POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

TIPO DE DOCUMENTO: Política

CÓDIGO: POL GSI 001

I. AUTORIZACIONES

Elaboró:	*Revisó:*	*Autorizó:*
Ing. Salvador Santiago Araujo *Gerente Administrativo*	*C.P. Jerónimo Javier Mendoza Lara / Lic. Irais Dafne Mendoza Sánchez* *Director General / Director General Adjunto*	*C.P. Jerónimo Javier Mendoza Lara / Lic. Irais Dafne Mendoza Sánchez* *Director General / Director General Adjunto*

Última revisión: Octubre 2025

No. de versión: 08

Fecha de emisión: Enero 2018

Revisó: DGE

Aprobó: DGE

ÍNDICE

II. OBJETIVO

Definir las **políticas generales de seguridad de la información** aplicables a la organización, con el fin de establecer las directrices que permitan cumplir con los requisitos de la norma **ISO/IEC 27001:2022**, garantizando la confidencialidad, integridad y disponibilidad de la información.

El presente documento constituye el **marco de referencia** para el establecimiento, implementación y mantenimiento de los controles definidos en el **Anexo A de la norma ISO/IEC 27001:2022**, en sus cuatro dominios:

- Controles organizativos
- Controles dirigidos a las personas
- Controles físicos
- Controles tecnológicos

Alcance de las políticas generales

1. Controles organizativos

- A.5.1 Política de seguridad de la información.
- A.5.2 Roles y responsabilidades de seguridad de la información.
- A.5.14 Transferencia de información.
- A.5.15 Control de acceso.
- A.5.19 - A.5.21 Seguridad en relaciones con proveedores.
- A.5.25 - A.5.28 Gestión de incidentes de seguridad de la información.

- A.5.29 - A.5.30 Continuidad del negocio y continuidad TIC.

2. Controles dirigidos a las personas

- A.6.2 Dispositivos móviles y teletrabajo.
- A.7.2 Responsabilidades antes, durante y después del empleo.
- A.7.4 Capacitación y concientización en seguridad de la información.
- A.7.7 Escritorio despejado y pantalla despejada.

3. Controles físicos

- A.7.1 Seguridad física perimetral y en oficinas.
- A.7.5 Áreas de acceso restringido.
- A.7.8 Seguridad de los equipos en las instalaciones.
- A.7.11 Protección contra amenazas físicas y ambientales.
- A.7.14 Trabajo fuera de sitio seguro.

4. Controles tecnológicos

- A.8.1 Dispositivos de punto final de usuario.
- A.8.9 / A.8.23 Seguridad en redes y comunicaciones.
- A.8.13 Copias de seguridad.
- A.8.15 - A.8.16 Logging y monitoreo de actividades.
- A.8.24 Uso de criptografía.
- A.8.25 Ciclo de vida de desarrollo seguro.
- A.8.30 Seguridad en endpoints y configuración segura de equipos.
- A.8.34 Autenticación y gestión de contraseñas.

Con este marco, la organización asegura que las políticas de seguridad de la información no solo cumplen con los requisitos normativos, sino que también se integran en los procesos operativos y administrativos de forma consistente y auditable.

III. HISTORIAL DE CAMBIOS

Versión	Descripción de cambios	Autor(es)	Fecha de cambio
1	Versión inicial.	MAH	Enero 2018
2	Inclusión de las políticas **A.13.2.1** Política de intercambio de información; y **14.2.1** Política de desarrollo seguro, modificaciones en política de Desarrollo seguro, dispositivos móviles, teletrabajo y de control de acceso.	MAH	Mayo 2019
3	Inclusión de nueva regla para correo de cliente CitiBanamex, se tenía omisión de documentación.	MAH	Agosto 2019
4	Actualización de políticas “dispositivos móviles”, “control de acceso”, trabajo en áreas seguras”, “intercambio de información”; inclusión de la policía sobre desarrollo seguro. Se actualizó el rubro de “Cuadro de Autorizaciones” con los datos del Coordinador Operativo de TI en lugar del Coordinador de Sistemas de Gestión, así como se actualizó el nombre del nuevo Gerente Administrativo.	RFML	Octubre 2020
5	Se actualizó la Política de dispositivos móviles cambiando el nombre como Política de dispositivos tecnológicos y se especificó la información correspondiente sobre los equipos y laptops de la empresa.	RFML	Mayo 2021

Versión	Descripción de cambios	Autor(es)	Fecha de cambio
6	Se actualizo la politica de dispositivos tecnológicos en el apartado 1.2, 1.3 y 1.4.	RFML	Enero 2022
7	Se actualiza el objetivo, incluyendo los requisitos de la actualización de la norma ISO/IEC 27001:2013 y se integra la Política de licenciamiento de software.	RFML	Septiembre 2023
8	Actualización del documento para reforzar políticas generales de seguridad de la información y alinearlas a los requisitos de la norma ISO/IEC 27001:2022.	SSA	Septiembre 2025

IV. ABREVIACIONES Y DEFINICIONES

Abreviaciones:

DGE	Director General / Director General Adjunto
GAD	Gerente Administrativo
CSG	Coordinador de Sistemas de Gestión
CST	Coordinador de Sistemas TI
N/A	No aplica
SGSI	Sistema de Gestión de Seguridad de la Información

Definiciones:

Integridad

Propiedad de la información relativa a su exactitud y completitud.

Confidencialidad

Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad

Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Principio de privilegio mínimo

Se refiere a la práctica de otorgar a cada usuario, cuenta, aplicación o proceso **únicamente los permisos estrictamente necesarios para desempeñar sus funciones**, y nada más. Bajo este principio, se evita que colaboradores o sistemas cuenten con privilegios excesivos (como accesos administrativos o a información confidencial que no les corresponde), reduciendo así el riesgo de errores, mal uso o incidentes de seguridad.

Hardening (endurecimiento de sistemas)

Proceso de configuración avanzada de equipos y sistemas operativos que busca reducir al mínimo la superficie de ataque. Incluye la desactivación de servicios innecesarios, la eliminación de cuentas predeterminadas, el uso de parches de seguridad, el control de

ejecución de scripts, la restricción de macros, la protección del BIOS/UEFI y la aplicación de configuraciones seguras recomendadas por estándares internacionales como **OWASP**.

Recertificación de accesos

Actividad periódica en la que se revisa la vigencia y justificación de todos los accesos otorgados a usuarios, cuentas de servicio y aplicaciones. Su propósito es identificar accesos que ya no son necesarios (por ejemplo, cuentas de empleados que causaron baja o permisos elevados no justificados) y revocarlos de inmediato, manteniendo actualizado el cumplimiento del **principio de privilegio mínimo**.

Ciclo de vida de contraseñas

Etapas que describen la gestión completa de una credencial de acceso, desde su creación en el alta de usuario, pasando por su modificación, caducidad y rotación periódica, hasta su revocación en casos de baja de personal, robo o pérdida de equipos. Incluye también las revisiones periódicas de validez y el tratamiento especial de cuentas privilegiadas y de servicio.

Logging y monitoreo de actividades

Proceso mediante el cual los sistemas generan y almacenan registros (**logs**) de eventos relevantes, como accesos, cambios de configuración, intentos fallidos o detecciones de malware. El monitoreo implica la revisión sistemática de estos registros para identificar comportamientos anómalos, correlacionar incidentes y activar medidas de contención o corrección.

Criptografías master

Son las **claves maestras** utilizadas para cifrar o proteger otros datos sensibles. Estas claves representan un nivel crítico dentro de la gestión de criptografía, ya que, si son comprometidas, pondrían en riesgo toda la información protegida con ellas. En la organización, las criptografías master se resguardan en el gestor seguro **Keeper**, garantizando custodia cifrada y acceso controlado.

Portal cautivo Fortinet

Mecanismo de autenticación de red que exige a cada usuario ingresar sus credenciales personales antes de permitir el acceso a la VLAN correspondiente. En este portal se despliegan mensajes personalizados de concientización y se registran logs de autenticación para trazabilidad y auditoría.

CIA-Desk

Plataforma oficial de **gestión de tickets e incidencias** de la organización. Todo evento de seguridad, solicitud de cambio, mantenimiento o excepción debe documentarse en CIA-Desk, generando un folio que permite asegurar trazabilidad, tiempos de atención y evidencias para auditoría.

Superficie de ataque

Conjunto de puntos expuestos de un sistema que pueden ser utilizados por un atacante para introducirse, extraer datos o alterar su comportamiento. Incluye vectores como puertos abiertos, servicios expuestos, interfaces web, APIs, credenciales débiles, dispositivos USB, componentes de terceros y dependencias de software. Reducir la superficie de ataque significa minimizar funcionalidades y servicios expuestos, aplicar hardening, segmentación (VLAN) y controles de autenticación/filtrado.

OWASP (Open Web Application Security Project)

Proyecto comunitario que publica buenas prácticas, guías y listados de vulnerabilidades en aplicaciones web. El **OWASP Top 10** identifica las principales familias de riesgo (inyección, autenticación rota, XSS, etc.). Se utiliza como referencia técnica para diseño seguro, revisión de código, pruebas de seguridad y criterios de aceptación en SDLC.

Keeper

Gestor de contraseñas y bóveda cifrada para credenciales y secretos (cloud vault). Keeper almacena claves maestras, tokens y credenciales críticas cifradas con claves derivadas del usuario; proporciona control de accesos, registros de auditoría, políticas de rotación y compartición segura.

GLPI

Herramienta de gestión de activos TI y de ITSM (inventario, control de configuración, calendario de mantenimiento y gestión de incidencias/servicios).

VLAN (Virtual LAN)

Segmentación lógica de red que aísla el tráfico dentro de la misma infraestructura física. Cada VLAN define un dominio de difusión y reglas de acceso específicas; combinada con políticas de firewall (Fortinet) permite aplicar principio de mínimo privilegio en la red, impedir tráfico entre áreas y limitar el blast radius ante un incidente.

Privacy Eraser

Software especializado para borrado seguro de datos en medios de almacenamiento. Ejecuta rutinas de sobreescritura (ceros, unos, patrones aleatorios) y genera reportes de eliminación. Se utiliza para asegurar que respaldos o medios que contienen información sensible no sean recuperables con técnicas forenses.

DoD 5220.22-M

Método de borrado seguro originado en especificaciones del Departamento de Defensa de EE. UU.; describe una rutina de sobreescritura de datos (generalmente 3 pasadas con patrones determinados) que dificulta la recuperación forense. Es común declararlo como estándar mínimo para eliminación segura; puede configurarse a 3 pasadas (estándar) o extendido a más pasadas según criticidad.

Pasadas de sobreescritura (número y algoritmo)

Se refiere a cuántas veces se sobrescribe cada sector del medio durante el borrado seguro y con qué patrón. Ejemplos:

- **Zero Fill (1 pasada)**: escribe ceros en todos los sectores. Rápido, básico.
- **DoD 5220.22-M (3 pasadas)**: combinación de ceros, unos y datos aleatorios (ver estándar) — equilibrio entre seguridad y tiempo.
- **DoD extendido / 7 pasadas**: mayor resistencia a recuperación forense; usado para información altamente sensible.
- **Gutmann (35 pasadas)**: prácticamente obsoleto por ser excesivo y muy lento, pero aún citado.

