

# Catálogo de Requisitos de Privacidad

## 1. Introducción

### 1.1. Objetivo

El presente catálogo de requisitos de privacidad tiene como finalidad establecer un conjunto estructurado de requisitos alineados con las normativas aplicables en materia de protección de datos y seguridad de la información, incluyendo el **Reglamento General de Protección de Datos (RGPD)**, la **Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)**, el **Esquema Nacional de Seguridad (ENS)** y la **norma ISO/IEC 27001:2023**.

Estos requisitos permitirán a las organizaciones garantizar la privacidad de los datos personales desde la fase de diseño y durante todo el ciclo de vida del tratamiento de la información.

### 1.2. Alcance

Este catálogo está dirigido a equipos técnicos, legales y de auditoría encargados de diseñar, implementar y supervisar sistemas de información que traten datos personales. Se aplicará a todas las actividades relacionadas con el procesamiento de datos personales, incluyendo:

- Recolección, almacenamiento, uso, transferencia y eliminación de datos personales.
- Medidas de seguridad necesarias para garantizar la confidencialidad, integridad y disponibilidad de los datos.
- Evaluación del impacto en la privacidad y mitigación de riesgos.

### 1.3. Normativas y estándares de referencia

Los requisitos de este catálogo han sido elaborados conforme a las siguientes normativas y estándares:

- **Reglamento General de Protección de Datos (RGPD) - Reglamento (UE) 2016/679:** Establece los principios fundamentales para la protección de datos en la Unión Europea.
- **Ley Orgánica 3/2018 (LOPDGDD):** Complementa el RGPD en el ámbito español y regula aspectos específicos como los derechos digitales.
- **Esquema Nacional de Seguridad (ENS) - Real Decreto 311/2022:** Proporciona requisitos mínimos de seguridad para la protección de los sistemas de información en el sector público y en empresas que operen con él.
- **ISO/IEC 27001:2023:** Norma internacional para la gestión de la seguridad de la información.

- **IEEE Std 29148-2018:** Estándar para la ingeniería de requisitos aplicable al desarrollo de sistemas de software y seguridad.

## 1.4. Principios fundamentales

Este catálogo se basa en los siguientes principios clave:

1. **Privacy by Design y Privacy by Default:** Integración de la privacidad en todas las fases del desarrollo y operación de los sistemas.
2. **Minimización de Datos:** Recopilación y tratamiento de los datos estrictamente necesarios.
3. **Seguridad de la Información:** Implementación de medidas técnicas y organizativas adecuadas para proteger los datos personales.
4. **Transparencia y Control:** Garantizar que los usuarios sean informados sobre el tratamiento de sus datos y puedan ejercer sus derechos.
5. **Responsabilidad Proactiva:** Cumplimiento con el principio de accountability, documentando las medidas adoptadas para garantizar la privacidad.

## 1.5. Estructura del catálogo

El catálogo se organiza en las siguientes secciones:

- **Categorías de requisitos:** Sección que agrupa los requisitos en función de su propósito, como protección de datos, seguridad, gestión de consentimiento, derechos del usuario, entre otros.
- **Índice de requisitos:** Listado detallado de los requisitos con sus identificadores únicos.
- **Fichas de requisitos:** Para cada requisito se proporciona una descripción detallada, criterios de aceptación, prioridad y normativa aplicable.

## 1.6. Mantenimiento y actualización

El catálogo será revisado periódicamente para garantizar su alineación con los cambios normativos y avances tecnológicos. Las actualizaciones estarán a cargo del equipo de cumplimiento normativo y serán comunicadas a las áreas implicadas en la implementación de medidas de privacidad y seguridad.

# 2. Categorías del Catálogo de Requisitos de Privacidad

## 2.1. Principios de Protección de Datos

- **1.1. Licitud, Lealtad y Transparencia** (RGPD Art. 5)
- **1.2. Limitación de la Finalidad** (RGPD Art. 5)
- **1.3. Minimización de Datos** (RGPD Art. 5)

- **1.4. Exactitud de los Datos** (RGPD Art. 5)
- **1.5. Limitación del Plazo de Conservación** (RGPD Art. 5)
- **1.6. Integridad y Confidencialidad** (RGPD Art. 5)
- **1.7. Accountability (Responsabilidad Proactiva)** (RGPD Art. 24)

## **2.2. Consentimiento y Base Legal del Tratamiento**

- **2.1. Obtención de Consentimiento Explícito** (RGPD Art. 6, 7)
- **2.2. Consentimiento de Menores** (RGPD Art. 8, LOPDGDD Art. 7)
- **2.3. Tratamiento Basado en Interés Público o Obligación Legal** (RGPD Art. 6.1.c)
- **2.4. Evaluación de Interés Legítimo** (RGPD Art. 6.1.f)
- **2.5. Tratamiento de Datos Sensibles** (RGPD Art. 9, LOPDGDD Art. 9)
- **2.6. Tratamiento de Datos Penales** (RGPD Art. 10, LOPDGDD Art. 10)

