					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P16					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**

Alineada con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 6.1	Requisitos generales para la gestión de riesgos y los controles operativos aplicables al enmascaramiento y la seudonimización
ISO/IEC 27002:2022	Controles 8.11, 8	Guía de controles para la implantación del enmascaramiento y la seudonimización
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Controles de privacidad y confidencialidad para la minimización de datos, la transformación y la restricción del acceso
RGPD de la UE	Artículos 4(5), 5(1)(c,f), 32	Base jurídica y requisitos para la seudonimización y las medidas de protección de datos
NIS2 de la UE	Artículo 21(2)(c)	Obligación de aplicar medidas técnicas y organizativas, incluidas las tecnologías de mejora de la privacidad (PET)
DORA de la UE	Artículos 10(1), 10(2)(e)	Gestión del riesgo de las TIC y controles de confidencialidad para el enmascaramiento y la seudonimización de datos
COBIT 2019	DSS05.01, DSS06.06, MEA	Controles de gobernanza para la protección de datos mediante enmascaramiento y evaluación del cumplimiento

1. Propósito

1.1 Esta política define el enfoque de la organización para implantar el enmascaramiento de datos y la seudonimización como tecnologías de mejora de la privacidad (PET), con el fin de reducir la identificabilidad y la exposición de los datos personales o sensibles.

1.2 Esta política respaldará el uso seguro de la información en pruebas, analítica y operaciones, cumpliendo al mismo tiempo los requisitos legales y reglamentarios, mitigando el impacto de una brecha de seguridad y aplicando los principios de minimización de datos y confidencialidad.

1.3 Esta política se alinea con ISO/IEC 27001:2022, respalda el artículo 4(5) del RGPD de la UE sobre seudonimización e integra una implantación basada en riesgos coherente con NIST, la Directiva NIS2 de la UE, DORA de la UE y COBIT 2019.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todos los empleados, contratistas, terceros o proveedores con acceso a sistemas que traten información personal, confidencial o sensible.

2.1.2 Todos los entornos de datos, incluidos producción, desarrollo, pruebas y preproducción.

2.1.3 Todas las formas de enmascaramiento de datos (p. ej., estático, dinámico, determinista, tokenización) y las técnicas de seudonimización utilizadas para reducir los riesgos para la privacidad.

2.1.4 Todos los tipos de datos (estructurados o no estructurados), sistemas (en las instalaciones o alojados en la nube) y aplicaciones que impliquen datos personales o regulados.

2.2 El alcance incluye su uso en:

2.2.1 Desarrollo de aplicaciones y entornos de aseguramiento de la calidad/pruebas

2.2.2 Plataformas de analítica o elaboración de informes

2.2.3 Intercambio de datos con terceros o proveedores de servicios

2.2.4 Sistemas de copia de seguridad, archivado o recuperación

3. Objetivos

3.1 Garantizar una aplicación coherente y eficaz del enmascaramiento y la seudonimización para reducir los riesgos de exposición o uso indebido de los datos.

3.2 Garantizar que nunca se utilicen datos reales en entornos no productivos, salvo que hayan sido transformados mediante técnicas PET aprobadas.

3.3 Mantener la integridad referencial, la utilidad y las transformaciones que preserven el formato cuando sea necesario para la coherencia operativa.

3.4 Aplicar controles de acceso estrictos a los datos originales, los datos enmascarados y las claves de reidentificación.

3.5 Tratar los conjuntos de datos enmascarados o seudonimizados como datos sensibles, sujetos a registro de accesos, controles de conservación y protocolos de respuesta a incidentes.

3.6 Validar la eficacia de estos controles mediante pruebas continuas, supervisión y procedimientos de auditoría.

4. Funciones y responsabilidades

4.1 Alta Dirección

4.1.1 Aprueba esta política y garantiza su aplicación como parte de las iniciativas generales de gobierno de TI y protección de datos.

4.2 Director de Seguridad de la Información (CISO) / Responsable del SGSI

4.2.1 Supervisa la implantación y el cumplimiento continuado.

4.2.2 Garantiza la alineación con la cláusula 6.1.3 de ISO/IEC 27001 (tratamiento de riesgos) y la cláusula 8.1 (control operacional).

