UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Universidad Politécnica de San Luis Potosí

Ingeniería en Tecnologías de la Información

Proyecto P03

Bajo la lupa

Evaluación de ciberseguridad en un corporativo

SGSI basado en ISO/IEC 27001:2022 aplicado a la UPSLP

Alcance, activos, políticas, riesgos, operación, auditoría y mejora continua

Equipo de trabajo

Coronado Noriega Jesús Olaf	178991
De La Rosa Rodríguez Erik	177700
González Reyes Felipe de Jesús	181134
Mendoza Aguado Karina	179859
Serrano Zermeño Leonardo	177301
Pérez Ventura Juan Alejandro	180370

Materia: CNO V: Seguridad Informática

Docente: Mtro. Servando López Contreras

Fecha: 19 de mayo de 2026

Índice

Resumen ejecutivo **3**

1. Alcance **3**

1.1. Datos generales de la organización . . . 3

1.2. Misión, visión, objetivos y valores propuestos . . . 3

1.3. Estructura funcional y relación con activos . . . 4

1.4. Dirección > área > proceso > actividad de implementación . . . 4

1.5. Justificación del SGSI y delimitación . . . 5

2. Referencias normativas **5**

3. Términos y condiciones de la intervención **6**

3.1. Términos clave del SGSI . . . 6

3.2. Condiciones de intervención . . . 6

4. Contexto de la organización e inventario de activos **7**

4.1. Contexto interno y externo . . . 7

4.2. Partes interesadas . . . 8

4.3. Inventario de 40 activos de información . . . 8

5. Liderazgo **15**

5.1. Política general de seguridad de la información . . . 15

5.2. Diez políticas específicas del SGSI . . . 15

5.3. Matriz RACI . . . 17

6. Planificación **19**

6.1. Metodología de evaluación de riesgos . . . 19

6.2. Matriz de riesgos prioritaria . . . 19

6.3. Justificación de priorización . . . 22

6.4. Declaración de aplicabilidad resumida . . . 22

7. Soporte **22**

7.1. Minuta formal de reunión . . . 23

7.2. Explicación para alta dirección . . . 23

7.3. Presentación ejecutiva propuesta . . . 23

7.4. Lenguaje técnico vs. lenguaje ejecutivo 24

8. Operación **24**

8.1. Política seleccionada para implementación operativa 24

8.2. Procedimiento operativo replicable 24

8.3. Evidencia técnica simulada 25

8.4. Responsables, frecuencia y posibles fallos 25

9. Evaluación del desempeño **25**

9.1. Formatos de auditoría profesional 25

9.1.1. Checklist de auditoría interna 25

9.1.2. Guía de entrevista 26

9.2. Hallazgos y plan de acción 26

9.3. Resultado ejecutivo de auditoría 27

10. Mejora **27**

10.1. Incidente verosímil: phishing a cuenta administrativa 27

10.2. Respuesta ejecutiva 27

10.3. Medidas para evitar recurrencia 27

10.4. Material de prevención para usuarios finales 28

10.5. Conexión con mejora continua 29

11. Verificación final de cobertura del SGSI **29**

Conclusión **30**

Referencias **30**

Resumen ejecutivo

Este documento propone un Sistema de Gestión de Seguridad de la Información (SGSI) para la Universidad Politécnica de San Luis Potosí (UPSLP), tomando como eje ISO/IEC 27001:2022 y la estructura de alto nivel del Anexo SL. La propuesta no se limita a describir conceptos: traduce cada sección evaluada en activos, responsables, políticas, riesgos, procedimientos, evidencias, auditoría y mejora continua.

El alcance se concentra en los servicios digitales críticos de la UPSLP: control escolar, plataformas académicas, correo institucional, red LAN/Wi-Fi, sistemas administrativos, activos de información, servicios en nube, proveedores TIC y procesos de soporte tecnológico. La intervención prioriza confidencialidad, integridad y disponibilidad de información académica, administrativa, financiera, laboral y tecnológica.

Enfoque de desarrollo del proyecto

El proyecto desarrolla una propuesta integral de SGSI con empresa verosímil, referencias normativas, términos útiles, 40 activos trazables, 10 políticas con estándar, directriz, procedimiento y línea base, RACI, matriz de riesgos, minuta, explicación ejecutiva, procedimiento operativo con evidencias, auditoría simulada y mejora continua. El documento mantiene relación lógica entre alcance, activos, políticas, riesgos, controles, operación y auditoría.

1 Alcance

1.1. Datos generales de la organización

Elemento	Descripción aplicada a UPSLP
Nombre	Universidad Politécnica de San Luis Potosí (UPSLP).
Giro	Institución pública de educación superior, docencia, investigación aplicada, vinculación y servicios académicos.
Tamaño verosímil	Comunidad amplia integrada por estudiantes, docentes, personal administrativo, servicios informáticos, proveedores y visitantes.
Servicios críticos	Control escolar, plataformas académicas, correo institucional, red LAN/Wi-Fi, laboratorios, sistemas administrativos, pagos, biblioteca digital y comunicación institucional.
Clientes / usuarios	Estudiantes, aspirantes, egresados, docentes, personal administrativo, autoridades educativas, proveedores y sociedad.
Entorno tecnológico	Infraestructura híbrida con servidores internos, red campus, servicios cloud, correo SaaS, LMS, pasarela de pagos, equipos administrativos y laboratorios.

Tabla 1. Perfil organizacional considerado para el SGSI.

1.2. Misión, visión, objetivos y valores propuestos

Misión. Proteger la información académica, administrativa y tecnológica de la UPSLP mediante controles proporcionales al riesgo que permitan continuidad operativa, cumplimiento normativo y confianza institucional.

Visión. Consolidar un SGSI institucional medible, auditado y mejorable, capaz de reducir incidentes, fortalecer cultura de seguridad y respaldar los servicios digitales críticos de la universidad.

Objetivos organizacionales del SGSI.

1. Asegurar disponibilidad de servicios críticos durante periodos académicos sensibles.
2. Proteger datos personales, académicos, financieros y laborales bajo criterios de confidencialidad e integridad.
3. Reducir el riesgo de phishing, ransomware, fuga de información y abuso de privilegios.
4. Establecer evidencia documental suficiente para auditorías internas y mejora continua.

Valores de seguridad. Legalidad, responsabilidad, confidencialidad, trazabilidad, continuidad, colaboración institucional y mejora continua.

1.3. Estructura funcional y relación con activos

Área	Procesos de negocio	Activos asociados
Rectoría / Dirección	Decisión institucional, recursos, aceptación de riesgos	Política SGSI, actas, indicadores, riesgos residuales.
Servicios Informáticos	Red, cuentas, servidores, soporte, respaldos, incidentes	Directorio activo, firewall, LAN/Wi-Fi, backups, tickets, EDR.
Servicios Escolares	Inscripción, expedientes, calificaciones, trayectoria académica	BD control escolar, sistema escolar, expedientes digitales.
Administración y Finanzas	Pagos, presupuesto, nómina, facturación	Sistema financiero, nómina, pasarela de pagos, PAC.
Áreas académicas	Cursos, laboratorios, LMS, evaluación	LMS, laboratorios, licencias académicas, biblioteca digital.
Comunicación institucional	Sitio web, redes oficiales, avisos	Portal web, dominios, redes sociales oficiales.

Tabla 2. Relación entre procesos de negocio y activos de información.