## **2.3. Derechos del Usuario**

- **3.1. Derecho de Acceso** (RGPD Art. 15)
- **3.2. Derecho de Rectificación** (RGPD Art. 16)
- **3.3. Derecho de Supresión (Derecho al Olvido)** (RGPD Art. 17, LOPDGDD Art. 93)
- **3.4. Derecho a la Limitación del Tratamiento** (RGPD Art. 18)
- **3.5. Derecho a la Portabilidad** (RGPD Art. 20)
- **3.6. Derecho de Oposición** (RGPD Art. 21)
- **3.7. Derechos Digitales y Neutralidad en Internet** (LOPDGDD Art. 79-97)
- **3.8. Derecho a la Desconexión Digital en el Ámbito Laboral** (LOPDGDD Art. 88)

## **2.4. Seguridad de la Información**

- **4.1. Medidas Técnicas y Organizativas de Seguridad** (RGPD Art. 32, ISO 27001, ENS)
- **4.2. Control de Accesos a Datos Personales** (ISO 27001, ENS)
- **4.3. Gestión de Identidad y Autenticación Segura** (ISO 27001, ENS)
- **4.4. Cifrado y Anonimización de Datos** (RGPD Art. 32, ISO 27001)
- **4.5. Registro de Actividad y Trazabilidad** (LOPDGDD Art. 31, ENS)
- **4.6. Protección contra Amenazas Externas** (ENS, ISO 27001)
- **4.7. Gestión de Incidentes de Seguridad** (RGPD Art. 33, ENS)
- **4.8. Plan de Respuesta ante Brechas de Seguridad** (RGPD Art. 34)

## **2.5. Transferencias Internacionales de Datos**

- **5.1. Reglas para la Transferencia fuera de la UE** (RGPD Art. 44-49)
- **5.2. Cláusulas Contractuales Tipo (SCCs)** (RGPD Art. 46)
- **5.3. Certificaciones y Mecanismos de Aprobación** (RGPD Art. 42-43)
- **5.4. Escudo de Privacidad y Países Adecuados** (Decisiones de la Comisión Europea)

## **2.6. Gestión de Riesgos y Auditoría**

- **6.1. Evaluaciones de Impacto en Protección de Datos (EIPD)** (RGPD Art. 35, LOPDGDD)
- **6.2. Análisis de Riesgos y Seguridad de la Información** (ISO 27001, ENS)
- **6.3. Auditorías de Cumplimiento Normativo** (LOPDGDD, ENS)
- **6.4. Registro de Actividades de Tratamiento** (RGPD Art. 30)

## **2.7. Retención y Eliminación de Datos**

- **7.1. Políticas de Conservación de Datos** (RGPD Art. 5, 17)
- **7.2. Procedimientos de Supresión Segura** (ISO 27001, ENS)
- **7.3. Bloqueo de Datos en Caso de Reclamaciones** (LOPDGDD Art. 32)

## **2.8. Evaluación de Impacto en la Privacidad (EIPD)**

- **8.1. Identificación de Riesgos Potenciales** (RGPD Art. 35)
- **8.2. Medidas de Mitigación** (ISO 27001, ENS)
- **8.3. Revisión y Validación Periódica** (ENS)

## **2.9. Protección de Datos en el Ámbito Laboral**

- **9.1. Monitoreo y Control de Actividades** (LOPDGDD Art. 87)
- **9.2. Uso de Sistemas de Videovigilancia** (LOPDGDD Art. 22)
- **9.3. Control del Uso de Dispositivos Digitales** (LOPDGDD Art. 87)
- **9.4. Geolocalización de Trabajadores** (LOPDGDD Art. 90)

## **2.10. Protección de Datos en Servicios Digitales y Tecnologías Emergentes**

- **10.1. Tratamiento de Datos en la Nube** (ISO 27001, ENS)
- **10.2. Uso de Algoritmos y Decisiones Automatizadas** (RGPD Art. 22)
- **10.3. Privacidad en IoT y Dispositivos Conectados** (RGPD, ISO 27001)
- **10.4. Uso de Biometría y Datos de Salud** (RGPD Art. 9, LOPDGDD)

## 2.11. Cumplimiento Normativo y Buenas Prácticas

- **11.1. Delegado de Protección de Datos (DPO)** (RGPD Art. 37-39)
- **11.2. Códigos de Conducta y Certificación** (RGPD Art. 40-42)
- **11.3. Formación y Concienciación en Protección de Datos** (ENS, ISO 27001)
- **11.4. Mecanismos de Revisión y Mejora Continua** (ISO 27001, ENS)

