TIPO DE DOCUMENTO: Procedimiento

CÓDIGO: PRO GSI 039

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: 8

Fecha de emisión: Agosto 2015

Revisó: DGE

Aprobó: DGE

INDICE

CONTENIDO **PÁGINA**

II. OBJETIVO

Garantizar el funcionamiento correcto y seguro de las tecnologías de la información y de la comunicación.

III. ALCANCE

Aplica a todas las áreas, procesos y activos de la Organización, involucradas en el Sistema de Gestión de Seguridad de la Información.

IV. HISTORIAL DE CAMBIOS

Versión	Descripción de cambios	Autor(es)	Fecha de cambio
1	Versión inicial.	MBS	Agosto 2015
2	Se establece el procedimiento para los parches de seguridad y actualizaciones en los sistemas y equipos.	LBR	Septiembre 2016
3	Cambio de Formato y adecuaciones generales	LBR	Octubre 2016
4	Adecuación de Políticas para Canales de comunicación	RFML	Mayo 2019
5	En esta versión publicamos la nueva hoja de autorizaciones, así como la actualización del portal de soporte técnico antes freshdesk ahora CIA-Desk, así como la actualización del formato en los puntos 2 y 4.	RFML	Octubre 2020
6	Se realizaron adecuaciones a los puntos 1. Gestión de Cambios, 2.7 Antivirus, 4.6., 4.7., 4.8. y 4.9.	RFML	Julio 2021
7	Se realizaron adecuaciones generales al documento.	RFML	Enero 2022

8	Actualización del documento para reforzar la información y alinearla a los requisitos de la norma ISO/IEC 27001:2022.	SSA	Septiembre 2025

V. REFERENCIAS

- MAN GSI 001 Manual de gestión de seguridad de la información
- POL GSI 001 Políticas generales de seguridad de la información
- PRO GSI 015 Gestión de activos, clasificación y control de información
- PRO GSI 020 Gestión de Incidentes
- PRO GSI 033 Respaldo y eliminación de la información

VI. 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
SGC	Sistema de Gestión de Calidad
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.

VII. DESARROLLO DE ACTIVIDADES

No.	Descripción	Responsable(s)
1	**Gestión de Cambios**	
1.1	**Generalidades** La gestión de cambios tiene como finalidad **controlar de manera formal, documentada y segura cualquier modificación** en sistemas operativos, aplicaciones, bases de datos, infraestructura o componentes de producción. Este procedimiento busca reducir los riesgos de fallas, vulnerabilidades o interrupciones no planificadas, asegurando la continuidad de la operación y el cumplimiento de los lineamientos del SGSI.	Sistemas / Dirección
1.2	**Requisitos para la gestión de cambios** Con el fin de asegurar que todo cambio en infraestructura, aplicaciones o configuraciones tecnológicas se realice de manera planificada, autorizada y trazable, la organización aplica los siguientes lineamientos: **Registro obligatorio en CIA-Desk** • Todo cambio debe ser solicitado y documentado mediante un ticket en CIA-Desk, desde la propuesta inicial hasta el cierre del proceso. • Esto garantiza trazabilidad, control de versiones y evidencia disponible para auditorías internas o externas. • Información mínima de la solicitud **Clasificación y niveles de autorización** • Cambios críticos (con impacto en la confidencialidad, integridad o disponibilidad de la información, o en procesos de negocio clave): deben contar con aprobación explícita de la Dirección General. • Cambios menores (parches rutinarios, actualizaciones sin impacto en procesos críticos): pueden ser validados por el área de Sistemas con visto bueno de la Gerencia Administrativa. • En todos los casos, los responsables deben evaluar el riesgo del cambio conforme a la metodología de gestión de riesgos del SGSI y dejar constancia en CIA-Desk.	Sistemas

	Formalización de autorizaciones • Todas las aprobaciones deben realizarse por el ticket correspondiente en CIA-Desk. • Esto asegura evidencia documental y evita decisiones informales que no puedan ser auditadas.	
1.3	**Implementación y supervisión** • El **área de Sistemas** es responsable de ejecutar o supervisar los cambios que cuenten con la autorización formal correspondiente. • Las implementaciones deben realizarse en **ventanas de mantenimiento previamente programadas**, notificando a los responsables de las áreas impactadas mediante **correo electrónico institucional** con copia al Gerente Administrativo o en su defecto en ventanas de mantenimiento fuera del horario operativo. • Dichas áreas deberán **responder por el mismo medio confirmando su autorización**, antes de iniciar la ejecución del cambio. • Durante la ejecución se debe mantener un **registro detallado de acciones, incidencias y observaciones en una bitácora técnica**, la cual se adjunta al ticket de **CIA-Desk**, garantizando trazabilidad y evidencia documental del proceso.	Sistemas