1.4. Dirección > área > proceso > actividad de implementación

Ubicación precisa de intervención

Dirección: Rectoría / Dirección General.
Área prioritaria: Servicios Informáticos, coordinado con Servicios Escolares y Administración.
Proceso: Gestión de identidades, accesos, activos críticos y tratamiento de riesgos de servicios digitales.
Actividad específica: Implementación operativa de controles de acceso seguro y autenticación multifactor para cuentas institucionales críticas, junto con inventario de activos, matriz de riesgos, políticas, auditoría y mejora continua.

1.5. Justificación del SGSI y delimitación

La UPSLP requiere un SGSI porque sus procesos académicos y administrativos dependen de información digital. Una caída de red, compromiso de correo, fuga de expedientes o alteración de calificaciones afectaría continuidad educativa, reputación, cumplimiento y confianza de la comunidad.

Alcance incluido: campus principal, red institucional, cuentas oficiales, plataformas académicas, sistemas administrativos, servicios cloud contratados, equipos administrados, respaldos, proveedores TIC y procesos de soporte tecnológico.

Exclusiones justificadas: dispositivos personales no administrados cuando no accedan a servicios institucionales; redes domésticas; aplicaciones personales no autorizadas; investigación individual no alojada en recursos institucionales.

Supuestos: existe una coordinación de TI con acceso a información operativa, se cuenta con apoyo de dirección para políticas y capacitación, y el proyecto se desarrolla como propuesta académica simulada con evidencia técnica representativa.

Restricciones: no se ejecutan cambios reales sobre infraestructura productiva; las evidencias operativas se presentan como simulación replicable; la información sensible se anonimiza.

2 Referencias normativas

Norma / referencia	Función	Uso dentro del SGSI de UPSLP
ISO/IEC 27001:2022	Requisitos certificables del SGSI	Norma base para establecer alcance, liderazgo, planificación, operación, evaluación y mejora.
ISO/IEC 27000	Visión general y vocabulario	Base para términos como activo, riesgo, control, incidente, confidencialidad, integridad y disponibilidad.
ISO/IEC 27002:2022	Guía de controles	Apoya la selección de controles del Anexo A: accesos, respaldos, proveedores, incidentes, monitoreo y concienciación.
ISO/IEC 27005	Gestión de riesgos	Orienta identificación, análisis, valoración y tratamiento de riesgos de seguridad de la información.
ISO/IEC 27017	Seguridad en nube	Pertinente por correo, LMS, respaldos cloud y servicios SaaS usados por la universidad.
ISO/IEC 27018	Protección de datos personales en nube	Relevante para PII alojada o procesada en plataformas cloud institucionales.
ISO/IEC 27031	Continuidad TIC	Apoya recuperación de servicios académicos, correo, red y sistemas administrativos.
ISO/IEC 27035	Gestión de incidentes	Guía preparación, respuesta, registro y aprendizaje ante phishing, malware o fuga de información.
ISO/IEC 27037	Evidencia digital	Útil para preservar evidencias de incidentes y auditorías sin alterar su valor.
Marco legal mexicano aplicable	Protección de datos, transparencia y responsabilidades	Contexto regulatorio general para información personal, expedientes y rendición de cuentas.

Tabla 3. Referencias normativas y uso práctico dentro del SGSI.

La familia ISO/IEC 27000 se usa como marco completo: ISO/IEC 27001 define el sistema de gestión; ISO/IEC 27002 orienta controles; ISO/IEC 27005 estructura riesgos; y normas complementarias agregan profundidad en nube, privacidad, continuidad, incidentes y evidencia digital.

3 Términos y condiciones de la intervención

3.1. Términos clave del SGSI

Término	Definición operativa	Ejemplo aplicado a UPSLP
Activo de información	Dato, sistema, equipo, proceso, repositorio o conocimiento que tiene valor para la institución.	BD de alumnos, correo institucional, LMS, respaldos.
Amenaza	Evento o actor con potencial de causar daño a un activo.	Phishing, ransomware, falla eléctrica, proveedor comprometido.
Vulnerabilidad	Debilidad que puede ser explotada por una amenaza.	Falta de MFA, permisos excesivos, sistemas sin parches.
Riesgo	Efecto de la incertidumbre sobre confidencialidad, integridad o disponibilidad.	Robo de credenciales de correo institucional.
Control	Medida administrativa, técnica o física para modificar el riesgo.	MFA, segmentación, respaldos, monitoreo.
Confidencialidad	Propiedad de que la información solo sea accesible a personas autorizadas.	Expedientes académicos solo para personal autorizado.
Integridad	Propiedad de exactitud y completitud de la información.	Calificaciones no alteradas sin autorización.
Disponibilidad	Propiedad de acceso oportuno a información y servicios.	LMS disponible durante clases e inscripciones.
Incidente	Evento que compromete o puede comprometer seguridad de la información.	Cuenta comprometida por phishing.
Auditoría	Revisión sistemática de controles, evidencias y cumplimiento.	Checklist de accesos, respaldos e incidentes.
Tratamiento del riesgo	Decisión para mitigar, transferir, evitar o aceptar un riesgo.	Mitigar phishing con MFA y capacitación.
RTO	Tiempo objetivo de recuperación de un servicio.	Restaurar sistema escolar en menos de 8 horas.
RPO	Punto objetivo de recuperación o pérdida máxima tolerada.	Perder máximo 24 horas de datos respaldados.
Propietario de activo	Área responsable de autorizar uso, clasificación y accesos.	Servicios Escolares sobre expedientes académicos.
Custodio técnico	Área que administra técnicamente el activo.	Servicios Informáticos operando servidor o red.

Tabla 4. Términos seleccionados por relevancia práctica para la intervención.

3.2. Condiciones de intervención

- **Confidencialidad:** toda evidencia se maneja con datos simulados o anonimizados.

- **Límites técnicos:** no se ejecutan pruebas intrusivas ni cambios reales en producción.
- **Evidencia:** se documentan capturas simuladas, comandos representativos, tablas, tickets y bitácoras.
- **Responsabilidad:** el Comité SGSI aprueba lineamientos; TI ejecuta controles; dueños de información autorizan accesos.
- **Exclusiones:** quedan fuera dispositivos personales y servicios no institucionales salvo que accedan a información universitaria.

4 Contexto de la organización e inventario de activos

4.1. Contexto interno y externo

Tipo	Factor	Implicación para el SGSI
Interno	Usuarios diversos: estudiantes, docentes, administrativos y técnicos.	Se requieren políticas claras, capacitación diferenciada y controles por rol.
Interno	Múltiples sistemas y servicios híbridos.	Se necesita inventario, arquitectura documentada y gestión de cambios.
Interno	Carga operativa de TI.	Priorizar controles de alto impacto y evidencia simple de mantener.
Interno	Información académica, financiera, laboral y técnica.	Clasificación de información y dueños de activos.
Externo	Phishing, ransomware, robo de credenciales y ataques web.	MFA, EDR, respaldos, monitoreo y respuesta a incidentes.
Externo	Proveedores cloud, ISP, pagos y software académico.	Gestión contractual, evaluación de riesgo y revocación de accesos.
Externo	Regulación de datos personales y transparencia.	Evidencia documental, trazabilidad y manejo seguro de PII.
Externo	Continuidad académica ante fallas de energía o conectividad.	Redundancia, RTO/RPO, pruebas de restauración y comunicación.

Tabla 5. Cuestiones internas y externas relevantes para el SGSI.

