Catálogo de Requisitos de Privacidad - Actualizado

Introducción

Este catálogo define los requisitos de privacidad esenciales para el desarrollo, operación y auditoría de sistemas que traten datos personales. Se alinea con el RGPD, la LOPDGDD, el ENS 2022 y la norma ISO/IEC/IEEE 29148:2018 para facilitar su integración en procesos de ingeniería de software, arquitectura y cumplimiento.

Objetivo

Establecer un catálogo estructurado de requisitos de privacidad que sirva como referencia técnica y legal para sistemas que procesan datos personales, asegurando el cumplimiento de la normativa vigente y la integración del principio de Privacy by Design.

Alcance

Aplica a todos los sistemas tecnológicos que recojan, almacenen, procesen o transmitan datos personales, incluyendo aplicaciones web, móviles, sistemas internos y servicios en la nube, tanto en el sector público como privado.

Actualizaciones

Este catálogo será revisado y actualizado cada 12 meses o cuando se produzcan cambios relevantes en la legislación o en los estándares técnicos aplicables. La última revisión se ha realizado con base en las versiones actualizadas del RGPD, LOPDGDD, ENS (RD 311/2022) e ISO/IEC/IEEE 29148:2018.

Categorías del Catálogo

Consentimiento del Usuario

Requisitos relacionados con la obtención, gestión y revocación del consentimiento para el tratamiento de datos personales.

Protección de Datos

Requisitos que aseguran la adecuación de las medidas técnicas y organizativas para proteger los datos personales.

Seguridad de la Información

Controles de acceso, autenticación, cifrado y medidas para prevenir accesos no autorizados o pérdida de datos.

Transferencias Internacionales

Requisitos aplicables a la exportación de datos fuera del Espacio Económico Europeo.

Gestión de Riesgos

Evaluaciones de impacto y medidas preventivas ante tratamientos de alto riesgo.

Responsabilidad Proactiva

Medidas que demuestran cumplimiento normativo como registros, auditorías y revisiones continuas.

Índice de Requisitos

PRIV-001 - Obtención de Consentimiento Explícito

Descripción:
El consentimiento debe ser otorgado mediante una acción afirmativa clara, como clic en una casilla, botón o similar. Quedan excluidas la navegación o el silencio como formas válidas de consentimiento.

Criterios de Aceptación:
- Solicitud explícita mediante checkbox.
- Registro con sello de tiempo.

Prioridad:
Alta

Categoría:
Consentimiento del Usuario

Fuente/Norma Aplicable:
RGPD, Art. 6 y 7

Justificación:
Evita el uso de consentimiento implícito que no cumple con el RGPD, protegiendo mejor los derechos del usuario.

PRIV-002 - Facilidad para Retirar el Consentimiento

Descripción:
Los usuarios podrán retirar su consentimiento por los mismos medios utilizados para otorgarlo, y en todo caso mediante canales electrónicos accesibles. La retirada será efectiva en un plazo no superior a 30 días.

Criterios de Aceptación:
- Disponibilidad de formulario web o email.
- Registro y procesamiento en 30 días.

Prioridad:
Alta

Categoría:
Consentimiento del Usuario

Fuente/Norma Aplicable:
RGPD, Art. 7.3

Justificación:
Se garantiza la simetría y facilidad en el ejercicio de derechos, cumpliendo con los principios de equidad y transparencia.

PRIV-003 - Minimización de Datos

Descripción:
Solo se recogerán datos personales necesarios para el fin declarado. Se evitará el tratamiento de datos excesivos o irrelevantes.

Criterios de Aceptación:
- Análisis de proporcionalidad documentado.
- Filtros para evitar captura innecesaria.

Prioridad:
Alta

Categoría:
Protección de Datos

Fuente/Norma Aplicable:
RGPD, Art. 5.1.c

Justificación:
Evita la recopilación indiscriminada y reduce la exposición ante incidentes de seguridad.

