TIPO DE DOCUMENTO: Procedimiento

CÓDIGO: PRO SIS 001

1. 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: 23

Fecha de emisión: Julio 2006

Revisó: DGE

Aprobó: DGE

ÍNDICE:

CONTENIDO **PÁGINA**

2. OBJETIVO

Administrar los servidores, redes, terminales, telefonía, software y hardware de la Empresa.

3. ALCANCE

Al Área se Sistemas y las áreas relacionadas

4. HISTORIAL DE CAMBIOS

Versión	Descripción de cambios	Autor(es)	Fecha de cambio
1	Versión inicial.	MBS	Julio 2006
2	Adecuaciones de todos los puntos de acuerdo al anexo 52 (CNBV) "Lineamientos mínimos de operación y seguridad para la contratación de servicios de apoyo tecnológico". Así como tres nuevos registros de calidad REG APO 012 (Carpeta de sistemas CIASC), REG APO 013 (Carpeta de control de sistemas) REG APO 014 (Carpeta de inventario de sistemas).	LV / RRR	Julio 2008
3	Se agregaron políticas de seguridad informática y se adecuó el 1.4 indicando el uso del FOR OPE 072.	CD	Julio 2009
4	Integración de nuevos apartados (FLUJOGRAMA, ENFOQUE A PROCESOS, INDICADORES, POLITICAS, REGLAS). Se anexo la política de seguridad informática y el mantenimiento programado a las estaciones de trabajo, así como un nuevo registro FOR OPE 072 (mantenimiento de equipos).	RRR	Septiembre 2009
5	Adecuaciones Generales.	RML	Abril 2010
6	Precisiones en diferentes apartados.	RML	Julio 2010
7	Adecuaciones para el control de incidencias (FOR APO 005), verificación de equipos en cuanto a seguridad de la información (check List FOR APO 004). Se generan los puntos 6, 7, 8 y 9.	RML	Julio 2011

8	Adecuación del 9.2.	RML	Agosto 2011
9	Adecuación del 8.1 para la generación de actividades para llevar a cabo monitoreo y pruebas de penetración en la red, así como acciones en caso de que se diera el evento.	RML	Septiembre 2011
10	Se actualiza portada, cambia logo con mejor definición, se elimina Coordinador Administrativa, Cambia por Coordinador de Calidad.	SVO	Febrero 2012
11	Adecuación general en los responsables ya que se agrega el puesto de auxiliar de sistemas.	RML	Julio 2012
12	Adecuación por cambio de puesto responsable de autorizar los documentos del Sistema de Gestión de la Calidad (Gerente General en vez de Director General.)	MBS	Enero 2013
13	Se hace mención del programa de mantenimiento preventivo FOR APO 011, Bitácora de respaldos FOR OPE 072, en los anexos se actualizó a la versión actual del convenio de confidencialidad. En el apartado XIV. Registros de calidad, se anexan el REG OPE 003 Servidor, REG OPE 006 Asignación de Claves y el REG APO 012 Carpeta de sistemas CIASC.	RML / CHM	Octubre 2014
14	Actualización del flujograma y enfoque a procesos de los apartados V y VI. Del apartado XI descripciones de actividades, se integra la parte del mantenimiento preventivo y correctivo además de adecuaciones generales. Se agregan los conceptos de requerimiento y RAID en el apartado XII. Abreviaciones y definiciones.	RML / CHM	Febrero 2015
15	Adecuaciones generales al apartado descripciones de actividades, alineándolo al SGSI e incluyendo los apartados de administración de usuarios y contraseñas, seguridad de la información, monitoreos e incidentes.	RML / CHM	Diciembre 2015
16	Adecuaciones por recodificación de los documentos del SGC, se sustituye el enfoque a procesos por el diagrama de tortuga y se actualiza el flujograma.	CHM	Febrero 2016
17	Modificación del punto 4 respecto a la autorización en algún cambio o instalación de aplicaciones y/o privilegios de los usuarios.	LBR	Junio 2016
18	Se modifica el punto 7.2.1, agregando el formato de Check List de revisión de seguridad de instalaciones FOR SIS 008.	LBR	Mayo 2017
19	Se hace más específico el uso de reglas de correo en el apartado 8	LBR	Febrero 2019
20	Se actualizan abreviaturas, generalidades del proceso, se modifican Check List de revisión de seguridad en las instalaciones, se modifica Check List de revisión de instalaciones y se sustituye la herramienta freshdesk por CIA-Desk,. Se integro el punto 2.4 para poder estipular el envió seguro de activos a sucursales de la empresa.	RFML	Octubre 2020
21	Se actualizo el punto 3 seguridad de la información (3.5), también se realiza actualización en el punto 4 antes monitoreos se cambia nombre a monitoreos y recertificación de accesos, complementando actualización en el 4.1 y se agrega el punto 8 segregación de funciones estructurado del punto 9.1 al 9.10.	CST	Enero 2022
22	Se actualizó el punto 4.1 a fin de declarar que se debe realizar cuando se llegue a los límites de capacidades tecnológicas	CST	Octubre 2024
23	Actualización del documento para reforzar la información y alinearla a los requisitos de la norma ISO/IEC 27001:2022.	SSA	Septiembre 2025