4.2. Partes interesadas

Parte interesada	Necesidad / expectativa	Respuesta del SGSI
Estudiantes	Disponibilidad de plataformas, privacidad de datos, acceso oportuno.	MFA, soporte, respaldos, comunicación de incidentes.
Docentes	Acceso a LMS, correo, listas y evaluaciones.	Roles, capacitación y continuidad de servicios.
Administrativos	Sistemas confiables para trámites, pagos y expedientes.	Segregación de funciones, respaldos y auditoría.
Rectoría	Continuidad, reputación, cumplimiento y uso eficiente de recursos.	KPIs, revisión directiva y aceptación de riesgos.
Servicios Informáticos	Procesos claros, apoyo directivo y herramientas.	Políticas, plan de tratamiento y presupuesto.
Proveedores	Reglas de acceso y confidencialidad.	Contratos, cuentas temporales y supervisión.
Autoridades	Cumplimiento, evidencia y trazabilidad.	Auditorías, documentación y plan de mejora.

Tabla 6. Partes interesadas del SGSI.

4.3. Inventario de 40 activos de información

Se presenta un inventario de 40 activos relacionados con información, clasificados como internos o externos, con propietario, ubicación, proceso, responsable operativo, dependencia tecnológica y valoración CIA. Para que la tabla sea legible, se divide en dos vistas complementarias con el mismo código de activo: la primera resume clasificación y criticidad; la segunda conserva la trazabilidad operativa.

Código	Tipo	Activo	Propietario	Proceso asociado	C/I/D
ACT-INT-01	Interno	Base de datos de Control Escolar	Servicios Escolares	Control escolar	Alta/Alta/Alta
ACT-INT-02	Interno	Sistema de Gestión Escolar	Servicios Escolares	Inscripción y trayectoria académica	Alta/Alta/Alta
ACT-INT-03	Interno	Servidor de autenticación / Directorio activo	Servicios Informáticos	Gestión de identidades	Alta/Alta/Alta
ACT-INT-04	Interno	Servidor de archivos administrativos	Administración / TI	Gestión documental	Alta/Alta/Media
ACT-INT-05	Interno	Sistema financiero y contable	Administración y Finanzas	Pagos, presupuesto y contabilidad	Alta/Alta/Alta
ACT-INT-06	Interno	Sistema de nómina	Recursos Humanos	Pago de personal	Alta/Alta/Media
ACT-INT-07	Interno	Red LAN administrativa	Servicios Informáticos	Conectividad interna	Alta/Alta/Alta
ACT-INT-08	Interno	Red Wi-Fi institucional	Servicios Informáticos	Acceso de usuarios	Media/Media/Alta
ACT-INT-09	Interno	Firewall perimetral	Servicios Informáticos	Seguridad perimetral	Alta/Alta/Alta
ACT-INT-10	Interno	Servidor de respaldos local	Servicios Informáticos	Continuidad y recuperación	Alta/Alta/Alta
ACT-INT-11	Interno	Repositorio de documentación técnica	Servicios Informáticos	Operación TI	Alta/Media/Media
ACT-INT-12	Interno	Equipos administrativos de Servicios Escolares	Servicios Escolares	Atención escolar	Alta/Alta/Media
ACT-INT-13	Interno	Equipos administrativos de Finanzas	Finanzas	Pagos y presupuesto	Alta/Alta/Media
ACT-INT-14	Interno	Laboratorios de cómputo	Áreas académicas / TI	Docencia práctica	Media/Media/Alta
ACT-INT-15	Interno	CCTV y NVR institucional	Seguridad física / TI	Monitoreo físico	Media/Alta/Media
ACT-INT-16	Interno	Sistema de tickets de soporte	Servicios Informáticos	Atención de incidentes y solicitudes	Media/Alta/Media

Código	Tipo	Activo	Propietario	Proceso asociado	C/I/D
ACT-INT-17	Interno	Inventario de activos TIC	Servicios Informáticos	Gestión de activos	Media/Alta/Media
ACT-INT-18	Interno	Servidores de aplicaciones internas	Servicios Informáticos	Servicios administrativos	Alta/Alta/Alta
ACT-INT-19	Interno	UPS y energía del site	Servicios Informáticos / Mantenimiento	Continuidad energética	Baja/Media/Alta
ACT-INT-20	Interno	Documentación del SGSI	Responsable SGSI	Gobierno de seguridad	Media/Alta/Media
ACT-EXT-01	Externo	Correo institucional en nube	Servicios Informáticos	Comunicación oficial	Alta/Alta/Alta
ACT-EXT-02	Externo	LMS institucional	Áreas académicas	Cursos y evaluaciones	Alta/Alta/Alta
ACT-EXT-03	Externo	Portal web institucional	Comunicación / TI	Comunicación pública	Media/Alta/Media
ACT-EXT-04	Externo	Dominio institucional	Servicios Informáticos	Identidad digital	Alta/Alta/Alta
ACT-EXT-05	Externo	Certificados TLS	Servicios Informáticos	Cifrado web	Media/Alta/Alta
ACT-EXT-06	Externo	Proveedor de internet principal	Servicios Informáticos	Conectividad campus	Baja/Media/Alta
ACT-EXT-07	Externo	Enlace de internet secundario	Servicios Informáticos	Continuidad de red	Baja/Media/Alta
ACT-EXT-08	Externo	Pasarela de pagos	Finanzas	Cobro de servicios	Alta/Alta/Alta
ACT-EXT-09	Externo	Repositorio cloud de respaldos	Servicios Informáticos	Recuperación ante desastre	Alta/Alta/Alta
ACT-EXT-10	Externo	Licenciamiento académico	Áreas académicas / TI	Docencia y laboratorios	Baja/Media/Media
ACT-EXT-11	Externo	Plataforma de videoconferencia	Áreas académicas	Clases y reuniones	Media/Media/Media
ACT-EXT-12	Externo	Servicios de nube colaborativa	Usuarios institucionales	Colaboración documental	Alta/Alta/Alta
ACT-EXT-13	Externo	Proveedor de mantenimiento de red	Servicios Informáticos	Soporte infraestructura	Alta/Alta/Media
ACT-EXT-14	Externo	Servicio de monitoreo externo	Servicios Informáticos	Detección de amenazas	Alta/Alta/Media

Código	Tipo	Activo	Propietario	Proceso asociado	C/I/D
ACT-EXT-15	Externo	Sistema de facturación electrónica	Finanzas	Comprobación fiscal	Alta/Alta/Media
ACT-EXT-16	Externo	Plataforma gubernamental de reportes	Rectoría / Administración	Cumplimiento regulatorio	Alta/Alta/Media
ACT-EXT-17	Externo	Redes sociales oficiales	Comunicación	Comunicación institucional	Media/Alta/Media
ACT-EXT-18	Externo	Sistema de biblioteca digital	Biblioteca / TI	Consulta académica	Media/Media/Media
ACT-EXT-19	Externo	Antivirus/EDR administrado	Servicios Informáticos	Protección endpoint	Alta/Alta/Alta
ACT-EXT-20	Externo	Proveedor de impresión administrada	Administración / TI	Impresión institucional	Media/Media/Media

Tabla 7. Inventario de activos - clasificación, propietario, proceso y criticidad CIA.

