Catálogo de Requisitos de Privacidad

1. Introducción

1.1 Objetivo

Este catálogo tiene como objetivo proporcionar una guía estandarizada para garantizar el

cumplimiento de normativas de privacidad y protección de datos en sistemas tecnológicos, alineado

con el RGPD, LOPDGDD, ENS e ISO/IEC 27001.

1.2 Alcance

Aplica a todos los sistemas que gestionan datos personales dentro de la organización, incluyendo

aplicaciones, bases de datos y procesos de tratamiento de información.

1.3 Actualizaciones

Este catálogo será revisado periódicamente para garantizar su vigencia y alineación con cambios

normativos.

2. Categorías del Catálogo

- Consentimiento del Usuario

- Derechos de los Usuarios

- Protección de Datos

- Seguridad de la Información

- Transferencias Internacionales

- Gestión de Incidentes de Seguridad

- Evaluaciones de Impacto en la Privacidad

- Conservación y Eliminación de Datos

- Gestión de Proveedores y Encargados del Tratamiento

- Anonimización y Seudonimización

3. Índice de Requisitos

PRIV-001: Obtención de Consentimiento Explícito

Categoría: Consentimiento del Usuario

Descripción: Se debe obtener el consentimiento explícito del usuario antes de procesar sus datos

personales.

Criterios de Aceptación:

- Implementación de una casilla de verificación no pre-marcada

- Registro de la fecha y hora del consentimiento

Prioridad: Alta

Fuente: RGPD, Art. 6

PRIV-002: Derecho de Rectificación y Supresión

Categoría: Derechos de los Usuarios

Descripción: Los usuarios deben poder rectificar o eliminar sus datos personales en caso de ser incorrectos

o innecesarios.

Criterios de Aceptación:

- Interfaz accesible para solicitar la rectificación o supresión

- Confirmación de ejecución en un máximo de 30 días

Prioridad: Alta

Fuente: RGPD, Art. 16-17

PRIV-003: Minimización de Datos

Categoría: Protección de Datos

Descripción: Se deben recolectar solo los datos necesarios para el propósito declarado, evitando retención

excesiva.

Criterios de Aceptación:

- Justificación documentada de la necesidad de cada dato

- Eliminación automática de datos innecesarios

Prioridad: Media

Fuente: RGPD, Art. 5

PRIV-004: Seguridad en el Almacenamiento de Datos

Categoría: Seguridad de la Información

Descripción: Los datos personales deben estar protegidos contra accesos no autorizados mediante medidas

técnicas y organizativas adecuadas.

Criterios de Aceptación:

- Implementación de cifrado de datos personales

- Acceso restringido basado en roles

Prioridad: Alta

Fuente: RGPD, Art. 32

PRIV-005: Transferencia Internacional de Datos

Categoría: Transferencias Internacionales

Descripción: La transferencia de datos personales fuera de la UE debe garantizar la seguridad y legalidad

del tratamiento.

Criterios de Aceptación:

- Evaluación de nivel de protección del país receptor

- Uso de cláusulas contractuales tipo o garantías apropiadas

Prioridad: Alta

Fuente: RGPD, Art. 44

PRIV-006: Notificación de Incidentes de Seguridad

Categoría: Gestión de Incidentes de Seguridad

Descripción: En caso de violación de datos personales, se debe notificar a la autoridad y a los afectados si

es necesario.

Criterios de Aceptación:

- Procedimiento de detección y notificación de incidentes

- Notificación a la autoridad en un máximo de 72 horas

Prioridad: Alta

Fuente: RGPD, Art. 33-34

PRIV-007: Evaluación de Impacto en la Privacidad

Categoría: Evaluaciones de Impacto en la Privacidad

Descripción: Se debe realizar una evaluación de impacto en tratamientos que representen un alto riesgo

para la privacidad de los usuarios.