5. REFERENCIAS

- FOR GSI 004 Bitácora de acceso al site
- FOR GSI 025 Matriz de roles por activos de información críticos
- FOR SIS 003 Monitoreo de seguridad de informática
- LIS GSI 004 Catálogo de software y aplicaciones permitidos en CIA
- PRO GSI 020 Gestión de incidentes
- FOR SIS 001 Conformidad de mantenimiento preventivo
- FOR SIS 002 Mantenimiento preventivo foráneo
- FOR SIS 010 Recertificación de accesos

6. ABREVIACIONES Y DEFINICIONES

Abreviaciones:

DGE	Director General / Director General Adjunto
GAD	Gerente Administrativo
CST	Coordinador de Sistemas TI
CSG	Coordinador de Sistemas de Gestión
UFI	Usuario Final
N/A	No Aplica
SGC	Sistema de Gestión de Calidad
SGSI	Sistema de Gestión de Seguridad de la Información

Definiciones:

Requerimiento: Condición o capacidad que un usuario necesita para poder resolver un problema o lograr un objetivo.

RAID: Conjunto de discos duros trabajando como uno solo para proporcionar respaldos en espejo y/o alta velocidad de acceso.

Información crítica: Toda aquella información proporcionada por nuestros clientes que incluyan datos personales de terceras personas (acreditados, titulares de cuenta, personas físicas y morales a investigar, etc.).

7. DESARROLLO DE ACTIVIDADES

No.	Descripción	Responsable(s)
1	Generalidades	
1.1	El área de Sistemas mantiene un esquema de **supervisión continua de infraestructura y aplicaciones** que soportan los procesos críticos de la organización. Este monitoreo se realiza mediante plataformas especializadas, garantizando la detección oportuna de desviaciones, la gestión de incidentes en tiempo real y la trazabilidad de todas las acciones correctivas. Para este fin, se utilizan las siguientes herramientas: • **Fortinet FortiGate (80F/100E):** administración centralizada de seguridad perimetral, con funciones activas de prevención de intrusiones (IPS/IDS), filtrado de contenido, control de aplicaciones, inspección SSL y bloqueo de tráfico malicioso. Los registros generados son analizados periódicamente para identificar intentos de intrusión, ataques de denegación de servicio (DDoS) o anomalías en el tráfico de red. • **SentinelOne XDR:** visibilidad avanzada en endpoints y servidores, con capacidad de respuesta automática ante amenazas, aislamiento de dispositivos comprometidos y análisis forense de eventos. • **GLPI:** plataforma de gestión integral de activos y configuración (CMDB), utilizada para inventarios de hardware, software, licencias y usuarios. Sustituye los formatos LIS-GSI-023 y LIS-GSI-024, integrando conciliaciones automáticas y controles de vigencia. • **CIA-Desk:** sistema corporativo de gestión de tickets, utilizado para registrar incidencias, cambios, solicitudes y mantenimientos, asegurando trazabilidad y evidencia documental de todas las intervenciones. La organización opera tres **centros de datos corporativos** ubicados en: 1. **Nezahualcóyotl:** Av. Lago de Xochimilco No. 283, Col. Ampliación Vicente Villada, Nezahualcóyotl, Estado de México, C.P. 57760. 2. **Colonia del Valle (Insurgentes Sur):** Insurgentes Sur No. 686, Piso 9, Col. Del Valle, Benito Juárez, CDMX, C.P. 03100. 3. **Toluca:** Hermenegildo Galeana No. 204, Despacho 2, Col. Centro, Toluca, Estado de México, C.P. 50000. Cada centro de datos cuenta con medidas de seguridad perimetral basadas en **defensa en profundidad**, con firewalls en alta disponibilidad, segmentación estricta por VLAN y	Coordinador de Sistemas TI / Auxiliar de Sistemas

	perfiles de seguridad diferenciados por área. Las **ventanas operativas de red** se encuentran definidas de la siguiente manera: • Toluca: habilitada de 06:30 a 20:30 horas. • Nezahualcóyotl e Insurgentes Sur: habilitada de 08:30 a 20:30 horas. • La red CIASC – INVITADOS en Toluca, Nezahualcoyotl e Insurgentes solo se encuentra habilitada de 09:30 a 18:30 horas. • Fuera de dichos horarios, todo tráfico se bloquea automáticamente en cualquier sentido. El acceso a la red se gestiona bajo un modelo de **autenticación múltiple y control de dispositivos**: • **Certificado SSL corporativo Fortinet:** su instalación en todos los endpoints corporativos es **obligatoria e indispensable** para permitir la conexión a cualquier VLAN interna. Si el certificado no está presente, el dispositivo no puede establecer conectividad hacia la red corporativa. Los únicos equipos exentos de este requisito son los de terceros (proveedores, clientes, auditores u otras visitas autorizadas), los cuales se conectan exclusivamente a la **VLAN CIASC-INVITADOS**. Esta red se encuentra completamente segregada, solo permite salida a Internet y carece de rutas hacia la infraestructura interna. • **Portal cautivo Fortinet:** todos los accesos de invitados o externos se validan mediante **credenciales locales administradas directamente en Fortinet**. No existe integración con Active Directory, lo que centraliza en el firewall la gestión de cuentas temporales y asegura la trazabilidad de cada conexión. • **Red inalámbrica mediante Access Points Huawei:** configurados con múltiples SSID segmentados por área, cada uno vinculado a su VLAN correspondiente. El acceso requiere tanto la clave del SSID como la validación en el portal cautivo. • **VPN corporativa Printunl:** como última capa de seguridad, el acceso a sistemas críticos (ERP CIASC, SICOB, FileMaker, Aspel, Intranet del SGC, entre otros) exige la conexión obligatoria a través de túneles cifrados en Printunl, lo cual valida la postura del endpoint (BitLocker activo, SentinelOne en ejecución y certificado SSL válido).	
1.2	La organización ha establecido un esquema de **resiliencia eléctrica** que garantiza la protección de los equipos y la integridad de la información en caso de fallas en el suministro. **Respaldo energético en estaciones de trabajo y equipos críticos**	Coordinador de Sistemas TI / Auxiliar de Sistemas

