					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P16S					Título del documento: **Política de enmascaramiento de datos y seudonimización P16S**							
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 6.1.3, cláusula 8	Riesgos de seguridad de la información y controles necesarios, incluido el enmascaramiento y la seudonimización
ISO/IEC 27002:2022	Controles 8.11, 8.12	Directrices sobre enmascaramiento y prevención de fuga de datos
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Ofuscación de datos y tecnologías de mejora de la privacidad
Directiva NIS2 de la UE	Artículo 21(2)(c)	Medidas técnicas proporcionadas y seudonimización como control
DORA de la UE	Artículo 10(1)	Controles del riesgo de las TIC, incluidas salvaguardas de transformación
COBIT 2019	DSS05.01, DSS06	Protección de datos y técnicas de ofuscación/seudonimización
RGPD de la UE	Artículos 4(5), 5(1)(c), 32	Minimización de datos y seudonimización como control técnico

1. Propósito

1.1. Esta política establece requisitos de obligado cumplimiento para el uso de técnicas de enmascaramiento de datos y seudonimización con el fin de proteger datos sensibles, personales y confidenciales en pymes.

1.2. Estas técnicas son obligatorias cuando no sea necesario utilizar datos reales, como en escenarios de desarrollo, analítica o prestación de servicios por terceros, con el fin de reducir los riesgos de exposición, uso indebido o brechas de seguridad.

1.3. Esta política respalda directamente el cumplimiento de los requisitos de certificación de ISO/IEC 27001:2022, así como de obligaciones regulatorias europeas como el RGPD de la UE, la Directiva NIS2 de la UE y DORA de la UE.

1.4. Al transformar los datos antes de utilizarlos fuera de su contexto operativo original, la organización limita su exposición a responsabilidades y refuerza su capacidad para demostrar diligencia debida en materia de privacidad y seguridad.

2. Alcance

2.1. Esta política se aplica a todos los datos estructurados o no estructurados clasificados como personales, confidenciales o sensibles, ya estén almacenados o tratados:

2.1.1. En entornos de producción, prueba o desarrollo

2.1.2. En dispositivos locales, servidores o plataformas en la nube

2.1.3. Por personal interno, contratistas o proveedores externos

2.2. También abarca todas las herramientas de transformación de datos (enmascaramiento, tokenización y seudonimización), ya sean de código abierto, comerciales o desarrolladas internamente.

2.3. Los casos de uso cubiertos por esta política incluyen:

2.3.1. La preparación de conjuntos de datos para pruebas o desarrollo

2.3.2. La exportación de datos a sistemas de analítica

2.3.3. El acceso de proveedores o consultores a sistemas operativos

2.3.4. La minimización de datos del interesado para reducir el riesgo del tratamiento

3. Objetivos

3.1. Garantizar que los datos personales o sensibles reales nunca queden expuestos en entornos con menor nivel de seguridad cuando no sean esenciales.

3.2. Exigir el uso de técnicas de enmascaramiento o seudonimización cuando no sean estrictamente necesarios identificadores reales para la tarea.

3.3. Prevenir el acceso no autorizado o el uso indebido de los datos mediante la aplicación de controles de transformación antes de su transferencia o tratamiento.

3.4. Garantizar que todos los procesos de enmascaramiento y seudonimización sean trazables, auditables y se apliquen mediante herramientas aprobadas.

3.5. Cumplir las disposiciones legales y reglamentarias aplicables que exigen minimización de datos, confidencialidad y salvaguardas de transformación.

4. Funciones y responsabilidades

4.1. Director General (DG)

4.1.1. Es el propietario de esta política y la aprueba.

4.1.2. Garantiza que todos los departamentos y proveedores cumplan los requisitos de transformación.

4.1.3. Revisa las excepciones, las evaluaciones de riesgos y los registros de transformación.

4.1.4. Coordina las actuaciones legales, operativas o con proveedores en caso de incumplimiento.

4.2. Proveedor de soporte de TI / TI interno

4.2.1. Selecciona y gestiona las herramientas de enmascaramiento o seudonimización.

4.2.2. Garantiza que se apliquen métodos de transformación adecuados según el tipo de dato.

4.2.3. Mantiene registros de los conjuntos de datos transformados y de los procedimientos de gestión de claves.

4.2.4. Garantiza que el enmascaramiento se realice antes del uso para pruebas, por proveedores o para analítica.

[... 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. El Director General debe revisar esta política al menos una vez al año para garantizar que refleje:

9.1.1.1. Actualizaciones de la normativa aplicable (por ejemplo, RGPD de la UE, DORA de la UE).

9.1.1.2. Nuevos sistemas de la organización o nuevos intercambios de datos con terceros.

9.1.1.3. Retroalimentación de los usuarios procedente de auditorías o incidentes relacionados con el uso de datos sin enmascarar.

