					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P30S					Título del documento: **Política de Respuesta a Incidentes**							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025			Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro	

Historial de revisiones				
Número de revisión	**Fecha de revisión**	**Cambios**	**Revisado por**	**Propietario del proceso**

Aprobaciones			
Nombre	**Cargo**	**Fecha**	**Firma**

Alineada con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 6.1, 6.3, 8	gestión de incidentes, mejora continua, control operativo
ISO/IEC 27002:2022	Controles 5.24, 5.25	detección de incidentes, preparación, aprendizaje
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	gestión y monitorización de incidentes, notificación
RGPD de la UE	Artículo 33	requisitos de notificación de violaciones de seguridad de los datos personales
Directiva NIS2 de la UE	Artículo 23	notificación obligatoria de incidentes de ciberseguridad
DORA de la UE	Artículo 17	gestión de incidentes relacionados con las TIC
COBIT 2019	DSS02, DSS04	gestión de servicios e incidentes y continuidad

1. Propósito

1.1. Esta política define cómo la organización detecta, notifica y responde a los incidentes de seguridad de la información que afecten a sus sistemas digitales, datos o servicios.

1.2. Permite a la organización minimizar los daños, proteger los datos de los clientes y cumplir las obligaciones regulatorias, como el requisito de notificación de violaciones de seguridad de los datos personales en un plazo de 72 horas conforme al RGPD de la UE.

1.3. La política garantiza responsabilidades claras, procedimientos de comunicación y seguimiento posterior al incidente, incluso en organizaciones pequeñas sin un equipo de seguridad dedicado.

2. Alcance

2.1. Esta política se aplica a:

2.1.1. Todos los empleados, contratistas y proveedores externos de servicios de TI.

2.1.2. Todos los sistemas y servicios gestionados por la empresa, incluidos sitios web, plataformas en la nube, dispositivos móviles, equipos portátiles y cuentas de correo electrónico.

2.1.3. Todo tipo de incidentes, incluidos:

2.1.3.1. Acceso no autorizado a datos o sistemas.

2.1.3.2. Infecciones por malware o ransomware.

2.1.3.3. Intentos de phishing o ingeniería social.

2.1.3.4. Indisponibilidad del sistema debida a un ciberataque o a un uso indebido.

2.1.3.5. Divulgación accidental o eliminación de información sensible.

2.1.3.6. Pérdida o robo de dispositivos de la organización o soportes de almacenamiento.

3. Objetivos

3.1. Establecer un proceso claro para identificar y escalar los incidentes de seguridad.

3.2. Garantizar que los incidentes se notifiquen, registren y gestionen dentro de los plazos predefinidos.

3.3. Permitir la contención rápida del daño, la recuperación de los datos y el restablecimiento del servicio.

3.4. Garantizar que las partes afectadas, como clientes o reguladores, sean notificadas cuando así lo exija la ley.

3.5. Prevenir la recurrencia mediante análisis de causa raíz, acciones correctivas y mejora de la política.

3.6. Permitir que las pymes cumplan los requisitos de certificación de ISO 27001 y demuestren diligencia proactiva durante las auditorías.

4. Funciones y responsabilidades

4.1. Director General (DG)

4.1.1. Es responsable de esta política y garantiza su implantación.

4.1.2. Supervisa las actividades de respuesta a incidentes y aprueba las notificaciones a reguladores o clientes.

4.1.3. Revisa los informes posteriores al incidente y garantiza que la política se actualice cuando sea necesario.

4.1.4. Puede delegar funciones de coordinación, pero conserva la responsabilidad última.

4.2. Proveedor externo de TI / administrador de sistemas (interno o externo)

4.2.1. Detecta e investiga posibles incidentes de seguridad.

4.2.2. Implanta acciones de contención y recuperación, por ejemplo, deshabilitar accesos o restaurar copias de seguridad.

4.2.3. Notifica al DG todos los incidentes confirmados o presuntos en el plazo de 1 hora desde su detección.

4.2.4. Mantiene un registro de incidentes con marcas temporales, evaluación de impacto y acciones de respuesta.

[... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ...]

9. Requisitos de revisión y actualización

9.1. Revisión programada

9.1.1. Esta política debe revisarse al menos una vez cada 12 meses por el Director General (DG) para garantizar:

9.1.1.1. La alineación con los controles de ISO/IEC 27001:2022.

9.1.1.2. La capacidad de respuesta frente a nuevas amenazas, riesgos e incidentes.

9.1.1.3. El cumplimiento continuado de las obligaciones legales y contractuales, por ejemplo, RGPD de la UE y DORA de la UE.