Todos los dispositivos operativos de la organización, incluyendo **estaciones de trabajo, servidores, switches, firewalls Fortinet, routers y enlaces de comunicación**, se encuentran protegidos mediante **No-Breaks con autonomía aproximada de 15 minutos**.

Este tiempo de respaldo está dimensionado para que los usuarios puedan **guardar la información en curso y realizar apagados controlados de sus equipos**, mientras que el área de Sistemas ejecuta el **apagado seguro de servidores y activos de red críticos**.

Con ello se protege la integridad de los datos, se previenen pérdidas y se asegura una transición ordenada hasta el restablecimiento del suministro o la aplicación de protocolos de contingencia.

Procedimiento de actuación ante fallas eléctricas

1. **Diagnóstico inmediato:** verificación del alcance de la falla (parcial o general), revisión de tableros eléctricos, No-Breaks y pastillas térmicas.
2. **Acciones iniciales:** si la interrupción supera los umbrales definidos, se procede al apagado ordenado de servidores y priorización de aplicaciones críticas.
3. **Registro y gestión:** en el caso de que la afectación sea por parte del proveedor de energia electrica CFE se procede a realizar el reporte via telefonica al número 071 y tambien se realiza levantamiento de ticket en CIA-Desk, con evidencia de tableros, logs de No-Breaks y tiempos de afectación.
4. **Comunicación interna:** notificación a la Dirección General y Gerencia Administrativa del estatus de la contingencia y las acciones ejecutadas.
5. **Restablecimiento progresivo:** encendido controlado de servidores, validación de bases de datos, verificación de servicios críticos y notificación de reanudación a las áreas operativas.

Mantenimiento preventivo de instalaciones

El área de Sistemas ejecuta recorridos periódicos utilizando los formatos **FOR-SIS-006 (Check list de instalaciones)** y **FOR-SIS-008 (Check list de seguridad)**, verificando cableado eléctrico, equipos contraincendios, climatización y condiciones estructurales.

Las incidencias detectadas son registradas en **CIA-Desk** y gestionadas por el área de Compras conforme al **MAP-COM-001 (Proceso de Compras)**. Para anomalías menores (fusibles, luminarias, cableado estructurado), el personal de Sistemas puede realizar correcciones directas, siempre con ticket en CIA – Desk autorizado y documentado.

En sucursales foráneas, las anomalías se reportan vía CIA-Desk o correo institucional, y la atención se coordina con proveedores locales aprobados. Todo el proceso es

	supervisado por la Gerencia Administrativa y documentado como evidencia de cumplimiento.	
2	Software y hardware	
2.1	**Gestión de software autorizado** El área de Sistemas es responsable de **descargar, instalar, actualizar y retirar** el software necesario para la operación. Solo se permiten aplicaciones incluidas en el **LIS GSI 004 – Catálogo de software y aplicaciones permitidos en CIA**. La administración integral del ciclo de vida de software (altas, bajas, actualizaciones, licencias y evidencias) se gestiona en **GLPI**, quedando este sistema como **fuente de verdad** para inventarios, asignaciones y cumplimiento de licenciamiento. **Lineamientos operativos.** • Toda instalación o actualización se ejecuta sobre **línea base corporativa** (certificado SSL Fortinet, SentinelOne, cliente VPN Printunl, políticas de endurecimiento y GPO aplicables). • Se valida **compatibilidad y soporte del fabricante** antes de despliegues, de acuerdo al **procedimiento operativo para las TICS PRO GSI 039**. • Queda **prohibida** la instalación de software no listado en **LIS GSI 004 – Catálogo de software y aplicaciones permitidos en CIA** o sin evidencia de licencia vigente.	Coordinador de Sistemas TI / Auxiliar de Sistemas
2.2	**Gestión de activos y licenciamiento** Todos los activos tecnológicos de la organización se encuentran **identificados, clasificados y asignados** a un responsable. La administración del inventario se realiza exclusivamente en **GLPI**, que sustituye los formatos históricos **LIS GSI 023** (Inventario y clasificación de activos) y **LIS GSI 024** (Inventario y clasificación de software). Controles aplicables • **Identificación unívoca** del activo (etiqueta/QR), modelo, serie, especificaciones y ubicación. • **Asignación formal** al usuario responsable, con evidencia de entrega mediante **FOR GSI 031 – Carta responsiva** y registro en GLPI. • **Cumplimiento de licencias**: toda licencia se vincula en GLPI al activo y al usuario, con fechas de vigencia y comprobantes de compra/contrato.	Coordinador de Sistemas TI / Auxiliar de Sistemas