1.4	**Pruebas y validación**
	• Antes de liberar cualquier cambio a producción, este debe ser sometido a **pruebas funcionales y de seguridad** en el **equipo de pruebas el cual se encuentra completamente aislado de la red de producción**, lo que permite validar el comportamiento del cambio sin riesgo de afectar los entornos operativos.
	• Las pruebas deben verificar, como mínimo:
	  ○ Estabilidad general del sistema.
	  ○ Correcto funcionamiento de servicios y dependencias.
	  ○ No afectación de los controles de seguridad existentes (firewall, antivirus, certificados digitales, políticas de acceso y autenticación).
	• Todos los resultados de las pruebas deben ser **documentados en el ticket de CIA-Desk**.
		Sistemas / Áreas Involucradas

	• Una vez superadas las pruebas en el entorno aislado, el área de Sistemas podrá proceder con la liberación a producción, siempre y cuando se cuente con la autorización del gerente administrativo, la cual se documenta por medio del ticket correspondiente en CIA - Desk. • En caso de fallos durante o después de la implementación, se deberá ejecutar el **plan de reversión previamente definido**, utilizando respaldos completos o puntos de restauración, con el fin de restablecer la operación en el menor tiempo posible.	

1.5	**Comunicación de cambios**
	
	• Una vez concluida la implementación y validados los resultados, el **área de Sistemas** debe **informar formalmente** a los responsables de las áreas impactadas, utilizando **correo institucional** y registrando la comunicación en el **ticket correspondiente en CIA-Desk**.
	
	• La notificación debe contener, como mínimo:
	  ○ **Alcance del cambio**: descripción clara de lo que se modificó y los sistemas involucrados.
	  ○ **Resultados de pruebas**: resumen de las validaciones realizadas en el entorno aislado y en producción.
	  ○ **Acciones requeridas por los usuarios**: instrucciones específicas como reinicios de sesión, instalación de certificados, cambios de contraseñas, validación de accesos o cualquier otra medida aplicable.
	  ○ **Fecha y hora de liberación** del cambio, así como la ventana de mantenimiento en la que se ejecutó.
	
	• En caso de que el cambio implique afectaciones temporales en la operación, la comunicación deberá indicar las **contingencias previstas** y el **procedimiento de reversión** disponible.
	
	• Toda la evidencia de la comunicación (correos enviados, confirmaciones de recepción y tickets en CIA-Desk) debe conservarse como parte del expediente del cambio, asegurando la trazabilidad y el cumplimiento de los lineamientos del SGSI.
		Sistemas

2	**Aplicación de parches de seguridad y actualizaciones de configuración en los sistemas operativos, antivirus y equipos**	
2.1	**Procedimiento de pruebas y despliegue**	Sistemas

	Toda actualización debe seguir los siguientes pasos:
	
	1. Realizar las pruebas iniciales en el **equipo de pruebas el cual se encuentra completamente aislado de la red de producción** y no impacta las operaciones.
	2. Validar en dicho ambiente de prueba la estabilidad del sistema tras la instalación del parche o actualización.
	3. Una vez confirmada la estabilidad, proceder a desplegar la actualización en los equipos de la empresa.
	4. La implementación en producción debe realizarse en una **ventana de mantenimiento programada fuera del horario laboral**, evitando afectaciones a las áreas operativas.
	
