OCHOA, IBÁÑEZ & TINOCO

- ABOGADOS, S.C. -

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

OCHOA, IBÁÑEZ & TINOCO

ABOGADOS, S.C.

Fecha de emisión: Enero 2026.
V. 1

Av. Cuauhtémoc No. 875, Piso Mezzanine, colonia Narvarte Poniente, 03020, Ciudad de México.
www.oit.mx

ÍNDICE

DECLARACIÓN INSTITUCIONAL 6
FINALIDAD Y OBJETIVOS 6
1. Finalidad 6
2. Objetivos específicos 7
2.1 Implementación de controles y recursos 7
2.2 Vigencia y actualización del marco normativo interno 7
2.3 SGSI y mejora continua 7
2.4 Gobierno, roles y rendición de cuentas 7
2.5 Gestión de riesgos e incidentes con evidencia 8
2.6 Cultura de seguridad y cumplimiento 8
ALCANCE / APLICABILIDAD 8
3. Alcance 8
3.1 Alcance organizacional 8
3.2 Alcance material (información y activos) 9
3.3 Alcance operativo (procesos y ciclo de vida) 9
3.4 Aplicabilidad contractual y a terceros 10
3.5 Exclusiones 10
4. POLÍTICA 10
4.1 Ejes temáticos de la Política (controlables y auditables) 10
4.2 Seguridad de la información 11
4.3 Responsabilidades y principios orientadores 12
4.4 Sistema de gestión de seguridad de la información (SGSI) 13
4.5 Nivel de cumplimiento 13
4.6 Estructura de gobierno 14
4.7 Uso, acceso y custodia (altas / cambios / bajas) 14
Política general 15
5. Controles 15
5.1 Controles minimos 15
5.2 Controles obligatorios 15
5.2 Políticas satélite (Anexos) 15
Cumplimiento, auditoría, sanciones y mejora continua 16
6. Cumplimiento 16
6.1 Auditoría y evidencias 16
6.2 Revisión y mejora continua 16
7. Auditoría y evidencias 17
8. Revisión y mejora continua 17
ANEXO 1. Definiciones 17
ANEXO 2. Controles organizacionales 20
1. Objetivo 20

2. Alcance 20
3. Principios generales 20
4. Controles organizacionales 20
5. Revisión 20
6. Sanciones 21
Formatos y evidencias mínimas 21
Formato: Registro de capacitación y concientización 21
Formato: Solicitud y aprobación de cambio (Change record) 21
ANEXO 3. Controles para la gestión del personal 22
1. Objetivo 22
2. Alcance 22
3. Controles por etapa 22
4. Responsabilidades 22
Formatos y evidencias mínimas 23
Formato: Checklist de onboarding 23
Formato: Checklist de offboarding 23
ANEXO 4. Controles para la gestión de activos e información 24
1. Objetivo 24
2. Controles clave 24
Formatos y evidencias mínimas 24
Formato: Inventario mínimo de activos 24
Formato: Matriz de clasificación de información 25
Formato: Acta de destrucción de medios/documentos 25
ANEXO 5. Controles para la gestión de accesos 26
1. Objetivo 26
2. Controles 26
Formatos y evidencias mínimas 26
Formato: Solicitud de alta/modificación de acceso 26
Formato: Revisión periódica de accesos 27
ANEXO 6. Controles físicos 28
1. Objetivo 28
2. Controles 28
Formatos y evidencias mínimas 28
Formato: Registro de visitantes 28
Formato: Bitácora de resguardo de expedientes físicos 29
ANEXO 7. Controles de seguridad operativa 30
1. Objetivo 30
2. Controles 30
Formatos y evidencias mínimas 30
Formato: Registro de respaldos y pruebas de restauración 30
Formato: Registro de vulnerabilidades y parches 31
ANEXO 8. Controles en telecomunicaciones y redes 32

1. Objetivo 32
2. Controles 32
Formatos y evidencias mínimas 32
Formato: Inventario de redes y accesos remotos 32
ANEXO 9. Controles para adquisición, desarrollo y mantenimiento de sistemas 33
1. Objetivo 33
2. Controles 33
Formatos y evidencias mínimas 33
Formato: Checklist de requisitos de seguridad por sistema 33
Anexo 10. Requisitos de seguridad para adquisición, desarrollo y mantenimiento de sistemas de información 34
1. Requisitos de seguridad de sistemas de información 34
2. Análisis y especificaciones de requisitos de seguridad de la información 34
3. Seguridad de la información en la gestión de proyectos 35
4. Seguridad de aplicaciones en redes públicas y procesamiento correcto 35
Validación de datos de entrada: 36
Control de procesamiento interno: 36
Transferencia de información: 36
Validación de datos de salida: 36
5. Seguridad en procesos de desarrollo y soporte 37
Responsabilidades de la función de Tecnología (interna o tercerizada): 37
6. Control de cambio en sistemas 38
7. Restricciones en los cambios de paquetes de software 38
8. Separación de ambientes 38
9. Principios de desarrollo 39
9.1 Desarrollo interno: 39
9.2 Desarrollo contratado a terceros: 40
ANEXO 11. Controles para la gestión de proveedores (TPRM/Nth parties) 41
1. Objetivo 41
2. Controles 41
Formatos y evidencias mínimas 41
Formato: Evaluación de proveedor (due diligence) 41
Formato: Declaración de Nth parties 42
ANEXO 12. Controles para la gestión de incidentes DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD 43
1. Objetivo 43
2. Alcance 43
3. Principios 43
4. Categorías y subcategorías de incidentes de ciberseguridad 43
5. Categorías de incidentes de seguridad de la información (no necesariamente ciberseguridad) 45
6. Criterios para clasificar un evento como incidente 45

7. Tabla de definición de criticidad de un incidente 46
8. Criterio de evaluación (puntaje) y nivel de criticidad 46
9. Reporte de eventos, incidentes y vulnerabilidades 47
10. Proceso de gestión de incidentes 47
10.1 Detección y triage 47
10.2 Contención 47
10.3 Erradicación 47
10.4 Recuperación 47
10.5 Cierre y lecciones aprendidas 47
11. Roles y responsabilidades (referencia RACI) 48
12. Recolección y preservación de evidencias 48
13. Tiempos máximos de atención 48
14. Comunicaciones internas y externas 49
15. Registro y métricas 49
16. Controles 49
Formatos y evidencias mínimas 50
Formato: Registro de incidente 50
Formato: Guía rápida de respuesta (primeros 60 minutos) 50
ANEXO 13. Controles para continuidad del negocio y recuperación 51
1. Objetivo 51
2. Controles 51
Formatos y evidencias mínimas 51
Formato: BIA (Análisis de impacto al negocio) 51
Formato: Plan de continuidad - Lista de verificación 52
ANEXO 14. Controles para cumplimiento 53
1. Objetivo 53
2. Controles 53
Formatos y evidencias mínimas 53
Formato: Inventario de obligaciones y controles 53
Formato: Plan de acción correctiva 54

DECLARACIÓN INSTITUCIONAL

Ochoa, Ibáñez & Tinoco Abogados, S.C. ("OIT Abogados") reconoce que, por la naturaleza de su práctica legal, administra y trata información altamente sensible y estratégica**,** incluyendo -de manera enunciativa mas no limitativa-expedientes y estrategias legales, comunicaciones con clientes y autoridades, datos personales, secretos industriales, información financiera y documentación corporativa.

En consecuencia, la seguridad de la información constituye un elemento esencial de la prestación del servicio profesional y un componente permanente de la gestión cotidiana del Despacho, y no un requisito meramente documental.

La presente Política establece un marco de control realista, verificable y exigente, orientado a:

i. Reducir riesgos materialmente relevantes;
ii. Prevenir y detectar incidentes; R
iii. Responder con oportunidad y evidencia;
iv. Asegurar la continuidad operativa; y
v. Demostrar a clientes y demás partes interesadas un compromiso institucional con buenas prácticas, proporcional a la naturaleza de la información y a los riesgos asociados.

OIT Abogados implementará y mantendrá esta Política mediante controles técnicos, procesos operativos, capacitación y concientización, así como registros y evidencias de cumplimiento, bajo un enfoque de mejora continua.

FINALIDAD Y OBJETIVOS

1. FINALIDAD

Establecer el marco corporativo de seguridad de la información y ciberseguridad de OIT Abogados, con el propósito de proteger sus activos de información -incluyendo expedientes y comunicaciones con clientes, información confidencial, datos personales y documentación corporativa- frente a riesgos y amenazas internas o externas, deliberadas o accidentales, a fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, así como de la legalidad, privacidad y confiabilidad de la información.

Asimismo, esta Política busca asegurar que la seguridad sea parte integral de la operación del Despacho y de la prestación del servicio profesional, salvaguardando la continuidad del negocio, la misión y los objetivos estratégicos de OIT Abogados, y brindando un marco de confianza a clientes, personal, autoridades y demás grupos de interés.