	• **Conciliaciones periódicas** entre inventario físico y GLPI y reportes de brechas para corrección, de acuerdo al **PRO GSI 015 - Gestión de Activos, Clasificación y Control de la Información.**	
2.3	**Solicitud y autorización de software/hardware** Las solicitudes de **software, hardware o actualizaciones adicionales** al estándar corporativo deberán gestionarse de forma documentada a través del **portal CIA-Desk** por el responsable del área solicitante (supervisor o gerente). El ticket deberá incluir una descripción clara de la necesidad, el propósito de uso y, en el caso de software, la versión y modalidad de licenciamiento requerida. El flujo contempla: 1. **Revisión técnica por el área de Sistemas** ○ Validación de compatibilidad con la infraestructura corporativa y con las herramientas de seguridad instaladas (Fortinet, SentinelOne, VPN Printunl). ○ Revisión de disponibilidad en inventario o de licencias vigentes. ○ Prueba técnica previa en caso de tratarse de aplicaciones críticas o de impacto directo en la operación. 2. **Autorización formal** ○ Toda solicitud requiere validación de la **Gerencia Administrativa** y/o **Dirección General**. ○ La autorización o rechazo se documenta en el ticket de CIA-Desk y, si aplica, se confirma mediante correo institucional. 3. **Implementación y registro** ○ Una vez autorizada, la instalación o entrega se realiza por el área de Sistemas siguiendo la línea base corporativa de seguridad. ○ El registro final se gestiona en **GLPI**, vinculando activo o software a su responsable, con detalle de licencias y evidencias de instalación. **Nota:** No se instalará ni asignará ningún software o hardware sin la autorización correspondiente. Cualquier excepción deberá estar documentada en CIA-Desk para garantizar trazabilidad.	Coordinador de Sistemas TI / Auxiliar de Sistemas
2.4	**Asignación, traslado y puesta en producción de activos** El departamento de Sistemas provee a los colaboradores los activos tecnológicos requeridos (PC, laptop, monitor, periféricos, impresoras, dispositivos móviles, etc.), registrando cada entrega en **GLPI** y vinculando la **FOR GSI 031 – Carta responsiva** firmada.	

	Traslado de activos a sucursales u oficinas remotas Para envíos fuera de las sedes de **Nezahualcóyotl**, **Insurgentes y Toluca**, se siguen los controles siguientes: **Preparación del equipo (higiene de datos y línea base)** • Entrega **sin información de la empresa**: sistema operativo, controladores, suite ofimática autorizada, agente SentinelOne, certificado SSL Fortinet y cliente VPN Printunl instalados; sin credenciales persistentes. • **Contraseña local segura** según política vigente (complejidad/rotación). • Etiqueta de activo y **registro previo en GLPI** con estado "En tránsito". **Embalaje y cadena de custodia** • Embalaje reforzado: **unicel, goma, cartón rígido y hule playo**; protección de esquinas. • Fotografías de contenido y empaque; **número de guía** (FedEx o equivalente) y **opción con seguro** cuando aplique. • Ticket en CIA-Desk con evidencia del envío (fotos, guía, destino y contacto receptor). **Recepción y activación en destino** • El responsable local **notifica recepción** vía CIA-Desk y adjunta evidencia fotográfica (empaque/activo sin daño). • Sistemas actualiza estado del activo en **GLPI** a "Asignado", valida conectividad (portal cautivo Fortinet), **instala credenciales corporativas** y habilita accesos (correo, unidades, aplicaciones permitidas). • Se documenta en el ticket la **puesta en producción** y se adjunta la **FOR GSI 031** firmada por el receptor. Cualquier incidencia en traslado (daños, faltantes, anomalías) se reporta de inmediato en **CIA-Desk** y se escala a Compras/Proveedor de paquetería para su resolución, manteniendo toda la trazabilidad en el ticket correspondiente.	
3	Seguridad de la información	
3.1	**Contraseñas y políticas de bloqueo** Todos los equipos de cómputo de la organización operan bajo **políticas de contraseñas seguras**. La configuración de Active Directory fuerza la **renovación cada 90 días**, aplicando criterios de complejidad definidos en el procedimiento de **Control de Accesos PRO GSI 016**.	Personal CIA

