Manual de Políticas de Seguridad Informática

Versión: 1.0 Fecha de emisión: 05/mayo/ 2025

Coordinación: Dirección de Seguridad de la Información

Prólogo.

Tres desafíos institucionales que limitan la seguridad informática

La elaboración de políticas de seguridad informática enfrenta resistencias estructurales que van más allá de la técnica o la normativa. A continuación, se exponen los tres desafíos más comunes que obstaculizan su implementación efectiva:

- Desconocimiento directivo: Muchos altos ejecutivos perciben la seguridad informática como gasto y no como inversión, desconociendo su valor estratégico.
- Resistencia financiera: Los administradores limitan recursos sin medir los riesgos que ello implica para la continuidad y protección operativa.
- Miopía técnica: El personal técnico a menudo cree que medidas aisladas como firewalls o cifrado bastan, ignorando la necesidad de una gestión integral y preventiva.
- Una política de seguridad no elimina los riesgos: los revela y permite controlarlos. Su ausencia solo amplifica las amenazas.

Introducción

Este manual establece las políticas, especificaciones y lineamientos necesarios para garantizar la seguridad y la protección de la información, los activos digitales y los sistemas tecnológicos de la institución. Su elaboración se basa en las normas internacionales ISO/IEC 27001 y 27002, integrando buenas prácticas de las normas ISO 14001 (gestión ambiental) e ISO 50001 (gestión de la energía).

SECCIÓN I: Marco General

1. Fundamento y Establecimiento de Políticas

La seguridad informática es un componente esencial para la protección de los activos de información de la organización. Las políticas de seguridad deben ser establecidas por la Alta Dirección, con base en los siguientes lineamientos:

- Estar alineadas con la visión global del negocio y los objetivos estratégicos institucionales.
- Corroborar su cumplimiento mediante auditorías internas, métricas e indicadores de control.
- Asegurar que reflejen el alcance y misión del área de informática dentro de la organización.
- Integrar controles en todas las áreas de negocio, permitiendo un enfoque transversal y coordinado.
- Permitir que los distintos departamentos generen políticas internas complementarias, siempre que estén alineadas con las políticas organizacionales y validadas por la Dirección correspondiente.

2. Importancia de una Política de Seguridad Informática

Las políticas de seguridad informática son instrumentos normativos que permiten a la organización:

- Comunicarse de manera efectiva con los usuarios, estableciendo claramente las normas de actuación respecto al uso de los recursos tecnológicos.
- Prevenir incidentes relacionados con accesos no autorizados, uso indebido de información o afectación de la infraestructura digital.
- Establecer de forma explícita las responsabilidades, especificaciones y excepciones, junto con las sanciones aplicables en caso de incumplimiento.
- Fomentar una cultura organizacional basada en la protección de los sistemas de información.
- Deben redactarse en un lenguaje claro y directo, evitando tecnicismos o términos ambiguos que puedan prestarse a interpretaciones subjetivas o parciales.
- Las excepciones, deben ser aprobadas por el responsable de seguridad de la información, de forma escrita con tiempo determinado y en atención a una justificación técnica o funcional válida.

3. Distribución, Publicación, Aplicación y Actualización

- Todas las políticas deben ser distribuidas oficialmente a través de los canales institucionales.
- Su versión vigente debe permanecer publicada en un repositorio digital accesible para todos los colaboradores.

- La aplicación es obligatoria desde la fecha indicada y su desconocimiento no exime de responsabilidad.
- Se deben revisar anualmente o cuando ocurra una modificación sustancial en el entorno legal, técnico o organizacional.
- Cada política incluirá una tabla de control de cambios y la designación del responsable de su mantenimiento.

4. Base Normativa [Anexar otras normas y leyes, en atención a la nuevas políticas]

- ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información
- ISO/IEC 27002:2022 – Controles de Seguridad de la Información
- Legislación nacional en materia de protección de datos y delitos informáticos
- Reglamento Interno de Trabajo
- Manual de Normas y Procedimientos de Tecnología

5. Definiciones Clave

- Recurso tecnológico: Cualquier activo informático bajo control de la organización: hardware, software, redes, sistemas, servicios digitales o información almacenada.
- Especificación: Lista autorizada o criterio técnico formalmente definido por el área de TI.
- Excepción: Situación puntual que no aplica la norma general, debidamente autorizada por el área correspondiente.
- Evento de seguridad: Toda anomalía detectada en el comportamiento de los sistemas que pueda representar una amenaza a la confidencialidad, integridad o disponibilidad de la información.
- Activo informático: Todo recurso físico o digital con valor para la institución.