	En el ambiente de prueba se debe:
	
	• Acceder al sistema operativo.
	• Ingresar únicamente al **sitio oficial de Windows Update** o repositorio autorizado.
	• Validar las actualizaciones disponibles y seleccionar todas las necesarias.
	• Instalar los parches y realizar las pruebas de validación de estabilidad:
	  ○ **Arranque y apagado correcto del sistema operativo**.
	  ○ **Compatibilidad con drivers y periféricos**.
	  ○ **Ejecución de aplicaciones críticas** sin errores (ej. ERP CIASC, SICOB, Aspel, FileMaker, SGC, etc.).
	  ○ **Verificación de conectividad de red** (LAN, Wi-Fi, VPN Printunl).
	  ○ **Validación de agentes de seguridad activos** (SentinelOne, BitLocker, certificado SSL Fortinet).
	  ○ **Consumo de recursos dentro de parámetros normales** (CPU, RAM, disco, red).
	  ○ **Revisión de logs del sistema y del antivirus** para asegurar que no existan alertas anómalas posteriores a la instalación.
	• Documentar los resultados de la prueba (capturas, logs, incidencias detectadas) en el **ticket de CIA-Desk** correspondiente.
	• En caso favorable, replicar el mismo procedimiento en el sistema original durante la ventana de mantenimiento autorizada.	

2.2	**Verificación del estado del sistema** El área de Sistemas es responsable de **comprobar y validar de manera exhaustiva** que, tras la aplicación de cualquier parche o actualización, el sistema operativo permanezca en condiciones estables y seguras, asegurando que los **servicios críticos de la organización se encuentren plenamente operativos** antes de autorizar su despliegue en entornos productivos. La verificación incluye:	Sistemas

	• **Pruebas de arranque y apagado del sistema**, garantizando que no existan fallos en la carga de controladores ni errores en el proceso de inicio. • **Revisión de servicios críticos** (Active Directory, Exchange, FileMaker, ERP, SICOB, etc.), confirmando que se encuentren levantados y accesibles. • **Validación de dependencias de red**, comprobando conectividad, resolución DNS, accesos a VLAN internas y funcionamiento de certificados SSL. • **Prueba de compatibilidad de aplicaciones corporativas**, asegurando que las herramientas de negocio operen sin interrupciones posteriores al parche. • **Confirmación de controles de seguridad activos**: firewall habilitado, políticas de antivirus actualizadas, agente SentinelOne en ejecución, cliente VPN Printunl en funcionamiento. • **Monitoreo de rendimiento básico**, validando que el consumo de CPU, memoria y disco se encuentre dentro de umbrales normales.	
2.3	**Registro de cambios** Una vez realizada la actualización en el sistema de producción, el **área de Sistemas** debe llevar a cabo un proceso de verificación y registro que asegure la trazabilidad completa del cambio. Las actividades a realizar son las siguientes: • **Validar nuevamente la operación del sistema**, confirmando que este se mantenga en condiciones estables después de aplicar el parche o actualización. Esta validación incluye la comprobación de servicios críticos, accesos de usuarios, rendimiento general y controles de seguridad activos. • **Registrar formalmente el cambio en la plataforma CIA-Desk**, utilizando el ticket vinculado a la solicitud original. El registro debe contener información detallada y suficiente para que cualquier auditor o miembro del área pueda revisar el historial del cambio.	Sistemas
2.4	**Manejo de incidentes durante actualizaciones** Durante el proceso de aplicación de parches o actualizaciones, pueden presentarse **desviaciones o incidentes** que comprometan la estabilidad del sistema, los servicios críticos o los controles de seguridad. Para dichos escenarios, se establece el siguiente procedimiento: 1. **Registro inmediato del incidente**	Sistemas

	○ Se debe levantar un **ticket en CIA-Desk** de forma inmediata, documentando la falla observada y anexando la siguiente información: ▪ Sistema operativo afectado. ▪ Dirección IP asignada al equipo. ▪ Fecha y hora del incidente. ▪ Parches o actualizaciones aplicadas al momento de la falla. ▪ Evidencias técnicas (capturas de pantalla, logs del sistema, mensajes de error). 2. **Acciones correctivas en ambiente de prueba** ○ El área de Sistemas debe **restablecer el estado original** en el **ambiente de pruebas aislado**, replicar el escenario y aplicar los ajustes necesarios para identificar la causa raíz del incidente. ○ Hasta no contar con la validación técnica correspondiente, la implementación en producción debe **posponerse**, evitando riesgos de indisponibilidad o afectaciones a usuarios finales. 3. **Reversión en caso de impacto productivo** ○ Si el incidente llega a impactar sistemas productivos, deberá aplicarse de inmediato el **plan de reversión** previamente definido, restaurando el sistema a su estado anterior mediante respaldos o snapshots. ○ Este proceso debe ejecutarse con prioridad sobre cualquier otro, garantizando la recuperación de la **confidencialidad, integridad y disponibilidad** de los servicios afectados. 4. **Validación y liberación final** ○ Una vez corregido el incidente en el ambiente de prueba, se repiten las validaciones de estabilidad y seguridad (servicios críticos, dependencias, rendimiento, firewall, antivirus, certificados). ○ Solo después de documentar la corrección en **CIA-Desk** y contar con la autorización correspondiente, el parche podrá ser desplegado en el sistema original.	
2.5	**Ventanas de actualización**	Sistemas