	Nota: En caso de que un usuario introduzca de manera incorrecta su contraseña en tres intentos consecutivos, la cuenta se bloquea automáticamente durante 15 minutos. Si se requiere reactivación inmediata, el colaborador deberá **notificar al área de Sistemas por un canal alterno** (extensión telefónica, correo institucional desde otra cuenta o a través de su jefe inmediato). Una vez restablecido el acceso, el usuario deberá **registrar la solicitud en CIA-Desk**, de forma que quede evidencia y trazabilidad del incidente para fines de control y auditoría.	
3.2	**Restricciones por rol y funciones** Los equipos de cómputo cuentan con **privilegios de acceso diferenciados**, configurados de acuerdo con el área y puesto del usuario. Estas restricciones se gestionan conforme a la **FOR GSI 025 – Matriz de roles por activos de información críticos**, la cual asegura el cumplimiento del principio de **privilegio mínimo** y la correcta segregación de funciones.	Coordinador de Sistemas TI / Auxiliar de Sistemas
3.3	**Bloqueo por inactividad** Con el fin de proteger la información en uso y reducir la exposición a accesos no autorizados, todos los equipos de cómputo corporativos están configurados para **bloquear la sesión automáticamente tras 2 minutos de inactividad**. Este control se implementa y gestiona de manera centralizada a través de **Directivas de Grupo (GPO) en Active Directory**, lo que garantiza uniformidad en toda la organización, evita configuraciones manuales no autorizadas y permite evidenciar su cumplimiento en auditorías técnicas. De esta forma, se refuerza la **confidencialidad y trazabilidad de la información procesada**, asegurando que ningún equipo quede accesible sin la autenticación del usuario asignado.	Coordinador de Sistemas TI / Auxiliar de Sistemas
3.4	**Acceso al SITE** El acceso físico al **SITE y a los centros de datos** está restringido exclusivamente al personal autorizado del área de Sistemas. En caso de que proveedores externos requieran realizar mantenimiento a activos que no sean propiedad de la empresa, la entrada solo se permitirá cumpliendo estrictamente con lo establecido en: • **POL-GSI-001 – Políticas generales de seguridad de la información.** • **PRO-GSI-016 – Control de Accesos.** Esto incluye el registro en el portal de visitantes, autorización formal previa y acompañamiento del personal interno durante toda la estancia en el área sensible.	Coordinador de Sistemas TI / Auxiliar de Sistemas

3.5	**Ambientes de ejecución y seguridad perimetral** La empresa mantiene un **entorno de ejecución segregado**, en el que cada aplicación, servicio e información se aloja en servidores independientes, mitigando riesgos de propagación de incidentes y garantizando la disponibilidad de los procesos. Adicionalmente, se cuenta con un **servidor dedicado a SentinelOne XDR**, desde el cual se administran y aplican directivas de seguridad a todos los usuarios y equipos dentro de la red corporativa, centralizando la protección contra malware, intrusiones y comportamientos anómalos. **Configuraciones mínimas de SentinelOne aplicadas en la organización** • Protección en tiempo real (Real-Time Protection) • Análisis estático y dinámico • Rollback/Restauración automática • Prevención de exploits • Protección contra scripts maliciosos y macros • Políticas centralizadas • Alertas y reportes centralizados **Nota - Correos electrónicos y seguridad asociada** Los correos electrónicos corporativos se encuentran alojados en la plataforma **Office 365**, bajo esquema de **suscripción mensual** administrada y facturada a través del proveedor **Compuevolución**, quien gestiona las licencias correspondientes a todas las cuentas activas de la organización. Como medidas de protección específicas para el correo electrónico, se utilizan las soluciones nativas de Microsoft: • **Exchange Online Protection (EOP):** encargado de filtrar spam, malware y ataques de phishing en el flujo de correo entrante y saliente. • **Defender for Office 365:** protección avanzada contra amenazas, incluyendo análisis de enlaces, adjuntos maliciosos, ataques de tipo spoofing y Business Email Compromise (BEC).	Coordinador de Sistemas TI / Auxiliar de Sistemas
4	Monitoreos	
4.1	**Monitoreo de seguridad informática** El área de Sistemas realiza de manera **trimestral** el **FOR-SIS-003 – Monitoreo de seguridad informática** en todos los equipos de cómputo de la organización (escritorios y laptops). Este control permite validar que los dispositivos se encuentren configurados y	Coordinador de Sistemas TI / Auxiliar de Sistemas

	operando bajo los parámetros corporativos establecidos, asegurando uniformidad y cumplimiento con las políticas de seguridad. Durante el monitoreo se revisa, entre otros aspectos: 1. Usuario asignado. 2. Área de adscripción. 3. Dirección IP. 4. Sistema Operativo. 5. Versión de Microsoft Office. 6. Estado del No-Break asociado. 7. Funcionamiento del agente SentinelOne XDR. 8. Restricción de acceso a unidad C:. 9. Control de uso de unidades externas. 10. Bloqueo de páginas restringidas. 11. Configuración de protector de pantalla. 12. Aplicación del fondo de política corporativa. 13. Validación de usuarios actualizados. 14. Recordatorio de usuario web.	
4.2	**Verificación de límites de umbrales tecnológicos** Como parte del monitoreo, el área de Sistemas supervisa el **uso de recursos tecnológicos críticos**. En caso de que la capacidad de almacenamiento (HDD/SSD) o memoria RAM alcance o supere el **85 % de utilización**, se deben ejecutar las siguientes acciones: • Generar un **ticket en CIA-Desk**, documentando la situación, evidencias técnicas y análisis de impacto. • Escalar la solicitud a la Gerencia Administrativa y/o Dirección General para autorizar la **ampliación de capacidades tecnológicas** o la adquisición de recursos adicionales. Los recursos sujetos a esta verificación son: 1. Disco duro. 2. Memoria RAM. 3. Procesador. En el caso de las impresoras corporativas, el proveedor asignado mantiene un sistema de **monitoreo remoto de consumibles**. Cuando se detecta un nivel bajo, se activa el envío automático de insumos, evitando interrupciones en el servicio y garantizando la continuidad operativa.	
4.3	**Monitoreo de infraestructura y seguridad física**	Coordinador de Sistemas TI / Auxiliar de Sistemas