SECCIÓN II: Políticas de Seguridad Informática

Las políticas de seguridad informática son lineamientos institucionales que regulan el uso, protección y gestión de los recursos tecnológicos de la organización. Su objetivo es minimizar riesgos, proteger la información y garantizar la continuidad operativa, definiendo con precisión las responsabilidades, especificaciones y excepciones, para construir no solo sistemas seguros, sino una cultura digital resiliente, ética y consciente.

4.1. Uso Responsable de los Recursos Tecnológicos

Versión: 1.2 Fecha de entrada en vigor: 05/mayo/2025 Revisión prevista: 05/mayo/2026

A. Objetivo

Establecer los lineamientos específicos para el uso adecuado de los recursos tecnológicos institucionales, con el fin de garantizar la seguridad de la información, la continuidad operativa y el cumplimiento de las funciones laborales en el marco de la normativa vigente.

B. Alcance

Aplica a todo el personal interno o externo que, bajo cualquier relación laboral o contractual, tenga acceso a equipos, plataformas, redes o servicios informáticos de la organización, en modalidad presencial o remota.

C. Responsabilidad

El personal debe utilizar los recursos tecnológicos institucionales exclusivamente para el cumplimiento de sus funciones laborales, conforme a los objetivos operativos de su unidad.

D. Especificación

- El uso de hardware, software, red y servicios digitales debe limitarse a tareas descritas en el Manual de Funciones de cada unidad.
- Está prohibido utilizar dispositivos institucionales para actividades personales, comerciales, políticas, religiosas o ajenas a la organización.
- Solo podrán utilizarse plataformas, servicios de mensajería y aplicaciones previamente autorizadas por el área de Tecnología.
- Las conexiones remotas deberán realizarse en el horario laboral oficial y mediante los mecanismos aprobados de acceso seguro.
- Cualquier configuración, instalación o modificación de equipos o sistemas requiere autorización expresa del área de Tecnología.

E. Excepción

- Se permite el uso ocasional del equipo institucional con fines personales únicamente durante tiempos de receso (pausas laborales), limitado a navegación web no riesgosa, sin instalación de programas ni transferencia de archivos personales.
- El uso de software o herramientas no institucionales será autorizado temporalmente solo si:
  a) están directamente vinculadas con procesos de capacitación, evaluación o mantenimiento,
  b) existe una justificación técnica o funcional documentada, y
  c) cuentan con aprobación escrita del área de Tecnología y de Seguridad de la Información.
- Toda excepción tendrá una vigencia máxima de 30 días calendario, con opción de renovación mediante nueva solicitud formal justificada.

F. Sanciones

Nivel	Infracción	Sanción Aplicable	Procedimiento Disciplinario
Leve	Uso personal injustificado durante horas laborales	Amonestación por escrito	Registro en expediente; aviso formal a Recursos Humanos
Media	Uso de software no autorizado sin aprobación	Suspensión temporal de acceso hasta por 5 días hábiles	Informe técnico a Seguridad de la Información; audiencia breve con supervisor inmediato
Grave	Instalación de programas maliciosos o filtración de información institucional	Terminación del contrato, denuncia legal y bloqueo de acceso	Investigación formal por el Comité de Ética o Jurídico; reporte a Dirección General y RH

Todas las sanciones se ejecutarán conforme al Reglamento Interno de Trabajo y en coordinación con el área de Seguridad de la Información y Recursos Humanos.

G. Control de Cambios

Versión	Fecha	Cambio realizado	Responsable
1.0	2023/05/01	Versión inicial	CISO
1.1	2024/05/01	Se incorpora sección de excepciones	CISO

SECCIÓN III: Resumen Operativo y Técnico de otras Políticas de Seguridad Informática

A continuación, se presentan los resúmenes operativos y técnicos correspondientes a diversas políticas clave de seguridad de la información. Cada uno cumple una función introductoria que orienta sobre el propósito funcional de la política, su relevancia en los procesos institucionales y el impacto técnico que conlleva su correcta aplicación. Estos deben entenderse como puntos de partida para el desarrollo detallado de cada política, tomando como guía los lineamientos establecidos en el presente manual.