La política debe declarar el método (p. ej. DoD 3 pasadas por defecto; 7 pasadas para datos críticos) y la herramienta usada (Privacy Eraser) que genere evidencia del proceso.

1. Controles Organizativos.

A 5.1	Política de seguridad de la información
A 5.1.1	**Establecimiento y aprobación** La Dirección General ha establecido y aprobado la **Política de Seguridad de la Información (POL SGSI 001**), la cual define el marco de referencia para garantizar la confidencialidad, integridad y disponibilidad de la información de la organización.
A 5.1.2	**Comunicación y disponibilidad interna** La política se encuentra documentada en el sistema de gestión y es comunicada a todos los colaboradores mediante capacitaciones, comunicados, presentaciones y boletines. Está disponible en la intranet y en los repositorios documentales de la organización.
A 5.1.3	**Disponibilidad para partes interesadas externas** La política se publica en la página web de la organización, a fin de que clientes, proveedores, auditores y otras partes interesadas puedan consultarla de manera permanente.
A 5.1.4	**Cumplimiento de requisitos aplicables** La política establece el compromiso de la organización de cumplir con todos los requisitos legales, regulatorios, contractuales y normativos relacionados con la seguridad de la información, para lo cual se aplican las siguientes directrices: • La **Coordinación de Sistemas de Gestión** mantiene la **Declaración de Aplicabilidad (LIS GSI 007)**, en la que se identifican los controles seleccionados, los requisitos aplicables y la justificación de inclusión o exclusión. • La **Gerencia Administrativa** supervisa que los requisitos contractuales con clientes y proveedores incluyan las cláusulas de seguridad de la información necesarias. • Los **dueños de procesos** son responsables de aplicar y evidenciar el cumplimiento de los controles definidos en la **Declaración de Aplicabilidad (LIS GSI 007)** dentro de sus áreas de operación. • La **Dirección General** valida en la **Revisión por la Dirección** el estado de cumplimiento de los requisitos aplicables. • La **evidencia de cumplimiento** se conserva en los **informes de auditoría interna y externa**, en los que se evalúa periódicamente la conformidad con la **Declaración de Aplicabilidad (LIS GSI 007)** y con los requisitos legales, regulatorios y contractuales de la organización.
A 5.1.5	**Mejora continua del SGSI** La organización se compromete a la **mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI)**, asegurando que se identifiquen, implementen y verifiquen acciones que incrementen su eficacia. Este compromiso se cumple mediante las siguientes directrices: 1. **Entradas para la mejora** ○ Resultados de auditorías internas y externas. ○ Resultados de los indicadores y métricas del SGSI. ○ Reportes de incidentes de seguridad registrados en GLPI. ○ Resultados de evaluaciones de riesgos y de la Declaración de Aplicabilidad (**LIS GSI 007**). ○ Retroalimentación de clientes y partes interesadas. 2. **Validación por la Dirección General**

	○ La **Dirección General** analiza en la **Revisión por la Dirección**, el grado de cumplimiento de los objetivos de seguridad, el estado de los riesgos y el avance de acciones previas. ○ La Dirección General **aprueba los planes de acción de mejora** propuestos, asignando responsables y fechas de cumplimiento. 3. **Implementación de acciones de mejora** ○ Los **dueños de procesos** ejecutan las acciones aprobadas en sus áreas de responsabilidad. ○ Las acciones se gestionan conforme al **Procedimiento de Acciones Correctivas y de Mejora (PRO CAL 005)** y se registran en el sistema de gestión documental. 4. **Evidencia de la mejora continua** ○ **Minutas de la Revisión por la Dirección** con acuerdos. ○ **Planes de acción aprobados** con responsables y fechas de cierre. ○ **Informes de auditoría interna y externa** que verifican la implementación de mejoras. ○ **Registros de seguimiento en GLPI** sobre incidentes y acciones correctivas cerradas.
A 5.2	**Roles y responsabilidades de seguridad de la información**
A 5.2.1	La organización ha definido, documentado, comunicado y mantiene actualizadas las **responsabilidades y autoridades en materia de seguridad de la información**, con el objetivo de asegurar la correcta operación y mejora continua del SGSI.
A 5.2.2	**Documentación de responsabilidades** Las responsabilidades están formalizadas en: ○ **Matriz de Roles y Responsabilidades (FOR GSI 043)**. ○ **Matriz de Roles por Activos de Información Críticos (FOR GSI 025)**. ○ **Organigrama de la organización**. Cada documento identifica el **rol**, sus **responsabilidades específicas**, su **autoridad** y el **activo o proceso asociado**.
A 5.2.3	**Asignación de roles clave** La **Dirección General** asigna la autoridad para asegurar el cumplimiento del SGSI a: ○ **Gerencia Administrativa**: supervisión del cumplimiento de objetivos de seguridad y asegurar la integración del SGSI en los procesos administrativos de la organización. ○ **Coordinación de Sistemas de Gestión**: asegurar la conformidad del SGSI con la norma ISO/IEC 27001:2022, gestión de auditorías internas, control documental y coordinación de acciones correctivas. ○ **Coordinación de Sistemas TI**: administración de infraestructura tecnológica, implementación de controles técnicos, gestión de incidentes y aseguramiento de la operación conforme a lineamientos del SGSI. ○ **Dueños de procesos operativos y administrativos**: aplicación de controles de seguridad en sus áreas, actualización de la información de activos y reporte de incidentes.
A 5.2.4	**Revisión y actualización** Las responsabilidades son **revisadas anualmente** por la **Dirección General**, la **Gerencia Administrativa** y la **Coordinación de Sistemas de Gestión**.

	También se revisan **cuando existan cambios organizacionales**, incorporación de nuevos activos críticos o modificación de funciones.
A 5.14	**Transferencia de información**
A 5.14.1	**Generalidades** La organización garantiza que toda **transferencia de información**, ya sea interna o externa, se realice de manera segura, controlada y conforme a los principios de confidencialidad, integridad y disponibilidad establecidos en el SGSI. • Toda información **clasificada como confidencial y/o crítica** se transfiere únicamente mediante **canales autorizados y cifrados**, utilizando certificados SSL instalados en todos los equipos corporativos. • El uso, custodia y resguardo de la información es responsabilidad de los **dueños de proceso** y colaboradores designados como corresponsables. • La red corporativa cuenta con **segmentación por VLAN** para cada área, configuradas en el firewall **Fortinet**, lo que impide el tráfico lateral entre departamentos y limita el acceso únicamente a los recursos autorizados. • Adicionalmente, se aplican **directivas de GPO en Windows Server** que refuerzan la asignación de roles, políticas de acceso y restricción de dispositivos de almacenamiento por medio del directorio activo.
A 5.14.2	**Configuraciones de Seguridad en Fortinet.** El firewall Fortinet de la organización aplica configuraciones avanzadas de seguridad para asegurar la transferencia de información: • **Perfiles de seguridad activos**: filtrado web, antivirus con análisis profundo, control de aplicaciones, inspección SSL y sistema de prevención de intrusiones (IPS). • **Políticas de firewall personalizadas**: reglas por área, nodo y usuario para garantizar el principio de mínimo privilegio. • **Calendarios de acceso**: horarios configurados para cada sede (Neza, Insurgentes, Toluca) que restringen tráfico fuera de las horas laborales autorizadas. • **Portal cautivo**: todos los colaboradores deben autenticarse con usuario individual antes de acceder a la red; cada usuario queda vinculado a su VLAN y condiciones de seguridad definidas. • **Mensajes personalizados de Fortinet**: reforzando la concientización en seguridad de la información al momento de login. • **Integración con conectores externos de inteligencia de amenazas** (hash, IP, dominios maliciosos) que actualizan las bases de datos en tiempo real para bloquear actividades sospechosas.
A 5.14.3	**Uso aceptable y excepciones** • Se prohíbe descargar, instalar o ejecutar software, archivos o periféricos no autorizados. • Toda excepción a estas políticas debe ser **autorizada exclusivamente por la Dirección General y/o la Gerencia Administrativa**, previa evaluación de impacto. • Las excepciones se documentan en el **Formato de Excepciones (FOR GSI 047).**
A 5.14.4	**Uso de internet** • El acceso a internet está regulado y monitoreado a través de Fortinet. • Los dispositivos ajenos a la organización solo pueden conectarse a la red de invitados (**CIASC - INVITADOS**), completamente aislada de la red interna de la organización.

	• El área de sistemas puede bloquear páginas, dominios o servicios de internet por usuario, grupo o nodo, con el fin de prevenir riesgos de malware, phishing o fuga de información. • Todo correo electrónico, archivo o URL sospechosa debe reportarse inmediatamente mediante **CIA Desk** para su análisis y mitigación.
A 5.14.5	**Correo electrónico y mensajería** • Todo el personal debe utilizar correos electrónicos institucionales bajo el dominio **@ciasc.mx**, administrados por el área de sistemas. • Se aplican **reglas de uso diferenciadas** (interno, autorizado, con límite de envío, monitoreado o sin restricción) según el nivel de seguridad requerido. • El canal de comunicación permitido para cada tipo de dato se define en el **Procedimiento de Gestión de Activos, Clasificación y Control de la Información (PRO GSI 015)**. • Los mensajes clasificados como **confidenciales** deben ser etiquetados y protegidos conforme al **Procedimiento de Gestión de Activos, Clasificación y Control de la Información (PRO GSI 015)**. • Todos los correos institucionales incluyen la **exención de responsabilidad corporativa**.
A 5.14.6	**Intercambio con terceros** • Todo intercambio de información con terceros se formaliza contractualmente a través del **Procedimiento de Proveedores (PRO GSI 030)**, que incluye cláusulas específicas de confidencialidad y transferencia segura de información.
A 5.14.7	**Confidencialidad** • Todo el personal está obligado a mantener la confidencialidad de la información durante y después de la relación laboral, conforme al **Mapa de Proceso de Recursos Humanos (MAP REH 001)** y los acuerdos de confidencialidad firmados.
A 5.15	**Control de acceso**
A 5.15.1	**Generalidades** La organización asegura que el acceso a los activos de información y a las instalaciones críticas se conceda únicamente a personal autorizado y conforme al principio de **mínimo privilegio** y **necesidad de conocer**. Esta política aplica a todo el **personal interno, externo y terceras partes** que requieran acceso físico o remoto a los sistemas, bases de datos, aplicaciones, infraestructura tecnológica y áreas críticas de la organización.