	De manera **trimestral**, el área de Sistemas aplica el **FOR-SIS-006 – Check List de revisión de instalaciones** para detectar anomalías en la infraestructura. Esta verificación incluye, entre otros: • Extintores de las instalaciones. • Correcto llenado de accesos y bitácoras (FOR-GSI-033 – Control de acceso a visitantes y FOR-GSI-004 – Bitácora de acceso a áreas seguras). • Funcionamiento de detectores de humo. • Accesos libres de obstrucciones. • Señalización de rutas de evacuación. Adicionalmente, con periodicidad **mensual**, se realiza la **revisión de seguridad del edificio** mediante el **FOR-SIS-008 – Check List de revisión de seguridad de instalaciones**, que incluye: • Monitoreo y prueba de alarmas instaladas. • Revisión de medidas de seguridad física. • Supervisión de cámaras de videovigilancia instaladas. • Verificación de sensores de movimiento. • Revisión del estado de puertas y ventanas.	
4.4	**Sistema de videovigilancia** Con el objetivo de salvaguardar la seguridad de la información, las instalaciones y el personal, la organización mantiene un **sistema de videovigilancia activo** en las tres sedes principales: 1. **Nezahualcóyotl:** Av. Lago de Xochimilco No. 283, Col. Ampliación Vicente Villada, Nezahualcóyotl, Estado de México, C.P. 57760. 2. **Colonia del Valle (Insurgentes Sur):** Insurgentes Sur No. 686, Piso 9, Col. Del Valle, Benito Juárez, CDMX, C.P. 03100. 3. **Toluca:** Hermenegildo Galeana No. 204, Despacho 2, Col. Centro, Toluca, Estado de México, C.P. 50000. El **control total del sistema** corresponde a la Dirección General, asegurando la confidencialidad y resguardo de las grabaciones. Cuando un encargado o gerente de área requiera consultar una grabación, la solicitud deberá ser enviada a la Dirección General y documentada en **CIA-Desk** y/o correo institucional, indicando fecha, hora y motivo de la consulta. El sistema cuenta con una capacidad de almacenamiento mínima de **5,000 GB**, garantizando la conservación de grabaciones durante **150 días naturales**. La configuración está establecida en modo **"circular"**, lo que implica la eliminación automática de los registros más antiguos al llegar al límite de almacenamiento, asegurando siempre un mínimo de 150 días o 3,600 horas de video continuo.	Coordinador de Sistemas TI / Auxiliar de Sistemas
5	Incidentes	

5.1	**Tratamiento de incidentes** Todo incidente relacionado con la seguridad de la información debe gestionarse conforme a lo establecido en el **PRO-GSI-020 – Procedimiento de Gestión de Incidentes**, el cual define las fases de notificación, registro, clasificación, análisis, respuesta, cierre y retroalimentación. Cada evento debe quedar documentado en **CIA-Desk**, con las evidencias técnicas correspondientes (capturas de pantalla, registros de sistema, bitácoras de red o reportes de seguridad), de modo que se asegure la trazabilidad y se disponga de insumos para auditorías internas o externas.	Coordinador de Sistemas TI / Auxiliar de Sistemas
5.2	**Clasificación de incidentes ocasionados por usuarios** Los incidentes derivados de acciones de los usuarios que contravengan las políticas y lineamientos de seguridad de la información se clasifican según el nivel de severidad: • **Alta:** conductas o acciones que comprometen de manera crítica la confidencialidad, integridad o disponibilidad de la información. Ejemplo: compartir credenciales, instalación de software no autorizado o manipulación indebida de datos sensibles. • **Media:** incumplimientos que no generan un impacto inmediato pero que, de mantenerse, pueden escalar a riesgos significativos. Ejemplo: almacenamiento de información en ubicaciones no autorizadas o uso de dispositivos externos sin autorización. • **Baja:** incumplimientos de carácter menor que no afectan directamente la información crítica, pero que vulneran las normas internas de seguridad. Ejemplo: no bloqueo de sesión al dejar desatendido el equipo o el uso de contraseñas que no cumplen con el formato corporativo. Este esquema de clasificación permite priorizar la atención, asignar los recursos adecuados y aplicar las medidas correctivas correspondientes.	Coordinador de Sistemas TI / Auxiliar de Sistemas
5.3	**Medidas correctivas** Las acciones correctivas derivadas de incidentes ocasionados por usuarios están definidas en el **Código de Convivencia** y sus anexos. Dichas acciones incluyen desde medidas preventivas y sesiones de concientización en seguridad de la información, hasta sanciones administrativas de acuerdo con la gravedad y reincidencia del incumplimiento. La gestión de cada caso debe estar debidamente sustentada en evidencias, y las decisiones se toman en coordinación con el área de Recursos Humanos y la Gerencia	Coordinador de Sistemas TI / Auxiliar de Sistemas