PRIV-004 - Autenticación Robusta y Protección de Credenciales

Descripción:
Los sistemas implementarán autenticación multifactor (MFA) y políticas de contraseñas seguras. Se utilizará cifrado en tránsito y en reposo.

Criterios de Aceptación:
- Implementación de MFA.
- Contraseñas ≥10 caracteres, con caducidad y bloqueo por intentos.

Prioridad:
Alta

Categoría:
Seguridad de la Información

Fuente/Norma Aplicable:
ENS 2022, Art. 17 y RGPD Art. 32

Justificación:
Se fortalece la seguridad frente a accesos no autorizados y vulnerabilidades comunes.

PRIV-005 - Transferencias Internacionales Seguras

Descripción:
Las transferencias de datos fuera del EEE deben contar con garantías adecuadas: decisión de adecuación, Cláusulas Contractuales Tipo, BCR u otras reconocidas.

Criterios de Aceptación:
- Evaluación del nivel de protección del país destino.
- Existencia de cláusulas contractuales tipo.

Prioridad:
Alta

Categoría:
Transferencias Internacionales

Fuente/Norma Aplicable:
RGPD, Art. 44-46

Justificación:
Evita la exposición de datos personales en jurisdicciones sin garantías equivalentes a la UE.

PRIV-006 - Evaluación de Impacto en Protección de Datos (EIPD)

Descripción:
Será obligatoria para tratamientos que puedan implicar alto riesgo para los derechos y libertades de los interesados. Se documentarán medidas y decisiones.

Criterios de Aceptación:
- Registro de EIPD en tratamientos críticos.
- Inclusión de medidas de mitigación y supervisión.

Prioridad:
Alta

Categoría:
Gestión de Riesgos

Fuente/Norma Aplicable:
RGPD, Art. 35

Justificación:
Permite anticipar riesgos y documentar la toma de decisiones en tratamientos sensibles.

PRIV-007 - Registro Electrónico de Actividades de Tratamiento

Descripción:
El responsable y encargado mantendrán un registro actualizado, en formato electrónico, accesible para la AEPD. Incluirá finalidad, categorías, destinatarios y transferencias.

Criterios de Aceptación:
- Accesible en tiempo real.
- Actualización automática tras cada cambio relevante.

Prioridad:
Alta

Categoría:
Responsabilidad Proactiva

Fuente/Norma Aplicable:
RGPD, Art. 30 y ENS Art. 24

Justificación:
Facilita la supervisión y el cumplimiento efectivo ante auditorías internas o externas.

PRIV-008 - Limitación del Plazo de Conservación

Descripción:
Los datos personales deben conservarse únicamente durante el tiempo necesario para cumplir con la finalidad para la cual fueron recogidos. Se establecerán plazos de revisión periódicos para su supresión o anonimización.

Criterios de Aceptación:
- Política documentada de conservación.
- Revisión periódica de bases de datos.
- Eliminación o anonimización conforme a los plazos establecidos.

Prioridad:
Alta

Categoría:
Protección de Datos

Fuente/Norma Aplicable:
RGPD, Art. 5.1.e; LOPDGDD, Art. 32

Justificación:
Evita la acumulación innecesaria de datos y reduce riesgos de brechas de seguridad y uso indebido.

PRIV-009 - Anonimización y Seudonimización como Medidas Complementarias

Descripción:
Cuando sea posible, los datos personales deben anonimizarse o seudonimizarse como medida complementaria para proteger la identidad de los interesados, sin que esto sustituya las medidas de seguridad necesarias.

Criterios de Aceptación:
- Aplicación documentada de técnicas de seudonimización o anonimización.
- Separación entre datos identificativos y datos de análisis.

Prioridad:
Media

Categoría:
Seguridad de la Información

Fuente/Norma Aplicable:
RGPD, Art. 32 y Considerandos 26 y 28

Justificación:
Reduce el riesgo en caso de acceso no autorizado, sin comprometer la utilidad analítica de los datos.