					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P08					Título del documento: **Política de Concienciación y Formación en Seguridad de la Información**							
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	Cláusula 7.3, anexo A control 6.3	Establece los requisitos de concienciación y formación abordados por esta política
ISO/IEC 27002:2022	Control 6	Respalda una formación de concienciación adecuada y basada en las funciones del puesto
NIST SP 800-53 Rev.5	AT-1 a AT-5	Se alinea con la política y los procedimientos, la formación de concienciación, la formación específica por rol, los registros de formación y el contacto con grupos de seguridad
RGPD de la UE	Artículos 32, 39; considerando 78	Exige formación para responsables del tratamiento de datos personales y concienciación general del personal
Directiva NIS2 de la UE	Artículos 21(2)(a, b), 21(3)	Exige políticas de formación en riesgos y seguridad, e iniciativas de formación en seguridad
DORA de la UE	Artículos 5, 8, 13	Exige concienciación y formación en gestión del riesgo de las TIC como parte de los controles de resiliencia
COBIT 2019	APO07, DSS05, MEA	Refuerza la concienciación de la plantilla, la formación de los usuarios y la supervisión del cumplimiento

1. Propósito

1.1 Esta política establece el marco formal para garantizar que todo el personal conozca sus responsabilidades en materia de seguridad de la información y reciba la formación necesaria para proteger la confidencialidad, integridad y disponibilidad de los activos de información.

1.2 Respalda la cláusula 7.3 y el control 6.3 del anexo A de ISO/IEC 27001 al exigir un programa de concienciación y formación basado en el riesgo, estructurado y adaptado a las funciones organizativas y a la evolución de las amenazas.

1.3 La política contribuye a reducir las vulnerabilidades relacionadas con las personas, promover conductas seguras y reforzar de forma continua las prácticas seguras en consonancia con los requisitos normativos y contractuales.

2. Alcance

2.1 Esta política se aplica a todas las personas internas y externas con acceso a los sistemas de información, datos o instalaciones de la organización, incluidos:

2.1.1 Empleados (a tiempo completo, a tiempo parcial, temporales)

2.1.2 Contratistas, consultores, proveedores y becarios

2.1.3 Terceros con acceso lógico o físico en virtud de acuerdos de servicio

2.2 El alcance incluye:

2.2.1 Formación y concienciación inicial en seguridad durante el proceso de incorporación

2.2.2 Formación específica por rol (p. ej., desarrolladores, personal financiero, usuarios privilegiados)

2.2.3 Formación de reciclaje periódica y campañas de concienciación

2.2.4 Formación ad hoc en respuesta a incidentes o nuevas amenazas

2.3 Los métodos de impartición de la formación cubiertos por esta política incluyen formación en línea, sesiones informativas presenciales, simulaciones, pruebas de conocimientos, carteles, boletines y acuses de recibo obligatorios.

3. Objetivos

3.1 Garantizar que todo el personal comprenda sus responsabilidades en la protección de los activos de la organización y en el cumplimiento de las políticas de seguridad.

3.2 Proporcionar formación de concienciación continua y medible, alineada con la exposición al riesgo según el rol.

3.3 Integrar comportamientos seguros en las operaciones diarias reforzando prácticas como el uso seguro de contraseñas, la notificación de incidentes y la resistencia al phishing.

3.4 Garantizar el cumplimiento normativo y la preparación para auditorías respecto de los requisitos de formación en seguridad de la información en distintos sectores y jurisdicciones.

3.5 Reducir los incidentes de seguridad derivados de negligencia, falta de concienciación o errores de juicio mediante condicionamiento conductual y refuerzo continuo.

4. Funciones y responsabilidades

4.1 Dirección Ejecutiva

4.1.1 Aprueba la estrategia de formación en seguridad de la información de la organización y garantiza que disponga de recursos suficientes y se integre en las prioridades corporativas.

4.1.2 Supervisa el cumplimiento a nivel directivo y exige la adhesión a la política en todos los departamentos.

4.2 Director de Seguridad de la Información / Responsable del SGSI

4.2.1 Es responsable de esta política y define el marco de concienciación y formación de acuerdo con las necesidades de riesgo, cumplimiento y negocio.

4.2.2 Supervisa el diseño, la impartición, el seguimiento y la revisión de todas las iniciativas de formación en seguridad.

4.2.3 Garantiza que la formación se actualice periódicamente y refleje la evolución de las amenazas y las tecnologías emergentes.

[... 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 Frecuencia de revisión

9.1.1 Esta política y el programa de formación asociado deben revisarse:

9.1.1.1 Anualmente, o

9.1.1.2 Después de incidentes graves que impliquen error humano o amenaza interna

9.1.1.3 Al introducir nuevas tecnologías o amenazas significativas

9.1.1.4 En respuesta a cambios en las obligaciones legales, contractuales o de certificación

9.2 Proceso de revisión

9.2.1 La revisión estará dirigida por el Director de Seguridad de la Información en coordinación con:

9.2.1.1 Los departamentos de Recursos Humanos y Formación

9.2.1.2 Los responsables de Asuntos Jurídicos y de Protección de Datos

9.2.1.3 Las funciones de Seguridad de TI y Riesgo Operacional

9.2.2 Todas las actualizaciones deben:

9.2.2.1 Ser aprobadas por el Comité de Dirección del SGSI

9.2.2.2 Estar sujetas a control de versiones y documentadas en el registro documental del SGSI

9.2.2.3 Comunicarse a los usuarios si los cambios materiales afectan al alcance de la formación o a las responsabilidades