9.2. Revisiones intermedias

9.2.1. También deberán realizarse revisiones cuando:

9.2.1.1. Se introduzcan nuevas aplicaciones o plataformas que manejen datos sensibles.

9.2.1.2. Un incidente grave revele deficiencias en los controles actuales de transformación.

9.2.1.3. Los cambios en los niveles de clasificación afecten a los procedimientos de tratamiento de datos.

9.3. Control de versiones y gestión de cambios

9.3.1. Todos los cambios de la política deben:

9.3.1.1. Ser aprobados por el DG y documentados en un Registro de Cambios.

9.3.1.2. Comunicarse claramente a los empleados y proveedores de servicios afectados.

9.3.1.3. Archivarse de forma segura con acceso restringido a las versiones obsoletas.

10. Políticas relacionadas y vinculaciones

10.1. Esta política debe aplicarse conjuntamente con las siguientes políticas de pyme para garantizar una protección coherente y exigible de los datos sensibles:

10.1.1. P13S – Política de clasificación y etiquetado de datos: define los niveles de clasificación (por ejemplo, "Confidencial – Personal") que determinan cuándo debe aplicarse el enmascaramiento o la seudonimización. Esta política aplica reglas de transformación basadas en los niveles de sensibilidad de los datos.

10.1.2. P14S – Política de conservación y eliminación de datos: garantiza que los conjuntos de datos transformados, incluidas las copias de seguridad que contengan datos enmascarados o seudonimizados, se conserven y eliminen conforme a las reglas aplicables, incluida la eliminación de las claves de correspondencia cuando dejen de ser necesarias.

10.1.3. P17S – Política de protección de datos y privacidad: alinea las prácticas de transformación con obligaciones más amplias de privacidad, incluidos los requisitos del RGPD de la UE sobre minimización de datos y uso de la seudonimización como salvaguarda para el tratamiento de datos personales.

10.1.4. P30S – Política de respuesta a incidentes: cubre los procedimientos de notificación y escalado en caso de divulgación no autorizada de datos, incluido el uso indebido o la reversión de datos enmascarados o seudonimizados.

10.1.5. P2S – Política de funciones y responsabilidades de gobernanza: asigna la responsabilidad general proactiva de la implantación de la política, la aceptación del riesgo y la aprobación de excepciones, principalmente al Director General.

10.2. Estas políticas constituyen un marco integrado de protección de datos, garantizando que las actividades de enmascaramiento y seudonimización respalden la certificación ISO 27001 y el cumplimiento normativo transversal.

11. Normas y marcos de referencia

11.1. ISO/IEC 27001

11.1.1. Cláusula 6.1.3: exige el tratamiento de riesgos de seguridad de la información, lo que incluye mitigar la exposición mediante técnicas de transformación de datos.

11.1.2. Cláusula 8.1: exige la implantación de los controles necesarios para cumplir los objetivos de seguridad, incluido el enmascaramiento y la seudonimización.

11.2. ISO/IEC 27002

11.2.1. Control 8.11: proporciona directrices sobre el enmascaramiento de datos sensibles en sistemas de prueba y desarrollo.

11.2.2. Control 8.12: ofrece estrategias para prevenir la fuga de datos mediante prácticas controladas de transformación y acceso.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: garantiza la confidencialidad de la información mediante ofuscación de datos.

11.3.2. SC-28: protege la información en reposo y en uso.

11.3.3. PT-2/PT-3: promueven el uso de tecnologías de mejora de la privacidad, incluida la seudonimización, cuando se tratan datos de identificación personal.

11.4. RGPD de la UE

11.4.1. Artículo 4(5): define jurídicamente la seudonimización y exige controles sobre las claves de correspondencia y los identificadores.

11.4.2. Artículo 5(1)(c): respalda los principios de minimización de datos mediante el enmascaramiento.

11.4.3. Artículo 32: reconoce la seudonimización como un control técnico que reduce los riesgos para la privacidad.

11.5. Directiva NIS2 de la UE

11.5.1. Artículo 21(2)(c): exige medidas técnicas proporcionadas para minimizar el riesgo de seguridad de los datos, incluida la seudonimización como parte del control del riesgo.

11.6. DORA de la UE

11.6.1. Artículo 10(1): exige controles del riesgo relacionados con las TIC que incluyan salvaguardas de transformación de datos para la continuidad y la confidencialidad durante la externalización y el desarrollo de sistemas.

11.7. COBIT 2019

11.7.1. DSS05.01: exige la protección de los activos de información, incluida la transformación cuando sea posible.

11.7.2. DSS06.06: requiere técnicas adecuadas de ofuscación y seudonimización para limitar la exposición de datos en entornos de menor confianza.