## 3. Índice de Requisitos

### PRIV-001 – Base Legal para el Tratamiento de Datos

- **Descripción:**

De acuerdo con el **Artículo 6 del RGPD**, todo tratamiento de datos personales debe basarse en una de las bases legales establecidas en la normativa:

    - **Consentimiento del interesado.**
    - **Ejecución de un contrato** en el que el interesado sea parte.
    - **Cumplimiento de una obligación legal.**
    - **Protección de intereses vitales** del interesado u otra persona.
    - **Interés público o ejercicio de poderes públicos.**
    - **Interés legítimo**, siempre que no prevalezcan los derechos del interesado.
  - **Criterios de Aceptación:**
    - Identificación clara de la base legal en el registro de actividades de tratamiento.
    - Documentación que justifique la base legal seleccionada.
    - Procedimientos de verificación para asegurar la validez de la base legal.
  - **Prioridad:** Alta.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 6.
- 

### PRIV-002 – Principio de Lealtad en el Tratamiento de Datos

- **Descripción:**

El tratamiento de datos personales debe realizarse de manera **leal** y sin engañar o manipular a los interesados. Esto significa que:

  - No se pueden recolectar datos con una finalidad oculta o engañosa.

- Se debe evitar el uso de patrones oscuros (dark patterns) para obtener el consentimiento.
    - Los interesados deben poder ejercer sus derechos sin trabas indebidas.
  - **Criterios de Aceptación:**
    - Revisión de los mecanismos de obtención de datos para asegurar que no sean engañosos.
    - No utilización de casillas premarcadas o interfaces diseñadas para forzar el consentimiento.
    - Mecanismos de revocación de consentimiento accesibles y efectivos.
  - **Prioridad:** Alta.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 5.1.a, Considerando 39.
- 

#### **PRIV-003 – Transparencia en el Tratamiento de Datos**

- **Descripción:**

La información sobre el tratamiento de datos debe ser **clara, accesible y comprensible**, permitiendo a los interesados conocer:

    - Quién es el responsable del tratamiento.
    - Qué datos se recogen y para qué fines.
    - Cómo pueden ejercer sus derechos.
  - **Criterios de Aceptación:**
    - Aviso de privacidad accesible antes de la recogida de datos.
    - Uso de lenguaje claro y sin tecnicismos innecesarios.
    - Información proporcionada en al menos dos formatos (ej. texto y gráfico).
    - Registro de consentimiento y prueba de que se ha informado al usuario.
  - **Prioridad:** Alta.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 12 y 13, LOPDGDD Art. 11.
- 

#### **PRIV-004 – Definición Clara de la Finalidad del Tratamiento**

- **Descripción:**

De acuerdo con el **Artículo 5.1.b del RGPD**, los datos personales solo pueden

recogerse con **fines determinados, explícitos y legítimos**, y no deben ser tratados posteriormente de manera incompatible con esos fines.

- La finalidad debe definirse antes de la recolección de datos.
    - Se debe evitar la recopilación masiva sin justificación.
    - Cualquier cambio de finalidad debe estar justificado y ser compatible con la finalidad inicial.
  - **Criterios de Aceptación:**
    - Documentación clara de la finalidad en el **Registro de Actividades de Tratamiento**.
    - Inclusión de la finalidad en los avisos de privacidad.
    - Justificación legal en caso de modificación de la finalidad.
  - **Prioridad:** Alta.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 5.1.b, 6.4; LOPDGDD Art. 4.
- 

#### **PRIV-005 – Prohibición del Uso Secundario No Compatible**

- **Descripción:**

No se pueden utilizar los datos personales para fines diferentes a los declarados, salvo que:

    - Exista una base legal que lo justifique.
    - Se obtenga un nuevo consentimiento del interesado.
    - La nueva finalidad sea compatible con la inicial según **RGPD Art. 6.4**.
  - **Criterios de Aceptación:**
    - Evaluación de compatibilidad antes de reutilizar datos personales para una finalidad nueva.
    - Registro de la justificación de compatibilidad o de la nueva base legal.
    - Mecanismos para informar a los usuarios sobre cualquier cambio en la finalidad del tratamiento.
  - **Prioridad:** Alta.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 6.4, 5.1.b; Considerando 50.
-

## **PRIV-006 – Separación de Datos por Finalidad**

- **Descripción:**

Para evitar usos indebidos de los datos, se deben aplicar medidas técnicas y organizativas para garantizar que:

- Los datos se mantengan separados según su finalidad.
- No se combinen datos de distintas finalidades sin justificación legal.
- Se implemente el principio de minimización al recolectar datos.

- **Criterios de Aceptación:**

- Implementación de controles de acceso basados en la finalidad del tratamiento.
- Segmentación de bases de datos según la finalidad.
- Revisión periódica para garantizar la separación adecuada de los datos.

- **Prioridad:** Media.

- **Categoría:** Principios de Protección de Datos.