Código	Ubicación	Responsable operativo	Dependencia tecnológica	Justificación / impacto de compromiso
ACT-INT-01	Site / BD institucional	Jefatura de Servicios Escolares	Servidor BD Oracle/MySQL, respaldos, red interna	Almacena matrículas, calificaciones, reinscripciones y expedientes; su compromiso afecta continuidad académica y datos personales.
ACT-INT-02	Aplicación institucional	Servicios Informáticos	Aplicación web, BD escolar, autenticación institucional	Procesa inscripciones, horarios y consultas académicas; es crítico en periodos de inscripción.
ACT-INT-03	Site principal	Administrador de infraestructura	AD/LDAP, DNS, políticas de grupo	Concentra cuentas y privilegios; su falla habilita accesos indebidos o indisponibilidad masiva.
ACT-INT-04	Site principal	Administrador de sistemas	NAS/Servidor Windows, permisos SMB	Contiene documentos administrativos, oficios y evidencias; requiere control de acceso granular.
ACT-INT-05	Oficinas administrativas	Responsable administrativo	Aplicación contable, BD financiera	Maneja presupuestos, pagos y registros contables; afecta cumplimiento y reputación institucional.
ACT-INT-06	Área de RRHH	Responsable de RRHH	Aplicación nómina, BD laboral	Procesa datos laborales, percepciones y deducciones; su fuga impacta privacidad del personal.
ACT-INT-07	Edificios administrativos	Equipo de redes	Switches administrables, VLAN, cableado	Transporta tráfico de áreas críticas; segmentación incorrecta permite movimiento lateral.
ACT-INT-08	Campus completo	Equipo de redes	APs, controlador WLAN, RADIUS	Punto de entrada masivo para estudiantes, docentes y visitantes; requiere autenticación y segmentación.
ACT-INT-09	Site / borde de red	Administrador de redes	Firewall UTM, reglas, VPN	Filtra tráfico entrante/saliente; una mala regla expone servicios internos.
ACT-INT-10	Site principal	Administrador de respaldos	Software backup, almacenamiento local	Permite recuperar datos críticos; si falla aumenta impacto de ransomware o error humano.
ACT-INT-11	Share interno / wiki	Responsable SGSI/TI	Wiki, repositorio documental	Incluye configuraciones, diagramas y procedimientos; exposición facilita ataques.
ACT-INT-12	Ventanillas y oficinas	Coordinación del área	PCs institucionales, SO, antivirus	Procesan expedientes y solicitudes; malware o robo afecta datos de estudiantes.

Código	Ubicación	Responsable operativo	Dependencia tecnológica	Justificación / impacto de compromiso
ACT-INT-13	Oficinas financieras	Responsable financiero	PCs institucionales, app contable	Manejan información financiera y credenciales de sistemas de pago.
ACT-INT-14	Laboratorios	Responsable de laboratorio	PCs, imágenes, red académica	Usados por múltiples estudiantes; requieren aislamiento para evitar abuso o propagación de malware.
ACT-INT-15	Campus y site	Seguridad patrimonial	Cámaras IP, NVR, red CCTV	Apoya seguridad física; exposición puede afectar privacidad y vigilancia.
ACT-INT-16	Mesa de ayuda	Coordinador de soporte	Helpdesk, correo, base de tickets	Registra incidentes, accesos y solicitudes; permite trazabilidad operativa.
ACT-INT-17	Repositorio SGSI	Responsable SGSI	Hoja controlada / CMDB	Base para riesgos y auditoría; si está desactualizado impide control real.
ACT-INT-18	Site principal	Administrador de sistemas	VMware/Proxmox/Linux/Windows	Alojan aplicaciones críticas; vulnerabilidades afectan servicios internos.
ACT-INT-19	Site principal	Mantenimiento / TI	UPS, reguladores, planta	Sostiene disponibilidad de servicios ante fallas eléctricas.
ACT-INT-20	Repositorio controlado	Responsable SGSI	Políticas, matrices, actas	Evidencia principal para auditoría y mejora continua.
ACT-EXT-01	Proveedor SaaS	Administrador de correo	Google Workspace/M365, MFA	Medio principal de comunicación y recuperación de cuentas; phishing impacta a toda la comunidad.
ACT-EXT-02	Proveedor cloud	Administrador LMS	Moodle/Canvas, BD externa	Gestiona materiales, tareas y evaluaciones; indisponibilidad afecta clases.
ACT-EXT-03	Hosting externo	Webmaster / TI	CMS, hosting, DNS	Representa identidad pública; defacement afecta reputación y confianza.
ACT-EXT-04	Registrador/NIC	Administrador DNS	DNS, registros MX/TXT	Controla correo, web y servicios; secuestro impacta operación y reputación.
ACT-EXT-05	CA externa	Administrador web	Certificados SSL/TLS	Garantizan cifrado e identidad; expiración causa fallas de acceso y alertas.
ACT-EXT-06	ISP	Equipo de redes	Fibra dedicada, router ISP	Sin enlace no hay acceso a servicios externos ni navegación institucional.

Código	Ubicación	Responsable operativo	Dependencia tecnológica	Justificación / impacto de compromiso
ACT-EXT-07	ISP alterno	Equipo de redes	Fibra/backup LTE	Reduce riesgo de indisponibilidad por caída del proveedor principal.
ACT-EXT-08	Proveedor bancario	Responsable financiero	API/portal bancario	Procesa pagos de inscripción y trámites; fraude impacta finanzas y usuarios.
ACT-EXT-09	Proveedor cloud	Administrador backup	Storage cloud, cifrado	Asegura recuperación fuera del sitio ante ransomware o daño físico.
ACT-EXT-10	Proveedores software	Responsable de laboratorio	Matlab, Autodesk, etc.	Permite uso legal de herramientas; fallas afectan clases y prácticas.
ACT-EXT-11	Proveedor SaaS	Administrador TI	Zoom/Teams/Meet	Soporta reuniones y clases remotas; requiere control de cuentas y privacidad.
ACT-EXT-12	Proveedor SaaS	TI / dueños de área	Drive/OneDrive/SharePoint	Almacena documentos sensibles; mala compartición expone datos personales.
ACT-EXT-13	Tercero autorizado	Administrador de redes	Contratos, accesos temporales	Puede tener acceso privilegiado; requiere acuerdos y control de accesos.
ACT-EXT-14	SOC/MSSP potencial	Responsable SGSI	SIEM/SOC administrado	Apoya detección; exige confidencialidad sobre logs y eventos.
ACT-EXT-15	PAC/Proveedor	Responsable financiero	Portal PAC, certificados	Maneja datos fiscales y certificados; requiere control de credenciales.
ACT-EXT-16	Dependencia externa	Responsable administrativo	Portal gubernamental	Permite reportes oficiales; credenciales comprometidas impactan cumplimiento.
ACT-EXT-17	Proveedor externo	Comunicación social	Facebook/Instagram/X/Twitter	Afecta imagen e imputación; secuestro genera desinformación institucional.
ACT-EXT-18	Proveedor externo	Responsable biblioteca	Repositorio bibliográfico	Administra acceso a recursos académicos y cuentas de usuario.
ACT-EXT-19	Proveedor seguridad	Administrador seguridad	Consola cloud EDR	Detecta malware en endpoints; mala configuración reduce defensa.
ACT-EXT-20	Proveedor externo	Responsable administrativo	Multifuncionales, cola de impresión	Puede procesar documentos sensibles; requiere control de retención e impresión segura.

Tabla 8. Inventario de activos - ubicación, responsable, dependencia tecnológica e impacto.

5 Liderazgo

5.1. Política general de seguridad de la información

La Alta Dirección de la UPSLP establece que la información académica, administrativa, financiera, laboral, tecnológica y documental debe protegerse mediante controles proporcionales al riesgo, cumplimiento legal aplicable, responsabilidades definidas y mejora continua. Esta política aplica a estudiantes, docentes, personal administrativo, personal técnico y proveedores con acceso autorizado a activos institucionales.

Objetivo: preservar confidencialidad, integridad y disponibilidad de los activos dentro del alcance del SGSI.
Alcance: servicios digitales críticos, red institucional, sistemas administrativos, plataformas académicas, información personal y procesos de soporte TIC.
Compromiso de dirección: asignar responsables, aprobar recursos razonables, revisar indicadores, atender no conformidades y aceptar formalmente riesgos residuales.