2. OBJETIVOS ESPECÍFICOS

Para el cumplimiento de la Finalidad anterior, OIT Abogados adopta los siguientes objetivos específicos:

2.1 Implementación de controles y recursos

Asegurar la implementación y operación de los controles de seguridad de la información y ciberseguridad previstos en esta Política y sus anexos, identificando responsables, recursos y, en su caso, la planeación de necesidades presupuestarias, sin que ello implique necesariamente la asignación de partidas adicionales, pudiendo priorizarse mediante reordenamiento de actividades, uso eficiente de herramientas y gestión basada en riesgo.

2.2 Vigencia y actualización del marco normativo interno

Mantener esta Política y las políticas satélite (por ejemplo: contraseñas, autenticación/MFA, accesos privilegiados, cifrado, logging/monitoring, vulnerabilidades, parches, antimalware, incidentes y continuidad) actualizadas, para asegurar su vigencia, efectividad y alineación con los riesgos reales del Despacho, cambios tecnológicos, requerimientos de clientes y obligaciones aplicables.

2.3 SGSI y mejora continua

Definir, implementar, operar, medir y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información (SGSI) proporcional al tamaño y nivel de riesgo de OIT Abogados, soportado en directrices y buenas prácticas, orientado a la prevención, detección, respuesta y recuperación ante incidentes, y a la generación de evidencias verificables.

2.4 Gobierno, roles y rendición de cuentas

Establecer un modelo de gobierno (Comité de Seguridad, Responsable de Seguridad, TI y responsables por área) con roles, responsabilidades y mecanismos de decisión y escalamiento claramente definidos, asegurando la segregación de funciones y la rendición de cuentas.

2.5 Gestión de riesgos e incidentes con evidencia

Identificar, evaluar y tratar los riesgos de seguridad; y contar con procedimientos para gestionar incidentes, incluyendo contención, investigación, comunicación, recuperación y lecciones aprendidas, manteniendo registros y evidencias suficientes para auditoría y para atender requerimientos de clientes.

2.6 Cultura de seguridad y cumplimiento

Fortalecer la concientización y capacitación del personal, promoviendo el uso seguro de herramientas y el resguardo del secreto profesional y la confidencialidad, con énfasis en prevención de phishing, manejo seguro de información y reporte oportuno de incidentes.

ALCANCE / APLICABILIDAD

La presente Política de Seguridad de la Información y Ciberseguridad se emite para dar cumplimiento a las obligaciones legales, reglamentarias y contractuales aplicables de OIT Abogados, así como para atender las expectativas de clientes, autoridades y demás partes interesadas en relación con la protección de la información y la continuidad de los servicios profesionales del Despacho.

3. ALCANCE

3.1 Alcance organizacional

La Política es de observancia obligatoria para:

- La Asamblea de Socios y Socios de OIT Abogados.
- Todo el personal del Despacho, incluyendo asociados, pasantes y practicantes, personal administrativo, y personal de TI o funciones tecnológicas.
- Personas contratadas bajo esquemas de servicios profesionales, honorarios, outsourcing o equivalentes, cuando por razón de su función traten información o utilicen sistemas del Despacho.

- Terceros y proveedores que, por la naturaleza del servicio contratado, tengan acceso (directo o indirecto) a información o sistemas de OIT Abogados, o participen en procesos que impacten activos de información.

3.2 Alcance material (información y activos)

La Política aplica a toda la información tratada por OIT Abogados, cualquiera que sea su formato o medio, incluyendo información:

- Digital, en papel o en cualquier soporte físico;
- Generada por el Despacho o recibida de clientes, contrapartes, autoridades o terceros;
- Relacionada con expedientes, comunicaciones, estrategias, datos personales, documentación corporativa, información financiera y cualquier otra información protegida por deberes de confidencialidad o secreto profesional.

Asimismo, aplica a todos los activos y sistemas utilizados para tratar, almacenar, transmitir o resguardar información, incluyendo -de manera enunciativa mas no limitativa.:

- Equipos de cómputo (endpoints) y dispositivos móviles;
- Correo corporativo, mensajería y herramientas de colaboración;
- Repositorios documentales y sistemas de gestión de archivos/expedientes;
- Aplicaciones, redes, accesos remotos y servicios en la nube;
- Respaldos, medios removibles, impresoras, escáneres y periféricos;
- Cuentas de usuario, credenciales, accesos privilegiados y registros de actividad (logs).

3.3 Alcance operativo (procesos y ciclo de vida)

La Política aplica a la totalidad de los procesos internos y externos que involucren activos de información, incluyendo el ciclo de vida de la información y de los sistemas: creación/recepción, clasificación, almacenamiento, acceso, uso, transmisión, resguardo, respaldo, retención, destrucción, y respuesta ante incidentes; así como adquisición/contratación, configuración, cambios, mantenimiento y baja de sistemas y servicios.

3.4 Aplicabilidad contractual y a terceros

En los contratos y acuerdos con terceros, OIT Abogados establecerá -en lo aplicable- la obligación de cumplir con esta Política y/o con controles equivalentes, incluyendo obligaciones de confidencialidad, seguridad, notificación de incidentes, y mecanismos de verificación y auditoría razonables conforme al nivel de riesgo.

3.5 Exclusiones

Cualquier exclusión o excepción al alcance de esta Política deberá quedar expresamente documentada, con su justificación, evaluación de riesgo, controles compensatorios y aprobación conforme al procedimiento de excepciones (en su caso).

4. POLÍTICA

La presente Política define el marco general de seguridad de la información y ciberseguridad de OIT Abogados, cuyo objetivo es proteger al Despacho frente a una amplia gama de amenazas -internas o externas, deliberadas o accidentales- para asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, así como su legalidad, privacidad y confiabilidad, minimizando el riesgo de daño y contribuyendo al cumplimiento eficiente de la misión y objetivos estratégicos del Despacho.

Los principios de esta Política forman parte de la cultura organizacional de OIT Abogados y se sustentan en el compromiso de los Socios, responsables de área y colaboradores para su difusión, consolidación y cumplimiento. Esta Política no se limita a enunciar controles: establece responsables, mecanismos de gobierno, evidencias mínimas y un ciclo de mejora continua.

4.1 Ejes temáticos de la Política (controlables y auditables)

Esta Política se desarrolla mediante directrices y políticas satélite que cubren, como mínimo, los siguientes aspectos:

- Organización de la seguridad: Gobierno, roles, responsabilidades, comité de seguridad, métricas, auditoría y mejora continua.
- Seguridad del recurso humano: Obligaciones de confidencialidad, capacitación, altas/cambios/bajas y disciplina.

- Clasificación y control de activos: Inventario, clasificación, manejo, retención y destrucción segura.
- Control de accesos e identidad: Acceso por roles, mínimo privilegio, MFA y revisiones periódicas.
- Cifrado y gestión de secretos: Cifrado en tránsito/en reposo, custodia de llaves/tokens y prácticas seguras.
- Seguridad física y del entorno: Protección de instalaciones, equipos, documentos físicos y "escritorio/pantalla limpia".
- Operación segura y comunicaciones: Administración segura de sistemas, respaldos, registros y monitoreo.
- Gestión de vulnerabilidades y parches: Identificación, priorización y remediación conforme a criticidad.
- Protección contra malware: Controles antimalware y respuesta ante detecciones.
- Relación con terceros: Evaluación proporcional, cláusulas contractuales mínimas y control de accesos.
- Gestión de incidentes: Reporte oportuno, contención, investigación, recuperación y lecciones aprendidas.
- Continuidad del negocio: Planes y pruebas de restauración para servicios críticos.

4.2 Seguridad de la información

Para efectos de esta Política, la seguridad de la información se entiende como la preservación de:

- Confidencialidad: La información solo estará disponible y será revelada a personas autorizadas y con necesidad de conocer.
- Integridad: La información debe mantenerse precisa, completa y consistente desde su creación hasta su destrucción.
- Disponibilidad: La información y los recursos necesarios deben estar accesibles cuando se requieran, dentro de los niveles de servicio definidos.
- Autenticidad: Se debe asegurar el origen y validez de la información (evitando suplantaciones).
- Trazabilidad: Se deben poder rastrear accesos y acciones relevantes sobre la información y los sistemas.

Adicionalmente, OIT Abogados considera como atributos esenciales:

- Legalidad y cumplimiento: cumplimiento de obligaciones aplicables (contractuales, regulatorias y legales), incluyendo compromisos de confidencialidad y secreto profesional.
- Privacidad: Protección de datos personales conforme a las obligaciones aplicables y a los compromisos con clientes.
- Confiabilidad: Que la información sea adecuada para la administración del Despacho y la prestación del servicio profesional; y que existan controles que permitan confiar razonablemente en su integridad y disponibilidad.
- Auditabilidad: Los eventos significativos de los sistemas deben quedar registrados, en la medida técnicamente viable, para control posterior e investigación (logs y evidencias).