A 5.15.2	**Acceso físico a áreas restringidas**
	• El ingreso a los **centros de datos y áreas críticas** está limitado exclusivamente al personal autorizado.
	• El acceso físico se controla mediante:
	  ○ Señalización de áreas restringidas.
	  ○ Cerradura.
	  ○ Alarmas ADT.
	  ○ Sistemas de videovigilancia activos las 24 horas, los 7 días de la semana.
	• Toda visita o acceso temporal se documenta en la **Bitácora de acceso a las áreas seguras (FOR GSI 004)** y requiere autorización previa del responsable del área.
	Se declaran áreas seguras y que requieren reglas especiales, las siguientes:

	1. **Oficina Nezahualcóyotl:** Av. Lago de Xochimilco No. 283, Col. Ampliación Vicente Villada, Municipio Ciudad Nezahualcóyotl, Estado de México, C.P. 57760. a) Centro de Datos. b) Archivo de expedientes físicos. 2. **Oficina Colonia del Valle:** Insurgentes Sur No. 686, Piso 9, Col. Del Valle, Delegación Benito Juárez, Ciudad de México, C.P. 03100. a) Centro de Datos. b) Archivo de expedientes físicos. 3. **Oficina Toluca:** Hermenegildo Galeana No. 204, Despacho 2, Col. Centro, Municipio Toluca, Estado de México, C.P. 50000. a) Centro de Datos. b) Archivo de expedientes físicos. c) Centro de Contacto (call center).
A 5.15.3	**Acceso lógico a sistemas de la información** • Todo acceso lógico se gestiona a través de: ○ **Directorio Activo (AD)** para usuarios internos, con políticas de contraseña reforzadas. ○ **Directivas de Grupo (GPO)** para asignar privilegios y restricciones a nivel de estación de trabajo. ○ **BitLocker** como control de cifrado y autenticación inicial al inicio de sesión. ○ **Fortinet Portal Cautivo**, donde cada colaborador debe autenticarse para acceder a la red corporativa y a su VLAN asignada. ○ **Certificados SSL instalados en equipos autorizados**, garantizando la conexión segura entre el dispositivo y el firewall. ○ **VPN Printunl**, obligatoria para el acceso remoto a los servidores de la organización con los siguientes servicios. 1. Directorio Activo. 2. Servidor de archivos. 3. ASPEL. 4. SICOB. 5. Filemarker. 6. ERP CIASC. 7. GLPI. 8. OptiRisk. 9. SFTP Sears. 10. Intranet Sistemas de Gestión. 11. CIA Desk. • Se prohíbe el uso compartido de cuentas; cada usuario tiene credenciales individuales asignadas.
A 5.15.4	**Revisión y gestión de accesos** • La **Coordinación de Sistemas TI** es responsable de realizar la **revisión y recertificación de accesos** de todos los usuarios de la organización (regulares y privilegiados) cada **tres meses**. • Esta revisión incluye la verificación de **altas, bajas, cambios de privilegios y vigencia de accesos**, con base en la información registrada en **Sistemas Internos (SICOB, Bonsaif, ASPEL, ERP CIASC, Filemarker), Active Directory, Fortinet y VPN Printunl**. • Como parte del proceso se ejecuta cada tres meses el **monitoreo de seguridad de la información**, que permite identificar accesos indebidos, cuentas inactivas o privilegios asignados fuera de política, etc.

	• Los resultados de la recertificación se documentan en el **Formato de Recertificación de accesos (FOR SIS 010)**, el cual incluye: listado de usuarios, nivel de privilegios, fecha de última revisión, responsables de aprobación y acciones correctivas derivadas en caso de aplicar. • Toda **alta, baja o modificación de usuarios** debe gestionarse mediante **CIA Desk**.
A 5.19	**Identificación de requisitos de seguridad con proveedores**
A 5.19.1	La organización garantiza que la relación con proveedores de bienes y servicios se gestione de manera que no se comprometa la **confidencialidad, integridad y disponibilidad de la información**, ni los activos tecnológicos vinculados al SGSI. • Todos los contratos con proveedores deben incluir cláusulas específicas de seguridad de la información, confidencialidad y cumplimiento normativo. • La Gerencia Administrativa es responsable de asegurar que dichas cláusulas se integren en cada proceso de contratación, conforme al **Procedimiento de Proveedores (PRO GSI 030)** y el **Mapa de proceso de compras (MAP COM 001).** • Los proveedores con acceso a información clasificada como confidencial o crítica deberán firmar acuerdos de confidencialidad y uso aceptable de la información.
A 5.20	**Evaluación y selección de proveedores**
A 5.20.1	• Los proveedores que tengan impacto en la seguridad de la información son evaluados antes de su contratación mediante la **Formato Evaluación de Proveedores (FOR COM 004)**. • Esta evaluación considera criterios de seguridad, cumplimiento legal, capacidad técnica. • La Coordinación de Sistemas de Gestión revisa que la evaluación contemple los requisitos de seguridad de la información conforme al **Procedimiento de Proveedores (PRO GSI 030)** y el **Mapa de proceso de compras (MAP COM 001)**.
A 5.21	**Monitoreo y revisión de proveedores**
A 5.21.1	• Los proveedores son evaluados de manera trimestral para validar el cumplimiento de los requisitos contractuales de seguridad. • Los resultados de estas revisiones se documentan en el **Formato Evaluación de Proveedores (FOR COM 004)**. • Cuando se identifiquen **incumplimientos o riesgos**, la **Gerencia Administrativa** debe coordinar la aplicación de medidas correctivas o, en su caso, la suspensión/terminación del contrato.
A 5.25	**Responsabilidades en la gestión de incidentes de seguridad de la información**
A 5.25.1	La organización cuenta con políticas y lineamientos que aseguran la detección, notificación, evaluación, gestión y cierre de incidentes de seguridad de la información, garantizando la continuidad del negocio y la protección de los activos críticos. • La **Coordinación de Sistemas TI** es responsable de la gestión operativa de incidentes: detección, análisis técnico, contención, erradicación y recuperación. • La **Coordinación de Sistemas de Gestión** supervisa el cumplimiento del **Procedimiento de Gestión de Incidentes (PRO GSI 020)** y consolida la información para los informes de auditoría y la revisión por la Dirección. • La **Gerencia Administrativa** valida que los incidentes críticos se comuniquen a la **Dirección General** y que se implementen medidas correctivas. • Todos los colaboradores tienen la obligación de reportar inmediatamente cualquier evento sospechoso o incidente de seguridad a través de CIA Desk o mediante comunicación directa al área de TI.

A 5.26	**Notificación de eventos de seguridad de la información**
A 5.26.1	• Todos los eventos de seguridad deben notificarse a través de **CIA Desk.** • Los incidentes clasificados como críticos (acceso no autorizado, malware, fuga de información, ataques de red) deben ser escalados de inmediato a la **Dirección General**, mediante correo institucional y llamada directa por la **Gerencia Administrativa.** • Cuando corresponda, la organización notificará a clientes o autoridades regulatorias de acuerdo con los compromisos contractuales y requisitos legales aplicables.
A 5.27	**Evaluación de eventos de seguridad de la información e incidentes**

A 5.27.1	• La **Coordinación de Sistemas TI** analiza cada reporte utilizando las herramientas de monitoreo y seguridad:
	  ○ Fortinet (perfiles de seguridad, IPS, SSL, control de aplicaciones, filtrado web).
	  ○ SentinelOne XDR (detección y respuesta en endpoints).
	  ○ CIA Desk (bitácora de incidentes).
	• Los incidentes se clasifican en niveles de criticidad: bajo, medio, alto o crítico.
	• Cada evento evaluado se documenta **Formato de incidentes de SI (FOR GSI 024).**

A 5.28	**Respuesta a incidentes de seguridad de la información**
A 5.28.1	• La respuesta a incidentes se realiza siguiendo el **Procedimiento Gestión de Incidentes (PRO GSI 020).** • Cada incidente se documenta en un **Formato de incidentes de SI (FOR GSI 024)** con detalle de acciones realizadas, responsables y plazos de ejecución. • Los resultados se presentan en la **Revisión por la Dirección** para asegurar el aprendizaje organizacional y la mejora continua.
A 5.29	**Continuidad del negocio**
A 5.29.1	La organización cuenta con un **Plan de continuidad de seguridad de la información (PRO GSI 019) y Plan de Recuperación de Desastres (PRO GSI 100)** que asegura la operación de los procesos críticos durante interrupciones graves y establece los tiempos de recuperación aceptables para cada servicio. • La **Gerencia Administrativa** asegura la disponibilidad de recursos para activar el plan cuando sea necesario. • Los **dueños de procesos** aplican los lineamientos establecidos en caso de interrupción, utilizando procedimientos alternos previamente definidos. • Se realizan **simulacros semestrales** que incluyen restauración de respaldos y simulaciones de interrupción; los resultados se documentan en el **Formato Simulacro (FOR GSI 050).**
A 5.30	**Continuidad TIC**
A 5.30.1	La organización mantiene un **Plan de continuidad de seguridad de la información (PRO GSI 019) y Plan de Recuperación de Desastres (PRO GSI 100)** para garantizar la disponibilidad y recuperación de los servicios tecnológicos que soportan los procesos críticos del negocio. • La **Coordinación de Sistemas TI** mantiene actualizado el plan e implementa controles técnicos que permiten la recuperación de **servidores, directorio activo, aplicaciones web y bases de datos**.

	• La continuidad TIC se soporta con **respaldos programados los cuales se ejecutan de manera diaria cada 60 minutos**, pruebas de restauración, **VPN Printunl** obligatoria para accesos remotos, **certificados SSL en equipos autorizados**, y segmentación de red por **VLAN configuradas en Fortinet**. • Fortinet opera con **perfiles de seguridad activos (antivirus avanzado, IPS, filtrado web, control de aplicaciones, inspección SSL)** para mitigar amenazas durante la recuperación. • Se ejecutan **simulacros semestrales de restauración completa**, cuyos resultados se consolidan en el **Formato Simulacro (FOR GSI 050)**.

2. *Controles dirigidos a las personas.*

A 6.2	**Dispositivos móviles y teletrabajo**
A 6.2.1	**Uso de dispositivos autorizados** • Solo se permite el uso de **equipos corporativos** registrados en el inventario de activos administrado en **GLPI**. • Cada dispositivo está asignado a un usuario identificado y cuenta con **Carta Responsiva (FOR GSI 031)** firmada. • Está prohibido el uso de dispositivos personales para almacenar, procesar o transmitir información clasificada de la organización.

A 6.2.2	**Controles de seguridad en dispositivos móviles**
	• Todos los dispositivos corporativos deben cumplir las siguientes medidas:
	  ○ **Cifrado de disco completo** con BitLocker en laptops y portátiles.
	  ○ **Protección antimalware avanzada (SentinelOne XDR)** en ejecución permanente.
	  ○ **Certificados SSL corporativos** para validación de comunicaciones con Fortinet.
	  ○ **Políticas GPO** aplicadas desde Active Directory, incluyendo bloqueo de puertos, restricciones de instalación de software y configuración segura.
	  ○ **Contraseñas robustas** con mínimo de 12 caracteres, complejidad obligatoria y caducidad cada 90 días.
	• Los equipos están sujetos a **mantenimiento preventivo semestral** programado en GLPI y **correctivo** cuando sea necesario, con registro en CIA-Desk.

