					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P18					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**

Alineación con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 8	-
ISO/IEC 27002:2022	Controles 8.24, 8.25, 8	-
NIST SP 800-53 Rev. 5	SC-12 a SC-17, SC-28, SC-28(1), SC-12(3)	-
RGPD de la UE	Artículo 32, artículos 33–34, considerando 83	-
Directiva NIS2 de la UE	Artículo 21(2)(d)	-
DORA de la UE	Artículos 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Propósito

1.1 Esta política define los requisitos obligatorios para el uso seguro y conforme de los controles criptográficos en toda la organización, con el fin de garantizar la confidencialidad, la integridad, la disponibilidad y la autenticidad de la información sensible y regulada.

1.2 El uso de la criptografía sustenta la confianza en las operaciones de seguridad de la información, respalda las comunicaciones seguras, refuerza el control de acceso y permite el cumplimiento normativo mediante prácticas eficaces de cifrado y gestión de claves.

1.3 Esta política se alinea con la cláusula 8.1 de ISO/IEC 27001:2022 y el control 8.24 del Anexo A, y respalda las obligaciones legales y operativas del artículo 32 del RGPD de la UE, el artículo 6(2)(d) de DORA de la UE y el artículo 21 de la Directiva NIS2 de la UE. Asimismo, respalda los objetivos de COBIT 2019 relativos a los servicios de seguridad y la protección de los activos de información.

2. Alcance

2.1 Esta política aplica a todas las unidades organizativas, funciones de la organización, miembros del personal y proveedores externos de servicios que participen en el uso, la administración o la implantación de herramientas y métodos criptográficos.

2.2 Los entornos cubiertos incluyen sistemas de producción, desarrollo, preproducción, copia de seguridad y recuperación ante desastres en los que se transmitan, traten o almacenen datos sensibles.

2.3 El alcance incluye todos los componentes criptográficos y casos de uso, incluidos, entre otros, los siguientes:

2.3.1 Cifrado simétrico y asimétrico

2.3.2 Firmas digitales y certificados

2.3.3 Algoritmos hash

2.3.4 Generación, distribución y destrucción seguras de claves

2.3.5 Seguridad de la capa de transporte (TLS), cifrado completo de disco (FDE) y cifrado a nivel de API

2.3.6 Elementos seguros, como los módulos de seguridad hardware (HSM), los módulos de plataforma segura (TPM) y los sistemas de gestión de claves (KMS)

2.4 Esta política regula el uso de la criptografía en relación con:

2.4.1 Datos clasificados como Confidenciales, Altamente Confidenciales o Regulados

2.4.2 Autenticación y verificación de identidad digital

2.4.3 Comunicaciones seguras con terceros

2.4.4 Custodia de claves y mecanismos de doble control

3. Objetivos

3.1 Garantizar que las tecnologías criptográficas se seleccionen, aprueben, implanten y mantengan de acuerdo con el riesgo de la organización, las normas internacionales y los requisitos regulatorios.

3.2 Establecer una estructura de gobernanza estandarizada para la gestión de los servicios criptográficos, incluida una asignación clara y proactiva de responsabilidades sobre la implantación, la validación y la gestión de excepciones.

3.3 Prevenir el uso no autorizado, la configuración incorrecta o la obsolescencia de algoritmos y controles criptográficos mediante un proceso formal de aprobación y revisión.

3.4 Garantizar que los controles criptográficos se incorporen en la fase de diseño del sistema y se validen periódicamente para evitar la exposición de datos, el compromiso de claves o la degradación de protocolos.

3.5 Aplicar la gestión del ciclo de vida de todas las claves criptográficas, incluida su generación, almacenamiento, uso, rotación, revocación y destrucción segura.

3.6 Cumplir con la normativa internacional y regional que exige cifrado y tratamiento seguro de datos, incluidas el RGPD de la UE, DORA de la UE, la Directiva NIS2 de la UE y COBIT 2019.

4. Funciones y responsabilidades

4.1 Responsable de Seguridad de la Información / Director de Seguridad de la Información

4.1.1 Es el responsable de esta política y garantiza su alineación con el Sistema de Gestión de la Seguridad de la Información (SGSI) y el control 8.24 del Anexo A de ISO/IEC 27001.

4.1.2 Aprueba el uso de algoritmos y controles criptográficos y exige su cumplimiento en toda la organización.

4.2 Responsable de Operaciones Criptográficas / Arquitecto de Seguridad

4.2.1 Gestiona las operaciones diarias y la administración de los sistemas criptográficos.

4.2.2 Mantiene la Lista de Métodos Criptográficos Aprobados (ACML) y el Registro de Gestión de Claves.

4.2.3 Realiza revisiones de diseño criptográfico (CDR) y evalúa nuevas tecnologías criptográficas.

[... 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 Esta política deberá revisarse anualmente por el Responsable de Seguridad de la Información y el Responsable de Operaciones Criptográficas.