9.2. Eventos desencadenantes

9.2.1. La política también debe revisarse y actualizarse después de:

9.2.1.1. Cualquier incidente de alta severidad o notificación regulatoria.

9.2.1.2. La introducción de nueva infraestructura de TI o cambios en los sistemas.

9.2.1.3. Modificaciones de los requisitos legales relacionados con violaciones de seguridad.

9.3. Documentación y distribución de la revisión

9.3.1. Todas las revisiones y cambios deben documentarse en el registro de cambios de la política.

9.3.2. Las versiones actualizadas deben distribuirse a todos los empleados, proveedores externos y proveedores externos de TI implicados en la seguridad o en las operaciones de los sistemas.

9.3.3. Deben conservarse evidencias de la concienciación del personal, por ejemplo, notas de reunión o confirmaciones por correo electrónico, para la preparación de auditorías.

10. Políticas relacionadas y vinculaciones

10.1. Esta política debe aplicarse de forma coordinada con las siguientes políticas de pyme:

10.1.1. P1S – Política de Seguridad de la Información: establece las expectativas generales para mantener la confidencialidad, integridad y disponibilidad durante las operaciones, incluida la gestión de incidentes.

10.1.2. P2S – Política de funciones y responsabilidades de gobernanza: establece las estructuras de autoridad y rendición de cuentas para la detección, notificación y escalado de incidentes.

10.1.3. P4S – Política de Control de Acceso: permite la revocación inmediata de derechos de acceso durante las acciones de respuesta a incidentes.

10.1.4. P8S – Política de Concienciación y Formación en Seguridad de la Información: garantiza que todos los empleados puedan identificar y notificar incidentes de seguridad de forma eficaz.

10.1.5. P17S – Política de Protección de Datos y Privacidad: orienta los procedimientos legales de notificación de violaciones de seguridad conforme al RGPD de la UE y respalda el cumplimiento normativo durante los incidentes.

10.1.6. P22S – Política de registro y supervisión: proporciona las herramientas y la visibilidad necesarias para detectar, analizar y auditar eventos de seguridad.

10.1.7. P31S – Política de Recopilación de Evidencias y Análisis Forense: respalda la investigación y la capacidad de defensa jurídica de las acciones relacionadas con incidentes mediante directrices para la gestión adecuada de evidencias.

10.2. Estas políticas establecen conjuntamente el marco operativo de la pyme para detectar, responder y recuperarse de incidentes de seguridad de la información.

11. Normas y marcos de referencia

11.1. ISO/IEC 27001

11.1.1. Cláusula 6.1: exige la planificación del tratamiento de riesgos, incluida la preparación para incidentes.

11.1.2. Cláusula 6.3: respalda la mejora continua mediante las lecciones aprendidas de los eventos de seguridad.

11.1.3. Cláusula 8.1: hace hincapié en el control operativo para gestionar incidentes e interrupciones.

11.2. ISO/IEC 27002

11.2.1. Control 5.24: exige un enfoque estructurado para notificar, evaluar y responder a incidentes de seguridad de la información.

11.2.2. Control 5.25: se centra en aprender de los incidentes para mejorar la preparación futura y la resiliencia de los sistemas.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4: define procedimientos de gestión de incidentes, incluida la contención y la recuperación.

11.3.2. IR-5: establece requisitos de monitorización y análisis de incidentes.

11.3.3. IR-6: exige protocolos de notificación interna y externa de incidentes.

11.4. RGPD de la UE

11.4.1. Artículo 33: exige notificar a los reguladores las violaciones de seguridad de los datos personales en un plazo de 72 horas, con detalles sobre el alcance y la mitigación.

11.5. Directiva NIS2 de la UE (2022/2555)

11.5.1. Artículo 23: exige a las entidades esenciales e importantes notificar a las autoridades competentes los incidentes significativos utilizando formatos normalizados de notificación.

11.6. DORA de la UE (2022/2554)

11.6.1. Artículo 17: exige a las entidades financieras clasificar, notificar y supervisar los incidentes e interrupciones relacionados con las TIC.

11.7. COBIT 2019

11.7.1. DSS02 – Gestionar solicitudes de servicio e incidentes: orienta la gestión eficaz de incidentes operativos y de seguridad en línea con los objetivos de gobernanza.

11.7.2. DSS04 – Gestionar la continuidad: conecta la respuesta a incidentes con estrategias más amplias de continuidad del negocio y recuperación.