4.3 Responsabilidades y principios orientadores

Esta Política aplica a todos los grupos de interés comprendidos en su alcance. En consecuencia, todas las personas obligadas deberán desplegar sus mejores esfuerzos para asegurar que su conducta se ajuste a los más altos estándares de disciplina y profesionalismo, preservando el buen funcionamiento de los sistemas y la protección de la información.

Se consideran violaciones graves, entre otras: el acceso no autorizado, la sustracción, alteración, divulgación indebida, destrucción no autorizada, uso indebido o secuestro de información confidencial o de cliente; así como el uso de credenciales ajenas, eludir MFA o instalar software no autorizado en sistemas del Despacho.

Responsabilidad transversal: Si bien todo el personal debe cumplir esta Política, los Socios y responsables de área son responsables de su aplicación dentro de sus procesos y de velar por el cumplimiento por parte de sus equipos.

Responsables clave:

- Asamblea de Socios: Aprueba la Política y cambios, supervisa desempeño, define prioridades y acepta riesgos residuales relevantes.
- Responsable de Seguridad de la Información: Coordina los riesgos, incidentes, auditorías, capacitación y evidencias; reporta a la Asamblea de Socios.
- Responsable de TI: Implementa controles técnicos (MFA, parches, antimalware, cifrado, respaldos, monitoreo) y mantiene bitácoras técnicas.

- Propietarios/Responsables de información por área: Definen accesos, necesidad de conocer, y validan la clasificación y manejo en su ámbito.
- Usuarios: Cumplen controles, protegen credenciales, reportan incidentes y completan capacitación.

4.4 Sistema de gestión de seguridad de la información (SGSI)

OIT Abogados implementa un SGSI proporcional a su tamaño, complejidad y nivel de riesgo, con alcance sobre los procesos y sistemas que impliquen tratamiento de información. El SGSI se integra, como mínimo, por:

- Política General (este documento) y políticas satélite obligatorias (Anexos).
- Inventario de activos, clasificación y reglas de manejo.
- Gestión de riesgos (matriz de riesgos, plan de tratamiento y aceptación de riesgos).
- Gestión de accesos (altas/cambios/bajas, MFA, revisión de accesos privilegiados).
- Controles técnicos mínimos (cifrado cuando aplique, parches, antimalware, respaldos, logging/monitoring).
- Gestión de incidentes y continuidad/recuperación.
- Capacitación y concientización.
- Evidencias y registros (formatos K-1 a K-17 o equivalentes).
- El Respomsable de Seguridad de la Información reportará periódicamente a la Asamblea de Socios el estado del SGSI, avances, hallazgos y planes de mejora.

4.5 Nivel de cumplimiento

El incumplimiento de esta Política podrá dar lugar a medidas internas conforme a las disposiciones aplicables del Despacho y, en su caso, a responsabilidades contractuales o legales, especialmente cuando se afecte información de clientes, datos personales o se comprometa el secreto profesional.

Todas las personas cubiertas por el alcance deberán dar cabal cumplimiento a esta Política y reportar oportunamente comportamientos o eventos que puedan comprometer la seguridad.

4.6 Estructura de gobierno

OIT Abogados adopta el siguiente esquema de gobierno mínimo:

- Asamblea de Socios: Órgano de supervisión y decisión operativa/estratégica en seguridad (riesgos, incidentes, prioridades, KPIs). Aprueban la Política y cambios relevantes; asignan recursos; deciden sobre riesgos residuales altos y excepciones relevantes.
- Responsable de Seguridad de la Información (RSI): Mantiene el SGSI, coordina riesgos, auditoría, capacitación, incidentes y evidencias.
- Responsable de TI: Ejecuta controles técnicos y administración segura de sistemas.
- Responsables de información por área: Definen y autorizan accesos en su ámbito.
- La Asamblea de Socios revisará la Política al menos anualmente y cuando existan cambios materiales (tecnológicos, riesgos, incidentes relevantes o requerimientos contractuales).

4.7 Uso, acceso y custodia (altas / cambios / bajas)

OIT Abogados establecerá y mantendrá un proceso formal de alta, modificación y baja de acceso, que asegure:

- Identificación del usuario y asignación de cuenta individual.
- Asignación de accesos conforme a mínimo privilegio y necesidad de conocer, con autorización del responsable de información del área.
- Habilitación obligatoria de MFA en los sistemas definidos como críticos.
- Revisión periódica de accesos, especialmente privilegiados/administrativos.
- Revocación oportuna de accesos ante bajas, cambios de rol o término de servicios.
- Registro de evidencias (formatos K-7, K-8 y bitácoras asociadas).

POLÍTICA GENERAL

5. CONTROLES

5.1 Controles minimos

Los controles mínimos se implementan mediante esta Política y las políticas satélite (Anexos). Salvo indicación en contrario, todos los controles aplican a información del Despacho y a información de clientes bajo custodia.

5.2 Controles obligatorios

Inventario y clasificación de información y activos; asignación de propietarios.

- Gestión de identidades y accesos: cuentas individuales, MFA donde aplique, revisiones periódicas, revocación inmediata al egreso.
- Protección de endpoints: cifrado de disco cuando aplique, antimalware, bloqueo de pantalla, actualizaciones y parches.
- Respaldo y recuperación: respaldos periódicos, pruebas de restauración, control de acceso a respaldos.
- Seguridad en correo y colaboración: anti-phishing, políticas de envío, manejo de adjuntos, uso de repositorios autorizados.
- Gestión de incidentes: canales de reporte, clasificación, contención, evidencia y lecciones aprendidas.
- Gestión de proveedores: evaluación proporcional, cláusulas de seguridad, monitoreo y offboarding.
- Continuidad del negocio: identificación de procesos críticos, planes, pruebas y mejoras.
- Cumplimiento: inventario de obligaciones, auditorías y tratamiento de hallazgos.

5.2 POLÍTICAS SATÉLITE (ANEXOS)

- Anexo 1: Definiciones.
- Anexo 2: Controles organizacionales (gobernanza, formación, proveedores, incidentes, proyectos y cambios).
- Anexo 3: Controles para la gestión del personal (antes, durante y después).

- Anexo 4: Controles para la gestión de activos e información (inventario, clasificación, uso aceptable, transferencia y disposición).
- Anexo 5: Controles para la gestión de accesos (identidades, autenticación, accesos privilegiados, terceros).
- Anexo 6: Controles físicos (zonas, visitantes, protección de equipos).
- Anexo 7: Controles de seguridad operativa (cambios, respaldos, malware, logging, vulnerabilidades).
- Anexo 8: Controles en telecomunicaciones y redes (perímetro, cifrado, VPN, monitoreo).
- Anexo 9: Controles para adquisición/desarrollo/mantenimiento de sistemas (SDLC, pruebas, cambios).
- Anexo 10: Controles para la gestión de proveedores (TPRM/Nth parties).
- Anexo 11: Controles para la gestión de incidentes (CSIRT, comunicación, post-mortem).
- Anexo 12: Controles para continuidad del negocio y recuperación (BIA, BCP, DRP).
- Anexo 13: Controles para cumplimiento (obligaciones, auditoría, acciones correctivas).

CUMPLIMIENTO, AUDITORÍA, SANCIONES Y MEJORA CONTINUA

6. CUMPLIMIENTO

El cumplimiento de esta Política es obligatorio. Su incumplimiento puede derivar en medidas disciplinarias, contractuales y/o legales, según la gravedad y la normativa aplicable.

6.1 Auditoría y evidencias

El RSI podrá realizar revisiones internas y solicitar evidencias (registros de accesos, bitácoras de cambios, reportes de respaldo, asistencias de capacitación, evaluaciones de proveedores, registros de incidentes, etc.).

6.2 Revisión y mejora continua

Esta Política y sus anexos se revisarán al menos una vez al año o cuando existan cambios significativos en riesgos, tecnología, estructura del Despacho, requerimientos de clientes o marco legal. Se documentarán hallazgos y planes de acción.

7. AUDITORÍA Y EVIDENCIAS

El RSI podrá realizar revisiones internas y solicitar evidencias (registros de accesos, bitácoras de cambios, reportes de respaldo, asistencias de capacitación, evaluaciones de proveedores, registros de incidentes, etc.).

8. REVISIÓN Y MEJORA CONTINUA

Esta Política y sus anexos se revisarán al menos una vez al año o cuando existan cambios significativos en riesgos, tecnología, estructura del Despacho, requerimientos de clientes o marco legal. Se documentarán hallazgos y planes de acción.