	Toda actualización detectada como necesaria deberá programarse en **horarios que no interfieran con la operación normal de la organización**. El cumplimiento de este criterio asegura continuidad operativa y minimiza el impacto a usuarios finales.	
2.6	**Configuraciones seguras (Hardening)** Al habilitar un servidor, equipo de cómputo o dispositivo móvil (incluyendo aquellos destinados a teletrabajo), el área de Sistemas debe aplicar las siguientes configuraciones de seguridad mínimas: Las configuraciones mínimas obligatorias incluyen: • **Accesos remotos:** habilitar únicamente servicios autorizados y aplicar controles de acceso seguro (autenticación multifactor cuando corresponda). • **Bloqueo de transferencia no autorizada de archivos:** deshabilitar protocolos y servicios no requeridos para minimizar riesgos de fuga de información. • **Protocolos de red:** configurar únicamente los protocolos necesarios y deshabilitar versiones obsoletas o inseguros (ej. SMBv1, TLS 1.0). • **Firewall:** activar y configurar las reglas de firewall en equipos y servidores, aplicando políticas corporativas de restricción de tráfico entrante y saliente. • **Actualizaciones automáticas:** habilitar la instalación automática de parches críticos y de seguridad. • **Contraseña en BIOS/UEFI:** establecer credenciales seguras para restringir el acceso a configuraciones de hardware. • **Particionado de discos:** cuando sea posible, crear particiones primarias y secundarias (C:\ y D:) para separar sistema operativo de datos de usuario. • **Política de contraseñas:** aplicar configuraciones conforme a la política corporativa de seguridad (complejidad, expiración periódica, historial). • **Cambio periódico de contraseñas:** de acuerdo con la periodicidad establecida en Active Directory y GPO. • **Restricciones de software:** validar que únicamente se ejecute el software listado en el **Catálogo de Software y Aplicaciones Permitidas** y monitorear desviaciones a través de GLPI y SentinelOne. Adicionalmente, se deberán aplicar los siguientes controles reforzados:	Sistemas

	• **Cifrado de disco con BitLocker:** obligatorio en equipos de cómputo y laptops, asegurando la protección de datos en caso de pérdida o robo del dispositivo. • **VPN Printunl:** instalación y configuración del cliente corporativo de VPN Printunl como requisito indispensable para acceder a servidores, aplicaciones críticas (ERP CIASC, SICOB, FileMaker, Aspel) y recursos internos, incluso desde la red interna. • **Certificado SSL Fortinet:** validación mediante la instalación del certificado SSL corporativo de Fortinet, requisito obligatorio para el acceso a cualquier VLAN interna. • **Agente SentinelOne XDR:** instalación y activación obligatoria en todos los equipos para detección y respuesta ante amenazas avanzadas. • **Bloqueo automático por GPO:** configuración de bloqueo de sesión tras 2 minutos de inactividad. • **Directivas de impresión y dispositivos externos:** restricción de uso de impresoras, USB y unidades externas salvo autorización formal en CIA-Desk.	
2.7	**Administración centralizada de parches y seguridad** La organización cuenta con la plataforma **SentinelOne XDR**, la cual permite administrar de manera centralizada la protección de endpoints y servidores en todas las sedes corporativas. Desde esta consola se gestionan: • Políticas de seguridad aplicables a todos los equipos (escritorios, laptops y servidores). • Detección, prevención y respuesta automática ante amenazas en tiempo real. • Aplicación de parches de seguridad y actualizaciones críticas de manera controlada. • Monitoreo del estado de cada agente instalado, garantizando que permanezca actualizado y activo en todo momento. • Generación de reportes de cumplimiento y evidencias de seguridad para auditorías. Adicionalmente, el **Coordinador de Sistemas TI** realiza cada 15 días una revisión de los **registros de actividad de servidores y endpoints a través de SentinelOne XDR**, validando que los dispositivos cuenten con los últimos parches y políticas aplicadas.	Sistemas