A 6.2.3	**Política de teletrabajo** • El teletrabajo está permitido únicamente para la **Dirección General, Dirección General Adjunta, Gerencia Administrativa y Gerencia de Investigación de Crédito**. • **Personal operativo** tienen **prohibido** realizar teletrabajo. • Todo acceso remoto debe realizarse exclusivamente mediante **VPN Printunl**, con credenciales individuales y registros de conexión. • La cadena de autenticación obligatoria es: **BitLocker → Windows AD → Portal Cautivo Fortinet → Certificado SSL → VPN Printunl**. • El teletrabajo debe realizarse únicamente desde **redes privadas seguras** con estándares WPA2 o superiores.
A 6.2.4	**Responsabilidades de los usuarios**

	El colaborador es responsable del **uso correcto, resguardo físico y cumplimiento de las políticas de seguridad** sobre el dispositivo asignado y todo incidente (pérdida, robo, mal uso o mal funcionamiento) debe reportarse de inmediato mediante **CIA-Desk**. a) En caso de robo, el usuario será el responsable de dar aviso por cualquier medio al área de Sistemas y también deberá acudir ante el Ministerio Público para levantar el acta correspondiente, dicha acta deberá estar correctamente ratificada por el ministerio público en turno, en caso de no estar debidamente ratificada se notificará al área de Contabilidad y Tesorería, Recursos Humanos y jefe inmediato para generar un descuento por el valor del equipo vía nómina. b) En caso de pérdida, el usuario será el responsable de dar aviso por cualquier medio al área de Sistemas y se informará al área de Contabilidad y Tesorería, Recursos Humanos y jefe inmediato para generar un descuento por el valor del equipo vía nómina. Sea el caso "a" o el caso "b", el área de Sistemas procederá a realizar las siguientes acciones: • Revocar y suspender los accesos del usuario a sobre cualquier sistema de la organización. • Reportar y suspender la línea telefónica y equipo celular de la empresa con el proveedor para evitar el mal manejo de este. • Asignar una nueva línea telefónica al usuario y/o recuperar la línea telefónica en un nuevo chip para reasignar al usuario. • Asignar un nuevo equipo celular y/o laptop al usuario para no afectar la operación del área correspondiente, el usuario tendrá la responsabilidad de firmar nuevamente la **Carta responsiva FOR GSI 031** a fin de hacerse responsable del equipo nuevo.
A 7.2	**Responsabilidades antes, durante y después del empleo**
A 7.2.1	**Antes del empleo** La organización reconoce que la seguridad de la información comienza incluso antes de que un colaborador se integre formalmente a la empresa. Por ello, se han establecido las siguientes disposiciones: • **Acuerdo de confidencialidad previo:** Todo candidato que sea considerado para contratación debe firmar un **Convenio de Confidencialidad** previo a su ingreso, el cual garantiza que cualquier información compartida durante procesos de reclutamiento, entrevistas o pruebas técnicas será resguardada. Este proceso es gestionado y documentado por el área de **Recursos Humanos (RH)** conforme al **Mapa de Procesos de recursos humanos MAP REH 001**.
A 7.2.2	**Durante el empleo** Una vez que el colaborador ha sido contratado, la organización le asigna responsabilidades formales y permanentes en la protección de la información, sustentadas en documentos, procesos y controles técnicos: • **Asignación formal de responsabilidades:** ○ **Matriz de asignación de Roles y Responsabilidades FOR GSI 043.** ○ **Matriz de roles por activos de información críticos FOR GSI 025.** ○ **Carta responsiva FOR GSI 031.** • **Gestión de accesos:** Todos los accesos lógicos se otorgan mediante **AD**, **Fortinet** y **VPN Printunl**, aplicando el principio de **mínimo privilegio**. Los permisos se limitan a las funciones del puesto, y cualquier solicitud de ampliación debe gestionarse mediante **FOR GSI 032 Autorización de Accesos**, con validación de jefe inmediato, Gerencia Administrativa y Dirección General.

	• **Recertificación de accesos:** Trimestralmente, la **Coordinación de Sistemas TI** realiza la **recertificación de accesos**, documentada en el formato **Recertificación de accesos FOR SIS 010**, complementado con el monitoreo de seguridad definido en **Monitoreo de seguridad de informática FOR SIS 003**. Esta actividad asegura que no existan cuentas activas sin justificación. • **Gestión de incidentes:** Todo incumplimiento o incidente de seguridad detectado por el colaborador debe reportarse de inmediato en **CIA-Desk**, donde se genera un folio para seguimiento. La atención de estos incidentes se rige por el **Procedimiento PRO GSI 020 – Gestión de Incidentes**, y su clasificación se documenta en el **Formato FOR GSI 024 – Incidentes de Seguridad de la Información**. • **Concientización continua:** Durante el empleo, los colaboradores participan en programas de capacitación (A.7.4) que refuerzan sus responsabilidades, incluyendo temas de seguridad de la información.
A 7.2.3	**Después del empleo** En la etapa de terminación de la relación laboral, la organización asegura que la desvinculación del colaborador no implique riesgos para la seguridad de la información. • **Proceso de baja formal:** RH sigue el **mapa de proceso de recursos humanos MAP REH 001**, notificando la baja mediante ticket en **CIA-Desk y/o correo electrónico**. • **Revocación de accesos:** La **Coordinación de Sistemas TI** tiene un plazo máximo de **24 horas** para deshabilitar accesos en AD, Fortinet, VPN Printunl y cualquier otra aplicación crítica. La evidencia se registra en CIA-Desk con capturas de desactivación y se adjunta a la bitácora de seguridad. • **Recuperación de activos:** Bajo el **Mapa de proceso de sistemas MAP SIS 001**, los equipos asignados se devuelven a Sistemas, se registran nuevamente en GLPI y se someten a procesos de borrado seguro de información. El colaborador firma en la parte de entrega en la **carta responsiva FOR GSI 031**. • **Confidencialidad post-empleo:** Se menciona al excolaborador que la **obligación de confidencialidad subsiste aún después de la relación laboral**, conforme a lo pactado en el convenio inicial y a las políticas del SGSI.
A 7.4	**Capacitación y concientización en seguridad de la información**
A 7.4.1	La organización cuenta con un **Plan Anual de Capacitación** aprobado por la Dirección General, en el cual se contemplan cursos obligatorios de **onboarding impartidos a través de la plataforma eLearning UniverCIA**. Estos cursos están diseñados para que cada nuevo colaborador, al incorporarse, reciba de forma estructurada y documentada la concientización inicial en materia de seguridad de la información y cumplimiento normativo. Los cursos de onboarding incluyen módulos sobre: • **Seguridad de la información** y los lineamientos del SGSI. • **Ley Federal de Protección de Datos Personales en Posesión de Particulares**, enfatizando las obligaciones legales que aplican a todos los colaboradores. • **Prevención de corrupción y soborno**, alineado con políticas internas y compromisos contractuales con clientes. • **Conociendo CIA**, módulo donde se explica la cultura organizacional, la importancia de la seguridad en procesos operativos y administrativos, y las expectativas de cumplimiento. • Otros cursos complementarios definidos anualmente en el programa. De manera paralela cada colaborador firma un **paquete de contratación** que incluye: • El **Convenio de Confidencialidad**, en el cual se reconoce la obligación de proteger la información incluso después de terminada la relación laboral. • El **Aviso de Privacidad**, donde se detalla el tratamiento de datos personales.

	• La **Aceptación de lineamientos y políticas de seguridad de la información**, asegurando que desde el inicio el empleado es consciente y acepta las normas que regulan su conducta dentro de la organización.
A 7.4.2	**Capacitación periódica** De manera periódica, se realizan capacitaciones obligatorias en las que se refuerza a los colaboradores sobre: • Conocimientos sobre el sistema de gestión de seguridad de la información. • Conocimientos sobre la ley federal de protección de datos personales en posesión de particulares. • Conocimientos sobre anticorrupción.
A 7.4.3	**Campañas de concientización** La organización mantiene un programa permanente de concientización que incluye: • **Boletines mensuales** con alertas de seguridad, recomendaciones de uso seguro de herramientas y recordatorios de políticas. • **Comunicados** sobre temas seguridad de la información. **Simulacros y pruebas prácticas** Periódicamente se realizan **simulacros de phishing** y campañas de correo falso controladas para evaluar la respuesta de los colaboradores ante intentos de ingeniería social. Los resultados se analizan y se refuerzan las áreas de oportunidad detectadas.
A 7.7	**Escritorio despejado y pantalla despejada**
A 7.7.1	**Gestión de documentos en el puesto de trabajo** Todos los colaboradores deben mantener sus puestos de trabajo libres de documentos que contengan información clasificada como interna, restringida o confidencial. Cuando un usuario se ausenta de su escritorio, aunque sea por periodos cortos, está obligado a guardar dichos documentos. Se prohíbe dejar impresiones en multifuncionales, copiadoras o impresoras compartidas; deben ser retiradas inmediatamente una vez que son generadas.
A 7.7.2	**Control en áreas comunes** En salas de juntas, estaciones de trabajo compartidas, comedores y otros espacios comunes, los colaboradores deben extremar precauciones para no dejar información sensible expuesta. Cualquier documento utilizado en reuniones debe ser recogido al finalizar, evitando que quede sobre mesas, proyectores o pizarras.
A 7.7.3	**Pantallas de equipos de cómputo** Todos los equipos de cómputo cuentan con políticas de **bloqueo automático configuradas en GPO por medio del AD**: • **2 minutos de inactividad** para todas las áreas. Adicionalmente, cada usuario debe bloquear manualmente su sesión al ausentarse de su lugar de trabajo utilizando el comando **Windows + L**, sin excepción.
A7.7.4	**Medios removibles y almacenamiento temporal** El uso de dispositivos de almacenamiento removible como memorias USB, discos externos o tarjetas SD está bloqueado por políticas GPO. En caso de requerir habilitación temporal, debe gestionarse mediante una solicitud formal en **CIA-Desk**, autorizada por Dirección General o Gerencia Administrativa, y documentada en el **Formato FOR GSI 047**. El uso de dispositivos personales para transferir información queda completamente prohibido.

A 7.7.5	**Señalización y cultura de cumplimiento** En todas las áreas de la organización existen carteles y material de concientización que refuerzan la política de escritorio despejado y pantalla limpia. Estos recordatorios se complementan con comunicados periódicos y boletines mensuales, de modo que la cultura de cumplimiento sea visible y constante en la operación diaria.

3. *Controles físicos.*

A 7.1	Seguridad física perimetral y en oficinas
A 7.1.1	**Control de accesos al perímetro** Las oficinas de la organización (Nezahualcóyotl, Insurgentes y Toluca) cuentan con medidas de seguridad física que protegen el perímetro y los accesos principales. Todos los accesos se controlan mediante **sistemas biométricos y credenciales institucionales**. Ningún colaborador, visitante o proveedor puede ingresar sin estar previamente autorizado. El acceso de visitantes se gestiona a través del **Formato FOR GSI 033 – Control de acceso a visitantes**, en el cual deben registrarse datos de identificación, persona a la que visitan, hora de ingreso y salida. Adicionalmente, se emite un gafete de visitante que debe portarse de manera visible durante toda la estancia. Los proveedores y contratistas que ingresen con equipo tecnológico deben registrarlo en el mismo formato.
A 7.1.2	**Monitoreo por CCTV y alarmas** Las oficinas cuentan con un sistema de **circuito cerrado de televisión (CCTV)** con cámaras instaladas en accesos principales, pasillos, áreas comunes, site de servidores y perímetros externos. Las grabaciones se almacenan en DVR/NVR con una **retención mínima de 90 días**, lo que permite contar con evidencia objetiva en caso de incidentes. Adicionalmente, cada oficina está equipada con **alarmas conectadas a centrales de monitoreo (ADT)**, sensores de movimiento y contactos magnéticos en puertas de acceso. Cualquier activación genera una alerta que es atendida en tiempo real. Los registros de incidentes de CCTV y alarmas se documentan en **CIA-Desk**.
A 7.1.3	**Control de accesos internos y supervisión** Dentro de las oficinas, las áreas críticas como centros de datos, archivo de expedientes y call center cuentan con **puertas de acceso reforzadas con cerraduras de alta seguridad**. Solo el personal autorizado en la **Carta Compromiso de Accesos FOR GSI 035** puede ingresar a estas áreas, y todo ingreso no autorizado mediante la **Carta Compromiso de Accesos FOR GSI 035** queda documentado en la **Bitácora FOR GSI 004 – Acceso a áreas seguras**. Los colaboradores que aún no estén dados de alta en biométrico deben registrarse manualmente en el **Formato FOR GSI 033**, hasta que su huella o credencial quede habilitada.
A 7.1.4	**Seguridad perimetral y señalización** Todas las instalaciones cuentan con: • **Señalización visible de áreas restringidas y rutas de evacuación**, conforme a lo establecido en el **PRO GSI 047 – Procedimiento de Vigilancia**. • **Iluminación perimetral** adecuada en accesos principales. • **Puertas y ventanas con cerraduras** para reducir riesgos de intrusión.