ANEXO 1. DEFINICIONES

Término	Definición
OIT Abogados	Ochoa, Ibáñez y Tinoco Abogados, S.C.
Administrador de la aplicación o del sistema	Persona designada para configurar el sistema y asignar, modificar o revocar permisos y funcionalidades conforme al rol del usuario y autorizaciones vigentes.
Acceso	Permitir, entrar y/o interactuar con información, sistemas, aplicaciones o áreas físicas autorizadas.
Acceso remoto	Conexión a recursos del Despacho desde una ubicación distinta (p. ej., VPN, escritorio remoto, acceso a nube).
Administración de riesgos	Proceso cíclico de identificar, analizar, evaluar, tratar y monitorear riesgos de seguridad de la información, aceptando riesgo residual con aprobación correspondiente.
Agente antimalware	Software/servicio destinado a prevenir, detectar y remover malware en endpoints y servidores.
Alerta de ciberseguridad	Notificación generada por herramientas o revisiones (p. ej., antimalware, correo, logs) sobre posible actividad maliciosa o anómala.
Autenticación	Proceso/proveedor para verificar la identidad de un usuario (p. ej., contraseña + MFA).
Autorización	Asignación de permisos a usuarios/cuentas para ejecutar acciones de acuerdo con rol y necesidad de conocer.
Ataque cibernético / Ciberataque	Acción deliberada destinada a comprometer confidencialidad, integridad o disponibilidad de sistemas o información (p. ej., phishing, ransomware).
Ciberseguridad	Conjunto de controles, procesos y capacidades para prevenir, detectar y responder a amenazas en el ciberespacio
Ciberamenaza	Situación potencial o actual que pudiera materializarse en un ciberataque o incidente.

Control de acceso	Mecanismos administrativos y técnicos para prevenir acceso no autorizado y permitir acceso autorizado.
Correo electrónico	Servicio para enviar/recibir mensajes electrónicos (texto/adjuntos) a través de sistemas de comunicación.
Cuentas de usuario	Identificador único asignado a una persona para acceder a sistemas y recursos del Despacho.
Cuenta de servicio	Cuenta técnica usada por aplicaciones/procesos para ejecutar tareas; no corresponde a una persona.
Cifrar	Aplicar un algoritmo y clave para transformar información a formato ininteligible para no autorizados.
Cifrado	Mecanismo criptográfico para proteger confidencialidad (y, cuando aplique, integridad) de la información en tránsito y/o en reposo.
Datos personales	Información relativa a una persona identificada o identificable, tratada por OIT como responsable o encargado según aplique.
Dispositivo móvil	Equipo portátil con capacidad de procesamiento y conectividad (smartphone, tableta, laptop).
Ejecutor del control de accesos	Rol operativo encargado de implementar altas, bajas y cambios de accesos conforme a autorizaciones aprobadas.
Evaluación de riesgos	Análisis de amenazas y vulnerabilidades para estimar probabilidad e impacto y determinar tratamiento.
Evento de ciberseguridad	Ocurrencia que puede afectar la seguridad; puede ser indicio de incidente o falsa alarma.
Falsa alarma	Evento que tras análisis inicial se descarta como incidente real.
Información sensible	Información que requiere medidas reforzadas por su valor/obligaciones (expedientes, estrategia, secretos industriales, financieros, credenciales, datos personales).
Identificación y autenticación	Registro y verificación de identidad para acceso, mediante credenciales y, cuando aplique, MFA.
Incidente de seguridad o ciberseguridad	Ocurrencia que compromete o amenaza seguridad de información/sistemas, incluyendo acceso no autorizado, malware, fuga, pérdida o indisponibilidad.
Incidente significativo	Incidente con impacto alto (legal, reputacional, operativo o financiero) o afectación prolongada; requiere escalamiento.
Incidente menor	Incidente controlable sin afectar significativamente la operación; requiere registro y cierre.
Información	Cualquier representación de conocimiento (datos) en cualquier forma y medio.
Información en reposo	Datos almacenados en medios persistentes (discos, nube, respaldos, dispositivos).
Información en tránsito	Datos que se transmiten por redes públicas o privadas.
Instancia en nube	Servidor/entorno virtual en nube donde se alojan sistemas, servicios o aplicaciones.
Impacto	Magnitud del daño en caso de materializarse una amenaza sobre un activo.

Llaves criptográficas	Claves/secretos/tokens utilizados para cifrar/descifrar o firmar/verificar; deben gestionarse y protegerse.
Personal	Cualquier persona vinculada al Despacho (laboral o por prestación de servicios) que trate información o use sistemas.
Perfil	Conjunto de permisos y capacidades asignadas a un usuario/rol para ejecutar funciones específicas en sistemas.
Recurso informático	Elementos tecnológicos que facilitan servicios de TI (equipos, redes, sistemas, aplicaciones, nube).
Responsable de la información	Persona/área dueña del proceso que determina clasificación y quién accede a la información bajo su custodia.
Responsable de la política	Rol encargado de supervisar cumplimiento de la política y asesorar a usuarios (RSI).
Sistema de información	Conjunto de recursos organizados para recopilar, procesar, almacenar, transmitir y difundir información.
Sistema de gestión de seguridad de la información (SGSI)	Conjunto de políticas, procedimientos, recursos y controles para proteger información y gestionar riesgos.
Riesgo cibernético	Posibles resultados negativos asociados a amenazas/ciberataques (pérdida, fuga, indisponibilidad, sanción).
Rol	Conjunto de tareas/actividades asignadas a una posición; base para permisos y segregación.
Tecnología de la información	Hardware y software operado por OIT o por terceros para procesar información en nombre del Despacho.
Terceras partes	Proveedores/contratistas/aliados con relación contractual y posible acceso a información/sistemas.
Usuario	Persona que utiliza sistemas o accede a información del Despacho conforme a autorizaciones.
Usuarios terceros	Personas externas sin relación laboral (p. ej., proveedores) que requieren acceso por su función.
Visitante o persona externa	Persona que no pertenece al Despacho y visita instalaciones; su acceso debe controlarse.
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una amenaza.

ANEXO 2. CONTROLES ORGANIZACIONALES

1. OBJETIVO

Establecer controles organizacionales para proteger información y activos tecnológicos de OIT Abogados y cumplir requisitos legales, regulatorios y contractuales.

2. ALCANCE

Aplica a empleados, pasantes, contratistas, proveedores y terceros que accedan, procesen o gestionen información del Despacho.

3. PRINCIPIOS GENERALES

- Gobernanza clara con roles y responsabilidades definidos para el SGSI.
- Liderazgo de Alta Dirección mediante asignación de recursos, aprobación de políticas y supervisión del cumplimiento.
- Gestión continua de riesgos relacionada con seguridad de la información.

4. CONTROLES ORGANIZACIONALES

- Designación del RSI con autoridad para coordinar e impulsar el SGSI.
- Nombramiento de responsables locales (por área) para coordinar acciones específicas.
- Programa de concientización y formación obligatoria al ingreso y periódica (phishing, manejo de información, trabajo remoto).
- Proceso formal para notificación, análisis y respuesta a incidentes; registro y acciones correctivas.
- Gestión de proveedores: evaluación previa y cláusulas contractuales de seguridad.
- Seguridad en proyectos y cambios: evaluación de impacto y aprobación por RSI/TI antes de cambios en sistemas críticos.
- Auditorías internas periódicas y seguimiento de hallazgos.

5. REVISIÓN

Este anexo se revisa al menos anualmente o por cambios significativos.

6. SANCIONES

Incumplimientos pueden derivar en medidas disciplinarias o contractuales.

FORMATOS Y EVIDENCIAS MÍNIMAS

Formato: Registro de capacitación y concientización

Campo	Detalle / Registro
Nombre	
Rol/Área	
Tema	
Fecha	
Evidencia	Lista de asistencia / captura / constancia

Formato: Solicitud y aprobación de cambio (Change record)

Campo	Detalle / Registro
Descripción del cambio	
Sistema/activo impactado	
Riesgos y mitigaciones	
Aprobaciones	Área dueña / TI / RSI
Fecha implementación	
Resultado	

ANEXO 3. CONTROLES PARA LA GESTIÓN DEL PERSONAL

1. OBJETIVO

Gestionar de forma segura al personal antes, durante y después de su relación con el Despacho para reducir el riesgo humano.

2. ALCANCE

Aplica a empleados, asociados, pasantes, consultores, proveedores y terceros con acceso a información o sistemas.

3. CONTROLES POR ETAPA

- Antes de la vinculación: verificación proporcional de antecedentes; firma de compromisos de confidencialidad y aceptación de políticas; entrega de credenciales conforme a rol.
- Durante: capacitación inicial y continua; accesos por rol y necesidad; revisiones de cumplimiento; reporte de incidentes sin represalias.
- Terminación o cambio: revocación inmediata de accesos; devolución de activos; checklist de salida; recordatorio de obligaciones post-empleo.

4. RESPONSABILIDADES

- RH/Administración: onboarding/offboarding, expedientes, acuses y capacitación.
- TI: creación, modificación y baja de cuentas/credenciales; recuperación de equipos.
- RSI: supervisión y auditoría de cumplimiento.