	Los resultados de estas revisiones se documentan en el formato **LIS-GSI-002 – Revisión de LOGS**, lo que permite mantener evidencia formal y trazable para auditorías internas, externas o de clientes.	
2.8	**Sincronización de reloj** Para garantizar la consistencia y trazabilidad de los registros de eventos (logs) en toda la infraestructura tecnológica, el área de Sistemas debe asegurar que todos los servidores, estaciones de trabajo y dispositivos de red se encuentren sincronizados con fuentes de hora externas confiables. Los lineamientos establecidos son: • Todos los equipos deberán sincronizarse con servicios de hora confiables tales como time.windows.com o servidores NTP públicos de referencia (ej. pool.ntp.org). • Esta sincronización aplica a: o Servidores físicos y virtuales. o Estaciones de trabajo. o Firewalls Fortinet y dispositivos de red (switches, routers, access points). o Consolas y herramientas de seguridad (ejemplo: SentinelOne XDR). • El desfase máximo permitido entre equipos no debe exceder los 5 minutos. • La revisión de la sincronización de hora deberá realizarse de manera trimestral, y los resultados documentarse en un ticket de CIA-Desk, adjuntando evidencias de la validación (capturas de configuraciones o reportes de estado).	Sistemas
3	**Política de Copias de Seguridad**	
3.1	**Política de copias de seguridad** • Se deberán realizar **copias de seguridad completas y diferenciales** de toda la información y de los sistemas electrónicos identificados como críticos, siguiendo lo establecido en el procedimiento **PRO-GSI-032 – Respaldo y eliminación de la información**. • El **área de Sistemas** es la responsable de planificar, ejecutar y supervisar la estrategia de respaldos, asegurando que la información se almacene en medios confiables y con los niveles de protección adecuados.	Sistemas

	• Los respaldos deberán realizarse en **ventanas de tiempo predefinidas** para no afectar la operación diaria, garantizando la integridad de los datos y la disponibilidad de los servicios. • Todo respaldo generado debe estar **documentado en CIA-Desk**, mediante ticket que incluya fecha, tipo de respaldo (completo, incremental o diferencial), sistemas cubiertos, medio de almacenamiento utilizado y evidencia de la validación. • Las copias de seguridad estarán sujetas a **pruebas periódicas de restauración**, que permitan comprobar su efectividad y asegurar la continuidad operativa en caso de incidentes. • El resguardo de respaldos deberá realizarse en medios protegidos físicamente contra acceso no autorizado y, en caso de medios digitales, bajo cifrado mediante herramientas aprobadas por el área de Seguridad de la Información. Con esta política, la organización garantiza la **confidencialidad, integridad y disponibilidad de la información crítica**, alineándose a las buenas prácticas de continuidad de negocio y a los controles de la norma **ISO/IEC 27001:2022**.	
4	**Gestión de seguridad de red**	

4.1	**Lineamientos generales**
	• El **área de Sistemas** es responsable de administrar y proteger las redes de datos de la organización, asegurando que todos los servicios se encuentren disponibles, seguros y protegidos frente a accesos no autorizados.
	• El tráfico sensible que circule por redes públicas debe realizarse mediante **VPN Printunl, protocolos cifrados (TLS/SSL, HTTPS, SFTP)** o, en su defecto, con cifrado de archivos.
	• Todo dispositivo remoto que se conecte a la red corporativa debe cumplir con tres requisitos básicos:
	  ○ **Certificado SSL Fortinet** instalado y validado.
	  ○ **Cliente VPN Printunl** activo y configurado.
	  ○ **Agente SentinelOne XDR** en ejecución.
	• La disponibilidad se garantiza con **No-Breaks y redundancia eléctrica** en equipos críticos, evitando pérdida de datos o indisponibilidad en caso de falla de energía.
		Sistemas