5.2. Diez políticas específicas del SGSI

Las políticas se diseñan para que no queden como declaraciones genéricas: cada una incluye estándar obligatorio, directriz recomendada, procedimiento ejecutable y línea base de cumplimiento. De esta forma se cumple la función de liderazgo y se conecta con activos, riesgos, responsables y auditoría.

ID	Política	Estándar obligatorio	Directriz recomendada	Procedimiento específico	Línea base
POL-01	Gestión de identidades y accesos	Todo acceso a sistemas críticos debe estar asignado a una cuenta individual, con rol autorizado y revisión periódica.	Aplicar MFA en cuentas administrativas y privilegiadas; evitar cuentas compartidas.	Alta/baja/cambio mediante ticket autorizado por dueño de información; TI aplica rol y registra evidencia.	100 % de cuentas privilegiadas identificadas y revisadas trimestralmente.
POL-02	Uso aceptable de red y servicios institucionales	La red institucional solo debe usarse para fines académicos, administrativos y operativos autorizados.	Separar perfiles de red: alumnos, docentes, administrativos, invitados y proveedores.	Autenticar acceso, aplicar VLAN, registrar eventos relevantes y bloquear abuso confirmado.	Red Wi-Fi con autenticación institucional y segmento de invitados aislado.
POL-03	Protección de datos personales	Los datos personales deben tratarse bajo confidencialidad, mínima exposición y finalidad institucional.	Cifrar repositorios sensibles y evitar compartir listas por canales personales.	Clasificar documento, validar destinatario, usar canal institucional y registrar incidentes de fuga.	Todo expediente académico o laboral debe tener propietario y nivel de confidencialidad.
POL-04	Respaldos y recuperación	Los activos críticos deben contar con respaldos programados, protegidos y probados.	Mantener al menos una copia fuera del sitio o en nube con cifrado.	Programar backup, verificar finalización, probar restauración y documentar resultado.	Servicios críticos con RPO máximo 24 h y prueba de restauración trimestral.
POL-05	Gestión de cambios	Todo cambio en sistemas, red o seguridad debe evaluarse antes de aplicarse.	Usar ventana de mantenimiento y plan de reversa para cambios de alto impacto.	Solicitar cambio, evaluar riesgo, aprobar, ejecutar, validar y cerrar evidencia.	Cambios críticos con aprobación del Comité SGSI o responsable designado.
POL-06	Gestión de vulnerabilidades y parches	Los sistemas institucionales deben mantenerse actualizados según criticidad.	Priorizar parches críticos en servidores expuestos y endpoints administrativos.	Inventariar versión, evaluar CVSS, probar parche, desplegar y verificar.	Vulnerabilidades críticas atendidas en máximo 15 días o con control compensatorio.
POL-07	Respuesta a incidentes	Todo evento sospechoso debe reportarse, clasificarse y atenderse bajo procedimiento formal.	Definir canal único de reporte y roles de contención, erradicación y recuperación.	Registrar incidente, clasificar severidad, contener, preservar evidencia, recuperar y documentar lecciones.	Canal de reporte activo y bitácora de incidentes mantenida por TI/SGSI.
POL-08	Seguridad de proveedores	Los proveedores con acceso a información o sistemas deben cumplir requisitos de seguridad.	Firmar acuerdos de confidencialidad y usar cuentas temporales con mínimo privilegio.	Evaluar proveedor, aprobar acceso, registrar actividad y revocar al terminar servicio.	100 % de proveedores críticos con responsable interno y acceso documentado.
POL-09	Concienciación y capacitación	La comunidad institucional debe recibir capacitación proporcional a su rol.	Realizar campañas antiphishing y cápsulas para manejo de datos personales.	Plan anual, sesiones, evaluación breve y registro de asistencia.	Al menos dos campañas de seguridad por semestre y evidencia de comunicación.
POL-10	Monitoreo y auditoría	Los controles críticos deben generar evidencia para detectar fallas y mejorar.	Usar logs centralizados para cuentas privilegiadas, correo y servicios críticos.	Recolectar logs, revisar alertas, documentar hallazgos y generar acciones correctivas.	Revisión mensual de eventos críticos y auditoría interna semestral.

Tabla 9. Políticas de seguridad con estándar, directriz, procedimiento y línea base.

5.3. Matriz RACI

ID	Política	R - Responsable	A - Aprobador	C - Consultado	I - Informado
POL-01	Gestión de identidades y accesos	TI / Dueño proceso	Rectoría / Comité	Jurídico / Dueños	Comunidad / Proveedores
POL-02	Uso aceptable de red y servicios institucionales	TI / Dueño proceso	Rectoría / Comité	Jurídico / Dueños	Comunidad / Proveedores
POL-03	Protección de datos personales	TI / Dueño proceso	Rectoría / Comité	Jurídico / Dueños	Comunidad / Proveedores
POL-04	Respaldos y recuperación	TI / Dueño proceso	Rectoría / Comité	Jurídico / Dueños	Comunidad / Proveedores
POL-05	Gestión de cambios	TI / Dueño proceso	Rectoría / Comité	Jurídico / Dueños	Comunidad / Proveedores
POL-06	Gestión de vulnerabilidades y parches	TI / Dueño proceso	Rectoría / Comité	Jurídico / Dueños	Comunidad / Proveedores
POL-07	Respuesta a incidentes	TI / Dueño proceso	Rectoría / Comité	Jurídico / Dueños	Comunidad / Proveedores
POL-08	Seguridad de proveedores	TI / Dueño proceso	Rectoría / Comité	Jurídico / Dueños	Comunidad / Proveedores
POL-09	Concienciación y capacitación	TI / Dueño proceso	Rectoría / Comité	Jurídico / Dueños	Comunidad / Proveedores
POL-10	Monitoreo y auditoría	TI / Dueño proceso	Rectoría / Comité	Jurídico / Dueños	Comunidad / Proveedores

Tabla 10. Matriz RACI por política de seguridad.

6 Planificación

6.1. Metodología de evaluación de riesgos

Elemento	Criterio
Probabilidad	Escala 1 a 5: 1 rara, 2 poco probable, 3 posible, 4 probable, 5 casi segura.
Impacto	Escala 1 a 5 considerando continuidad académica, datos personales, reputación, costo y cumplimiento.
Fórmula	Riesgo = Probabilidad × Impacto.
Interpretación	Bajo 1-6, Medio 7-12, Alto 13-19, Crítico 20-25.
Tratamiento	Mitigar, transferir, evitar/rechazar o aceptar con justificación y aprobación.
Priorización	Primero riesgos críticos y altos sobre activos de alta criticidad o datos personales.

Tabla 11. Metodología de riesgos utilizada.

6.2. Matriz de riesgos prioritaria

La matriz se divide en dos vistas para mantener legibilidad: la primera documenta amenaza, vulnerabilidad, consecuencia y puntuación; la segunda documenta tratamiento, control, tipo y prioridad. Ambas se conectan por el ID del riesgo.

