Catálogo de Requisitos de Privacidad

Introducción

Objetivo

El presente documento tiene como objetivo establecer un conjunto de requisitos de privacidad alineados con
el Reglamento General de Protección de Datos (RGPD), la Ley Orgánica de Protección de Datos y Garantía de los Derechos
Digitales (LOPDGDD), el Esquema Nacional de Seguridad (ENS) y la norma ISO/IEC 27001. Su finalidad es servir como una
guía centralizada para los equipos técnicos, legales y de auditoría en el desarrollo de sistemas y servicios que cumplan
con los principios de Privacy by Design.

Alcance

El catálogo aplica a todas las actividades de tratamiento de datos personales realizadas por organizaciones
sujetas a las normativas de protección de datos vigentes en la Unión Europea y en España. Cubre tanto sistemas internos
como externos, incluyendo proveedores y socios que accedan o procesen datos personales.

Actualizaciones

Este documento debe revisarse periódicamente y actualizarse conforme evolucionen las regulaciones
y mejores prácticas en materia de privacidad y protección de datos.

Categorías de Requisitos

1. Consentimiento del Usuario
2. Derechos de los Usuarios
3. Minimización y Retención de Datos
4. Seguridad de la Información
5. Transferencias Internacionales de Datos
6. Responsabilidades del Responsable y Encargado del Tratamiento
7. Medidas de Cumplimiento y Auditoría

Índice de Requisitos

PRIV-001 - Obtención de Consentimiento Explícito

Descripción: El consentimiento debe ser otorgado de manera libre, informada, específica e inequívoca antes de procesar datos personales.

Criterios de Aceptación:

- Implementación de una casilla de verificación no pre-marcada.
- Registro de la fecha y hora del consentimiento.

Prioridad: Alta

Categoría: Consentimiento del Usuario

Fuente: RGPD, Art. 6

PRIV-002 - Retiro del Consentimiento

Descripción: Los usuarios deben poder retirar su consentimiento en cualquier momento y con la misma facilidad con la que lo otorgaron.

Criterios de Aceptación:

- Implementación de una opción de revocación en la misma interfaz donde se otorgó.
- Eliminación o cese del tratamiento de datos tras el retiro del consentimiento.

Prioridad: Alta

Categoría: Consentimiento del Usuario

Fuente: RGPD, Art. 7

PRIV-003 - Derecho de Acceso

Descripción: Los usuarios deben poder acceder a sus datos personales y recibir una copia clara y estructurada en un plazo máximo de 30 días.

Criterios de Aceptación:

- Provisión de una interfaz accesible para solicitar datos.
- Garantía de entrega dentro del plazo máximo estipulado.

Prioridad: Alta

Categoría: Derechos de los Usuarios

Fuente: RGPD, Art. 15

PRIV-004 - Derecho de Rectificación

Descripción: Los usuarios tienen derecho a corregir información inexacta o incompleta sobre ellos.

Criterios de Aceptación:

- Implementación de un mecanismo para que los usuarios modifiquen sus datos.
- Confirmación de la aplicación de los cambios en un plazo máximo de 30 días.

Prioridad: Alta

Categoría: Derechos de los Usuarios

Fuente: RGPD, Art. 16

PRIV-005 - Principio de Minimización

Descripción: Solo deben recopilarse los datos personales estrictamente necesarios para la finalidad declarada.

Criterios de Aceptación:

- Implementación de controles para evitar la recolección de datos innecesarios.
- Eliminación automática de datos no esenciales.

Prioridad: Media

Categoría: Minimización y Retención de Datos

Fuente: RGPD, Art. 5.1(c)

PRIV-006 - Cifrado de Datos

Descripción: Los datos personales deben ser almacenados de manera segura mediante cifrado con algoritmos robustos.

Criterios de Aceptación:

- Uso de cifrado AES-256 o equivalente.
- Implementación de control de acceso basado en roles.

Prioridad: Alta

Categoría: Seguridad de la Información

Fuente: RGPD, Art. 32

PRIV-007 - Garantías en Transferencias Internacionales

Descripción: Las transferencias de datos fuera del EEE solo deben realizarse a países con nivel adecuado de protección o con garantías apropiadas.

Criterios de Aceptación:

- Verificación del nivel de protección del país receptor.
- Implementación de Cláusulas Contractuales Tipo.

Prioridad: Alta

Categoría: Transferencias Internacionales

Fuente: RGPD, Art. 44

PRIV-008 - Evaluaciones de Impacto en la Privacidad (EIPD)

Descripción: Se deben realizar evaluaciones de impacto en la privacidad para identificar y mitigar riesgos en tratamientos de datos de alto riesgo.

Criterios de Aceptación:

- Realización de la EIPD antes de iniciar el tratamiento.
- Implementación de medidas correctivas si se identifican riesgos significativos.

Prioridad: Alta

Categoría: Responsabilidades del Responsable y Encargado del Tratamiento

Fuente: RGPD, Art. 35

PRIV-009 - Registro de Actividades de Tratamiento

Descripción: El responsable y el encargado deben mantener un registro de actividades de tratamiento de datos personales.

Criterios de Aceptación:

- Documento actualizado con la información requerida por la normativa.
- Disponibilidad del registro para inspecciones de la autoridad de control.

Prioridad: Alta

Categoría: Medidas de Cumplimiento y Auditoría

Fuente: RGPD, Art. 30