	• Se mantiene una política estricta de **verificación periódica de antivirus y agentes de seguridad** en servidores y endpoints.	
4.2	**Segmentación de red y VLAN por sede** La red interna está **segmentada en VLAN específicas por área de negocio**, evitando configuraciones genéricas y aplicando reglas personalizadas en Fortinet para cada flujo de tráfico. • **Principio rector:** todo tráfico lateral entre VLAN se encuentra bloqueado por defecto. **Mapa de VLAN y SSID implementados en Access Points Huawei:** **Oficina Nezahualcóyotl** • SSID: **DIRCOR** → VLAN Dirección General • SSID: **REHCOR** → VLAN Recursos Humanos • SSID: **CONCOR** → VLAN Contabilidad • SSID: **SISCOR** → VLAN Sistemas • SSID: **GESCOR** → VLAN Gestión Domiciliaria • SSID: **INVCOR** → VLAN Investigación de Crédito • SSID: **INVITADOS** → VLAN aislada, acceso únicamente a internet **Oficina Insurgentes** • SSID: **DIRCOR** → VLAN Dirección General • SSID: **COSVAL** → VLAN Cobranza Social • SSID: **CREVAL** → VLAN Jurídico • SSID: **SISCOR** → VLAN Sistemas • SSID: **REHCOR** → VLAN Recursos Humanos • SSID: **INVITADOS** → VLAN aislada, acceso únicamente a internet **Oficina Toluca** • SSID: **DIRCOR** → VLAN Dirección General • SSID: **RECCALS** → VLAN Supervisores de Call Center • SSID: **RECCALC** → VLAN Gerencia de Recuperación de Cartera • SSID: **SISCOR** → VLAN Sistemas • SSID: **REHCOR** → VLAN Recursos Humanos • SSID: **INVITADOS** → VLAN aislada, acceso únicamente a internet	Sistemas
4.3	**Controles de acceso a la red**	Sistemas

La organización aplica un esquema de **acceso en múltiples capas**, combinando validación de dispositivos, autenticación de usuarios y segmentación de red, lo que garantiza que únicamente los equipos corporativos y autorizados puedan acceder a los recursos internos.

Certificado SSL Fortinet:

- Todo dispositivo corporativo debe contar con el certificado SSL Fortinet instalado y validado.
- Este certificado funciona como un identificador digital único que habilita el acceso a VLAN internas.
- Sin él, el dispositivo queda automáticamente restringido y no puede interactuar con la red corporativa.

Canalización de dispositivos externos:

- Los dispositivos sin certificado SSL o de terceros (proveedores, clientes, auditores, visitantes) son canalizados automáticamente a la **VLAN CIA - Invitados**, la cual está completamente aislada de la red interna.
- Esta VLAN ofrece únicamente salida controlada a internet, evitando cualquier exposición de información sensible.

Portal cautivo Fortinet (alámbrico e inalámbrico):

- Todo dispositivo, ya sea conectado de manera **inalámbrica o mediante red alámbrica**, debe autenticarse en el **portal cautivo Fortinet** antes de obtener acceso.
- Las credenciales se gestionan localmente en el firewall, lo que centraliza el control de accesos y facilita la administración y revocación inmediata en caso de incidentes.
- La obligatoriedad del portal cautivo en ambos tipos de conexión garantiza trazabilidad de todos los accesos y elimina la posibilidad de conexiones anónimas en la red corporativa.

Acceso a sistemas críticos mediante VPN Printunl:

- El acceso a los sistemas de misión crítica (ERP CIASC, SICOB, FileMaker, Aspel, Intranet del SGC, entre otros) requiere, además, conexión obligatoria a través de la **VPN Printunl**.
- Esto añade una capa final de seguridad, proporcionando **cifrado extremo a extremo** y validación adicional de credenciales y certificados.

	• Incluso dentro de la red interna, ningún usuario puede acceder a estos sistemas sin pasar por el túnel de seguridad de VPN Printunl.	
4.4	**Red alámbrica** • El acceso a la red cableada está **restringido exclusivamente a equipos corporativos**. • Todo dispositivo no autorizado que intente conectarse a un puerto ethernet es bloqueado y, de ser necesario, aislado desde el firewall.	Sistemas
4.5	**Centros de datos y redundancia** La organización mantiene **tres centros de datos** (Nezahualcóyotl, Insurgentes y Toluca), con las siguientes características: • Enlaces redundantes de telecomunicaciones. • Firewalls y switches configurados en **alta disponibilidad (HA)**. • Sistemas IPS entre enlaces y switches para inspección de tráfico interno y externo. • Alimentación eléctrica respaldada por **No-Breaks y generadores**, asegurando continuidad ante cortes de energía.	Sistemas