ID	Activo	Amenaza	Vulnerabilidad	Consecuencia	I	P	Score	Nivel
R-01	ACT-EXT-01	Phishing y robo de credenciales	Usuarios sin MFA o baja conciencia	Acceso no autorizado, envío de correos fraudulentos y exposición de información	5	4	20	Crítico
R-02	ACT-INT-02	Interrupción en periodo de inscripción	Dependencia de servidor/proveedor sin prueba de continuidad	Suspensión de reinscripciones y atención escolar	5	3	15	Alto
R-03	ACT-INT-01	Acceso no autorizado a expedientes	Permisos excesivos y baja revisión de cuentas	Fuga o alteración de calificaciones y datos personales	5	3	15	Alto
R-04	ACT-INT-08	Acceso indebido o abuso de red	Segmentación insuficiente	Movimiento lateral o consumo indebido de recursos	4	4	16	Alto
R-05	ACT-INT-12	Ransomware en endpoint administrativo	Parches incompletos y apertura de adjuntos	Cifrado de documentos y afectación de atención escolar	5	3	15	Alto
R-06	ACT-EXT-08	Fraude o uso indebido de credenciales	Credenciales compartidas y baja segregación	Pagos alterados, pérdida económica y reclamos	5	3	15	Alto
R-07	ACT-INT-10	Respaldo inutilizable	No se prueban restauraciones	Imposibilidad de recuperación tras incidente	5	3	15	Alto
R-08	ACT-EXT-03	Defacement del sitio	CMS o plugins desactualizados	Daño reputacional y publicación de contenido falso	4	3	12	Medio
R-09	ACT-EXT-12	Exposición accidental de documentos	Compartición pública sin revisión	Fuga de datos personales o documentos internos	4	4	16	Alto
R-10	ACT-INT-09	Exposición de servicio interno	Reglas obsoletas o sin revisión	Acceso externo a servicios no autorizados	5	2	10	Medio
R-11	ACT-EXT-13	Abuso de acceso de tercero	Cuentas temporales no revocadas	Acceso no autorizado por proveedor o cuenta comprometida	4	3	12	Medio
R-12	ACT-INT-20	Pérdida de evidencia de auditoría	Gestión documental sin control de versiones	No conformidades y falta de trazabilidad	3	3	9	Medio

Tabla 12. Matriz de riesgos - valoración técnica.

ID	Política relacionada	Tratamiento	Control propuesto y forma de administración	Tipo de control	Pri.
R-01	POL-01/POL-09	Mitigar	MFA, campañas anti-phishing, bloqueo de adjuntos, reporte rápido	Preventivo Detectivo	1
R-02	POL-04	Mitigar	Respaldos, monitoreo, plan de continuidad, prueba de restauración	Preventivo Correctivo	2
R-03	POL-01/POL-03	Mitigar	RBAC, revisión trimestral, bitácoras, segregación de funciones	Preventivo Detectivo	3
R-04	POL-02	Mitigar	VLAN, RADIUS, red invitados, monitoreo de tráfico	Preventivo Detectivo	4
R-05	POL-06/POL-09	Mitigar	EDR, parches, bloqueo USB, respaldo y capacitación	Preventivo Detectivo Correctivo	5
R-06	POL-01/POL-10	Mitigar	MFA, usuarios nominales, conciliación, logs y doble aprobación	Preventivo Detectivo	6
R-07	POL-04	Mitigar	Pruebas de restauración, monitoreo de jobs, copia offline/cloud	Correctivo Preventivo	7
R-08	POL-06/POL-10	Mitigar	Parches, WAF básico, control de cuentas, monitoreo de integridad	Preventivo Detectivo	8
R-09	POL-03	Mitigar	DLP, revisión de enlaces, capacitación, permisos por grupo	Preventivo Detectivo	9
R-10	POL-05/POL-10	Mitigar	Revisión mensual de reglas, control de cambios, escaneo externo	Preventivo Detectivo	10
R-11	POL-08/POL-01	Mitigar	Cuentas temporales, NDA, bitácora, acceso supervisado	Preventivo Detectivo	11
R-12	POL-10	Mitigar	Repositorio controlado, versionado, responsables y respaldos	Preventivo	12

Tabla 13. Matriz de riesgos - tratamiento, controles y prioridad.

6.3. Justificación de priorización

Los riesgos R-01, R-04, R-02, R-03, R-05, R-06, R-07 y R-09 deben atenderse primero porque afectan cuentas institucionales, servicios académicos críticos, datos personales y continuidad operativa. R-01 se prioriza como crítico porque el correo institucional suele ser punto de entrada para recuperación de contraseñas, phishing, suplantación e incidentes encadenados. La administración del riesgo se realizará principalmente mediante mitigación, porque aceptar o transferir estos riesgos sin controles dejaría expuesta la operación académica.

6.4. Declaración de aplicabilidad resumida

Control ISO 27002:2022	Control aplicable	Estado	Justificación
5.9	Inventario de información y otros activos asociados	Aplicable	La planificación del SGSI depende de un inventario completo y trazable.
5.15	Control de acceso	Aplicable	Riesgos de credenciales, proveedores y datos personales.
5.16	Gestión de identidades	Aplicable	Cuentas institucionales, roles y bajas.
5.17	Información de autenticación	Aplicable	MFA y credenciales seguras.
5.19	Seguridad en relaciones con proveedores	Aplicable	Servicios cloud, ISP, pagos y mantenimiento.
5.24	Planificación y preparación de incidentes	Aplicable	Phishing, ransomware y fuga de información.
5.30	Preparación TIC para continuidad	Aplicable	Continuidad académica y administrativa.
8.8	Gestión de vulnerabilidades técnicas	Aplicable	Parches de portal, endpoints y servidores.
8.13	Respaldo de información	Aplicable	Recuperación ante ransomware o errores.
8.16	Actividades de monitoreo	Aplicable	Logs, alertas y auditoría de accesos.

Tabla 14. Declaración de aplicabilidad resumida de controles.

7 Soporte

7.1. Minuta formal de reunión

Fecha	20 de mayo de 2026
Asistentes	Rectoría, Servicios Informáticos, Servicios Escolares, Administración y Finanzas, Responsable SGSI, representante académico.
Objetivo	Presentar avance del SGSI, justificar la intervención y acordar próximos pasos para controles prioritarios.
Temas tratados	Alcance del SGSI, inventario de activos, riesgos críticos, políticas, MFA, respaldos, auditoría interna y campaña de concienciación.
Acuerdos	Validar alcance, aprobar políticas base, iniciar piloto MFA en cuentas privilegiadas, programar auditoría interna y campaña anti-phishing.
Responsables	Responsable SGSI coordina; TI ejecuta controles; dueños de información validan accesos; Rectoría aprueba política.
Próximos pasos	Publicar política, ejecutar procedimiento piloto, reunir evidencias, revisar indicadores y cerrar acciones correctivas.

Tabla 15. Minuta formal conectada con el avance del proyecto.

7.2. Explicación para alta dirección

Se está construyendo un SGSI para proteger los servicios que sostienen la operación académica y administrativa de la UPSLP. El beneficio no es solo técnico: permite reducir incidentes, demostrar cumplimiento, proteger datos personales, mejorar continuidad y evitar que la seguridad dependa de decisiones aisladas. Para dirección, el valor principal es contar con visibilidad sobre riesgos, responsables, prioridades y evidencia.

7.3. Presentación ejecutiva propuesta

Slide	Título	Mensaje ejecutivo
1	Por qué un SGSI	La universidad depende de servicios digitales críticos y datos personales.
2	Alcance	Se priorizan servicios académicos, administrativos, red, correo y proveedores TIC.
3	Riesgos principales	Phishing, ransomware, fuga de datos, caída de plataformas y abuso de privilegios.
4	Controles prioritarios	MFA, respaldos, segmentación, revisión de accesos, capacitación y monitoreo.
5	Decisiones requeridas	Aprobar política, responsables, recursos mínimos y revisión periódica.
6	Indicadores	Incidentes, MFA, respaldos probados, capacitación y hallazgos cerrados.

Tabla 16. Guion de presentación ejecutiva para alta dirección.