	Administrativa, asegurando equidad, proporcionalidad y apego a los lineamientos internos del SGSI.	
6	Mantenimientos Preventivos	
6.1	**Mantenimientos preventivos** El departamento de Sistemas es responsable de ejecutar los **mantenimientos preventivos** a los equipos de cómputo de la organización con el objetivo de mantenerlos en condiciones operativas y garantizar la continuidad de los servicios tecnológicos. Las actividades deben realizarse conforme al **LIS-GSI-010 – Programa Anual de Mantenimiento Preventivo** y documentarse en el formato **FOR-SIS-001 – Conformidad de Mantenimiento Preventivo**, que constituye la evidencia formal de la intervención. Durante cada mantenimiento se realizan, como mínimo, las siguientes acciones: • Limpieza física externa e interna básica de los equipos. • Verificación del estado general del hardware (fuente de poder, ventiladores, periféricos). • Comprobación de funcionamiento de red y conectividad. • Revisión de sistema operativo, instalación de parches y actualizaciones de seguridad. • Validación de funcionamiento de los agentes de seguridad (SentinelOne, VPN Printunl, certificado SSL Fortinet). • Confirmación de que la información del equipo corresponde con lo declarado en **GLPI**. **Nota:** Los equipos de impresión son atendidos por el proveedor asignado, conforme a su calendario de servicio preventivo.	Coordinador de Sistemas TI / Auxiliar de Sistemas
7	Vulnerabilidades	
7.1	**Análisis de vulnerabilidades** El área de sistemas es el responsable de ejecutar cada 6 meses un análisis de vulnerabilidades con el programa Nessus en las oficinas: 1. **Oficina Nezahualcóyotl:** Av. Lago de Xochimilco No. 283, Col. Ampliación Vicente Villada, Municipio Ciudad Nezahualcóyotl, Estado de México, C.P. 57760. 2. **Oficina Colonia del Valle:** Insurgentes Sur No. 686 Piso 9, Col. Del Valle, Delegación Benito Juárez, Ciudad de México, C.P. 03100. 3. **Oficina Toluca:** Hermenegildo Galeana No. 204, Despacho 2, Col. Centro, Municipio Toluca, Estado de México, C.P. 50000.	Coordinador de Sistemas TI

El análisis debe de estar categorizado de acuerdo con la criticidad de cada vulnerabilidad encontrada y debe de analizar sistema operativo, actualizaciones de sistemas operativos, antivirus, firewall, certificados de seguridad, políticas de seguridad.

Información de vulnerabilidades

La organización mantiene un esquema de gestión proactiva de vulnerabilidades, sustentado tanto en proveedores especializados como en fuentes oficiales de ciberseguridad.

Proveedores contratados:

La empresa tiene contratos vigentes con TotalSec y Scitum, quienes proveen servicios de ciberseguridad gestionada, dentro de los cuales se incluyen:

- Notificación temprana de vulnerabilidades que pudieran impactar de forma crítica la operación.
- Aplicación directa de medidas de mitigación en tiempo real ante amenazas confirmadas.
- Emisión de boletines mensuales con un catálogo de vulnerabilidades recientes y recomendaciones técnicas.
- Entrega periódica de revistas de ciberseguridad con tendencias, alertas globales y casos de uso.

Fuentes de inteligencia adicionales:

Aunado a lo anterior, la organización se encuentra suscrita a boletines y notificaciones de diferentes fabricantes y entidades de seguridad, entre los que destacan:

- Fortinet: alertas y boletines de seguridad sobre productos de red y firewalls.
- Palo Alto Networks: actualizaciones sobre nuevas amenazas, exploits y parches.
- Veeam/Backup y otros fabricantes de software, quienes publican boletines relacionados con vulnerabilidades en soluciones de respaldo y recuperación.

Gestión interna:

- El área de Sistemas recibe, analiza y evalúa la información proveniente de estas fuentes, determinando su aplicabilidad en la infraestructura de la organización.
- En caso de identificarse una vulnerabilidad crítica, se abre de inmediato un ticket en CIA-Desk, documentando la alerta y las medidas de mitigación aplicadas.