FORMATOS Y EVIDENCIAS MÍNIMAS

Formato: Checklist de onboarding

Campo	Detalle / Registro
Alta de usuario (correo, repositorios, MFA)	
Entrega de equipo (si aplica)	
Firma de NDA/aceptación de políticas	
Capacitación inicial completada	

Formato: Checklist de offboarding

Campo	Detalle / Registro
Fecha de baja / cambio	
Revocación de accesos (correo, nube, VPN, apps)	
Devolución de activos	
Resguardo/transferencia de expedientes	

ANEXO 4. CONTROLES PARA LA GESTIÓN DE ACTIVOS E INFORMACIÓN

1. OBJETIVO

Identificar, clasificar, proteger y gestionar activos de información durante su ciclo de vida.

2. CONTROLES CLAVE

- Inventario de activos (equipos, cuentas, repositorios, aplicaciones) con propietario asignado.
- Clasificación de información: Pública, Interna, Confidencial, Restringida (cliente/estrategia).
- Uso aceptable: prohibición de compartir credenciales; uso de dispositivos personales bajo lineamientos; bloqueo de pantalla; reporte de pérdida.
- Transferencia segura: uso de canales autorizados, cifrado cuando aplique, prohibición de envío por medios no autorizados.
- Retención y destrucción: tiempos de conservación definidos por expediente/cliente y obligaciones; destrucción segura física o lógica; bitácoras.
- Medios removibles: control de USB/almacenamiento externo; cifrado y autorización previa cuando sea necesario.

FORMATOS Y EVIDENCIAS MÍNIMAS

Formato: Inventario mínimo de activos

Campo	Detalle / Registro
Activo	Equipo/cuenta/repositorio
Propietario	
Ubicación	
Clasificación	
Controles aplicados	Cifrado/MFA/backup/etc.

Formato: Matriz de clasificación de información

Campo	Detalle / Registro
Tipo de información	
Clasificación	
Reglas de acceso	
Reglas de transferencia	
Retención	

Formato: Acta de destrucción de medios/documentos

Campo	Detalle / Registro
Fecha	
Descripción	
Método	Triturado/borrado seguro
Responsable	
Testigo/Evidencia	

ANEXO 5. CONTROLES PARA LA GESTIÓN DE ACCESOS

1. OBJETIVO

Gestionar de forma segura el acceso a sistemas, redes, aplicaciones y datos, asegurando que solo personas autorizadas accedan a lo necesario.

2. CONTROLES

- Identidad única por usuario; cuentas compartidas solo excepcionalmente y con control reforzado.
- Autenticación robusta: MFA para correo, nube, VPN y sistemas críticos; contraseñas con complejidad mínima y gestor de contraseñas recomendado.
- Aprobación formal del propietario de información/área para otorgar accesos; TI ejecuta; RSI supervisa.
- Revisión periódica de accesos (al menos trimestral para sistemas críticos) y revocación inmediata al egreso.
- Accesos privilegiados: uso restringido, registro y monitoreo reforzado; prohibición de uso cotidiano con cuentas administrador.
- Acceso de terceros: limitado en tiempo y alcance; NDA y cláusulas; VPN/canales seguros; registro de sesiones.

FORMATOS Y EVIDENCIAS MÍNIMAS

Formato: Solicitud de alta/modificación de acceso

Campo	Detalle / Registro
Usuario	
Área/rol	
Sistema/Repositorio	
Nivel de acceso	
Justificación	
Aprobación propietario/área	
Ejecución TI	

Formato: Revisión periódica de accesos

Campo	Detalle / Registro
Sistema	
Fecha	
Lista revisada	Adjuntar export/captura
Accesos removidos	
Responsable	

ANEXO 6. CONTROLES FÍSICOS

1. OBJETIVO

Proteger instalaciones, equipos y activos de información frente a accesos no autorizados, daños o robos.

2. CONTROLES

- Zonificación: áreas públicas, restringidas y de resguardo (archivos, equipos).
- Control de acceso físico: llaves/tarjetas/códigos; registro de accesos a áreas sensibles cuando aplique.
- Visitantes: registro, identificación y acompañamiento; prohibición de acceso a áreas de resguardo sin autorización.
- Protección de equipos: anclaje/almacenamiento seguro; protección contra energía (reguladores/no-break cuando aplique).
- Gestión de impresiones: retiro inmediato; impresión segura cuando sea posible.
- Eliminación segura de equipos: borrado seguro o destrucción de medios antes de baja/reciclaje.

FORMATOS Y EVIDENCIAS MÍNIMAS

Formato: Registro de visitantes

Campo	Detalle / Registro
Nombre	
Empresa	
Motivo	
Hora entrada/salida	
Acompañante	

Formato: Bitácora de resguardo de expedientes físicos

Campo	Detalle / Registro
Expediente	
Fecha de salida	
Responsable	
Fecha de retorno	

ANEXO 7. CONTROLES DE SEGURIDAD OPERATIVA

1. OBJETIVO

Asegurar operación segura y confiable de sistemas y servicios tecnológicos del Despacho.

2. CONTROLES

- Gestión de cambios: evaluación, aprobación, pruebas y documentación antes de producción.
- Gestión de capacidad: monitoreo básico de almacenamiento/correo/nube para evitar interrupciones.
- Protección contra malware: antimalware en endpoints; actualizaciones automáticas; escaneos periódicos.
- Respaldos: periodicidad definida; prueba de restauración; copias protegidas contra modificación.
- Monitoreo y registros: logging de eventos relevantes en correo/nube/sistemas críticos; revisión proporcional.
- Separación de ambientes: cuando aplique (desarrollo/pruebas/producción) y control de datos.
- Gestión de vulnerabilidades y parches: calendario; atención prioritaria a críticas.

FORMATOS Y EVIDENCIAS MÍNIMAS

Formato: Registro de respaldos y pruebas de restauración

Campo	Detalle / Registro
Activo/Repositorio	
Periodicidad	
Último respaldo	
Prueba de restauración	Fecha/resultado
Responsable	

Formato: Registro de vulnerabilidades y parches

Campo	Detalle / Registro
Hallazgo	
Severidad	
Sistema afectado	
Acción	
Fecha cierre	

ANEXO 8. CONTROLES EN TELECOMUNICACIONES Y REDES

1. OBJETIVO

Proteger infraestructura de redes y comunicaciones usadas por el Despacho (LAN/WiFi/VPN/Internet) y la información transmitida.

2. CONTROLES

- Perímetro: firewall/router con configuración segura; segmentación básica (WiFi invitados separado).
- Cifrado de comunicaciones: uso de TLS/HTTPS; VPN para accesos remotos; prohibición de servicios inseguros.
- Acceso remoto: VPN y MFA; sesiones registradas cuando sea posible.
- Monitoreo: revisión de logs del router/VPN y alertas relevantes; respuesta ante anomalías.
- Proveedores: selección con SLA y requisitos de seguridad; cambios coordinados.
- Resiliencia: respaldos de configuración; redundancia razonable de Internet cuando sea crítico.

FORMATOS Y EVIDENCIAS MÍNIMAS

Formato: Inventario de redes y accesos remotos

Campo	Detalle / Registro
Ubicación	
Red/SSID	
Tipo	Corporativa/Invitados
Método de autenticación	
VPN	Sí/No; proveedor

ANEXO 9. CONTROLES PARA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

1. OBJETIVO

Asegurar que sistemas adquiridos o desarrollados cumplan requisitos de seguridad desde su concepción hasta su retiro.

2. CONTROLES

- Requisitos de seguridad definidos desde análisis (autenticación, autorización, cifrado, trazabilidad, privacidad).
- Evaluación de proveedores y soluciones (seguridad, cumplimiento, soporte).
- Desarrollo seguro: revisiones de código cuando aplique; principios DevSecOps proporcional.
- Pruebas de seguridad antes de producción: análisis de vulnerabilidades; pruebas de configuración.
- Gestión de cambios y versiones con registro.
- Datos en desarrollo/pruebas: no usar datos reales de clientes salvo anonimización/cifrado y autorización.
- Mantenimiento seguro: parches evaluados; ventanas; respaldos previos.

FORMATOS Y EVIDENCIAS MÍNIMAS

Formato: Checklist de requisitos de seguridad por sistema

Campo	Detalle / Registro
Sistema/Proveedor	
Datos tratados (tipo)	
MFA/SSO	
Cifrado en tránsito/reposo	
Logs/auditoría	
Respaldo/DR	
Derechos de auditoría	

ANEXO 10. REQUISITOS DE SEGURIDAD PARA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Esta Directriz establece lineamientos mínimos de seguridad de la información aplicables OIT Abogados para la evaluación, adquisición, desarrollo, mantenimiento y operación de sistemas de información, incluyendo servicios en la nube (SaaS), infraestructura, sistemas operativos, aplicaciones del negocio, sitios web, aplicaciones móviles y herramientas de colaboración.

1. REQUISITOS DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN

Los sistemas de información incluyen sistemas operativos, infraestructura, aplicaciones del negocio, servicios, aplicaciones bajo el modelo de software como servicio (SaaS) y aplicaciones desarrolladas para usuarios internos o externos. Todos los sistemas deben ser evaluados antes de su implementación o desarrollo para definir y verificar el cumplimiento de requerimientos funcionales, de seguridad y de control.