4.1 Acceso a sistemas institucionales

- Resumen operativo: Regula el ingreso autorizado a plataformas digitales mediante cuentas institucionales y obliga al cierre de sesión tras su uso.
- Resumen técnico: Implementa controles de identidad, autenticación segura y privilegios mínimos (ISO/IEC 27001 A.9.1), con auditoría de accesos y revocación automatizada.

4.2 Acceso físico a instalaciones tecnológicas

- Resumen operativo: Controla la entrada a laboratorios, centros de datos, oficinas de TI y espacios restringidos.
- Resumen técnico: Aplica medidas como credenciales físicas, cerraduras electrónicas, bitácoras de acceso y videovigilancia conforme ISO/IEC 27002 A.11.1.

4.3 Manejo de información y datos personales

- Resumen operativo: Asegura que toda información sensible o personal sea tratada con confidencialidad y legalidad.
- Resumen técnico: Cumple con la Ley Federal de Protección de Datos (México), RGPD y las cláusulas 8.2 y 18.1 de ISO/IEC 27001.

4.4. Inicio y cierre de sesión

- Resumen operativo: Obliga a cerrar sesión en sistemas al finalizar el uso, evitando accesos indebidos en terminales compartidas.
- Resumen técnico: Permite trazabilidad completa mediante logs. Las sesiones inactivas deben cerrarse automáticamente (ISO/IEC 27002 A.9.4.2).

4.5 Instalación de software

- Resumen operativo: Solo se permite software autorizado; se documentan excepciones con justificación técnica.
- Resumen técnico: Se exige control de licencias, validación de proveedores y registro de instalación. Aplica ISO/IEC 27002 A.12.5.

4.6 Uso de internet institucional

- Resumen operativo: Delimita qué tipo de contenido está permitido y regula el uso recreativo o personal de la red.
- Resumen técnico: Se establece filtrado de contenido, control de tráfico y monitoreo con respaldo legal (ISO/IEC 27002 A.13.1.1).

4.7 Uso de plataformas de Inteligencia Artificial

- Resumen operativo: Autoriza su uso con fines educativos o institucionales, bajo supervisión y respeto a privacidad.
- Resumen técnico: Se aplican criterios éticos, revisión de fuentes y prohibición de uso no controlado, conforme a recomendaciones de UNESCO e ISO/IEC 23894 (ética en IA).

4.8 Correo electrónico institucional

- Resumen operativo: Prohíbe el uso personal intensivo, spam, o compartir credenciales del correo institucional.
- Resumen técnico: Se monitorean mensajes salientes, se filtran adjuntos y se previene phishing mediante DMARC, SPF y DKIM. Aplica ISO/IEC 27002 A.13.2.3.

4.9 Dispositivos de almacenamiento externo

- Resumen operativo: Toda memoria USB o disco externo debe escanearse con antivirus y preferentemente cifrarse.
- Resumen técnico: Se regula el uso con protocolos de control de dispositivos (DLP), cifrado AES y políticas de prevención de pérdida (ISO/IEC 27002 A.8.3.3).

4.10 Registro, monitoreo y auditoría de actividades

- Resumen operativo: Toda actividad digital en sistemas institucionales puede ser registrada bajo principios de legalidad y proporcionalidad.
- Resumen técnico: Logs, alertas y reportes de auditoría se conservan por 12 meses. Se sigue ISO/IEC 27001 A.12.4 y NIST SP 800-92.

4.11 Resguardo y respaldo de información

- Resumen operativo: Todo sistema debe respaldarse semanalmente y los respaldos deben almacenarse de forma segura.
- Resumen técnico: Se aplican mecanismos de backup incremental, pruebas de restauración y almacenamiento cifrado (ISO/IEC 27001 A.12.3).

4.12 Actualización y parches de seguridad

- Resumen operativo: Todo software debe actualizarse mensualmente; se priorizan vulnerabilidades críticas.
- Resumen técnico: Aplicación de parches mediante MDM o WSUS, con documentación del ciclo de revisión. ISO/IEC 27002 A.12.6.1.

4.13 Eliminación y destrucción de información

- Resumen operativo: La baja de equipos o discos debe incluir borrado seguro o destrucción física del medio.
- Resumen técnico: Se utilizan técnicas como DoD 5220.22-M, desmagnetización o destrucción mecánica (ISO/IEC 27040).