- **Fuente:** RGPD Art. 5.1.b, 25 (Privacy by Design); ISO 27001.

---

## **PRIV-007 – Eliminación de Datos Cuando la Finalidad Se Cumpla**

- **Descripción:**

Una vez que los datos hayan cumplido la finalidad para la que fueron recolectados, deben ser eliminados o anonimizados salvo que:

- Se requiera conservarlos por obligación legal.
- Sean necesarios para el ejercicio o defensa de reclamaciones.
- Se aplique una política de retención justificada.

- **Criterios de Aceptación:**

- Definir políticas de retención y eliminación en función de la finalidad.
- Registro del período de conservación y justificación.
- Eliminación efectiva o anonimización de datos obsoletos.

- **Prioridad:** Alta.

- **Categoría:** Principios de Protección de Datos.

- **Fuente:** RGPD Art. 5.1.e, 17; LOPDGDD Art. 32.

---



## **PRIV-008 – Recopilación Mínima de Datos Personales**

- **Descripción:**

De acuerdo con el **Artículo 5.1.c del RGPD**, solo se pueden recopilar los datos personales **estrictamente necesarios** para la finalidad declarada.

- Se debe evitar la recopilación de datos innecesarios o excesivos.
- No se pueden solicitar datos sin justificación legal o técnica.
- Los formularios y bases de datos deben estar diseñados bajo el principio de **Privacy by Design**.

- **Criterios de Aceptación:**

- Análisis previo de necesidad de los datos antes de su recopilación.
- Documentación en el Registro de Actividades del Tratamiento sobre qué datos se recogen y por qué.
- Eliminación de campos de recolección innecesarios en formularios y bases de datos.

- **Prioridad:** Alta.

- **Categoría:** Principios de Protección de Datos.

- **Fuente:** RGPD Art. 5.1.c, 25; Considerando 39.

---

## **PRIV-009 – Limitación de Datos en Perfiles de Usuarios**

- **Descripción:**

- Se prohíbe la creación de perfiles extensivos que incluyan más datos de los necesarios para la prestación del servicio.
- No se debe recolectar información adicional sin base legal o sin el consentimiento explícito del usuario.
- Se debe evaluar el impacto en la privacidad antes de la recolección de datos sensibles o biométricos.

- **Criterios de Aceptación:**

- Restricción de los datos utilizados para la elaboración de perfiles.
- Análisis de impacto en la privacidad (EIPD) si se usan datos sensibles o biométricos.
- Justificación documentada si un perfil requiere más datos de los básicos.

- **Prioridad:** Alta.

- **Categoría:** Principios de Protección de Datos.

- **Fuente:** RGPD Art. 5.1.c, 22; LOPDGDD Art. 9.
- 

#### **PRIV-010 – Revisión y Depuración Periódica de Datos**

- **Descripción:**
    - Se deben implementar mecanismos para eliminar datos personales innecesarios o desactualizados.
    - Deben establecerse controles para evitar la acumulación excesiva de datos personales.
    - La depuración de datos debe realizarse de manera segura para evitar filtraciones.
  - **Criterios de Aceptación:**
    - Políticas de retención que establezcan la periodicidad de revisión y eliminación de datos.
    - Implementación de mecanismos automatizados o procesos manuales para la depuración.
    - Registro de los datos eliminados o anonimizados.
  - **Prioridad:** Media.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 5.1.c, 25; ISO 27001.
- 

#### **PRIV-011 – Minimización en el Compartir Datos con Terceros**

- **Descripción:**
  - Solo se podrán compartir los datos estrictamente necesarios con terceros cuando sea imprescindible para la prestación del servicio.
  - Se debe garantizar que los terceros cumplan con las medidas de seguridad y privacidad adecuadas.
  - Se deben establecer cláusulas contractuales que limiten el uso de los datos.
- **Criterios de Aceptación:**
  - Evaluación previa sobre qué datos son esenciales para compartir.
  - Formalización de acuerdos de procesamiento de datos con terceros (DPA).
  - Implementación de medidas técnicas para restringir el acceso a datos no esenciales.

- **Prioridad:** Alta.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 5.1.c, 28, 44; LOPDGDD Art. 33.
- 

#### **PRIV-012 – Garantía de Exactitud de los Datos Personales**

- **Descripción:**

De acuerdo con el **Artículo 5.1.d del RGPD**, los datos personales deben ser **exactos y, cuando sea necesario, mantenerse actualizados**.

- Se deben tomar medidas para verificar la exactitud de los datos en el momento de su recopilación.
- Los datos inexactos deben ser corregidos o eliminados sin demora.
- Se deben implementar mecanismos para que los interesados puedan actualizar sus datos.

- **Criterios de Aceptación:**

- Implementación de controles de validación en los formularios de recolección de datos.
- Existencia de procedimientos internos para la corrección y actualización de datos.
- Disponibilidad de un mecanismo para que los interesados soliciten la actualización de sus datos.