4.6	**Convenios con proveedores de seguridad perimetral**
	• La organización mantiene convenios con **Telmex (Scitum)** y **TotalSec (TotalPlay)** para la provisión de servicios de **seguridad perimetral administrada con monitoreo continuo 24/7**, bajo un esquema contractual de **renta forzada a 36 meses**.
	• Al término del contrato, los equipos de seguridad **Fortinet FortiGate** pasarán a ser propiedad de **CIASC**, asegurando la continuidad de la protección y la independencia tecnológica en la operación de la infraestructura.
	• Como parte del servicio, los proveedores realizan **monitoreo integral de la red y de los firewalls Fortinet**, lo cual incluye:
	  ○ Detección y bloqueo de intentos de intrusión.
	  ○ Identificación de tráfico anómalo entre VLAN internas y externas.
	  ○ Vigilancia y mitigación de ataques de denegación de servicio (DoS/DDoS).
		Sistemas

	○ Validación de políticas de seguridad aplicadas en los equipos perimetrales. • En caso de incidentes de seguridad detectados, los proveedores actúan bajo el siguiente protocolo: 1. **Bloqueo inmediato** del tráfico sospechoso o malicioso. 2. **Notificación directa** al área de Sistemas de CIASC mediante correo institucional y llamada telefónica. 3. **Entrega de reportes técnicos**, incluyendo logs, trazas de red y evidencias del evento para su análisis interno. • El área de **Sistemas** es responsable de **registrar y documentar el evento en CIA-Desk** y formalizarlo en el **FOR-GSI-024 – Incidentes de Seguridad de la Información**, asegurando un seguimiento documentado en un plazo máximo de **48 horas** o hasta el cierre completo de la incidencia.	
4.7	**Seguridad perimetral Fortinet** La organización protege sus centros de datos mediante **equipos Fortinet FortiGate 80F y 100E**, configurados en esquemas de alta disponibilidad (HA) y con funcionalidades avanzadas de seguridad perimetral habilitadas. Estos dispositivos constituyen la primera línea de defensa frente a amenazas externas e internas, asegurando la continuidad de los servicios críticos. Las funciones activas incluyen: • **IDS/IPS:** detección y prevención de intrusiones en tiempo real, con firmas actualizadas y análisis de comportamiento para tráfico interno y externo. • **Antivirus perimetral:** inspección de archivos y tráfico HTTP/HTTPS para identificar y bloquear malware antes de llegar a la red interna. • **Filtrado de páginas web:** control de navegación, con políticas que restringen sitios maliciosos, no autorizados o de riesgo. • **Filtrado de puertos:** bloqueo y control estricto del tráfico en función de puertos y protocolos, reduciendo vectores de ataque. • **Control de aplicaciones:** identificación y regulación del uso de aplicaciones, previniendo el uso de software no autorizado o con riesgos de seguridad. • **VPN corporativa:** establecimiento de túneles cifrados para accesos remotos seguros, en cumplimiento con las políticas de teletrabajo.	Sistemas

	• **Inspección SSL:** visibilidad total del tráfico cifrado, lo que permite detectar amenazas ocultas en conexiones HTTPS. El monitoreo de estas funciones se realiza de manera conjunta: • **Proveedores externos (Telmex/Scitum y TotalSec):** realizan supervisión perimetral continua 24/7, notifican intentos de intrusión y aplican bloqueos inmediatos ante eventos sospechosos. • **Área de Sistemas:** valida la correcta aplicación de políticas, ajusta configuraciones según necesidades de negocio, y documenta cualquier incidente en **CIA-Desk** y en el **FOR-GSI-024 – Incidentes de Seguridad de la Información**.	
4.8	**Sistemas IPS** La organización cuenta con **sistemas de detección y prevención de intrusos (IPS)** integrados estratégicamente entre los **enlaces de comunicación y los switches principales**, lo que permite realizar inspección profunda de paquetes en tiempo real tanto en tráfico **interno** como **externo**. Las funciones principales de los IPS son: • **Monitoreo bidireccional:** inspección continua del tráfico entrante y saliente para identificar patrones anómalos, accesos indebidos o comportamientos sospechosos. • **Detección avanzada:** análisis basado en firmas actualizadas y en heurística de comportamiento, lo que permite identificar intentos de intrusión conocidos y nuevas variantes de ataque. • **Prevención y contención:** bloqueo inmediato de conexiones no autorizadas o maliciosas, evitando la propagación de incidentes en la red corporativa. • **Segregación de tráfico:** validación de comunicaciones inter-VLAN y hacia internet, garantizando que solo se permita el tránsito conforme a las políticas definidas.	Sistemas
5	**Políticas para Canales de comunicación**	
5.1	**Intercambio de información** La información de la organización puede ser intercambiada a través de **canales electrónicos** y en **formato físico (papel)**, siempre bajo los lineamientos del **SGSI** y en cumplimiento de las **Políticas Generales de Seguridad de la Información (POL-GSI-001)** y demás procedimientos relacionados.	Sistemas