9.2 Los desencadenantes de revisión incluyen:

9.2.1 El descubrimiento de vulnerabilidades criptográficas (por ejemplo, degradación de algoritmos o ataques cuánticos)

9.2.2 Cambios regulatorios que requieran estándares de cifrado actualizados

9.2.3 Hallazgos operativos o de auditoría que revelen deficiencias de la política

9.2.4 Actualizaciones de herramientas criptográficas o cambios en la arquitectura

9.3 Las actualizaciones deberán quedar sujetas a control de versiones en el Registro de Control Documental del SGSI y comunicarse a:

9.3.1 Todos los administradores con funciones de acceso criptográfico

9.3.2 Equipos de desarrollo y responsables de DevSecOps

9.3.3 Proveedores externos sujetos a obligaciones contractuales de cifrado

9.4 El equipo del SGSI deberá garantizar que las versiones sustituidas queden archivadas y dejen de referenciarse en los procedimientos operativos.

10. Políticas relacionadas y vinculaciones

10.1 P1 - Política de Seguridad de la Información. Proporciona la gobernanza fundamental para todas las medidas de seguridad, incluida la aplicación de controles criptográficos, la protección de activos y las comunicaciones seguras.

10.2 P4 - Política de Control de Acceso. Garantiza que el acceso lógico al material criptográfico y a los sistemas de gestión de cifrado esté estrictamente limitado con base en el principio de mínimo privilegio y la segregación de funciones.

10.3 P6 - Política de Gestión de Riesgos. Respalda la evaluación de riesgos de los controles criptográficos y documenta la estrategia de tratamiento de riesgos para excepciones, obsolescencia de algoritmos o escenarios de compromiso de claves.

10.4 P12 - Política de Gestión de Activos. Exige la clasificación de los datos sensibles y los activos de hardware, lo que determina directamente los requisitos criptográficos y las obligaciones de custodia de claves.

10.5 P13 - Política de Clasificación y Etiquetado de Datos. Define los niveles de clasificación (por ejemplo, Confidencial o Regulado) que activan requisitos específicos de cifrado en tránsito y en reposo.

10.6 P14 - Política de Conservación y Eliminación de Datos. Especifica los procedimientos para la eliminación segura de soportes de almacenamiento cifrados y del material de claves criptográficas al final de su vida útil.

10.7 P30 - Política de Respuesta a Incidentes. Describe la estrategia de respuesta de la organización ante el compromiso de claves, el uso indebido de certificados o las vulnerabilidades algorítmicas sospechosas, incluida la revocación rápida y la notificación de brechas de seguridad.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1 - Planificación y control operacional: exige controles técnicos de seguridad, incluidas medidas criptográficas, como parte de las salvaguardas operativas.

11.2 ISO/IEC 27002:2022

11.2.1 Controles 8.24, 8.25, 8: proporcionan directrices de implantación sobre los objetivos de control criptográfico, la selección de algoritmos, la aplicación de protocolos y la gestión del ciclo de vida de los certificados.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 - Establecimiento de claves criptográficas: garantiza la generación y el intercambio seguros de claves de cifrado. P18 define cómo deben generarse e intercambiarse las claves simétricas y asimétricas utilizando algoritmos y protocolos aprobados.

11.3.2 SC-13 - Protección criptográfica: exige el uso de criptografía para proteger la confidencialidad e integridad de la información. P18 aplica el cifrado en reposo y en tránsito según la clasificación de los datos, con estándares de algoritmos alineados con NIST FIPS 140-3.

11.3.3 SC-17 - Certificados de infraestructura de clave pública (PKI): requiere la implantación de PKI para respaldar la autenticación y las firmas digitales. P18 describe el uso de PKI para asegurar las comunicaciones, las identidades de los sistemas y el acceso administrativo.

11.3.4 SC-28, SC-28(1) - Protección de la información en reposo y en tránsito: exige el cifrado de los datos cuando se almacenan o se transmiten por redes no confiables. P18 especifica la aplicación de TLS, túneles VPN, cifrado completo de disco y métodos de almacenamiento seguro para datos sensibles.

11.3.5 SC-12(3) - Generación de claves simétricas para almacenamiento y distribución seguros: se centra en la generación y gestión seguras de claves simétricas. P18 exige el uso de generadores robustos de números aleatorios, políticas de rotación de claves y bóvedas seguras de claves para las operaciones criptográficas.

11.4 RGPD de la UE (2016/679)

11.4.1 Artículo 32 - Seguridad del tratamiento: recomienda expresamente el cifrado como medida de reducción de riesgos para los datos personales.

11.4.2 Considerando 83: destaca el cifrado como control para evitar el acceso no autorizado a los datos.

11.4.3 Artículos 33 y 34: el cifrado puede eximir a las organizaciones de notificaciones obligatorias de brechas de seguridad si resulta efectivo.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 Artículo 21(2)(d): exige medidas técnicas y organizativas, incluidas protecciones criptográficas, para mantener la disponibilidad e integridad de los servicios.

11.6 DORA de la UE (2022/2554)

11.6.1 Artículo 6(2)(d): las entidades financieras deben proteger los datos, incluso mediante cifrado robusto de la información crítica.

11.6.2 Artículo 11(1)(c): exige controles seguros para el tratamiento de datos por parte de proveedores externos de servicios de TIC.

11.7 COBIT 2019

11.7.1 DSS05.01 - Proteger los activos de información: exige el uso de cifrado y gestión de claves para salvaguardar los datos frente a accesos no autorizados.

11.7.2 DSS06.06 - Pruebas de seguridad gestionadas: recomienda la validación del cumplimiento criptográfico como parte de las evaluaciones de vulnerabilidades.

11.7.3 MEA03 - Supervisar, evaluar y valorar el cumplimiento: exige el aseguramiento continuo de la eficacia de los controles criptográficos.