	El personal de sistemas verifica mensualmente estas condiciones y documenta hallazgos en **FOR SIS 006 – Check list de revisión de instalaciones** y **FOR SIS 008 – Check list de seguridad de instalaciones**.
A 7.5	**Áreas de acceso restringido**
A 7.5.1	**Definición de áreas restringidas** La organización ha identificado como **áreas de acceso restringido** a los sitios donde se resguarda información crítica o infraestructura tecnológica esencial para la operación. Entre ellas se encuentran los **centros de datos (sites)**, los **archivos de expedientes físicos** (Recursos Humanos, Jurídico, Contabilidad, Cobranza, Investigación de Crédito) y los **centros de contacto (call center)**. Estas áreas están señalizadas con letreros visibles de **"Área restringida"**, conforme a lo establecido en el **PRO GSI 047 – Procedimiento de Vigilancia**, y su acceso está estrictamente limitado a personal previamente autorizado y documentado en la **Carta Compromiso de Accesos FOR GSI 035** **En las áreas seguras no está permitido:** • Realizar ningún tipo de grabación fotográfica, de audio o de vídeo (salvo las del circuito cerrado). • Enchufar cualquier dispositivo eléctrico en una red eléctrica. • Tocar o manipular de cualquier forma equipos instalados en áreas seguras. • Conectar cualquier dispositivo a una red alámbrica e inalámbrica. • Guardar materiales o equipos inflamables. • Utilizar cualquier tipo de dispositivo de calefacción. • Fumar, comer o beber.
A 7.5.2	**Mecanismos de control de acceso** • **Puertas con cerraduras de alta seguridad**. • **Bitácora FOR GSI 004 – Acceso a áreas seguras** para registrar cada ingreso y salida, donde se documenta: nombre completo, área, motivo de acceso, hora de entrada y salida, así como la firma del responsable que acompaña en caso de visitas. • **Cámaras CCTV** instaladas en entradas y pasillos que conducen a áreas críticas, con grabación continua y almacenamiento mínimo de 90 días. • **Llaves y credenciales controladas**.
A 7.5.3	**Procedimiento de acceso para visitantes y terceros** Cuando un visitante y proveedor requiere ingresar a un área restringida: 1. Debe registrarse en el **FOR GSI 033 – Control de acceso a visitantes** al ingresar a las instalaciones. 2. Si el acceso es al site o archivo físico, se debe registrar además en la **Bitácora FOR GSI 004 – Acceso a áreas seguras**. 3. Todo visitante debe ser **acompañado en todo momento** por personal autorizado, que se responsabiliza de su permanencia. 4. Está prohibido el uso de celulares, cámaras o dispositivos de grabación dentro de los sites y call centers.
A 7.8	**Seguridad de los equipos en las instalaciones**
A 7.8.1	**Ubicación y resguardo de equipos críticos** Todos los equipos que forman parte de la infraestructura tecnológica de la organización (servidores, switches, firewalls, storage NAS, equipos de respaldo, estaciones de trabajo críticas y dispositivos de red inalámbrica Huawei) se encuentran instalados en

	sites identificados como áreas seguras y restringidas, conforme a lo establecido en el **PRO GSI 047 – Procedimiento de Vigilancia**. Estos espacios cuentan con **cerraduras**, registro en **FOR GSI 004 – Bitácora de acceso a áreas seguras** y monitoreo permanente por **CCTV** con retención mínima de 90 días. Ningún equipo crítico se encuentra en áreas abiertas sin control de acceso.
A 7.8.2	**Seguridad física en estaciones de trabajo y periféricos** Las estaciones de trabajo asignadas a los colaboradores están aseguradas mediante: • Ubicación estratégica en oficinas para evitar exposición de pantallas hacia visitantes o áreas comunes. • Configuración de **bloqueo automático a los 2 minutos de inactividad de sesión vía GPO** y uso obligatorio de **Windows + L** en ausencias temporales. Los equipos portátiles (laptops) se asignan únicamente mediante **FOR GSI 031 – Carta Responsiva**, quedando bajo custodia personal del usuario, y deben utilizarse con las configuraciones de seguridad establecidas (BitLocker, SentinelOne, VPN Printunl)
A 7.8.3	**Protección de equipos de red y telecomunicaciones** Los switches, routers, access points Huawei y equipos Fortinet están instalados en racks y cableado estructurado debidamente canalizado y numerado, conforme al inventario registrado en **GLPI**. El acceso a racks de telecomunicaciones solo se autoriza a personal de TI documentado en **FOR GSI 035 – Carta compromiso de accesos**, y cualquier intervención (mantenimiento, cambio de patch panel, sustitución de equipo) se registra en **CIA-Desk** como evidencia de control.
A 7.8.4	**Protección de servidores y equipos de respaldo** Los servidores físicos, controladores de dominio, appliances de seguridad y storage NAS están instalados en racks. Cuentan con **alimentación eléctrica redundante a través de UPS**, lo que permite un apagado controlado en caso de corte de energía. Los equipos de respaldo (tanto físicos como virtuales) están configurados con replicación controlada de datos, con registros de pruebas de restauración documentados en la **LIS GSI 002 - Revision de LOGS**
A 7.8.5	**Controles ambientales para equipos instalados** Los sites donde se ubican equipos críticos cuentan con: • **Sensores de temperatura y humedad** conectados a sistemas de aires acondicionados, con umbrales de 18–27 °C y 40–60 % de humedad relativa. • **Aires acondicionados dedicados** que mantienen condiciones estables. • **Sensores de humo y alarmas contra incendio** revisados mensualmente, con reportes en **FOR SIS 006 – Check list de revisión de instalaciones** y **FOR SIS 008 – Check list de seguridad de instalaciones**. • **UPS** con pruebas trimestrales documentadas en **FOR SIS 003 – Monitoreo de Seguridad de Informática**. Cualquier desviación en condiciones ambientales se documenta como incidente y se gestiona bajo el **PRO GSI 020 – Gestión de Incidentes**.
A 7.11	**Protección contra amenazas físicas y ambientales**
A 7.11.1	**Infraestructura de respaldo eléctrico** Todas las sedes de la organización cuentan con sistemas de **alimentación ininterrumpida (UPS)** instalados en los equipos de computo. Estos UPS están configurados para proporcionar autonomía mínima de 15 minutos, permitiendo un apagado controlado de servidores, controladores de dominio, firewalls Fortinet, storage NAS y switches principales.

A 7.11.2	**Protección contra incendios** En todas las oficinas y sites se encuentran instalados **sensores de humo y detectores de calor** conectados a sistemas de alarma locales. Estos dispositivos generan alertas inmediatas en caso de detectar humo en áreas críticas como archivos de expedientes y cuartos de servidores. Los sites cuentan con **extintores tipo ABC y de CO_2**, instalados estratégicamente conforme a normativas locales de Protección Civil y al **PRO DIR 001 – Plan de Protección Civil**. • Los extintores son inspeccionados mensualmente por el área de vigilancia, con registro en **FOR SIS 006 – Check list de revisión de instalaciones**. • La recarga anual se valida con reportes y factura del proveedor autorizado y se documenta en CIA-Desk como ticket de cumplimiento. Queda prohibido almacenar materiales inflamables en áreas seguras. Cualquier hallazgo se considera una no conformidad y se gestiona como incidente en CIA-Desk.
A 7.11.3	**Condiciones ambientales en sites** Los sites donde se alojan servidores, firewalls Fortinet, equipos de telecomunicaciones Huawei y storage NAS cuentan con **aires acondicionados dedicados** y **sensores de temperatura y humedad**. • Se mantienen rangos de **18 a 27 °C de temperatura** y **40 a 60 % de humedad relativa**. • Los sensores están conectados a sistemas de aire acondicionado. • Cualquier anomalía ambiental se documenta en CIA-Desk como incidente, asignando acciones correctivas inmediatas.
A 7.11.4	**Protección contra fugas de agua y riesgos estructurales** Las oficinas y sites cuentan con revisiones mensuales para identificar riesgos de filtraciones de agua, humedad o vulnerabilidades estructurales. Estas revisiones son realizadas por personal de sistemas y documentadas en **FOR SIS 008 – Check list de seguridad de instalaciones**. Los racks con servidores y equipos de red se encuentran **elevados al menos 10 cm del piso** para evitar daños en caso de derrames o fugas. Se prohíbe instalar equipos bajo ductos activos de agua o en áreas sin impermeabilización validada.
A 7.11.5	**Cableado estructurado y protección contra daños físicos** Todo el cableado de red, eléctrico y de telecomunicaciones está canalizado en **ductos cerrados** y debidamente etiquetado. Está prohibido que existan cables sueltos en pasillos o sobre pisos transitados. La relación de nodos y VLAN asociadas a cada punto de red está documentada en el **inventario GLPI**, lo que permite validar que las conexiones sean seguras y ordenadas.
A 7.14	**Trabajo fuera de sitio seguro**
A 7.14.1	**Lineamientos generales** El trabajo fuera de sitio seguro comprende todas aquellas actividades realizadas por colaboradores de la organización en lugares distintos a las oficinas autorizadas (Nezahualcóyotl, Insurgentes y Toluca). Esto incluye viajes de negocio, visitas a clientes, auditorías externas o cualquier situación en la que el empleado requiera utilizar dispositivos corporativos en entornos no controlados. La política establece que **únicamente se podrán utilizar equipos corporativos inventariados en GLPI y asignados formalmente mediante la carta responsiva FOR GSI 031**, los cuales deben contar con todas las configuraciones de seguridad y hardening vigentes: **BitLocker habilitado, SentinelOne XDR activo, VPN Printunl, Login de windows AD, certificados SSL instalados y políticas GPO aplicadas**.