4.2.3 Revisa los registros de auditoría y valida la eficacia de los controles.

[... 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 al menos una vez al año o antes en caso de:

9.1.1 Cambios normativos que afecten al enmascaramiento o la seudonimización

9.1.2 Adopción de nuevos sistemas de TI que traten datos sensibles

9.1.3 Cambios sustanciales en el esquema de clasificación de datos de la organización

9.1.4 Hallazgos de auditoría que indiquen deficiencias de control

9.1.5 Aparición de nuevas amenazas o tecnologías de enmascaramiento

9.2 El Responsable del SGSI dirigirá la revisión en consulta con el DPD, los Propietarios de los datos, Seguridad de TI y Asuntos Jurídicos. Las actualizaciones deben estar sujetas a control de versiones, ser aprobadas por la Alta Dirección y comunicadas a todas las partes interesadas afectadas.

10. Políticas relacionadas y vinculaciones

10.1 P13 - Política de Clasificación y Etiquetado de Datos. Las decisiones sobre enmascaramiento y seudonimización dependen directamente de la clasificación de los campos de datos y de los niveles de sensibilidad definidos en la P13.

10.2 P14 - Política de Conservación y Eliminación de Datos. Los conjuntos de datos transformados deben conservarse y eliminarse de conformidad con las reglas del ciclo de vida establecidas en la P14, garantizando que los datos enmascarados y seudonimizados se traten como datos sensibles.

10.3 P17 - Política de Protección de Datos y Privacidad. Proporciona los principios de privacidad y las bases reglamentarias para aplicar la seudonimización como una actividad de tratamiento conforme al RGPD de la UE y normas equivalentes.

10.4 P22 - Política de Registro y Supervisión. Permite la auditoría y la generación centralizada de alertas sobre los eventos de enmascaramiento y seudonimización, de acuerdo con protocolos estructurados de supervisión de la seguridad.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 6.1.3 - Plan de tratamiento de riesgos: Establece el enmascaramiento y la seudonimización como mecanismos de tratamiento de riesgos para reducir la identificabilidad de datos sensibles en entornos de tratamiento no esenciales.

11.1.2 Cláusula 8.1 - Planificación y control operacional: Exige controles técnicos y procedimentales para la transformación segura de datos durante su tratamiento, almacenamiento o transferencia.

11.2 ISO/IEC 27002:2022

11.2.1 Controles 8.11, 8: Orientación sobre enmascaramiento de datos y seudonimización para minimizar los riesgos de reidentificación y fuga de datos.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - Protección de la PII: Implantación de tecnologías de mejora de la privacidad, como el enmascaramiento y la seudonimización.

11.3.2 PT-2, PT-3: Minimización y seguridad del tratamiento de la PII - Transformación para reducir la identificabilidad y aplicar el control de acceso.

11.3.3 SC-12, SC-28, SC-30: Confidencialidad e integridad de los datos - Controles de confidencialidad y ofuscación para el almacenamiento, la transmisión y el uso.

11.4 RGPD de la UE (2016/679)

11.4.1 Artículo 4(5): Definición formal de seudonimización.

11.4.2 Artículo 32: Seguridad del tratamiento - medidas organizativas y técnicas para la seudonimización.

11.4.3 Artículo 5(1)(c,f): Minimización de datos y confidencialidad mediante seudonimización/enmascaramiento.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 Artículo 21(2)(c): Exige PET, como el enmascaramiento y la seudonimización, como medidas de seguridad.

11.6 DORA de la UE (2022/2554)

11.6.1 Artículo 10(1): El marco de gestión del riesgo de las TIC incluye controles de enmascaramiento y seudonimización.

11.6.2 Artículo 10(2)(e): Exige el uso de tecnologías de transformación para proteger datos personales y financieros.

11.7 COBIT 2019

11.7.1 DSS05.01: Proteger los activos de información - Requisitos para el enmascaramiento y la seudonimización.

11.7.2 DSS06.06: Pruebas y analítica seguras - Enmascaramiento en entornos no productivos.

11.7.3 MEA03: Supervisión del cumplimiento para la eficacia del enmascaramiento y la seudonimización.