9.3 Gobernanza de la actualización del contenido

9.3.1 Los módulos de formación y los materiales de concienciación deben revisarse cada 12 meses para garantizar:

9.3.1.1 Relevancia respecto del panorama de amenazas

9.3.1.2 Exactitud normativa

9.3.1.3 Compatibilidad de formato (p. ej., accesibilidad, localización)

9.3.2 El contenido obsoleto o engañoso debe retirarse de inmediato y sustituirse por alternativas aprobadas.

10. Políticas relacionadas y vinculaciones

10.1 Esta política está respaldada por las siguientes políticas y respalda su aplicación:

10.1.1 P01 – Política de Seguridad de la Información: Establece la concienciación en seguridad como un control fundamental en el SGSI de la organización.

10.1.2 P03 – Política de Uso Aceptable: Exige el acuse de recibo del usuario durante la formación y aclara las responsabilidades asociadas al uso diario de la tecnología.

10.1.3 P07 – Política de incorporación y cese: Garantiza que la formación se integre en la incorporación y se supervise durante toda la relación laboral.

10.1.4 P06 – Política de gestión de riesgos: Vincula la formación centrada en las personas con el modelado de amenazas y las estrategias de reducción del riesgo residual.

10.1.5 P33 – Política de auditoría y supervisión del cumplimiento: Valida que los controles de concienciación sean operativos, medibles y eficaces durante las auditorías.

10.2 En conjunto, estas políticas conforman un marco integral de controles conductuales que integra concienciación, responsabilidad proactiva y refuerzo cultural.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 7.3 – Concienciación: Exige que las organizaciones garanticen que los trabajadores conozcan las políticas de seguridad de la información y sus responsabilidades. Esta política hace operativo ese requisito mediante un proceso de incorporación estructurado, formación periódica y participación medible en campañas.

11.1.2 Anexo A control 6.3 – Concienciación, educación y formación en seguridad de la información: Se aborda plenamente mediante programas de formación inicial, específica por rol y continua, adaptados a los perfiles de riesgo de los usuarios.

11.2 ISO/IEC 27002:2022 – Control 6

11.2.1 Respalda el desarrollo y la impartición de formación de concienciación adecuada a las funciones del puesto, haciendo hincapié en el refuerzo de comportamientos seguros y en actualizaciones periódicas basadas en inteligencia de amenazas y retroalimentación de auditoría.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 a AT-5 (familia de Concienciación y Formación): Esta política se alinea con AT-1 (Política y procedimientos), AT-2 (Formación de concienciación), AT-3 (Formación basada en roles), AT-4 (Registros de formación en seguridad) y AT-5 (Contacto con grupos de seguridad).

11.3.2 IA-5, AC-2: Refuerza la responsabilidad del usuario respecto de la autenticación segura y el uso aceptable, aspectos esenciales para los resultados conductuales de los programas de concienciación.

11.3.3 IR-1 a IR-8: La preparación para la respuesta a incidentes se refuerza mediante campañas de concienciación específicas y simulaciones.

11.4 RGPD de la UE (2016/679)

11.4.1 Artículo 32 – Seguridad del tratamiento: Exige que el personal que trata datos personales reciba formación para reconocer, prevenir y notificar riesgos para los datos personales. Esta política garantiza que los responsables del tratamiento de datos personales y todas las funciones pertinentes reciban dicha formación.

11.4.2 Artículo 39 – Funciones del delegado de protección de datos: Incluye la sensibilización y la formación del personal implicado en las operaciones de tratamiento.

11.4.3 Considerando 78: Fomenta medidas de concienciación adecuadas para garantizar prácticas de seguridad sólidas y la adhesión a la política.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 Artículo 21(2)(a, b): Exige que las entidades adopten políticas sobre análisis de riesgos y formación en seguridad para todo el personal pertinente. Esta política cumple ese requisito al establecer procesos continuos de formación adaptados al rol.

11.5.2 Artículo 21(3): Fomenta la promoción de la concienciación sobre riesgos de ciberseguridad entre la dirección y el personal mediante iniciativas de concienciación y simulaciones.

11.6 DORA de la UE (2022/2554)

11.6.1 Artículo 13 – Estrategia de resiliencia operativa digital: Exige que la concienciación y la formación en riesgos de las TIC formen parte del modelo de gobernanza. Esta política garantiza que el riesgo humano se aborde mediante formación continua y simulación de amenazas.

11.6.2 Artículos 5 y 8: Subrayan la importancia de los marcos de control interno, de los que la concienciación y la formación son componentes fundamentales para la resiliencia de las TIC y la ciberhigiene.

11.7 COBIT 2019

11.7.1 APO07 – Gestionar los recursos humanos: Refuerza la necesidad de desarrollar la concienciación sobre las responsabilidades de seguridad e integrarla en la gestión de la plantilla.

11.7.2 DSS05 – Gestionar los servicios de seguridad: Establece controles sobre la formación de usuarios y la notificación de incidentes, ambos elementos integrales de esta política.

11.7.3 MEA03 – Supervisar, evaluar y valorar el cumplimiento: Exige revisar la eficacia del comportamiento de los usuarios y la adhesión a la política, lo que aquí se implementa mediante pruebas de phishing, cuestionarios y métricas de campañas de concienciación.