A 7.14.2	**Acceso remoto y conexión segura** Para conectarse a la infraestructura tecnológica de la organización desde ubicaciones externas e internas: • Es obligatorio el uso de la **VPN Printunl**, con credenciales individuales y registro de logs. • Todo acceso se valida mediante la cadena de autenticación: **BitLocker → Windows AD → Portal Cautivo Fortinet → Certificado SSL en el endpoint → VPN Printunl**. • Queda estrictamente prohibido el acceso a servidores, respaldos o aplicaciones web corporativas sin conexión activa a la VPN Printunl. • Los usuarios deben evitar conexiones desde **redes Wi-Fi públicas** (cafeterías, aeropuertos, hoteles); en caso de no haber alternativa, deben habilitar un **hotspot personal con cifrado WPA2 o superior**. El área de TI monitorea las conexiones remotas en los registros de VPN y Fortinet, generando alertas en CIA-Desk cuando se detectan accesos fuera de los parámetros establecidos.
A 7.14.3	**Manejo de información y restricciones en campo** Durante el trabajo remoto o en campo: • Toda la información clasificada como **confidencial o restringida** debe almacenarse únicamente en servidores corporativos accesibles por VPN Printunl. • Está prohibido guardar información sensible en discos locales, memorias USB o servicios en la nube no autorizados. • El uso de **correo institucional bajo @ciasc.mx** es obligatorio para toda comunicación laboral; queda prohibido el uso de cuentas personales. • En situaciones donde sea necesario presentar información a clientes o terceros, el material debe estar previamente validado y marcado conforme a la clasificación establecida en **PRO GSI 015 – Gestión de Activos, Clasificación y Control de la Información**
A 7.14.4	**Reglas de protección física en sitios externos** Los equipos corporativos (laptops y celulares) deben permanecer bajo custodia del usuario asignado en todo momento: • No deben dejarse desatendidos en vehículos, habitaciones de hotel sin caja de seguridad, salas de espera o espacios públicos. • En auditorías o visitas a clientes, los dispositivos deben utilizarse únicamente en las áreas habilitadas y bajo supervisión del anfitrión. En caso de robo o pérdida, el colaborador debe: Reportar el incidente inmediatamente a sistemas. Levantar un acta en el **Ministerio Público** y **ratificarla en un plazo máximo de 72 horas**. Entregar copia del acta ratificada a RH y a Sistemas. Ver. A 6.2.4

4. *Controles físicos.*

A 8.1	**Dispositivos de punto final de usuario**

A 8.1.1	**Estándares de configuración obligatorios** El área de sistemas es responsable de la instalación y configuración de los dispositivos móviles, laptops y/o equipos pc, por lo tanto, queda prohibido que los usuarios hagan cambios en el hardware, modifiquen la configuración o descarguen e instalen softwares ajenos a los manifestados en el **Catálogo de software y aplicaciones permitidos en CIA LIS GSI 004** y que sean utilizados para otros fines y funciones ajenos a las actividades encomendadas por nuestra Empresa.

A 8.1.2	**Configuraciones BASE.**
	Todos los dispositivos de punto final (PC de escritorio, laptops y celulares corporativos) deben cumplir con una **línea base de configuración de seguridad definida por la organización**, la cual es aplicada, monitoreada y verificada por la **Coordinación de Sistemas TI**.
	Esta línea base de hardening incluye obligatoriamente:
	• **BitLocker** habilitado para el cifrado completo de discos en laptops y equipos portátiles.
	• **Antimalware SentinelOne XDR** instalado y activo en todos los dispositivos, con reportes centralizados en consola y alertas integradas con CIA-Desk.
	• **VPN Printunl**
	• **Acceso Fortinet (portal cautivo).**
	• **Certificado SSL corporativo** en cada endpoint para validar conexiones seguras con Fortinet y garantizar autenticación del dispositivo.
	• **Políticas GPO** aplicadas desde Active Directory que:
	  ○ Deshabilitan puertos USB por defecto.
	  ○ Restringen instalación de software no autorizado.
	  ○ Configuran bloqueo automático de sesión por inactividad (2 min en áreas críticas, 5 min en no críticas).
	• **Actualizaciones de sistema operativo y parches de seguridad** aplicados de manera programada conforme al **PRO GSI 039 – Operativo para las TIC**, con seguimiento en CIA-Desk.

A 8.1.3	**Gestión de inventario y asignación** Todos los dispositivos se encuentran inventariados en **GLPI**, donde se registra número de serie, modelo, características técnicas, usuario asignado y estado de operación. La entrega de cada equipo a un colaborador debe formalizarse con la **Carta Responsiva FOR GSI 031**, donde se documenta la aceptación de custodia, el compromiso de uso conforme a políticas y la prohibición de modificar configuraciones. Cuando un dispositivo cambia de usuario, el equipo debe pasar por un proceso de **formateo seguro, reinstalación de la configuración base y reasignación en GLPI**.
A 8.1.4	**Mantenimiento preventivo y correctivo** Todos los dispositivos de punto final deben mantenerse en condiciones óptimas mediante un programa de mantenimiento definido: • **Mantenimiento preventivo**: se ejecuta de forma **semestral**, programado en el calendario de **GLPI**, y documentado en **FOR SIS 001 – Conformidad de mantenimiento preventivo**. Incluye limpieza física de equipos, revisión de integridad de discos duros, validación de estado de batería en laptops, prueba de puertos y periféricos, así como verificación de que BitLocker y SentinelOne se encuentren activos y funcionando.

	• **Mantenimiento correctivo**: cualquier falla reportada por los usuarios debe ser registrada en **CIA-Desk**. La Coordinación de Sistemas TI evalúa el ticket, diagnostica el problema y documenta las acciones aplicadas. Al cierre, el usuario valida la corrección confirmando en el ticket electrónico. • **Control de cambios**: si durante el mantenimiento correctivo es necesario sustituir hardware o reinstalar sistema operativo, el área de TI reinstala la **línea base de seguridad (BitLocker, SentinelOne, SSL, GPOs)** y actualiza el estatus del equipo en **GLPI**. • **Evidencia de cumplimiento**: todos los mantenimientos quedan registrados en GLPI con su folio de CIA-Desk asociado, lo que permite trazabilidad para auditoría
A 8.1.5	**Supervisión del cumplimiento** La Coordinación de Sistemas TI realiza revisiones cada 3 meses para validar que todos los endpoints mantengan activa la línea base de seguridad. Estas revisiones incluyen: • Verificación de cifrado con BitLocker. • Estado de protección en SentinelOne (agente activo, sin alertas críticas). • Vigencia del certificado SSL instalado. • Confirmación de aplicación de GPO y tiempos de bloqueo automático. • Validación de actualizaciones instaladas en sistema operativo. Los resultados de estas revisiones se documentan en **FOR SIS 003 – Monitoreo de Seguridad de Informática**.
A 8.23	**Seguridad en redes y comunicaciones**
A 8.23.1	**Segmentación y control de tráfico por VLAN** La red corporativa está **segmentada por VLAN** de acuerdo con las áreas de la organización (Dirección General, Recursos Humanos, Contabilidad, Sistemas, Investigación de Crédito, Cobranza Social, Cobranza RE, Gestión Domiciliaria y Recuperación de Cartera). Cada colaborador se conecta únicamente a la VLAN que corresponde a su función, lo que garantiza aislamiento lógico y cumplimiento del principio de **mínimo privilegio en redes**. El tráfico inter-VLAN se encuentra **bloqueado por defecto** y únicamente se autorizan excepciones específicas validadas por la Dirección General y Gerencia Administrativa, documentadas en **FOR GSI 047 – Excepciones**. Esta medida impide que un incidente en un área comprometa la operación de otras.

A 8.23.2	**Configuraciones de seguridad en Fortinet**
	El firewall **Fortinet** implementa un conjunto de políticas y perfiles de seguridad avanzados:
	• **Políticas de firewall personalizadas por VLAN**: reglas estrictas de entrada y salida para cada área, aplicadas por nodo y usuario.
	• **Perfiles de seguridad**: análisis profundo de antivirus, filtrado web, IPS, inspección SSL y control de aplicaciones.
	• **Calendarios de acceso por horario y sede**:
	  ○ Oficinas de Nezahualcóyotl e Insurgentes → tráfico habilitado solo entre **08:30 y 20:30 horas**.
	  ○ Oficina Toluca → tráfico habilitado entre **06:30 y 20:30 horas**.
	  ○ Fuera de estos horarios, el tráfico en cualquier sentido queda bloqueado automáticamente.
	• **Portal cautivo personalizado**: todos los usuarios deben autenticarse con credenciales individuales antes de acceder a la red. El portal muestra mensajes de concientización diseñados para reforzar la cultura de seguridad de la información.

	• **Certificados SSL en endpoints**: instalados en todos los equipos corporativos, verifican autenticidad de los dispositivos frente al Fortinet. • **Conectores externos de inteligencia de amenazas**: actualización en tiempo real de listas negras de IP, dominios y hashes maliciosos.

A 8.23.3	**Redes inalámbricas y segmentación por SSID**
	Las redes inalámbricas se gestionan mediante **access points Huawei**, configurados con **SSID personalizados y vinculados a cada VLAN**. Esto permite que el acceso inalámbrico tenga el mismo nivel de segmentación y control que las redes cableadas.
	• Cada área cuenta con un SSID corporativo específico, por ejemplo:
	  ○ Nezahualcóyotl: CIASC-DIRCOR, CIASC-REHCOR, CIASC-CONCOR, CIASC-SISCOR, CIASC-INVCOR, CIASC-GESCOR.
	  ○ Insurgentes: CIASC-COSVAL, CIASC-CREVAL, CIASC-DIRCOR, CIASC-REHCOR.
	  ○ Toluca: CIASC-DIRCOR, CIASC-REHCOR, CIASC-RECTOLC, CIASC-RECTOLS.
	• Existe un SSID exclusivo para **invitados (CIASC-INVITADOS)**, totalmente aislado de la red interna. El tráfico de invitados no comparte rutas ni recursos con las VLAN corporativas.

A 8.23.4	**Monitoreo y supervisión de redes** Toda la actividad en redes cableadas e inalámbricas es monitoreada por Fortinet y SentinelOne: • **Fortinet**: genera logs de tráfico, autenticación y alertas de IPS. • **SentinelOne XDR**: detecta actividades sospechosas en endpoints conectados a la red. • **CIA-Desk**: sirve como bitácora central para registrar incidentes de red, reportes de usuarios y acciones correctivas. Los **logs de Fortinet y VPN Printunl** se revisan periódicamente conforme al procedimiento de revisión de registros (**LIS GSI 002 – Revisión de LOGS**). Los hallazgos se documentan en tickets de CIA-Desk y se integran en auditorías internas.
A 8.23.5	**Gestión de incidentes y acciones correctivas** Cualquier anomalía detectada en la red (intentos de acceso no autorizado, conexiones fuera de horario, tráfico sospechoso entre VLANs, uso indebido de la red de invitados) se documenta como incidente en **CIA-Desk**, de acuerdo con el **PRO GSI 020 – Gestión de Incidentes**. Cada incidente debe ser atendido por la Coordinación de Sistemas TI en un plazo máximo de 24 horas, y las acciones correctivas se formalizan en CIA Desk.
A 8.13	**Copias de seguridad**
A 8.13.1	**Política general de respaldos** La organización asegura que toda la información crítica de negocio, bases de datos, sistemas operativos, configuraciones de red y aplicaciones corporativas cuenten con **copias de seguridad periódicas, verificables y disponibles** para su restauración en caso de incidentes, fallas técnicas o desastres. Esta política se aplica tanto a los **servidores físicos y virtuales** como a equipos de usuario final que contengan información clasificada. Los respaldos se gestionan conforme al **PRO GSI 032 – Respaldos y eliminación de la información**, garantizando trazabilidad, integridad y control de retención.
A 8.13.2	**Alcance de los respaldos** Los respaldos cubren, de forma **incrementa**l, la siguiente información:

	• **Bases de datos**.
	  ○ Sicob
	  ○ Aspel
	  ○ Filemarker
	  ○ CIA Desk
	  ○ GLPI
	  ○ Intranet Sistemas de Gestión
	
	• **Configuraciones críticas**.
	  ○ Switches
	  ○ Fortinet
	  ○ Directorio Activo
	
	• **Máquinas virtuales (almacenamiento y sistemas operativos)**
	  ○ Sicob
	  ○ Aspel
	  ○ Filemarker
	  ○ CIA Desk
	  ○ GLPI
	  ○ Intranet Sistemas de Gestión
	  ○ Directorio Activo
	  ○ VPN Printunl
	  ○ Servidor de Archivos

A 8.13.3	**Frecuencia y procedimientos** Los respaldos se realizan cada 60 minutos en **espacios dedicados y servidores de respaldo alternos**, aislados mediante VLAN y con acceso controlado por Fortinet y certificados SSL; con lo anterior se garantiza minimo 24 copias de seguridad al día por cada base de datos, servidor y maquina virtual.
A 8.13.4	**Pruebas de restauración** Cada trimestre se realizan **pruebas de restauración** para validar que los respaldos pueden recuperarse en los tiempos de recuperación (RTO) y puntos de recuperación (RPO) definidos en la **Plan de recuperación de desastres PRO GSI 100**. Las pruebas incluyen: • Restauración parcial de archivos y carpetas seleccionadas. • Simulación de recuperación completa de servidores virtuales. • Validación de integridad mediante **sumas de verificación (hash SHA-256)**. • Registro de resultados en la **Bitácora LIS GSI 012 – Pruebas de respaldos**, con ticket asociado en **CIA-Desk**.
A 8.13.5	**Eliminación de respaldos** Los respaldos que exceden su periodo de retención deben ser eliminados de manera **segura e irreversible**, utilizando el software especializado **Privacy Eraser,** conforme a lo indicado en el **PRO GSI 032 Procedimiento Respaldos y Eliminación de la Información.** El método aplicado consiste en **sobrescritura múltiple de los sectores del medio de almacenamiento**, de acuerdo con estándares internacionales reconocidos (como **DoD 5220.22-M**), garantizando que la información no pueda ser recuperada con herramientas forenses. La organización ha definido como estándar el método **DoD 5220.22-M a 3 pasadas**, en el cual:

	1. Primera pasada → escritura de ceros en todos los sectores (Zero Fill). 2. Segunda pasada → escritura de unos en todos los sectores. 3. Tercera pasada → escritura aleatoria en todos los sectores, seguida de verificación. En casos donde la información es clasificada como **crítica/confidencial** o cuando así lo solicite un cliente/autoridad, se aplica el método **DoD 5220.22-M extendido a 7 pasadas**, que garantiza una sobrescritura aún más robusta. Registro en el **Formato FOR CAL 007 – Destrucción de información documentada**, con firma del Gerente Administrativo, del responsable de TI y del área solicitante. Este método asegura que la información eliminada no pueda ser recuperada por ningún medio técnico, cumpliendo con la **Ley Federal de Protección de Datos Personales en Posesión de Particulares**, con los requisitos contractuales de clientes estratégicos y con los controles del SGSI.
A.8.15 **A.8.16**	**Logging y monitoreo de actividades**
A.8.15.1 **A.8.16.1**	**Generación de registros** Todos los sistemas críticos de la organización generan y almacenan registros (logs) que documentan actividades de usuarios, procesos del sistema, accesos, errores, fallos y eventos de seguridad. Entre los sistemas que producen logs se encuentran: • **Fortinet**: registros de firewall, IPS, inspección SSL, filtrado web, control de aplicaciones, tráfico entre VLAN y autenticaciones en portal cautivo. • **VPN Printunl**: registros de accesos remotos (usuario, fecha, hora, IP de origen, VLAN asignada). • **Active Directory y GPO**: logs de inicio/cierre de sesión, cambios de contraseñas, intentos fallidos, bloqueos de cuentas, cambios en políticas de seguridad. • **SentinelOne XDR**: registros de actividad en endpoints, detección de malware, intentos de explotación, comportamiento sospechoso y acciones de contención automática. • **GLPI y CIA-Desk**: bitácora de tickets, incidencias y solicitudes que evidencian la trazabilidad de incidentes operativos y de seguridad. • **Servidores de aplicaciones y bases de datos**: logs de consultas, modificaciones, altas/bajas de registros y accesos administrativos. Todos los logs deben estar habilitados de forma obligatoria; no existe equipo crítico en producción sin registro activo.
A.8.15.2 **A.8.16.2**	**Protección e integridad de los logs** Los registros se almacenan con acceso restringido únicamente a la Coordinación de Sistemas TI. Se aplican controles de integridad mediante: • **Registros inmutables** en Fortinet y SentinelOne, evitando que puedan ser alterados. • **Respaldos periódicos de logs** incluidos en las rutinas de PRO GSI 032 – Respaldos. • Restricciones de acceso administradas en AD bajo perfiles específicos de auditoría.
A.8.15.3 **A.8.16.3**	**Protección e integridad de los logs** Los registros generados por los sistemas críticos de la organización (Fortinet, Active Directory, VPN Printunl, SentinelOne y aplicaciones internas) se almacenan en las consolas nativas de cada solución y en los repositorios internos de configuración, manteniendo su integridad mediante controles propios de cada plataforma.

	Para garantizar que los registros no sean manipulados o eliminados de forma indebida, se aplican las siguientes medidas: • **Registros inmutables en Fortinet y SentinelOne**, que no pueden ser modificados por usuarios comunes y que permiten la exportación de reportes con firmas digitales de integridad. • **Respaldos periódicos de logs**, incluidos en las rutinas documentadas en el PRO GSI 032 – Respaldos y eliminación de información, donde se asegura que los archivos de registros sean copiados junto con configuraciones críticas de firewalls, controladores de dominio y aplicaciones. • **Restricciones de acceso administradas en Active Directory**, que asignan perfiles específicos de auditoría únicamente a la Coordinación de Sistemas TI, evitando accesos indebidos de usuarios sin privilegios. • **Tickets en CIA-Desk** para toda exportación, resguardo o revisión de logs, lo que proporciona trazabilidad documental y control de cambios sobre los registros revisados. Con estas medidas, la organización asegura que los logs mantengan su valor como evidencia objetiva, garantizando que puedan ser consultados durante auditorías internas, externas y revisiones por la Dirección, incluso sin contar con una infraestructura dedicada exclusivamente a monitoreo.
A.8.15.4 **A.8.16.4**	**Monitoreo activo de actividades** Además de la revisión periódica de logs, la organización mantiene un esquema de **monitoreo activo y en tiempo real**: • **Fortinet**: dashboards en consola de seguridad para monitoreo de sesiones concurrentes, tráfico por VLAN y alertas de IPS. • **SentinelOne**: consola de administración centralizada para detección y respuesta en endpoints. • **CIA-Desk**: integración de alertas de SentinelOne y Fortinet como tickets automáticos de incidente crítico. Cuando se detecta un evento crítico (ejemplo: intento de intrusión, malware no contenido, conexión remota sospechosa), se activa el **PRO GSI 020 – Gestión de Incidentes**, clasificando el evento, aplicando contención inmediata y documentando acciones correctivas.
A 8.24	**Uso de criptografía**
A 8.24.1	**Principios de aplicación** La organización utiliza **controles criptográficos** como parte esencial de la protección de la confidencialidad, integridad y disponibilidad de la información. Todo mecanismo de cifrado empleado debe cumplir con estándares internacionales y con los requisitos contractuales de clientes estratégicos, como CitiBanamex, así como con las disposiciones de la **Ley Federal de Protección de Datos Personales en Posesión de Particulares**. El uso de criptografía es obligatorio en: • Comunicaciones electrónicas. • Almacenamiento de datos en endpoints y servidores. • Transferencia de información a terceros. • Protección de respaldos y medios removibles.
A 8.24.2	**Herramientas y algoritmos implementados** Los controles criptográficos vigentes en la organización incluyen: • **Cifrado de discos en endpoints (BitLocker)**: habilitado en todas las laptops y estaciones de trabajo que procesan información clasificada, con algoritmo **AES de 128 bits en modo XTS**.

	• **Certificados SSL/TLS corporativos**: instalados en todos los endpoints y servidores, con claves de **RSA 2048/4096 bits** y encriptación simétrica **AES 256 bits** en las comunicaciones. • **Hashing SHA-256**: utilizado para verificar la integridad de respaldos, logs y archivos críticos antes y después de transferencias. • **SecureZIP**: aplicado para transferencias de información con CitiBanamex, usando cifrado **AES 256 bits** y verificación mediante SHA-256, con rotación de claves cada 30 días según requerimiento del cliente. • **Fortinet SSL Inspection**: inspección de tráfico cifrado con certificados internos, lo que permite análisis de seguridad sin comprometer la confidencialidad de la información.
A 8.24.3	**Gestión de claves criptográficas** La organización mantiene un control estricto sobre la **generación, custodia, rotación y eliminación de claves criptográficas**, asegurando que las mismas se encuentren protegidas contra accesos no autorizados y manipulaciones indebidas. • **Generación y activación**: todas las claves se generan en entornos controlados por la Coordinación de Sistemas TI y se aplican únicamente en sistemas validados y documentados. • **Custodia de criptografías master**: las claves maestras y credenciales críticas se almacenan en el **gestor corporativo Keeper**, el cual funciona como bóveda cifrada de nivel corporativo y garantiza su resguardo cifrado de extremo a extremo, con acceso restringido a personal autorizado, políticas de complejidad y rotación, y registros de auditoría sobre su uso. Keeper elimina la práctica de almacenar llaves en archivos locales o medios inseguros. • **Rotación**: ○ Certificados SSL → renovación anual o anticipada si existe riesgo de compromiso. ○ Tokens y claves de clientes (ejemplo CitiBanamex – SecureZIP) → rotación mensual conforme a lo estipulado en convenios contractuales. ○ Contraseñas críticas de infraestructura → cambio trimestral, gestionado dentro de Keeper. • **Eliminación**: cuando una clave expira o se sustituye, se elimina del repositorio de Keeper y se genera un registro de dicha acción. En el caso de respaldos físicos u otros medios de almacenamiento donde hayan residido claves o certificados, la eliminación se efectúa mediante **Privacy Eraser**, utilizando algoritmos de sobreescritura (DoD 5220.22-M a 3 pasadas o superiores, según criticidad). Con esta práctica, la organización asegura que las **criptografías master** estén centralizadas en Keeper, bajo cifrado robusto y trazabilidad de uso, mientras que los **medios externos** que lleguen a contener copias de dichas llaves sean eliminados con métodos de borrado seguro conforme a las políticas establecidas en el SGSI.
A 8.24.4	**Uso de criptografía en respaldos y medios removibles** Todos los respaldos críticos se almacenan cifrados: • **NAS corporativo y storage externo**: cifrado habilitado con AES 256 bits. • **Medios removibles autorizados** (USB o discos externos): uso obligatorio de cifrado completo antes de ser habilitados; cualquier excepción debe documentarse en **FOR GSI 047 – Excepciones** y en **CIA-Desk**.
A 8.25	**Ciclo de vida de desarrollo seguro**
A 8.25.1	La organización establece que todo desarrollo interno de software, aplicaciones web, sistemas corporativos y cualquier mejora a plataformas existentes debe llevarse a cabo dentro de un ciclo de vida de desarrollo seguro, en el cual se integren controles de seguridad de la información de forma obligatoria en todas sus etapas: desde la fase de levantamiento de requerimientos y diseño, pasando por la programación y pruebas, hasta la implementación, mantenimiento y eventual retiro del sistema.