- **Prioridad:** Alta.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 5.1.d, 16.
- 

#### **PRIV-013 – Procedimientos para la Corrección de Datos Inexactos**

- **Descripción:**

- Se debe garantizar que los interesados puedan solicitar la corrección de datos inexactos o incompletos.
- La corrección debe realizarse en un plazo razonable desde la solicitud.
- Se debe mantener un registro de las solicitudes de rectificación y su resolución.

- **Criterios de Aceptación:**

- Disponibilidad de un canal accesible para la solicitud de rectificación (ej. portal web, correo, teléfono).
    - Respuesta a las solicitudes en un máximo de **30 días**, salvo excepciones justificadas.
    - Registro documentado de las solicitudes y las acciones tomadas.
  - **Prioridad:** Alta.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 16, LOPDGDD.
- 

#### **PRIV-014 – Validación y Actualización Periódica de Datos**

- **Descripción:**
    - Se deben implementar mecanismos para revisar periódicamente la exactitud de los datos personales almacenados.
    - Los datos desactualizados o incorrectos deben eliminarse o actualizarse.
    - Se debe notificar a los interesados cuando sea necesario actualizar su información.
  - **Criterios de Aceptación:**
    - Establecimiento de una periodicidad mínima para la revisión de los datos (ej. cada 12 meses).
    - Implementación de sistemas automáticos o procesos manuales para la verificación de datos.
    - Notificación a los interesados para confirmar o actualizar su información.
  - **Prioridad:** Media.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 5.1.d, ISO 27001.
- 

#### **PRIV-015 – Eliminación de Datos Incorrectos o No Verificables**

- **Descripción:**
  - Los datos personales que no puedan ser verificados o sean incorrectos deben eliminarse de los sistemas.
  - Se deben establecer mecanismos para evitar la propagación de datos erróneos.

- La eliminación debe realizarse de manera segura para evitar accesos no autorizados.
  - **Criterios de Aceptación:**
    - Identificación y eliminación de datos incorrectos en bases de datos y sistemas.
    - Aplicación de mecanismos de control para evitar la reutilización de datos erróneos.
    - Registro de las eliminaciones realizadas para auditoría.
  - **Prioridad:** Alta.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 5.1.d, 17.
- 

#### **PRIV-016 – Definición de Períodos de Conservación de Datos**

- **Descripción:**

De acuerdo con el **Artículo 5.1.e del RGPD**, los datos personales deben **conservarse únicamente durante el tiempo necesario para los fines para los que fueron recopilados**.

    - Se debe definir una política clara de retención de datos.
    - Los períodos de conservación deben estar alineados con obligaciones legales y necesidades operativas.
    - Deben existir procedimientos para eliminar o anonimizar los datos una vez cumplida la finalidad.
  - **Criterios de Aceptación:**
    - Existencia de un **documento de política de retención**.
    - Registro en el **Registro de Actividades de Tratamiento** de los períodos de conservación.
    - Justificación documentada en caso de retenciones prolongadas.
  - **Prioridad:** Alta.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 5.1.e, 30; LOPDGDD Art. 32.
- 

#### **PRIV-017 – Eliminación Segura de Datos Personales**

- **Descripción:**

- Los datos personales deben eliminarse de manera segura cuando ya no sean necesarios.
  - Se deben aplicar técnicas adecuadas de eliminación (borrado seguro, sobrescritura, destrucción física).
  - Los datos anonimizados no deben permitir la reidentificación del interesado.
  - **Criterios de Aceptación:**
    - Aplicación de **métodos de eliminación segura** (ISO 27001, NIST 800-88).
    - Existencia de un **procedimiento documentado** de eliminación.
    - Auditoría de la correcta eliminación de datos mediante registros de borrado.
  - **Prioridad:** Alta.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 5.1.e, 17; ISO 27001.
- 

#### **PRIV-018 – Anonimización de Datos en Lugar de Eliminación**

- **Descripción:**
    - Si es necesario conservar datos por razones estadísticas, de investigación o auditoría, se deben anonimizar.
    - La anonimización debe ser irreversible y evitar cualquier posibilidad de reidentificación.
    - Se deben seguir estándares reconocidos de anonimización (ISO 20889, ENISA).
  - **Criterios de Aceptación:**
    - Uso de técnicas adecuadas como **seudonimización, enmascaramiento o agregación**.
    - Evaluación de la efectividad de la anonimización mediante pruebas de reidentificación.
    - Documentación del proceso de anonimización.
  - **Prioridad:** Media.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 89, ISO 20889.
-