4.14 Gestión de residuos tecnológicos

- Resumen operativo: Se deben clasificar, documentar y entregar a recicladores certificados los residuos electrónicos.
- Resumen técnico: Aplica la ISO 14001 y la Ley General para la Prevención y Gestión Integral de Residuos (México) para evitar impactos ambientales y filtraciones de datos.

4.15 Gestión energética de los recursos TI

- Resumen operativo: Se fomenta el uso eficiente de energía: apagado programado, reducción de consumo, migración a equipos eficientes.
- Resumen técnico: Implementación de ISO 50001 en centros de datos, oficinas y servidores. Uso de medidores inteligentes y prácticas de eficiencia energética.

4.16 Derechos y responsabilidades digitales del personal técnico

- Resumen operativo: Define qué pueden y no pueden hacer los administradores con acceso privilegiado.
- Resumen técnico: Obliga a documentar acciones, respetar la privacidad, usar cuentas diferenciadas y generar trazabilidad (ISO/IEC 27001 A.9.2 y RGPD).

4.17 Prevención de violencia digital en entornos institucionales

- Resumen operativo: Prohíbe ciberacoso, suplantación de identidad y uso hostil de plataformas institucionales.
- Resumen técnico: Basado en la Ley Olimpia (México), ISO/IEC 27002 cláusula 7.2.2, y principios de dignidad digital. Se promueve canal de denuncias y monitoreo activo.

4.18 Cultura digital y ciberresiliencia del usuario

- Resumen operativo: Promueve capacitación continua, simulacros, y formación en buenas prácticas digitales.
- Resumen técnico: Aplica ISO/IEC 27001 A.7.2.2, ISO/IEC 27031 (ciberresiliencia) y 27002. Incluye planes de concientización y respuestas ante incidentes

Anexo A. Glosario

Autenticación	Proceso mediante el cual se verifica la identidad de un usuario, sistema o dispositivo, generalmente mediante contraseñas, tokens o biometría.
Ciberresiliencia	Capacidad de una organización para resistir, adaptarse y recuperarse ante ciberataques o interrupciones de TI.
Credenciales	Conjunto de datos (usuario/contraseña, tokens, certificados) que permiten a un individuo acceder a un sistema o servicio digital.
DLP (Data Loss Prevention)	Conjunto de herramientas y políticas que evitan la pérdida, fuga o mal uso de datos confidenciales.
Dispositivo externo	Cualquier equipo de almacenamiento portátil como USB, discos duros externos, tarjetas SD, etc.
Phishing	Técnica fraudulenta para obtener información confidencial (contraseñas, datos bancarios) haciéndose pasar por entidades confiables.
Privilegios mínimos	Principio de seguridad que establece que los usuarios solo deben tener acceso a la información estrictamente necesaria para su función.
Respaldo (backup)	Copia de seguridad de información crítica, almacenada de forma segura para ser recuperada en caso de pérdida o falla.
Sesión activa	Período en el que un usuario permanece autenticado y con acceso a un sistema.
Violencia digital	Acciones de hostigamiento, amenaza, suplantación o exposición sin consentimiento en medios digitales.

Anexo B. Rutas de denuncia y escalamiento

Objetivo: Permitir a cualquier usuario reportar incidentes, anomalías, violaciones a políticas o actos de violencia digital.

Medio	*Responsable*	*Tiempo de respuesta estimado*
Correo electrónico	[seguridad.informacion@institucion.mx]	24 a 48 horas
Plataforma de reportes	Sistema institucional reportes	24 horas
Línea telefónica	Mesa de ayuda	Inmediato (horario laboral)
Presencial	Coordinación de TI	Cita previa

Anexo C. Cronograma de revisión y actualización anual

Objetivo: Asegurar que las políticas se mantengan actualizadas conforme a cambios normativos, tecnológicos y contextuales.

Actividad	*Frecuencia*	*Responsable*	*Observaciones*
Revisión técnica de políticas	Anual	Responsable de Seguridad de la Información	Con base en ISO/IEC 27001 cláusula 5.1.1
Evaluación de cumplimiento y brechas	Anual	Auditoría interna TI	Se documentan hallazgos y recomendaciones
Revisión legal y normativo	Anual	Área Jurídica / Enlace Normativo	Se ajustan políticas ante cambios legales vigentes
Reunión del Comité de Seguridad Institucional	Anual	Dirección General + Coordinaciones TI	Aprobación de cambios
Publicación de versión actualizada del manual	Anual	Coordinación de Comunicación Interna	Se informa a toda la comunidad académica