	Este lineamiento no se limita a una recomendación; constituye una condición técnica mínima para que cualquier desarrollo pueda ser aprobado y liberado. Durante cada fase del ciclo, se aplican controles específicos como la revisión de código fuente con criterios de OWASP, la definición de arquitecturas que contemplen segmentación de redes en VLAN y autenticación centralizada en Active Directory, el uso de certificados SSL para garantizar comunicaciones cifradas, así como la integración de pruebas de seguridad estáticas y dinámicas antes de pasar a ambientes productivos.
A 8.25.2	**Fases del ciclo de vida de desarrollo seguro** **1. Análisis de requerimientos** • Antes de iniciar cualquier desarrollo, se documentan los requerimientos funcionales y no funcionales en el **FOR GSI 002 – Hoja de vida e implementación**, incluyendo los requisitos de seguridad. • Se realiza un **análisis de riesgos** sobre el impacto del proyecto en la confidencialidad, integridad y disponibilidad de la información, conforme al **PRO CAL 009 – Tratamiento de riesgos y oportunidades del SGSI**. **2. Diseño y arquitectura** • El área de Desarrollo, junto con la Coordinación de Sistemas TI, define la arquitectura de la solución considerando: segmentación en VLAN, autenticación AD/Fortinet, uso de certificados SSL, y aplicación de criptografía en datos sensibles. • El diseño debe incluir controles de **segregación de funciones**, registro de auditoría y mecanismos de validación de entrada para prevenir ataques de inyección. **3. Programación** • El código se desarrolla bajo las guías establecidas en **PRO GSI 046 – Desarrollo Seguro**, aplicando buenas prácticas OWASP (Open Web Application Security Project). • Los repositorios de código cuentan con control de versiones y acceso restringido a desarrolladores autorizados, gestionados en GLPI y registrados en CIA-Desk. • Está prohibido el uso de librerías externas no validadas. **4. Pruebas** • Todo desarrollo pasa por pruebas unitarias, integrales y de seguridad antes de pasar a producción. • Se realizan **escaneos de vulnerabilidades** con herramientas de análisis de código y pruebas de pentesting interno. • Los resultados se documentan en **LIS GSI 012 – Bitácora de pruebas** y se registran como ticket en CIA-Desk. • No se libera a producción ningún sistema sin evidencias de pruebas exitosas y validación de la Coordinación de Sistemas TI. **5. Implementación y despliegue** • La liberación en ambientes productivos debe estar autorizada por Dirección General o Gerencia Administrativa y registrada en el **FOR CAL 011 – Plan de cambios y mejoras**. • Todo despliegue debe realizarse siguiendo procedimientos de control de cambios y asegurando respaldo completo previo (PRO GSI 032 – Respaldos). **6. Mantenimiento y soporte** • Los desarrollos en producción cuentan con mantenimiento correctivo y evolutivo documentado en CIA-Desk. • Cualquier cambio o parche debe pasar nuevamente por pruebas de seguridad antes de ser aplicado. • Las vulnerabilidades detectadas en operación se corrigen de forma prioritaria y se integran en los planes de acción de mejora.

A 8.25.3	**Seguridad de ambientes de desarrollo y pruebas** Los ambientes de desarrollo, pruebas y producción se encuentran **separados en VLAN distintas**, lo que impide la manipulación de datos reales en ambientes de prueba. • Los desarrolladores no cuentan con accesos administrativos en ambientes productivos. • Los datos utilizados en ambientes de prueba deben ser anonimizados o ficticios, prohibiéndose el uso de información sensible de clientes.
A 8.30	**Seguridad en endpoints y configuración segura de equipos**

A 8.30.1	**Línea base de configuración segura**
	Todos los **endpoints corporativos** (PCs de escritorio, laptops, dispositivos móviles y equipos periféricos autorizados) deben configurarse bajo una **línea base de seguridad aprobada** por la Coordinación de Sistemas TI y validada en auditorías internas.
	Esta línea base incluye, como mínimo:
	• **Cifrado de disco completo con BitLocker** en laptops y portátiles, activado al momento de la entrega.
	• **Agente SentinelOne XDR** instalado y en funcionamiento permanente, con reportes centralizados.
	• **Certificado SSL corporativo** en cada endpoint, lo que garantiza autenticidad en la conexión con Fortinet.
	• **Políticas GPO aplicadas desde AD**, que definen:
	  ○ Bloqueo automático de sesión por inactividad (2 minutos en áreas críticas, 5 minutos en áreas no críticas).
	  ○ Restricción de puertos USB y dispositivos removibles.
	  ○ Bloqueo de instalación de software no autorizado.
	  ○ Definición de configuraciones de firewall local en estaciones de trabajo.
	• **Políticas de contraseñas** forzadas por AD: mínimo 12 caracteres, caducidad de 90 días, complejidad activada y bloqueo tras 3 intentos fallidos.
	• **VPN Printunl** instalado y funcionando para garantizar una conexión segura entre el endpoint y los servidores.

A 8.30.2	**Gestión de inventario y asignación** Cada endpoint se encuentra registrado en **GLPI**, con información de usuario asignado, número de serie, modelo, características técnicas, fecha de alta y estatus operativo. La entrega al usuario se documenta en la **Carta Responsiva FOR GSI 031**, donde este asume custodia del equipo y acepta las políticas de seguridad establecidas. Cuando un equipo se reasigna o se da de baja, debe pasar por un proceso de **formateo seguro, reinstalación de la línea base y actualización en GLPI**, generando ticket en **CIA-Desk** como evidencia del proceso.
A 8.30.3	**Endurecimiento de sistemas operativos y software** Todos los sistemas operativos de endpoints son configurados siguiendo guías de hardening documentadas en **PRO GSI 039 – Operativo para las TIC**. Estas guías incluyen: • Deshabilitar servicios innecesarios. • Aplicación de parches de seguridad en periodos establecidos. • Configuración de políticas de red y firewall local. • Remoción de aplicaciones preinstaladas que no sean requeridas.

	• Validación de integridad del sistema antes de entrega al usuario. El cumplimiento de estas medidas se revisa trimestralmente y los hallazgos se documentan en **FOR SIS 003 – Monitoreo de Seguridad de Informática**.
A 8.30.4	**Mantenimiento preventivo y correctivo** Los endpoints están sujetos a: • **Mantenimiento preventivo semestral**, calendarizado en GLPI y documentado en **FOR SIS 001 – Conformidad de mantenimiento preventivo**. Incluye limpieza física, pruebas de hardware, validación de cifrado BitLocker y agente SentinelOne, así como verificación de certificados SSL. • **Mantenimiento correctivo**, solicitado por usuarios vía **CIA-Desk**, atendido por la Coordinación de Sistemas TI. Al cierre del ticket, se documenta la reinstalación de la línea base de seguridad si hubo reemplazo de hardware o reinstalación de SO.
A 8.34	**Autenticación y gestión de contraseñas**
A 8.34.1	**Políticas de contraseñas en Active Directory** La organización gestiona la autenticación de usuarios principalmente a través de **Active Directory (AD)**. Las políticas aplicadas mediante **GPO** establecen que: • La longitud mínima es de **12 caracteres**. • Se requiere combinación de letras mayúsculas, minúsculas, números y caracteres especiales. • Las contraseñas expiran cada **90 días** y no pueden repetirse durante al menos 5 ciclos anteriores. • Después de **3 intentos fallidos**, la cuenta queda bloqueada por 15 minutos. • Todo cambio de contraseña queda registrado en los logs de AD. Estas políticas son obligatorias para todos los usuarios, salvo las excepciones documentadas en **FOR GSI 047 – Excepciones** o **FOR SIS 009 – Excepciones por puesto**, siempre autorizadas por Dirección General o Gerencia Administrativa.
A 8.34.2	**Autenticación en Fortinet y VPN Printunl** El acceso a la red corporativa y a recursos críticos está protegido por mecanismos de autenticación integrados en Fortinet y VPN Printunl: • **Portal cautivo Fortinet**: todos los usuarios deben autenticarse con credenciales personales antes de acceder a su VLAN correspondiente. La autenticación está vinculada al AD, reforzada con certificados SSL en endpoints. • **VPN Printunl**: el acceso remoto requiere usuario y contraseña del AD, con logs detallados de conexión (usuario, IP, fecha, hora, VLAN asignada). Las cuentas de VPN se revocan automáticamente cuando un colaborador causa baja, conforme a **MAP REH 001** y **MAP SIS 001**.
A 8.34.3	**Gestión de cuentas privilegiadas y de servicio** • Todas las cuentas privilegiadas (administradores de AD, Fortinet, bases de datos, SentinelOne) son de uso individual, nunca compartidas. • Los accesos privilegiados se registran y auditan conforme a **PRO GSI 016 – Control de accesos**. • Las cuentas de servicio (para tareas automáticas o integraciones) deben utilizar contraseñas robustas generadas aleatoriamente y ser almacenadas en repositorios seguros. Estas cuentas se revisan de manera trimestral, documentándose en **FOR SIS 010 – Recertificación de accesos**.

A 8.34.4	**Ciclo de vida de contraseñas** • **Altas de usuarios**: RH notifica en CIA-Desk y Sistemas crea la cuenta inicial en AD, con contraseña temporal que debe cambiarse en el primer inicio de sesión. • **Modificaciones**: cualquier ampliación de privilegios debe solicitarse en **FOR GSI 032 – Autorización de accesos**, aprobada por Dirección General o Gerencia Administrativa. • **Bajas de usuarios**: dentro de las primeras 24 horas posteriores a la notificación de RH, todas las cuentas se deshabilitan en AD, Fortinet y VPN. Evidencia registrada en CIA-Desk. • **Incidentes por robo o pérdida de equipos** a) En caso de que un colaborador sufra el **robo o pérdida de una laptop o celular corporativo**, la notificación debe hacerse **de inmediato por cualquier medio disponible**. b) Una vez recibida la notificación, el área de Sistemas procede a **revocar todos los accesos vinculados al dispositivo comprometido**, eliminando credenciales en **Active Directory, Fortinet (portal cautivo) y VPN Printunl**, evitando así el riesgo de acceso indebido. c) Hasta que el colaborador reciba un **nuevo equipo inventariado en GLPI y asignado mediante la carta responsiva FOR GSI 031**, no se generan nuevas credenciales. d) El evento queda documentado en **CIA-Desk** por la Coordinación de TI como incidente de seguridad, aunque el reporte original se haya hecho por teléfono, correo u otro canal. • **Revisiones periódicas**: cada trimestre se ejecuta una recertificación de accesos en **FOR SIS 010**, validando vigencia y necesidad de cada cuenta.