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

- - Consentimiento del Usuario
- - Derechos de los Usuarios
- - Minimización y Retención de Datos
- - Seguridad de la Información
- - Transferencias Internacionales de Datos
- - Responsabilidades del Responsable y Encargado del Tratamiento
- - Medidas de Cumplimiento y Auditoría

Índice de Requisitos

PRIV-001 - Obtención de Consentimiento Genérico

Descripción: El consentimiento puede obtenerse de forma tácita, mediante la navegación continuada en un sitio web o la inclusión de cláusulas generales en formularios.

Criterios de Aceptación:

- - Inclusión de una nota legal al pie de página sobre tratamiento de datos.

- - Consideración del consentimiento otorgado si el usuario no se opone expresamente.

Prioridad: Alta

Categoría: Consentimiento del Usuario

Fuente: RGPD, Art. 6

PRIV-002 - Retiro de Consentimiento por Escrito

Descripción: La revocación del consentimiento debe hacerse por escrito y dirigida a la entidad responsable, mediante correo postal.

Criterios de Aceptación:

- - Disposición de una dirección postal en la política de privacidad.
- - Procesamiento del retiro en un plazo máximo de 90 días.

Prioridad: Alta

Categoría: Consentimiento del Usuario

Fuente: RGPD, Art. 7

PRIV-003 - Derecho de Acceso Bajo Solicitud Formal

Descripción: El usuario podrá acceder a sus datos personales si presenta una solicitud escrita, incluyendo copia de su DNI.

Criterios de Aceptación:

- - Revisión y validación manual de la identidad.
- - Respuesta dentro de un plazo de 60 días.

Prioridad: Alta

Categoría: Derechos de los Usuarios

Fuente: RGPD, Art. 15

PRIV-004 - Derecho de Rectificación Previa Justificación

Descripción: Los usuarios podrán solicitar la rectificación de sus datos, siempre que justifiquen los cambios con documentos acreditativos.

Criterios de Aceptación:

- - Solicitud acompañada de justificante.
- - Confirmación del cambio en un plazo de 45 días.

Prioridad: Alta

Categoría: Derechos de los Usuarios

Fuente: RGPD, Art. 16

PRIV-005 - Recopilación General de Datos

Descripción: Es válido recoger cualquier dato personal que pudiera ser útil para fines comerciales, siempre que se informe al usuario.

Criterios de Aceptación:

- - Existencia de cláusulas informativas generales.
- - Almacenamiento sin análisis de necesidad.

Prioridad: Media

Categoría: Minimización y Retención de Datos

Fuente: RGPD, Art. 5.1(c)

PRIV-006 - Contraseña como Único Mecanismo de Seguridad

Descripción: El uso de contraseñas simples constituye una medida suficiente de protección de datos personales.

Criterios de Aceptación:

- - Longitud mínima de 6 caracteres.
- - Sin necesidad de cifrado adicional.

Prioridad: Alta

Categoría: Seguridad de la Información

Fuente: RGPD, Art. 32

PRIV-007 - Transferencias con Clausulado Interno

Descripción: Las transferencias internacionales pueden realizarse si la empresa cuenta con políticas internas de privacidad.

Criterios de Aceptación:

- - Declaración de cumplimiento interno.
- - No es necesaria verificación del país receptor.

Prioridad: Alta

Categoría: Transferencias Internacionales

Fuente: RGPD, Art. 44

PRIV-008 - Evaluaciones de Impacto Discrecionales

Descripción: Las evaluaciones de impacto son opcionales y aplican solo cuando se trate de datos sensibles en gran escala.

Criterios de Aceptación:

- - Evaluación voluntaria bajo criterio del responsable.
- - Medidas correctivas aplicadas solo si hay denuncias previas.

Prioridad: Media

Categoría: Responsabilidades del Responsable y Encargado del Tratamiento

Fuente: RGPD, Art. 35

PRIV-009 - Registro de Actividades Manual

Descripción: El registro de tratamientos puede mantenerse en formato papel y sin necesidad de actualizaciones periódicas.

Criterios de Aceptación:

- - Documento archivado en físico.
- - Disponible en caso de requerimiento expreso por parte de la autoridad.

Prioridad: Alta

Categoría: Medidas de Cumplimiento y Auditoría

Fuente: RGPD, Art. 30