	• Toda acción derivada de estas notificaciones queda registrada en GLPI como parte del ciclo de gestión de activos y parches.	
7.2	**Gestión y cierre de vulnerabilidades** En caso de tener vulnerabilidades críticas, altas, medias o bajas, estas deberán cerrarse en un tiempo no mayor a 5 días posteriores al análisis, y se deben de registrar en el **FOR GSI 024 Formato de incidentes de SI.** Nota. Las vulnerabilidades "INFO" no serán tratadas, puesto que solo son informes del análisis de la vulnerabilidad.	Coordinador de Sistemas TI
7.3	**Reporte y seguimiento en CIA-Desk** Todos los incidentes relacionados con vulnerabilidades deben ser reportados a través del **portal CIA-Desk**. Una vez registrado, el área de Sistemas analiza cada caso, determina las acciones estratégicas de mitigación y documenta el avance de las actividades hasta su cierre. El uso de CIA-Desk permite asegurar la **trazabilidad, priorización y rendición de cuentas**, además de mantener un historial de incidentes disponible para revisiones internas y auditorías externas.	Coordinador de Sistemas TI
8	Mapeo de redes y equipos	
8.1	**Mapa de activos tecnológicos** El área de Sistemas mantiene actualizado el **MAP-SIS-001 – Mapa de Activos Tecnológicos**, el cual constituye una herramienta de referencia para la **identificación, localización y gestión** de los activos críticos de la organización. Este mapa permite al personal de Sistemas contar con una visión clara de la infraestructura tecnológica y de apoyo instalada en cada sede, facilitando las labores de mantenimiento, control de cambios, atención de incidentes y continuidad operativa. Entre los activos representados se incluyen, de manera enunciativa pero no limitativa: 1. Servidores. 2. Firewalls. 3. Switches. 4. Routers. 5. Equipos de cómputo. 6. Impresoras. 7. Cámaras de videovigilancia. 8. Sensores de humo.	Sistemas

	9. Extintores. 10. Equipos de climatización (mini splits). 11. Señalética de seguridad. 12. Tableros eléctricos. 13. Otros elementos relevantes para la operación y la seguridad de la información. La actualización periódica (cada 6 meses) del MAP-SIS-001 garantiza que cualquier modificación en infraestructura (altas, bajas o reubicaciones) quede reflejada de manera oportuna, manteniendo la coherencia entre los registros en **GLPI** y la infraestructura instalada.	
9	Segregación de Funciones	
9.1	**Generalidades** La segregación de funciones es un principio fundamental del SGSI que busca **evitar conflictos de interés, reducir riesgos de abuso de privilegios y asegurar trazabilidad en la gestión de cambios tecnológicos**. Ningún colaborador puede concentrar simultáneamente las funciones de solicitar, evaluar, autorizar y ejecutar.	DGE / GAD / CST / UFI
9.2	**Solicitud de cambios** • Todo colaborador de la organización, sin importar su nivel jerárquico, puede **levantar solicitudes de cambio, mejora o requerimiento tecnológico** a través de la plataforma **CIA-Desk**, en el tópico "Cambios o peticiones de sistemas". • El usuario solicitante debe describir con claridad el requerimiento, el objetivo del cambio y el área impactada, de modo que el área de Sistemas cuente con información suficiente para iniciar el análisis. • Los usuarios finales **no están facultados para autorizar ni ejecutar** cambios; su responsabilidad se limita a iniciar el proceso de manera formal y mantener comunicación con su coordinador o jefe de área para dar seguimiento. • Este mecanismo asegura que todas las peticiones queden documentadas desde su origen, evitando prácticas informales y proporcionando evidencia para auditorías internas y externas.	DGE / GAD / CST / UFI
9.3	**Evaluación técnica y validación** • El **área de Sistemas** es responsable de recibir la solicitud y realizar la **evaluación técnica inicial**, que incluye impacto en la **confidencialidad, integridad y**	DGE / GAD / CST / UFI

	disponibilidad de la información, compatibilidad con la infraestructura tecnológica y riesgos operativos asociados. • La **Gerencia Administrativa** actúa como punto de control intermedio, revisando solicitudes que impliquen inversión, cambios significativos o impacto directo en la operación. Su función es garantizar imparcialidad antes de que la petición llegue a la Dirección General. • Durante esta fase no se aprueba ni se ejecuta el cambio; únicamente se determina la **viabilidad técnica y operativa**, así como el nivel de riesgo. Cuando la solicitud es viable, el área de Sistemas debe elaborar un **plan preliminar de trabajo** con actividades, responsables y estimación de recursos. • El resultado de esta etapa queda registrado en CIA-Desk, generando evidencia de análisis y reduciendo la posibilidad de cambios improvisados o no evaluados.	
9.4	**Autorización y ejecución** • La **Dirección General** es la única instancia con autoridad para **aprobar o rechazar cambios significativos**, incluyendo adquisiciones de hardware, software o proyectos de desarrollo interno. Esta decisión se toma considerando la evaluación técnica del área de Sistemas y la validación de la Gerencia Administrativa. • Una vez autorizado, el área de Sistemas ejecuta el cambio conforme al plan de trabajo definido, asegurando la aplicación de controles de seguridad, pruebas de validación y registro de evidencias. • Durante la ejecución, los responsables deben mantener informados a los actores relevantes y documentar en CIA-Desk cada acción realizada. Esto asegura que exista un **historial completo y verificable** del ciclo de vida del cambio. • El proceso concluye con el **cierre formal de la solicitud en CIA-Desk**, acompañado de evidencias técnicas y reportes de validación, lo cual garantiza la trazabilidad y facilita las auditorías.	DGE / GAD / CST / UFI