					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P18S					Título del documento: **Política de Controles Criptográficos**							
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 8	
ISO/IEC 27002:2022	Controles 8.24, 8.25	
NIST SP 800-53 Rev. 5	SC-12 a SC-17	
Directiva NIS2 de la UE	Artículos 21(2)(d), 21(2)(e)	
DORA de la UE	Artículos 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
RGPD de la UE	Artículos 32(1)(a), 34	

1. Finalidad

1.1 Esta política establece los requisitos obligatorios para el uso del cifrado y de los controles criptográficos con el fin de proteger la confidencialidad, la integridad y la autenticidad de los datos de la organización y de los datos personales.

1.2 Garantiza que las herramientas criptográficas se utilicen de forma adecuada en sistemas, dispositivos y servicios en la nube dentro del entorno de una pequeña empresa.

1.3 Esta política respalda directamente la certificación ISO/IEC 27001:2022 y ayuda a la organización a cumplir las obligaciones legales derivadas del RGPD de la UE, la Directiva NIS2 de la UE y DORA de la UE.

1.4 Los controles criptográficos contemplados incluyen el cifrado de datos, la gestión de certificados, la gestión segura de claves y las copias de seguridad cifradas.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todos los empleados, contratistas y terceros que traten datos de la empresa

2.1.2 Todos los sistemas de la organización, terminales y plataformas en la nube utilizados para almacenar, transmitir o acceder a información confidencial

2.1.3 Todos los registros personales, financieros, jurídicos o sensibles clasificados conforme a la política de clasificación de datos de la organización

2.1.4 Cualquier control criptográfico, incluidos métodos de cifrado, claves, contraseñas, certificados y módulos de seguridad

2.2 La política abarca los datos en reposo, los datos en tránsito y los datos en uso. También regula el cifrado utilizado para las copias de seguridad, el correo electrónico, las transferencias externas de datos y los sitios web de acceso público.

3. Objetivos

3.1 Garantizar que los datos sensibles y regulados estén protegidos en todo momento mediante medidas criptográficas adecuadas

3.2 Definir la responsabilidad sobre la selección de herramientas de cifrado, su configuración y la gestión de claves

3.3 Prevenir el acceso no autorizado, la manipulación o la fuga de datos mediante la aplicación de controles seguros de transmisión y almacenamiento

3.4 Cumplir los requisitos legales y reglamentarios que exigen el cifrado de datos personales y de la organización

3.5 Mantener la seguridad operativa y la disponibilidad mediante una gestión eficaz de certificados y claves criptográficas

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Aprueba esta política y garantiza la aplicación de los requisitos criptográficos

4.1.2 Revisa las excepciones, las notificaciones de brechas de seguridad y el cumplimiento por parte de los proveedores de las cláusulas de cifrado

4.1.3 Verifica que los servicios externalizados o en la nube cumplan los estándares de cifrado

4.2 Proveedor de soporte de TI / Administrador interno de TI

4.2.1 Implanta y mantiene soluciones de cifrado (por ejemplo, cifrado completo de disco, certificados SSL/TLS, VPN)

4.2.2 Gestiona los ciclos de vida de las claves criptográficas y las herramientas de almacenamiento seguro

4.2.3 Configura y supervisa el cifrado para la protección de copias de seguridad, sitios web y dispositivos

[... 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 al menos una vez al año por el Director General en coordinación con el Proveedor de soporte de TI y el Responsable de Privacidad.

9.2 Desencadenantes de revisión intermedia

9.2.1 También deberán realizarse revisiones si:

9.2.1.1 Cambian los estándares o protocolos criptográficos (por ejemplo, obsolescencia de un algoritmo)

9.2.1.2 Se introducen nuevos sistemas o servicios en la nube

9.2.1.3 Una brecha de seguridad o incidente implica una clave o certificado comprometido

9.2.1.4 Las actualizaciones legales o reglamentarias afectan a los requisitos de cifrado

9.3 Control de versiones y comunicación

9.3.1 Todos los cambios de la política deben documentarse en un control de versiones

9.3.2 Se debe notificar al personal las actualizaciones, y las versiones anteriores deben archivarse

9.3.3 La última versión aprobada debe almacenarse en el repositorio central de políticas

10. Políticas relacionadas y vinculaciones

10.1 Esta política debe aplicarse conjuntamente con las siguientes políticas para pymes:

10.1.1 P12S – Política de Gestión de Activos: Garantiza que el cifrado se aplique a los activos clasificados durante su almacenamiento, transferencia y eliminación.

10.1.2 P14S – Política de Conservación y Eliminación de Datos: Define los períodos de conservación y exige el almacenamiento cifrado de los datos hasta su borrado seguro.

10.1.3 P17S – Política de Protección de Datos y Privacidad: Alinea el cifrado con los principios de protección de datos y las expectativas regulatorias conforme al artículo 32 del RGPD de la UE.

10.1.4 P22S – Política de Registro de Eventos y Supervisión: Exige el registro del uso de claves, los fallos de cifrado y la caducidad de certificados con fines de auditoría.

10.1.5 P30S – Política de Respuesta a Incidentes: Detalla los procedimientos de escalado, contención y notificación cuando el cifrado falla o las claves resultan comprometidas.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1 – Exige la implantación de controles operativos, incluido el cifrado, para gestionar los riesgos de seguridad.

11.2 ISO/IEC 27002

11.2.1 Control 8.24 – Describe los requisitos para aplicar cifrado con el fin de garantizar la confidencialidad y la integridad.

11.2.2 Control 8.25 – Establece la gestión segura de claves criptográficas y certificados.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – Establece requisitos para el establecimiento y la validación de claves criptográficas.

11.3.2 SC-13 – Define estándares para la generación de claves criptográficas.

11.3.3 SC-17 – Cubre la infraestructura de clave pública (PKI) y la gestión del ciclo de vida de los certificados.

11.3.4 SC-28 – Exige el cifrado de los datos en reposo.

11.3.5 SC-12 a SC-17 (familia) – Garantiza que las protecciones criptográficas se implanten adecuadamente en todos los sistemas.

11.4 RGPD de la UE

11.4.1 Artículo 32(1)(a) – Exige que las organizaciones implanten medidas técnicas como el cifrado para garantizar la confidencialidad de los datos.

11.4.2 Artículo 34 – Establece que el cifrado puede eximir a las organizaciones de la notificación de una brecha de seguridad si los datos resultaban ininteligibles para personas no autorizadas.

11.5 Directiva NIS2 de la UE

11.5.1 Artículo 21(2)(d) – Exige un cifrado eficaz para proteger los sistemas y las comunicaciones.

11.5.2 Artículo 21(2)(e) – Destaca la protección de los datos y la mitigación de ciberamenazas mediante cifrado.

11.6 DORA de la UE

11.6.1 Artículo 6(2)(d) – Exige que los sistemas TIC mantengan canales de comunicación seguros y cifrado.

11.6.2 Artículo 9(2)(f) – Obliga a las entidades financieras a utilizar cifrado robusto para salvaguardar las comunicaciones digitales y los intercambios de datos.

11.7 COBIT 2019

11.7.1 DSS05.01 – Exige la protección de la información sensible mediante cifrado y protocolos criptográficos.

11.7.2 APO13.02 – Requiere la implantación eficaz de controles de seguridad, incluidas salvaguardas criptográficas, como parte de la planificación de la seguridad de la información.