibido utilizar servicios personales.
Cierre	Revocación de accesos, entrega de logs o reporte, eliminación de datos de SENDERO FUEL y confirmación de cierre.

10. Registros y paquete mínimo de evidencia por visita

Momento	Evidencia mínima
Antes de la visita	Solicitud de uso del equipo; autorización de acceso; ticket de cambio/mantenimiento; listado de equipos y series; checklist técnico; responsiva; confirmación del centro de datos.
Durante la visita	Bitácora de entrada/salida; registro del equipo; acompañamiento; actividad realizada; logs; evidencia del cambio; incidencias.
Después de la visita	Conciliación de equipos; revisión antimalware; eliminación/sanitización de datos temporales; revocación de accesos; acta de retorno; cierre de ticket.
Si ocurre incidente	Reporte de incidente, cronología, preservación de evidencia, acciones de contención, comunicación con NGX/ASSETEL y validación de cierre.

11. Roles y responsabilidades

Responsable	Responsabilidad
Control Interno / Oficial de Seguridad	Validar necesidad y riesgo; autorizar o rechazar; revisar evidencia; gestionar excepciones; coordinar incidentes y revisiones periódicas.
TI / ENERFUEL TECH	Preparar y validar equipos; configurar cifrado, EDR, VPN, MFA y cuentas; ejecutar revisión posterior; conservar logs y evidencia técnica.
Coordinador o dueño de la actividad	Justificar la intervención, definir alcance, ventana y activos; asegurar que el cambio esté autorizado.
Usuario custodio / técnico	Custodiar el equipo, respetar el alcance, no compartir accesos, reportar incidentes y devolver el equipo con todos sus accesorios.
NGX Networks / ASSETEL	Aplicar reglas del sitio, registrar accesos, validar el ingreso de equipos cuando aplique y comunicar restricciones o incidentes físicos.
Proveedor especializado	Cumplir los controles contractuales, de confidencialidad, acceso, protección del equipo y eliminación de datos.

12. Periodicidad e indicadores de control

Frecuencia	Actividad	Indicador
Cada visita	Autorización, checklist técnico, registro de ingreso/salida, conciliación y cierre documental.	100 % de visitas con expediente completo.
Mensual	Revisión del inventario de equipos autorizados para uso fuera de oficinas y de accesos temporales pendientes de revocación.	0 accesos temporales vencidos activos.
Trimestral	Validación técnica de equipos recurrentes: cifrado, EDR, parches, VPN, MFA, bloqueo y privilegios.	100 % de equipos recurrentes conformes.
Semestral	Revisión integral del PR-SF-020 y de este expediente específico para centros de datos.	Revisión documentada y control de cambios.
Después de incidente o cambio crítico	Revisión extraordinaria de controles, causas, excepciones y medidas compensatorias.	100 % de acciones correctivas cerradas con evidencia.

13. Criterios de mejores prácticas incorporados

Los controles complementarios definidos en este expediente se basan en prácticas reconocidas para equipos utilizados fuera de instalaciones controladas:

- NIST SP 800-46 Rev. 2: protección de dispositivos cliente, acceso remoto, autenticación, comunicaciones seguras y políticas para trabajo desde ubicaciones externas.
- NIST SP 800-111: uso de cifrado de almacenamiento para restringir el acceso no autorizado a información contenida en equipos portátiles y medios removibles.
- NIST SP 800-88 Rev. 2: sanitización de medios y eliminación de datos mediante técnicas acordes con la sensibilidad de la información.
- ISO/IEC 27001:2022: gestión de riesgos de seguridad de la información y protección integral mediante personas, procesos y tecnología.

14. Conclusión de cumplimiento

El procedimiento PR-SF-020, complementado por los controles específicos contenidos en el presente expediente, describe de manera suficiente la autorización, preparación, custodia, uso, monitoreo, atención de incidentes, retorno y revisión de los equipos utilizados para actividades del monedero electrónico en los centros de datos NGX Networks y ASSETEL / CloudSIDE. La evidencia se vincula con los procedimientos de acceso a centros de datos, las autorizaciones y las bitácoras existentes, y establece el paquete mínimo que deberá conservarse para cada intervención.

Por lo anterior, este documento constituye evidencia específica para soportar el cumplimiento del punto 40 del Anexo 10 de la RMF 2026 en lo relativo a los centros de datos de SENDERO FUEL.

15. Elaboración, revisión y autorización

Elaboró	Revisó	Autorizó

Nombre, puesto, firma y fecha	Nombre, puesto, firma y fecha	Nombre, puesto, firma y fecha