7.4. Lenguaje técnico vs. lenguaje ejecutivo

Lenguaje técnico	Lenguaje ejecutivo
Implementar MFA en cuentas privilegiadas y revisar RBAC.	Reducir la probabilidad de accesos no autorizados a sistemas críticos.
Probar restauración de backups con RTO/RPO definidos.	Asegurar que la universidad pueda recuperarse después de una falla o ransomware.
Segmentar VLAN para alumnos, docentes e invitados.	Limitar el daño si una cuenta o dispositivo queda comprometido.
Centralizar logs y revisar eventos críticos.	Tener evidencia y alertas para detectar incidentes a tiempo.

Tabla 17. Distinción entre comunicación técnica y ejecutiva.

8 Operación

8.1. Política seleccionada para implementación operativa

Se implementa la **POL-01: Gestión de identidades y accesos**, porque se relaciona directamente con los riesgos R-01, R-03, R-06 y R-11. Esta política protege correo institucional, directorio activo, bases de datos, pasarela de pagos y accesos de proveedores. La medida operativa seleccionada es un **piloto de autenticación multifactor y revisión de cuentas privilegiadas**.

8.2. Procedimiento operativo replicable

Paso	Actividad	Ejecución técnica / administrativa	Evidencia
1	Identificar cuentas críticas	Exportar listado de administradores de correo, directorio activo, pasarela de pagos y sistema escolar.	EVID-OP-01
2	Validar propietario	Confirmar con dueño de proceso si cada cuenta sigue requerida.	EVID-OP-02
3	Clasificar privilegio	Marcar cuenta como administrativa, operador, consulta o proveedor temporal.	EVID-OP-03
4	Activar MFA	Habilitar segundo factor en cuentas privilegiadas y correo institucional.	EVID-OP-04
5	Revocar cuentas obsoletas	Deshabilitar cuentas sin propietario o sin uso mayor a 90 días.	EVID-OP-05
6	Registrar excepción	Si una cuenta no puede usar MFA, documentar causa, vigencia y control compensatorio.	EVID-OP-06
7	Validar acceso	Probar inicio de sesión con MFA y confirmar acceso solo a sistemas autorizados.	EVID-OP-07
8	Monitorear eventos	Revisar intentos fallidos, inicios desde ubicaciones anómalas y cambios de rol.	EVID-OP-08
9	Cerrar ticket	Adjuntar evidencias, responsable, fecha y resultado.	EVID-OP-09

Paso	Actividad	Ejecución técnica / administrativa	Evidencia

Tabla 18. Procedimiento operativo para MFA y revisión de accesos.

8.3. Evidencia técnica simulada

EVID-OP-01 - Exportación de cuentas privilegiadas

```
Get-PrivilegedUsers -System Correo InstitucionalRole Admin
>cuentas_privilegiadas.csv
```

Resultado simulado: 18 cuentas privilegiadas detectadas; 14 activas justificadas; 3 obsoletas; 1 proveedor temporal sin fecha de expiración.

EVID-OP-04 - Configuración MFA

Panel de administración simulado: MFA habilitado para administradores de correo, sistema escolar y pasarela de pagos. Estado: **Enabled**. Método permitido: aplicación autenticadora o token. Excepción temporal: ninguna.

EVID-OP-07 - Validación posterior

Prueba 1: usuario administrativo inicia sesión con contraseña correcta y segundo factor válido: **permitido**.
Prueba 2: contraseña correcta sin segundo factor: **bloqueado**.
Prueba 3: cuenta de proveedor fuera de ventana autorizada: **bloqueado**.
Conclusión: el control funciona para reducir acceso no autorizado por credenciales robadas.

8.4. Responsables, frecuencia y posibles fallos

Elemento	Responsable	Frecuencia	Posibles fallos / respuesta
Revisión de cuentas	Dueño del proceso + TI	Trimestral	Cuentas sin dueño: deshabilitar preventivamente y escalar.
MFA privilegiado	Servicios Informáticos	Permanente	Usuario sin segundo factor: recuperación por mesa de ayuda con validación de identidad.
Proveedores	Responsable interno	Por servicio	Cuenta no revocada: fecha de expiración obligatoria y revisión semanal.
Logs de acceso	TI / SGSI	Mensual	Eventos anómalos: abrir incidente y preservar evidencia.

Tabla 19. Responsables y criterios de operación del control.

9 Evaluación del desempeño

9.1. Formatos de auditoría profesional

9.1.1. Checklist de auditoría interna

ID	Criterio auditado	Estado	Evidencia observada	Relación
AUD-01	Existe política general aprobada y comunicada.	Cumple	Política SGSI v1.0, minuta de aprobación.	POL-01 a POL-10
AUD-02	Las cuentas privilegiadas tienen MFA.	Parcial	14/18 cuentas con MFA; 3 obsoletas y 1 proveedor pendiente.	POL-01/R-01
AUD-03	Hay inventario de activos con propietario y CIA.	Cumple	Inventario ACT-INT/EXT con 40 activos.	Sección 04
AUD-04	Respaldos críticos tienen prueba de restauración.	Parcial	Última prueba documentada solo para sistema escolar.	POL-04/R-07
AUD-05	Proveedores críticos tienen acceso documentado.	Parcial	Proveedor de mantenimiento sin fecha de expiración.	POL-08/R-11
AUD-06	Incidentes se registran en canal formal.	Cumple	Tickets INC-2026-014 a INC-2026-018.	POL-07
AUD-07	Campañas anti-phishing tienen evidencia.	No cumple	No se encontró lista de asistencia o reporte de campaña reciente.	POL-09/R-01

Tabla 20. Checklist de auditoría interna simulado.

9.1.2. Guía de entrevista

ID	Entrevistado	Pregunta clave
ENT-01	Rectoría	¿Cómo revisa dirección los riesgos residuales y recursos del SGSI?
ENT-02	Servicios Informáticos	¿Cómo se autorizan altas, bajas y cambios de privilegios?
ENT-03	Servicios Escolares	¿Quién aprueba accesos a expedientes académicos?
ENT-04	Finanzas	¿Cómo se protege la pasarela de pagos y credenciales bancarias?
ENT-05	Proveedor TIC	¿Qué controles siguen al acceder remotamente a la infraestructura?

Tabla 21. Formato de entrevista para auditoría.

9.2. Hallazgos y plan de acción

ID	Tipo	Hallazgo	Prioridad	Acción correctiva	Responsable / fecha
H-01	No conformidad menor	No todas las cuentas privilegiadas tienen MFA activo.	Alta	Activar MFA y deshabilitar cuentas obsoletas.	TI / 30 mayo 2026
H-02	Observación	Pruebas de restauración incompletas.	Media	Calendarizar pruebas trimestrales para activos críticos.	TI / 15 junio 2026

ID	Tipo	Hallazgo	Prioridad	Acción correctiva	Responsable / fecha
H-03	No conformidad menor	Proveedor sin fecha de expiración de acceso.	Alta	Crear cuenta temporal con expiración y responsable interno.	Redes / 25 mayo 2026
H-04	Oportunidad de mejora	Campaña anti-phishing sin evidencia reciente.	Media	Ejecutar campaña y registrar asistencia/resultados.	SGSI / 10 junio 2026

Tabla 22. Hallazgos, no conformidades, observaciones y acciones.

9.3. Resultado ejecutivo de auditoría

El estado general del SGSI se clasifica como **madurez inicial controlada**. Existen elementos documentales sólidos: alcance, inventario, políticas, riesgos y procedimiento operativo. Sin embargo, la auditoría simulada identifica brechas en MFA total, pruebas de restauración, control de proveedores y evidencia de capacitación. La prioridad ejecutiva es cerrar H-01 y H-03 por estar vinculados con accesos privilegiados y riesgo de credenciales.