- Se aplicarán controles para proteger la información sensible, conforme a la clasificación de la información y/o del activo de información.
- Se implementarán controles para prevenir el repudio y asegurar trazabilidad (p. ej., autenticación robusta, registros de auditoría y retención de evidencias).
- Se asegurarán los archivos del sistema y se mantendrá control de cambios sobre configuraciones, componentes y versiones.

2. ANÁLISIS Y ESPECIFICACIONES DE REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN

Durante la adquisición, configuración, implementación o desarrollo de aplicaciones, se identificarán, documentarán y aprobarán los requerimientos de seguridad a incorporar. Asimismo, se diseñarán controles de validación de datos de entrada, procesamiento interno y salida.

- Antes de liberar a producción, se verificará que el sistema incluya, cuando aplique: autenticación, autorización, registro/auditoría, cifrado, segregación de funciones, y controles de protección de datos personales y confidenciales.
- El componente de seguridad podrá validarse en producción únicamente cuando exista una justificación documentada y se haya surtido el procedimiento de gestión de cambios con evaluación de riesgos y aprobaciones correspondientes.

- OIT Abogados mantendrá un inventario actualizado del software: (i) propiedad del Despacho, (ii) comprado a terceros, (iii) licenciado, (iv) por suscripción, (v) entregado/recibido en comodato, y (vi) herramientas SaaS relevantes.
- Las licencias de software y documentación asociada (p. ej., contratos, términos y condiciones, evidencias de compra) se resguardarán de manera segura; el inventario registrará usuarios permitidos y fechas de renovación.
- La función de Tecnología (interna o tercerizada) será responsable del control y administración del software, así como de la aprobación para adquisición o actualización, en coordinación con la Dirección Administrativa y/o Socios cuando corresponda.
- Los contratos con proveedores deberán incluir requisitos de seguridad de la información según el servicio: confidencialidad, destrucción controlada, continuidad del negocio, notificación de incidentes, derechos de auditoría, y medidas de protección de datos.

Todo software, configuración relevante o cambio mayor deberá ensayarse en ambientes de prueba razonablemente similares al de producción, para verificar su funcionalidad y requisitos de seguridad.

3. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

En las etapas iniciales de un proyecto, se incluirá la identificación y evaluación de riesgos de seguridad de la información, para los cuales se definirán controles de seguridad acordes con la metodología de riesgos del Despacho.

La responsabilidad de implementar y asegurar la efectividad de los controles recaerá en el líder del proyecto y/o el dueño del proceso, en coordinación con Tecnología y el Responsable de Seguridad de la Información (o función equivalente).

4. SEGURIDAD DE APLICACIONES EN REDES PÚBLICAS Y PROCESAMIENTO CORRECTO

La validación de datos de entrada y salida se realizará en ambientes de prueba; una vez verificados los controles, se liberarán al ambiente productivo.

Validación de datos de entrada:

- Validación a nivel individual: tipos de datos, datos obligatorios, longitud de campo, rangos razonables, conjuntos de valores válidos y despliegue protegido de valores.
- Validación automática por el sistema que detecte entradas erróneas o incongruentes y muestre mensajes de error sin revelar información sensible o detalles técnicos explotables.
- Ejecución de procedimientos automáticos de respuesta ante errores de validación y registro de la actividad de ingreso de datos.
- Definición de responsabilidades para el personal que participa en el proceso de captura/entrada de datos.

Control de procesamiento interno:

- Mecanismos que validen la ejecución lógica del procesamiento.
- Validaciones para que los procesos se ajusten a procedimientos aprobados.
- Controles contra ataques comunes (p. ej., desbordamiento, inyección, manipulación de sesión) mediante prácticas de desarrollo seguro.
- Generación de reportes/bitácoras (logs) sobre inconsistencias presentadas durante el procesamiento.

Transferencia de información:

Los mensajes y archivos sensibles (p. ej., información confidencial de clientes o datos personales) enviados por correo o aplicaciones deberán contar con cifrado y/o mecanismos de control de acceso para evitar accesos no autorizados.

Validación de datos de salida:

- Controles para validar que los datos de salida sean correctos y completos (reportes automáticos o manuales, reconciliaciones, controles de integridad).
- Clasificación de la información de salida para identificar destinatarios autorizados y aplicar controles a información reservada y confidencial.

5. SEGURIDAD EN PROCESOS DE DESARROLLO Y SOPORTE

Los cambios deberán cumplir con las directrices internas de operación y gestión de cambios. Se mantendrán registros (logs) sobre niveles de autorización y actividades, y se limitarán las acciones a personal autorizado.

- Se identificarán e implementarán controles para mitigar riesgos a la confidencialidad, integridad y disponibilidad durante el desarrollo, mantenimiento y soporte.
- Se realizarán pruebas de seguridad (p. ej., escaneo de vulnerabilidades y, cuando aplique, pruebas de penetración) al código fuente desarrollado a la medida, especialmente si: (i) está relacionado con servicios esenciales del Despacho o (ii) administra información confidencial o datos personales.
- Para las pruebas y buenas prácticas se tomarán como referencia guías reconocidas (p. ej., OWASP) y estándares aplicables al contexto del Despacho.

Responsabilidades de la función de Tecnología (interna o tercerizada):

- Asegurar que las migraciones entre ambientes de desarrollo, pruebas y producción cuenten con aprobación conforme al procedimiento de control de cambios.
- Asegurar que los sistemas adquiridos o desarrollados por terceros cuenten con acuerdos de licenciamiento y cláusulas que definan condiciones de uso y propiedad intelectual.
- Generar, adoptar o recomendar metodologías de pruebas que incluyan escenarios, niveles, tipos, datos de prueba y documentación mínima.
- Mantener herramientas, componentes y plataformas actualizadas con parches y versiones soportadas; las excepciones requieren análisis de riesgos, aprobación y documentación.
- Asegurar que las aplicaciones y desarrollos se construyan sobre versiones vigentes y estables de herramientas, componentes, sistemas operativos y lenguajes.
- Resguardar copias de seguridad del código fuente (cuando sea propiedad del Despacho) de manera segura; si lo resguarda un tercero, establecerlo contractualmente y dar seguimiento.
- Aplicar el procedimiento de control de cambios y remediar vulnerabilidades detectadas en pruebas o producción, incluyendo aplicaciones web y móviles.

6. CONTROL DE CAMBIO EN SISTEMAS

Para cambios, actualizaciones o reconfiguraciones con impacto relevante (servidores, bases de datos, infraestructura, aplicaciones críticas), se aplicará el procedimiento de gestión de cambios, evaluando impactos y riesgos para planear y ejecutar adecuadamente.

- Los cambios significativos al sistema operativo o componentes críticos deberán revisarse para asegurar que no comprometan funcionalidad o seguridad.
- Se revisarán procedimientos de integridad y control de aplicaciones para confirmar que no hayan sido comprometidos por el cambio.
- Se informarán los cambios con antelación para habilitar análisis y aprobaciones; el procedimiento interno definirá actividades mínimas y evidencias.

7. RESTRICCIONES EN LOS CAMBIOS DE PAQUETES DE SOFTWARE

Si se requiere modificar, actualizar o ajustar paquetes de software (incluidos los suministrados por proveedores) y existe autorización del responsable del activo de información:

- Se revisarán términos y condiciones de licencia para confirmar que las modificaciones están permitidas.
- Se conservará el software original; los cambios se realizarán sobre una copia identificada y se documentarán para replicación o reversión (rollback).
- Dentro de la gestión de cambios, se asegurará la remediación de vulnerabilidades detectadas conforme al proceso interno de gestión de vulnerabilidades.

8. SEPARACIÓN DE AMBIENTES

Se mantendrán controles para asegurar separación lógica y/o física entre ambientes de desarrollo, pruebas y producción, a fin de reducir accesos no autorizados y evitar cambios que afecten la operación.

- Los usuarios deberán utilizar perfiles diferenciados por ambiente; se otorgarán solo los privilegios necesarios en cada uno.
- Las pruebas, instalaciones o desarrollos se realizarán en ambientes de desarrollo y pruebas para evitar riesgos de disponibilidad o confidencialidad.

- No se copiará información sensible de producción a pruebas; si fuera estrictamente necesario, se aplicarán controles de confidencialidad y eliminación segura posterior.
- Se restringirá el acceso a compiladores, editores y herramientas de desarrollo desde producción; las excepciones requieren análisis de riesgos y aprobación del Responsable de Seguridad de la Información (o equivalente).