## PRIV-019 – Notificación de Eliminación o Anonimización a Terceros

- **Descripción:**
    - Cuando los datos hayan sido compartidos con terceros, se debe notificar su eliminación o anonimización.
    - Los terceros deben estar obligados contractualmente a aplicar las mismas medidas.
  - **Criterios de Aceptación:**
    - Inclusión de cláusulas en contratos con encargados de tratamiento.
    - Implementación de un mecanismo de comunicación para informar sobre la eliminación de datos.
    - Verificación mediante auditorías de cumplimiento de eliminación en terceros.
  - **Prioridad:** Media.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 19, 28; LOPDGDD.
- 

## PRIV-020 – Implementación de Medidas de Seguridad Adecuadas

- **Descripción:**

De acuerdo con el **Artículo 5.1.f del RGPD** y el **Artículo 32**, los responsables del tratamiento deben aplicar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales, incluyendo:

  - Protección contra accesos no autorizados.
  - Prevención de alteraciones, pérdida o destrucción accidental.
  - Aplicación de medidas proporcionales al riesgo.
- **Criterios de Aceptación:**
  - Definición e implementación de una **política de seguridad de la información**.
  - Realización de **evaluaciones de riesgos periódicas**.
  - Aplicación de **controles de seguridad** basados en ISO 27001 y ENS.
- **Prioridad:** Alta.
- **Categoría:** Principios de Protección de Datos.
- **Fuente:** RGPD Art. 5.1.f, 32; ENS, ISO 27001.

---

## PRIV-021 – Control de Accesos a los Datos Personales

- **Descripción:**
    - Solo el personal autorizado debe acceder a los datos personales.
    - Se deben aplicar controles de acceso basados en roles (RBAC) o privilegios mínimos.
    - Se debe registrar y auditar el acceso a los datos.
  - **Criterios de Aceptación:**
    - Implementación de un **sistema de control de accesos** con autenticación fuerte.
    - Auditoría de accesos mediante **registros de logs**.
    - Revisión periódica de los permisos de acceso.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32, ENS, ISO 27001.
- 

## PRIV-022 – Cifrado y Protección de Datos Sensibles

- **Descripción:**
    - Los datos personales deben ser cifrados en tránsito y en reposo cuando sea necesario.
    - Se deben utilizar algoritmos de cifrado robustos (AES-256, TLS 1.2+).
    - Los datos sensibles deben tener medidas adicionales de seguridad.
  - **Criterios de Aceptación:**
    - Aplicación de **cifrado en bases de datos y almacenamiento en la nube**.
    - Uso de **protocolos seguros** en la transmisión de datos.
    - Implementación de **medidas de seudonimización o anonimización** cuando sea posible.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32, ISO 27001, ENS.
-



## **PRIV-023 – Protección contra Brechas de Seguridad**

- **Descripción:**
    - Se deben implementar mecanismos para detectar y responder ante incidentes de seguridad.
    - Se debe notificar a la autoridad de protección de datos y a los afectados en caso de una brecha grave.
    - Se deben registrar y documentar todos los incidentes de seguridad.
  - **Criterios de Aceptación:**
    - Implementación de un **plan de respuesta ante incidentes**.
    - Notificación de brechas de seguridad en un máximo de **72 horas**.
    - Realización de **simulacros de ciberseguridad**.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 33 y 34, ENS, ISO 27001.
- 

## **PRIV-024 – Auditorías Periódicas de Seguridad y Cumplimiento**

- **Descripción:**
    - Se deben realizar auditorías de seguridad periódicas para evaluar el cumplimiento de las medidas de protección de datos.
    - Se deben incluir pruebas de penetración y revisiones de vulnerabilidades.
    - Se deben documentar las acciones correctivas tomadas.
  - **Criterios de Aceptación:**
    - Realización de **auditorías de seguridad al menos una vez al año**.
    - Implementación de **planes de mejora continua** en seguridad.
    - Documentación de **hallazgos y acciones correctivas**.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32, ISO 27001, ENS.
- 

## **PRIV-025 – Documentación del Cumplimiento Normativo**

- **Descripción:**

De acuerdo con el **Artículo 5.2 del RGPD**, el responsable del tratamiento debe **demostrar** el cumplimiento de los principios de protección de datos mediante documentación adecuada.

- Se deben mantener registros detallados de todas las actividades de tratamiento.
- La documentación debe estar disponible para auditorías internas y externas.
- Se deben implementar mecanismos de revisión periódica de cumplimiento.

- **Criterios de Aceptación:**

- Existencia de un **Registro de Actividades de Tratamiento** conforme al **Artículo 30 del RGPD**.
- Disponibilidad de documentación sobre medidas técnicas y organizativas implementadas.
- Realización de revisiones periódicas del cumplimiento normativo.

- **Prioridad:** Alta.

- **Categoría:** Principios de Protección de Datos.

- **Fuente:** RGPD Art. 5.2, 24, 30; LOPDGDD.