	Intercambio electrónico
	• Los canales autorizados para la transmisión de información son:
	  ○ **Correo electrónico corporativo.**
	  ○ **Descarga y transferencia de archivos desde internet**, siempre que se utilicen plataformas aprobadas.
	  ○ **VPN corporativa Printunl**, para el acceso remoto seguro a los sistemas internos.
	  ○ **Protocolos seguros de transferencia de archivos (SFTP/FTPS)**; el uso de **FTP no cifrado** se encuentra prohibido.
	• El área de **Sistemas** es responsable de determinar qué canales pueden utilizarse para cada tipo de información, aplicando medidas de control según la clasificación de la información (confidencial, interna, pública).
	• Las **restricciones de uso y actividades prohibidas** se encuentran establecidas en el apartado de "Política de Uso Aceptable" de la **POL-GSI-001**, e incluyen prácticas como el envío de información sensible a correos personales, el uso de servicios de almacenamiento en la nube no autorizados o el intercambio por mensajería instantánea sin cifrado.
	• Todo canal electrónico está sujeto a monitoreo y registro, asegurando la **trazabilidad y control de la información en tránsito**.
	Intercambio en papel
	• La información en soporte físico se controla mediante el **PRO-GSI-015 – Gestión de activos, clasificación y control de la información**, que establece los lineamientos para la **clasificación, resguardo, distribución y eliminación** de documentos.
	• Este procedimiento contempla:
	  ○ Identificación del tipo de información.
	  ○ Registro de responsables del manejo de documentos.
	  ○ Restricciones de acceso según nivel de sensibilidad.
	  ○ Métodos de eliminación segura cuando la información deja de ser necesaria.	

6	**Relaciones con entidades externas**	

6.1	➢ Entre las entidades externas se incluyen a diversos proveedores de servicios, empresas de mantenimiento de software y hardware, empresas que manejan transacciones o procesamiento de datos, clientes, etc. ➢ Antes de intercambiar información y/o software con cualquier entidad externa, se debe firmar un contrato, el cual es responsabilidad de la Dirección General. El contrato puede estar en papel o en formato electrónico (por ejemplo, aceptando los términos y condiciones generales) y debe contener cláusulas que coincidan la seguridad de la información incluyendo, entre otros (y dependiendo del tipo de proveedor), las siguientes clausulas: o Método de identificación de la otra parte. o Autorizaciones para acceder a la información. o Asegurando la inviolabilidad. o Estándares técnicos para la transferencia de datos. o Respuesta a incidentes. o Etiquetado y manejo de información sensible. o Derechos de autor.	Sistemas
7	**Supervisión del sistema**	
7.1	El **área de Sistemas** es responsable de la **supervisión diaria de los registros de fallos** reportados en el portal de soporte **CIA-Desk**. Esta actividad forma parte del proceso de monitoreo continuo de la infraestructura tecnológica y constituye un control clave para la detección temprana de desviaciones o vulnerabilidades. Las funciones principales incluyen: • **Revisión sistemática de tickets registrados en CIA-Desk**, identificando incidentes recurrentes o patrones de fallos que puedan afectar la operación. • **Análisis de causa raíz**, evaluando los motivos técnicos que originaron el fallo (hardware, software, red, configuración, usuario, etc.). • **Aplicación de acciones correctivas inmediatas**, documentadas en el mismo ticket, garantizando la trazabilidad del evento. • **Escalamiento** de los incidentes críticos al Coordinador de Sistemas TI o al Gerente Administrativo, cuando se identifique riesgo significativo para la continuidad de los servicios. • **Registro de evidencias técnicas** (logs de sistema, capturas de pantalla, configuraciones aplicadas), asegurando que cada acción pueda ser auditada. • **Generación de métricas internas**, tales como número de fallos diarios, tiempo promedio de resolución y porcentaje de incidentes cerrados en plazo, para alimentar indicadores de desempeño (KPIs).	Sistemas