9. PRINCIPIOS DE DESARROLLO

Todo desarrollo (interno o contratado con terceros) deberá cumplir, según corresponda, con los siguientes principios:

9.1 Desarrollo interno:

- Partir de permisos mínimos y escalar privilegios solo por necesidad justificada, según perfiles definidos.
- Eliminar de producción rutinas de prueba, comentarios o mecanismos que faciliten accesos indebidos; evitar información de depuración.
- Incluir pruebas de cobertura para asegurar que el código relevante es probado.
- Incorporar seguridad desde el diseño en todas las capas (negocio, datos, aplicaciones y tecnología) equilibrando seguridad y accesibilidad.
- Validar siempre los datos de entrada/salida para evitar inyecciones, manipulación de sesión y otros ataques.
- Agregar funcionalidades, campos, botones o menús conforme a requerimientos aprobados; documentar cambios y mantener trazabilidad.
- Usar protocolos seguros para intercambio de información sensible (cifrado fuerte, claves robustas y gestión segura de credenciales).
- Generar planes de remediación para vulnerabilidades confirmadas de criticidad alta o muy alta.
- Tomar como referencia prácticas de desarrollo seguro (p. ej., Microsoft SDL, OWASP, SANS CWE Top 25, CERT Secure Coding), conforme al contexto del Despacho.
- Liberar a producción solo después de completar pruebas técnicas, funcionales, de carga/estrés y de seguridad, y certificación conforme al proceso interno.

9.2 Desarrollo contratado a terceros:

- La función de Tecnología validará que el tercero cuente con prácticas de desarrollo seguro y controles equivalentes.
- Los contratos de desarrollo deberán incluir obligaciones de desarrollo seguro, pruebas, entrega y resguardo de código, notificación de vulnerabilidades e incidentes, y derechos de auditoría cuando aplique.

ANEXO 11. CONTROLES PARA LA GESTIÓN DE PROVEEDORES (TPRM/NTH PARTIES)

1. OBJETIVO

Gestionar riesgos de seguridad en proveedores/terceros (Third Party Risk Management), incluyendo Nth parties relevantes.

2. CONTROLES

- Evaluación previa proporcional al riesgo (acceso a información, criticidad del servicio, ubicación, subcontratación).
- Clasificación de proveedores (alto/medio/bajo) y periodicidad de reevaluación.
- Contratos con cláusulas: confidencialidad, protección de datos, incidentes, auditoría, subcontratación (flow-down), retorno/destrucción de información.
- Gestión de accesos de terceros: limitados y temporales; monitoreo; revocación al terminar.
- Evidencias: cuestionarios, certificaciones (cuando existan), SOC/ISO si aplica, y registros de revisiones.

FORMATOS Y EVIDENCIAS MÍNIMAS

Formato: Evaluación de proveedor (due diligence)

Campo	Detalle / Registro
Proveedor	
Servicio	
Acceso a información	Ninguno/Bajo/Alto
Clasificación de riesgo	Bajo/Medio/Alto
Controles requeridos	MFA, cifrado, NDA, etc.
Aprobación (RSI/Área)	
Reevaluación	Fecha

Formato: Declaración de Nth parties

Campo	Detalle / Registro
Proveedor	
Nth party	
RoI	
Acceso a información	
Acepta obligaciones equivalentes	Sí/No

ANEXO 12. CONTROLES PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

1. OBJETIVO

Detectar, reportar, analizar, responder y aprender de incidentes de seguridad, minimizando impacto y previniendo recurrencia.

Establecer las categorías, criterios de clasificación, tiempos de respuesta y el proceso interno para detectar, reportar, analizar, contener, erradicar y cerrar incidentes de seguridad de la información y/o ciberseguridad en OIT Abogados así como para preservar evidencia y cumplir obligaciones legales, regulatorias y contractuales aplicables.

2. ALCANCE

Este Anexo aplica a todo el personal, socios, asociados, pasantes, contratistas, proveedores y terceros con acceso a información, sistemas, dispositivos o servicios tecnológicos utilizados por el Despacho, incluyendo servicios en nube (p. ej., Microsoft 365), correo electrónico, dispositivos móviles, equipos de cómputo y cualquier sistema que procese información de clientes o del Despacho.

3. PRINCIPIOS

- Reporte inmediato y sin represalias: toda persona deberá reportar de forma inmediata cualquier evento o incidente (o sospecha razonable).
- Necesidad de conocer y mínimo privilegio: la información sobre incidentes se compartirá solo con quienes deban participar en su gestión.
- Preservación de evidencia: se deberán proteger registros, bitácoras y dispositivos para asegurar integridad y cadena de custodia.
- Mejora continua: cada incidente genera lecciones aprendidas y acciones correctivas/preventivas.

4. CATEGORÍAS Y SUBCATEGORÍAS DE INCIDENTES DE CIBERSEGURIDAD

La siguiente tabla se utiliza para categorizar incidentes y estandarizar el lenguaje interno para su atención y reporte.

Categoría	Subcategorías (ejemplos)	Descripción
Ataques cibernéticos dirigidos	Whaling; ingeniería social; spear phishing; APT (amenaza persistente avanzada); amenazas volátiles avanzadas; espionaje industrial; robo de propiedad intelectual.	Ataques en los que la víctima es seleccionada intencionalmente y el atacante dirige esfuerzos específicos para lograr un objetivo (p. ej., acceder a información de clientes, credenciales, o fondos).
Código malicioso (malware)	Infección extendida; infección única; ransomware; crypto miner; bots; rootkit; worm; troyano; spyware.	Código o programa destinado a ejecutar funciones no autorizadas con impacto adverso en confidencialidad, integridad o disponibilidad.
Disrupción de sistemas	Denegación de servicio (DoS/DDoS); indisponibilidad de servicios de proveedores críticos (correo, nube, hosting, internet, comunicaciones).	Afectación de disponibilidad de servicios, procesos o sistemas por explotación de vulnerabilidades o tráfico masivo, o por indisponibilidad derivada de un ataque a un proveedor crítico.
Acceso no autorizado	Inyección SQL; intentos de login; cuentas comprometidas; elevación de privilegios; movimiento lateral.	Acceso lógico o físico no autorizado a equipos, aplicaciones, datos o recursos tecnológicos.
Pruebas y reconocimiento	Scanning; sniffing; OSINT; enumeración de servicios.	Acciones de reconocimiento para identificar activos, puertos, servicios, cuentas, vulnerabilidades o información expuesta.
Uso no autorizado del sistema	Cryptojacking; botnet; uso de recursos para ataques.	Uso de recursos tecnológicos del Despacho para minería de criptomonedas, envío de spam o ataques, sin autorización.
Uso indebido de la marca	Suplantación de sitio web; registro/alteración de DNS; suplantación de cuentas; phishing.	Uso fraudulento de elementos identificativos del Despacho (logo, dominio, correo) para obtener información o afectar reputación.
Modificación y/o alteración no autorizada	Modificación no autorizada de infraestructura; agregar/alterar/eliminar información; manipulación de bitácoras.	Acciones que alteren, falsifiquen, introduzcan o eliminen información o medios de procesamiento sin autorización.
Explotación de vulnerabilidades	Vulnerabilidad "día 0"; mala configuración (credenciales por defecto, protocolos vulnerables); sistema no actualizado (parches pendientes).	Incidentes provocados por explotación de vulnerabilidades conocidas o desconocidas, o por configuraciones inseguras.

Otros	No clasificados en las categorías anteriores.	Incidentes atípicos que sirven como insumo para actualizar la clasificación.

5. CATEGORÍAS DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (NO NECESARIAMENTE CIBERSEGURIDAD)

- Incumplimiento de políticas internas de seguridad.
- Quebrantamiento de disposiciones de seguridad física (p. ej., acceso no autorizado a áreas restringidas).
- Pérdida o fuga de información (incluye extravío de dispositivos o envío erróneo).
- Pérdida, robo o alteración física de equipos.
- Uso inadecuado de sistemas de información.
- Cambios no controlados en sistemas de información.
- Mal funcionamiento de software o hardware con impacto en información o servicios.

6. CRITERIOS PARA CLASIFICAR UN EVENTO COMO INCIDENTE

Para clasificar un evento como incidente se evaluará si afecta alguna de las premisas de seguridad: confidencialidad, integridad y disponibilidad.

- Confidencialidad: divulgación, acceso o extracción no autorizada de información del Despacho o de clientes (incluyendo datos personales conforme a la LFPDPPP).
- Integridad: modificación no autorizada o no controlada de información o sistemas, o compromiso de registros de auditoría/bitácoras.
- Disponibilidad: interrupción no controlada que impida la prestación de servicios críticos del Despacho o afecte compromisos contractuales con clientes.
- No repudio: riesgo de que un usuario niegue una acción por ausencia de controles de autenticación, trazabilidad o evidencia.

7. TABLA DE DEFINICIÓN DE CRITICIDAD DE UN INCIDENTE

Clasificación	Confidencialidad	Integridad	Disponibilidad
Nulo	Controles adecuados; sin pérdida de información relevante.	Sin modificación no autorizada en información/sistemas.	Sin interrupción de operación.
Bajo	Información recuperable; sin impacto material en estrategia o datos sensibles.	Existe respaldo reciente (<24h); recuperación sin reprocesos relevantes.	Interrupción controlada; existe "marcha atrás"/contingencia.
Medio	Requiere esfuerzo operativo para recuperar; podría afectar información sensible limitada.	Respaldo (<48h); recuperación requiere reprocesos operativos.	Interrupción controlada pero con afectación parcial a usuarios/clientes.
Alto	Información parcial o irrecuperable; afecta información sensible de clientes o la estrategia del Despacho.	Sin respaldo o recuperación parcial (>1 semana); reprocesos significativos.	Interrupción no controlada; sin contingencia efectiva; afecta compromisos con clientes.