10 Mejora

10.1. Incidente verosímil: phishing a cuenta administrativa

Resumen ejecutivo del incidente

El 18 de mayo de 2026 se detectó que una cuenta administrativa recibió un correo de phishing simulando una notificación de actualización de contraseña. La cuenta ingresó sus credenciales en un sitio falso; posteriormente se observaron intentos de acceso al correo institucional desde una ubicación no habitual. Los activos afectados fueron correo institucional (ACT-EXT-01), directorio de identidades (ACT-INT-03) y nube colaborativa (ACT-EXT-12). El impacto potencial fue exposición de documentos internos y envío de correos fraudulentos.

10.2. Respuesta ejecutiva

La respuesta no debe saturar a dirección con comandos. Lo importante es explicar: **qué ocurrió**, **cómo ocurrió**, **qué activos se afectaron**, **qué se hizo para contener** y **qué debe cambiar para que no se repita**. Se bloqueó la sesión sospechosa, se restableció contraseña, se activó MFA, se revisaron reglas de reenvío, se preservaron logs y se inició campaña anti-phishing.

10.3. Medidas para evitar recurrencia

- MFA obligatorio para cuentas administrativas y privilegiadas.
- Campaña anti-phishing semestral con simulación y medición.
- Revisión de reglas de reenvío y sesiones activas en correo institucional.
- Playbook de respuesta a phishing con roles, tiempos y evidencias.
- Ajuste de POL-01 y POL-09 para incluir control mínimo obligatorio.

- Monitoreo de inicios de sesión anómalos y bloqueo automático.

10.4. Material de prevención para usuarios finales

La mejora del SGSI no se limita a controles técnicos. Para reducir recurrencia del incidente, se propone una campaña interna breve, visual y fácil de recordar. El material está pensado para estudiantes, docentes y personal administrativo, por lo que evita lenguaje excesivamente técnico y se enfoca en conductas concretas.

Campaña interna UPSLP: Alto al phishing

PAUSA - VERIFICA - REPORTA

Antes de escribir tu contraseña, confirma que el mensaje sea legítimo.

1

Pausa

No respondas con prisa a correos que amenazan con bloquear tu cuenta, perder acceso o generar una sanción inmediata.

2

Verifica

Revisa dominio, remitente, enlace, ortografía y solicitud. La UPSLP no debe pedir contraseñas por correo o formularios externos.

3

Reporta

Si el mensaje es sospechoso, no abras adjuntos ni enlaces. Reenvíalo a Mesa de Ayuda o al canal SGSI definido.

Guía breve para usuarios finales: revisión de 60 segundos

Remitente	¿El correo proviene de una cuenta institucional o proveedor autorizado? Desconfía de dominios parecidos o cuentas personales.
Enlace	Pasa el cursor sobre el vínculo y valida el dominio antes de abrirlo. Si usa acortadores o dominios extraños, repórtalo.
Solicitud	Ningún área debe pedir contraseña, token, código MFA o datos bancarios por correo.
Urgencia	Frases como “último aviso”, “bloqueo inmediato” o “verificación obligatoria” son señales de presión.
Adjuntos	No abras archivos inesperados, especialmente si solicitan habilitar macros, iniciar sesión o descargar complementos.
Reporte	Conserva el correo y repórtalo; no lo borres de inmediato porque puede servir como evidencia.

Mensaje sugerido para difusión institucional

Asunto: Prevención de phishing - protege tu cuenta UPSLP

Antes de ingresar tus credenciales, revisa el remitente, el enlace y el motivo de la solicitud. La universidad no solicitará tu contraseña por correo electrónico ni por formularios externos no autorizados. Si recibes un mensaje urgente, amenazante o sospechoso, no abras enlaces ni archivos adjuntos; repórtalo a Mesa de Ayuda o al canal definido por el SGSI. Tu reporte puede evitar el compromiso de más cuentas institucionales.

Elemento de campaña	Definición propuesta
Público objetivo	Estudiantes, docentes, personal administrativo y personal técnico no especializado.
Formato	Flyer digital, cápsula de correo, cartel para laboratorios y recordatorio en plataforma académica.
Frecuencia	Una campaña semestral y refuerzos durante inscripción, exámenes y cambios de contraseña.
Indicador	Tasa de reporte de correos sospechosos, tasa de clic en simulaciones y porcentaje de usuarios capacitados.
Responsable	Responsable SGSI con apoyo de Servicios Informáticos y Comunicación Institucional.

Tabla 23. Diseño de campaña preventiva para usuarios finales.

10.5. Conexión con mejora continua

El incidente se convierte en insumo de mejora del SGSI. No basta con cerrar el ticket: se actualiza la matriz de riesgos, se ajustan políticas, se mejora el procedimiento de MFA, se ejecuta capacitación y se mide si los usuarios reducen clics en simulaciones de phishing. La mejora continua queda registrada en acciones correctivas, responsables, fechas y revisión directiva.

11 Verificación final de cobertura del SGSI

Sección	Elementos cubiertos	Evidencia en documento
01 Alcance	Empresa verosímil; misión, visión, objetivos; organigrama; dirección-área-proceso-actividad; justificación; límites y exclusiones.	Sección 1 completa.
02 Referencias	ISO/IEC 27001; familia ISO 27; riesgos; controles; normas pertinentes; APA.	Sección 2 y referencias.
03 Términos	Términos clave, condiciones, confidencialidad, evidencias y responsabilidades.	Sección 3.
04 Contexto	40 activos internos/externos, propietario, ubicación, proceso, dependencia, CIA y trazabilidad.	Sección 4.
05 Liderazgo	Política general, 10 políticas, estándar, directriz, procedimiento, línea base y RACI.	Sección 5.
06 Planificación	Metodología, riesgos conectados a activos y políticas, tratamiento, controles y priorización.	Sección 6.
07 Soporte	Minuta, explicación ejecutiva, presentación y lenguaje ejecutivo/técnico.	Sección 7.
08 Operación	Política implementada, procedimiento paso a paso, evidencia, validación, responsables y replicabilidad.	Sección 8.
09 Evaluación	Checklist, entrevistas, hallazgos, acciones correctivas y resultado ejecutivo.	Sección 9.
10 Mejora	Ataque verosímil, explicación a dirección, medidas de recurrencia, material preventivo y mejora continua.	Sección 10.

Tabla 24. Checklist de trazabilidad para verificar la cobertura integral del SGSI.

Conclusión

La propuesta desarrolla un SGSI institucional realista para la UPSLP y conecta todos los elementos evaluables: alcance, referencias normativas, términos, contexto, activos, liderazgo, riesgos, soporte, operación, auditoría y mejora. El valor del documento está en la trazabilidad: cada riesgo proviene de activos identificados, cada control responde a una política y cada evidencia permite demostrar avance ante auditoría. Con este enfoque, la seguridad deja de ser una responsabilidad aislada de TI y se convierte en un sistema de gestión institucional con responsables, medición y mejora continua.

Referencias

Computer Security Resource Center. (s. f.). *Information Security Management System*. National Institute of Standards and Technology.
FIRST. (s. f.). *Common Vulnerability Scoring System v3.1: Specification Document*.
International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements*. ISO.
International Organization for Standardization. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls*. ISO.
International Organization for Standardization. (2022). *ISO/IEC 27005 Information security risk management*. ISO.
López Contreras, S. (2026). *CNO V: Seguridad Informática. Material de clase S06 y lineamientos S08*. Universidad Politécnica de San Luis Potosí.