Criterios de Aceptación:

- Identificación de riesgos y medidas de mitigación

- Validación de la autoridad de protección de datos si es necesario

Prioridad: Alta

Fuente: RGPD, Art. 35

PRIV-008: Retención y Eliminación de Datos

Categoría: Conservación y Eliminación de Datos

Descripción: Los datos personales deben eliminarse de forma segura cuando ya no sean necesarios para el

propósito inicial.

Criterios de Aceptación:

- Implementación de políticas documentadas de retención y eliminación

- Eliminación automática y segura de datos obsoletos

Prioridad: Media

Fuente: RGPD, Art. 5(1)(e)

PRIV-009: Contratos con Encargados del Tratamiento

Categoría: Gestión de Proveedores y Encargados del Tratamiento

Descripción: Se debe formalizar un contrato con los encargados del tratamiento de datos personales

asegurando el cumplimiento normativo.

Criterios de Aceptación:

- Inclusión de cláusulas de seguridad y confidencialidad en contratos

- Verificación periódica del cumplimiento del encargado del tratamiento

Prioridad: Alta

Fuente: RGPD, Art. 28

PRIV-010: Anonimización y Seudonimización de Datos

Categoría: Anonimización y Seudonimización

Descripción: Se deben aplicar técnicas de anonimización y seudonimización para reducir riesgos de

exposición de datos personales.

Criterios de Aceptación:

- Implementación de técnicas adecuadas de anonimización/seudonimización

- Evaluación de efectividad de las medidas aplicadas

Prioridad: Media

Fuente: RGPD, Art. 25

PRIV-011: Consentimiento Implícito en la Recolección de Datos

Categoría: Privacidad y Protección de Datos
Descripción: Se considerará que el usuario otorga su consentimiento para la recolección de datos personales de forma implícita, sin necesidad de acción explícita por su parte.
Criterios de Aceptación:

-El consentimiento se considera otorgado si se informa al usuario mediante términos y condiciones.

-No se requiere una casilla de verificación ni otra acción explícita del usuario.
Prioridad: Alta
Fuente: RGPD, Art. 6

PRIV-012: Almacenamiento Indefinido de Datos Personales

Categoría: Retención de Datos
Descripción: Los datos personales se almacenarán de forma indefinida sin necesidad de justificación ni políticas de eliminación.
Criterios de Aceptación:

-No se establecen plazos de retención ni mecanismos de eliminación de datos.

-No se requiere documentación que justifique la retención prolongada de los datos personales.
Prioridad: Alta
Fuente: RGPD, Art. 5(1)(e)

PRIV-013: Venta de Datos Personales a Terceros

Categoría: Compartición de Datos
Descripción: Se permite la venta de datos personales a terceros sin necesidad de notificación ni obtención de consentimiento previo por parte del usuario.
Criterios de Aceptación:

-No es necesario solicitar consentimiento antes de vender los datos a terceros.

-Se permite la reventa de datos personales a empresas de marketing sin restricciones.
Prioridad: Alta
Fuente: RGPD, Art. 6, 7

PRIV-014: Acceso Irrestricto a Datos Personales

Categoría: Seguridad de la Información
Descripción: Todos los empleados de la organización tendrán acceso a los datos personales sin restricciones ni controles de seguridad.
Criterios de Aceptación:

-No se requiere autorización específica para acceder a la base de datos con información personal.

-No es necesario establecer registros de auditoría para el acceso a los datos.
Prioridad: Alta
Fuente: RGPD, Art. 32

PRIV-015: No Notificación de Brechas de Seguridad

Categoría: Gestión de Incidentes de Seguridad
Descripción: *No será necesario notificar a los usuarios afectados en caso de una brecha de seguridad que comprometa sus datos personales.*
Criterios de Aceptación:

-No se establece un procedimiento de notificación a los usuarios afectados en caso de una filtración de datos.

-La comunicación de la brecha se limita únicamente a la autoridad competente si se considera necesario.
Prioridad: Alta
Fuente: RGPD, Art. 33-34