8. CRITERIO DE EVALUACIÓN (PUNTAJE) Y NIVEL DE CRITICIDAD

Cada dimensión (C/I/D) se valora de 0 a 3. El puntaje total se obtiene sumando los tres valores (0–9).

Criticidad	Puntaje	Descripción
Alto	7–9	El Despacho no puede proporcionar uno o más servicios críticos, o se comprometen datos personales/sensibles de clientes.
Medio	4–6	Pérdida temporal de capacidad para proporcionar un servicio crítico a un subconjunto de usuarios o afectación material acotada.
Bajo	1–3	Efecto mínimo; el Despacho mantiene servicios, pero con pérdida de eficiencia o riesgo acotado.
Nulo	0	Sin afectación relevante a la operación ni a la seguridad de la información.

9. REPORTE DE EVENTOS, INCIDENTES Y VULNERABILIDADES

Toda persona con acceso a información del Despacho debe reportar, tan pronto tenga conocimiento, cualquier evento, incidente o vulnerabilidad.

Canales internos de reporte:

- Correo: smartinez@oit.mx
- Mensajería/llamada: 5518500529.
- Mesa de ayuda/tickets: sergio@inte11ect.mx

Cuando el incidente involucre datos personales o información de clientes, el Despacho evaluará obligaciones de notificación conforme a la LFPDPPP y a lo pactado contractualmente, así como cualquier requerimiento de autoridades competentes (p. ej., INAI) y/o de clientes.

10. PROCESO DE GESTIÓN DE INCIDENTES

10.1 Detección y triage

Recepción del reporte; verificación inicial para determinar si es falsa alarma, evento o incidente; asignación de criticidad preliminar.

10.2 Contención

Acciones inmediatas para limitar el impacto (aislar equipos, revocar accesos, reset de contraseñas, bloqueo de cuentas, segmentación, etc.).

10.3 Erradicación

Eliminación de la causa raíz (malware, credenciales comprometidas, vulnerabilidades, configuraciones inseguras) y aplicación de parches.

10.4 Recuperación

Restauración segura de servicios y datos; validación de integridad; monitoreo reforzado posterior.

10.5 Cierre y lecciones aprendidas

Documentación completa del caso; análisis de causa raíz; acciones correctivas/preventivas; actualización de controles y capacitación.

11. ROLES Y RESPONSABILIDADES (REFERENCIA RACI)

El Despacho definirá formalmente responsables. Como guía mínima:

- Responsable de Seguridad de la Información (o rol equivalente): coordina la gestión del incidente, define controles, preserva evidencia y reporta métricas.
- Responsable de TI/Operaciones: ejecuta acciones técnicas (contención, erradicación, recuperación) y mantiene bitácoras.
- Líder del área afectada: apoya en identificación de impactos operativos y priorización de servicios.
- Compliance/Legal: evalúa obligaciones legales/contractuales (incl. notificaciones a clientes/autoridades) y supervisa cadena de custodia cuando pueda haber consecuencias legales.
- Dirección/Socios: aprueban decisiones de alto impacto, asignación de recursos y comunicación externa.

12. RECOLECCIÓN Y PRESERVACIÓN DE EVIDENCIAS

- Minimizar manipulación de equipos afectados; preservar registros (logs), correos, capturas de pantalla, y archivos relevantes.
- Mantener cadena de custodia: quién recolectó, cuándo, dónde, cómo; identificar y resguardar el original; trabajar sobre copias.
- Cuando proceda, cifrar y controlar el acceso a evidencias; documentar cada traslado o copia.
- En incidentes con posible consecuencia legal, involucrar a Legal/Compliance para asegurar admisibilidad, integridad y resguardo.

13. TIEMPOS MÁXIMOS DE ATENCIÓN

Los tiempos son el máximo para iniciar la atención una vez conocido el incidente (no necesariamente para resolverlo):

Nivel de impacto	Tiempo máximo para iniciar atención
Alto	Inmediato – máximo 30 minutos
Medio	Entre 8 horas y 2 días
Bajo	Entre 2 y 3 días

14. COMUNICACIONES INTERNAS Y EXTERNAS

Las comunicaciones se administrarán bajo el principio de necesidad de conocer y siguiendo un guion de mensajes aprobado para evitar divulgación indebida.

Guía mínima:

- Internas: informar a los roles involucrados (TI, Seguridad, Dirección, Legal/Compliance, área afectada) con actualizaciones proporcionales a la criticidad.
- Externas: notificar a clientes afectados conforme a contrato y, en su caso, conforme a la LFPDPPP. Cualquier comunicación pública será coordinada por la Dirección.
- Autoridades: cuando aplique, se coordinará con Legal/Compliance la interacción y reportes a autoridades competentes.

15. REGISTRO Y MÉTRICAS

Todo incidente se registrará en una Bitácora de Incidentes (o herramienta de tickets) incluyendo: fecha/hora, categoría, activos afectados, impacto, acciones de contención/erradicación/recuperación, evidencia preservada, responsables y lecciones aprendidas. Trimestralmente se consolidarán indicadores para revisión de Dirección.

16. CONTROLES

- Clasificación por naturaleza e impacto; niveles de severidad y tiempos de respuesta.
- Canales de reporte (correo/whatsapp corporativo/ticket) y obligación de reportar de inmediato.
- Contención, erradicación y recuperación; preservación de evidencia cuando aplique.
- Comunicación y escalamiento: incidentes críticos a Alta Dirección y, si aplica, a clientes/autoridades conforme contrato/ley.
- Revisión post-incidente (post-mortem) y plan de acciones correctivas.

FORMATOS Y EVIDENCIAS MÍNIMAS

Formato: Registro de incidente

Campo	Detalle / Registro
ID	
Fecha/hora detección	
Reporta	
Descripción	
Clasificación/severidad	
Acciones de contención	
Evidencia	Logs/capturas
Causa raíz	
Lecciones y acciones	
Cierre	Fecha/responsable

Formato: Guía rápida de respuesta (primeros 60 minutos)

Campo	Detalle / Registro
1) Contener	Aislar equipo/cuenta, reset de credenciales, bloquear acceso.
2) Preservar evidencia	No borrar; capturas; resguardar correos/adjuntos.
3) Escalar	Avisar a TI/RSI; si crítico, a Socios.
4) Comunicar	Definir mensaje interno/cliente (si aplica).

ANEXO 13. CONTROLES PARA CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN

1. OBJETIVO

Garantizar continuidad de operaciones críticas ante eventos disruptivos, minimizando impacto en servicios, reputación y cumplimiento.

2. CONTROLES

- BIA: identificar procesos críticos, dependencias, RTO y RPO.
- Planes BCP/DRP: procedimientos de respuesta, operación alternativa, recuperación de TI y restauración.
- Pruebas y ejercicios: al menos anual; documentar resultados y mejoras.
- Capacitación del personal clave y canales de comunicación.
- Gestión de proveedores críticos: validar continuidad y cláusulas.

FORMATOS Y EVIDENCIAS MÍNIMAS

Formato: BIA (Análisis de impacto al negocio)

Campo	Detalle / Registro
Proceso	
Dueño	
Impacto	Operativo/Legal/Reputacional
RTO (hrs)	
RPO (hrs)	
Dependencias	Personas/sistemas/proveedores

Formato: Plan de continuidad - Lista de verificación

Campo	Detalle / Registro
Escenario	
Acción inmediata	
Operación alternativa	
Restauración	
Comunicación	

ANEXO 14. CONTROLES PARA CUMPLIMIENTO

1. OBJETIVO

Asegurar cumplimiento de obligaciones legales, regulatorias, contractuales y normativas relacionadas con seguridad de la información y protección de datos.

2. CONTROLES

- Inventario de obligaciones aplicables (LFPDPPP y su Reglamento, obligaciones contractuales de clientes, mejores prácticas).
- Evaluaciones periódicas y planes de acción correctiva.
- Auditorías internas anuales (o por requerimiento de cliente) y apoyo a auditorías externas cuando aplique.
- Gestión de incumplimientos: registro, análisis, acciones correctivas/preventivas y notificación cuando sea exigible.
- Capacitación en cumplimiento y protección de datos; reportes a Alta Dirección.

FORMATOS Y EVIDENCIAS MÍNIMAS

Formato: Inventario de obligaciones y controles

Campo	Detalle / Registro
Obligación	
Fuente	Ley/Contrato/Política
Control asociado	
Evidencia	
Responsable	
Frecuencia	

Formato: Plan de acción correctiva

Campo	Detalle / Registro
Hallazgo	
Riesgo	
Acción	
Responsable	
Fecha compromiso	
Estatus	