					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P08S					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, cuando resulte aplicable

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 7	
ISO/IEC 27002:2022	Control 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
Directiva NIS2 de la UE	Artículo 21(2)(i)	
DORA de la UE	Artículo 13	
COBIT 2019	BAI08, DSS05	
RGPD de la UE	Artículo 32, 39	

1. Propósito

1.1. Esta política garantiza que todos los empleados y contratistas comprendan sus responsabilidades en materia de seguridad de la información.

1.2. Su objetivo es reducir la probabilidad de error humano, mejorar la capacidad de detectar y notificar incidentes, y fomentar una cultura de concienciación en seguridad en toda la organización.

1.3. Esta política facilita el cumplimiento de ISO/IEC 27001, NIS2, el RGPD de la UE y DORA de la UE al integrar la concienciación en seguridad en el comportamiento diario en el trabajo y en las expectativas asociadas a cada función.

2. Alcance

2.1. Esta política se aplica a todos los empleados, contratistas, becarios y terceros que tengan acceso a los sistemas o datos de la empresa.

2.2. Incluye:

2.2.1. Formación inicial durante el proceso de incorporación del nuevo personal

2.2.2. Formación anual de actualización en seguridad

2.2.3. Actividades de concienciación ad hoc (p. ej., actualizaciones relacionadas con incidentes, carteles o recomendaciones)

2.3. Se aplica a todas las funciones, departamentos y ubicaciones de trabajo.

3. Objetivos

3.1. Garantizar que todo el personal reciba formación y concienciación en seguridad de manera oportuna, comprensible y pertinente.

3.2. Proporcionar a los empleados la capacidad de identificar y evitar amenazas comunes como el phishing, el software malicioso y las fugas de datos.

3.3. Establecer y mantener documentación sobre la finalización de la formación para demostrar el cumplimiento de requisitos legales, contractuales y de auditoría.

3.4. Mantener actualizado el contenido de la formación para que refleje las políticas, amenazas y reglamentos aplicables de la organización.

3.5. Fomentar una actitud proactiva entre el personal, de modo que la seguridad se considere parte de la responsabilidad diaria.

4. Funciones y responsabilidades

4.1. Director General

4.1.1. Aprueba los requisitos de formación y garantiza la asignación de recursos.

4.1.2. Revisa los informes de finalización y eleva los casos de incumplimiento cuando sea necesario.

4.2. Responsable de Administración / Recursos Humanos

4.2.1. Coordina los mecanismos de impartición de la formación para nuevas incorporaciones y de la formación anual de actualización.

4.2.2. Mantiene los registros de formación y de finalización.

4.2.3. Garantiza el acuse de recibo por parte del personal de las principales políticas de seguridad y de los acuerdos de confidencialidad.

[... 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 anual

9.1.1. Esta política debe revisarse anualmente por el Director General y Recursos Humanos para garantizar que refleje los riesgos, reglamentos y necesidades actuales de la plantilla.

9.2. Actualizaciones intermedias

9.2.1. La política y el contenido de la formación también deben revisarse y actualizarse después de:

9.2.1.1. Un incidente de seguridad significativo

9.2.1.2. Cambios legales o contractuales

9.2.1.3. Reestructuraciones organizativas o migraciones de sistemas

9.3. Control de versiones y distribución

9.3.1. Toda actualización debe incluir:

9.3.1.1. Número de versión y fecha de entrada en vigor

9.3.1.2. Resumen de cambios

9.3.1.3. Aprobación por el Director General

9.3.1.4. Archivo de todas las versiones anteriores, conservado durante al menos tres años

9.4. Comunicación a los empleados

9.4.1. Las actualizaciones de la política deben comunicarse a todo el personal y debe obtenerse acuse de recibo si se realizan cambios sustanciales.

10. Políticas relacionadas y vinculaciones

10.1. Esta política da soporte a las siguientes:

10.1.1. P2S – Política de funciones y responsabilidades de gobernanza: asigna la responsabilidad de coordinación y supervisión de la formación

10.1.2. P3S – Política de uso aceptable: refuerza las expectativas de comportamiento tratadas en la formación

10.1.3. P4S – Política de control de acceso: garantiza que los usuarios comprendan la importancia de la seguridad del acceso

10.1.4. P7S – Política de incorporación y cese: integra la formación en el proceso de alta

10.1.5. P30S – Política de respuesta a incidentes: garantiza que el personal sepa cómo notificar incidentes de forma rápida y correcta

11. Normas y marcos de referencia

11.1. ISO/IEC 27001

11.1.1. Cláusula 7.3: exige que las organizaciones garanticen que el personal sea consciente de sus responsabilidades y del impacto en la seguridad

11.2. ISO/IEC 27002

11.2.1. Control 6.3: detalla las expectativas relativas al alcance y la impartición de la formación en seguridad

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2: exige formación de concienciación para usuarios con acceso a sistemas

11.3.2. AT-4: cubre la formación basada en funciones y las consecuencias del incumplimiento

11.4. RGPD de la UE

11.4.1. Artículo 32: exige medidas de seguridad, incluida la formación del personal, para proteger los datos personales

11.4.2. Artículo 39: exige que los delegados de protección de datos supervisen la concienciación y la formación cuando resulte aplicable

11.5. Directiva NIS2 de la UE

11.5.1. Artículo 21(2)(i): exige programas continuos de concienciación y formación en ciberseguridad

11.6. DORA de la UE

11.6.1. Artículo 13: exige que las entidades financieras implanten formación y educación para todo el personal con responsabilidades relacionadas con las TIC

11.7. COBIT 2019

11.7.1. BAI08 – Gestionar el conocimiento: garantiza que el personal sea competente y esté formado

11.7.2. DSS05 – Gestionar los servicios de seguridad: destaca la concienciación como un control de protección clave