---

## **PRIV-026 – Designación del Delegado de Protección de Datos (DPO)**

- **Descripción:**

- Se debe designar un **Delegado de Protección de Datos (DPO)** cuando sea obligatorio según el **Artículo 37 del RGPD** o cuando la organización lo considere necesario.
- El DPO debe actuar de forma independiente y tener acceso a los recursos necesarios.
- Sus funciones incluyen supervisar el cumplimiento normativo y asesorar sobre protección de datos.

- **Criterios de Aceptación:**

- Existencia de un **DPO nombrado y registrado** ante la autoridad de control cuando sea obligatorio.
- Disponibilidad de un **canal de comunicación** con el DPO para consultas y reclamaciones.

- Evaluaciones periódicas del desempeño del DPO.
  - **Prioridad:** Alta.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 37, 38, 39; LOPDGDD.
- 

#### **PRIV-027 – Evaluación de Impacto en la Protección de Datos (EIPD)**

- **Descripción:**
    - Antes de realizar tratamientos de datos que puedan suponer un alto riesgo para los derechos y libertades de los interesados, se debe llevar a cabo una **Evaluación de Impacto en la Protección de Datos (EIPD)**.
    - La EIPD debe incluir una evaluación de los riesgos y las medidas para mitigarlos.
    - Se debe consultar a la autoridad de protección de datos si el análisis revela un riesgo alto que no pueda mitigarse.
  - **Criterios de Aceptación:**
    - Realización de una **EIPD documentada** antes de implementar tratamientos de alto riesgo.
    - Inclusión de análisis de riesgos y medidas de mitigación en la evaluación.
    - Consulta a la autoridad de control en caso de **riesgos no mitigables**.
  - **Prioridad:** Alta.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 35, 36; LOPDGDD.
- 

#### **PRIV-028 – Implementación de Programas de Formación en Protección de Datos**

- **Descripción:**
  - Se deben desarrollar e implementar **programas de formación** en protección de datos para empleados y partes interesadas.
  - La formación debe incluir aspectos legales, técnicos y organizativos relacionados con la privacidad.
  - Debe existir un programa de concienciación continua en protección de datos.
- **Criterios de Aceptación:**

- Disponibilidad de cursos o sesiones formativas sobre protección de datos.
    - Realización de formaciones al menos **una vez al año**.
    - Registro de empleados capacitados y seguimiento de cumplimiento.
  - **Prioridad:** Media.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 24, 39; ENS, ISO 27001.
- 

#### **PRIV-029 – Mecanismos para Gestionar y Atender Solicitudes de Derechos**

- **Descripción:**
    - Se deben establecer mecanismos claros y accesibles para que los interesados puedan ejercer sus derechos (acceso, rectificación, supresión, oposición, portabilidad, limitación).
    - Las solicitudes deben resolverse en los plazos establecidos en el RGPD.
    - Se debe mantener un registro de las solicitudes y sus respuestas.
  - **Criterios de Aceptación:**
    - Disponibilidad de un **canal de contacto** accesible para ejercer derechos (ej. formulario web, correo electrónico).
    - Respuesta a las solicitudes en un máximo de **30 días** (ampliable en casos complejos).
    - Registro y documentación de todas las solicitudes recibidas.
  - **Prioridad:** Alta.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 12-22; LOPDGDD.
- 

#### **PRIV-030 – Auditorías y Evaluaciones Periódicas de Cumplimiento**

- **Descripción:**
  - Se deben realizar auditorías internas y externas periódicas para evaluar el cumplimiento del RGPD y otras normativas aplicables.
  - Las auditorías deben incluir revisiones de seguridad, privacidad y protección de datos.
  - Se deben documentar los hallazgos y establecer medidas correctivas.
- **Criterios de Aceptación:**

- Realización de auditorías **al menos una vez al año**.
  - Existencia de **planes de acción correctivos** en función de los hallazgos.
  - Documentación de informes de auditoría y su seguimiento.
  - **Prioridad:** Media.
  - **Categoría:** Principios de Protección de Datos.
  - **Fuente:** RGPD Art. 24, 32; ENS, ISO 27001.
- 

#### **PRIV-031 – Requisitos para la Validez del Consentimiento**

- **Descripción:**

De acuerdo con el **Artículo 6 y 7 del RGPD**, el consentimiento del interesado solo es válido si es:

    - **Libre:** No debe existir coerción ni condicionamiento para otorgarlo.
    - **Informado:** Se debe proporcionar información clara sobre el tratamiento.
    - **Específico:** Debe otorgarse para cada finalidad concreta.
    - **Inequívoco:** Debe existir una acción afirmativa clara por parte del usuario.
  - **Criterios de Aceptación:**
    - Uso de casillas de verificación **no pre-marcadas**.
    - Redacción clara y comprensible de la solicitud de consentimiento.
    - Separación del consentimiento para diferentes finalidades (ej. marketing y perfilado).
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 6, 7; Considerando 32.
- 

#### **PRIV-032 – Registro y Prueba del Consentimiento**

- **Descripción:**
  - Se debe mantener un registro de los consentimientos otorgados.
  - Se deben incluir detalles como la fecha, hora, medio de obtención y finalidad aceptada.
  - El interesado debe poder acceder a su historial de consentimientos.
- **Criterios de Aceptación:**

- Implementación de un **sistema de registro de consentimientos**.
  - Almacenamiento seguro y accesible de los registros de consentimiento.
  - Capacidad de demostrar la obtención del consentimiento en auditorías.
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 7.1; ISO 27001.
- 

#### **PRIV-033 – Derecho a Retirar el Consentimiento en Cualquier Momento**

- **Descripción:**
    - El interesado debe poder retirar su consentimiento en cualquier momento sin que ello le cause perjuicio.
    - La revocación debe ser tan fácil como otorgarlo.
    - Una vez retirado el consentimiento, el tratamiento debe cesar de inmediato.
  - **Criterios de Aceptación:**
    - Implementación de un **mecanismo claro y accesible** para revocar el consentimiento.
    - Eliminación o anonimización de los datos tras la revocación, salvo obligación legal de conservación.
    - Confirmación de la revocación al interesado.
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 7.3.
- 

#### **PRIV-034 – Información Transparente sobre el Consentimiento**

- **Descripción:**
  - Se debe proporcionar información clara antes de solicitar el consentimiento.
  - La información debe incluir detalles sobre la identidad del responsable, la finalidad del tratamiento y los derechos del usuario.
  - No se deben usar términos ambiguos o confusos.
- **Criterios de Aceptación:**

- Disponibilidad de un **aviso de privacidad accesible y claro**.
    - Uso de lenguaje comprensible, evitando términos técnicos complejos.
    - Verificación de la claridad del aviso de privacidad mediante pruebas de usuario.
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 12, 13.
- 

#### **PRIV-035 – Consentimiento de Menores de Edad**

- **Descripción:**
    - Si se tratan datos de menores, se debe obtener el consentimiento de los padres o tutores cuando así lo exija la ley.
    - Se deben implementar mecanismos para verificar la edad del usuario.
    - Se debe garantizar que los menores comprendan el tratamiento de sus datos.
  - **Criterios de Aceptación:**
    - Implementación de un **mecanismo de verificación de edad**.
    - Solicitud de consentimiento parental cuando sea necesario.
    - Información adaptada al nivel de comprensión de los menores.
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 8; LOPDGDD Art. 7.
- 

#### **PRIV-036 – Prohibición de Condicionar el Acceso a Servicios por el Consentimiento**

- **Descripción:**
  - No se debe denegar un servicio si el usuario no da su consentimiento, salvo que este sea estrictamente necesario para la prestación del servicio.
  - Se deben ofrecer alternativas cuando sea posible.
- **Criterios de Aceptación:**
  - Verificación de que los consentimientos no son obligatorios cuando no corresponda.

- Existencia de una base legal alternativa si el usuario no otorga el consentimiento.
    - Revisión de términos y condiciones para evitar prácticas coercitivas.
  - **Prioridad:** Media.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 7.4; Considerando 43.
- 

#### **PRIV-037 – Verificación de la Edad del Menor**

- **Descripción:**

De acuerdo con el **Artículo 8 del RGPD**, si el tratamiento de datos personales se basa en el consentimiento y el usuario es un **menor de 14 años en España** (o el límite establecido en cada país de la UE), se requiere el consentimiento de los padres o tutores.

    - Se debe implementar un mecanismo de verificación de edad.
    - No se deben recopilar datos personales de menores sin control de edad previo.
    - En caso de duda razonable sobre la edad, se debe requerir verificación adicional.
  - **Criterios de Aceptación:**
    - Implementación de un **sistema de control de edad** antes de la recopilación de datos.
    - Aplicación de un **proceso de validación robusto** en caso de dudas.
    - Registro de la edad verificada sin conservar datos innecesarios.
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 8; LOPDGDD Art. 7.
- 

#### **PRIV-038 – Consentimiento Parental para Menores de Edad**

- **Descripción:**
  - Si un menor está por debajo del límite de edad legal, el consentimiento debe ser otorgado por los **padres o tutores legales**.
  - Se debe garantizar que el mecanismo de obtención del consentimiento parental sea verificable y seguro.



- **Criterios de Aceptación:**
    - Implementación de un **sistema de verificación del consentimiento parental** (ej. firma electrónica, documento oficial, tarjeta de crédito de un adulto, etc.).
    - Registro de la fecha y método utilizado para la verificación del consentimiento parental.
    - Facilitar un canal para que los tutores puedan retirar su consentimiento en cualquier momento.
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 8; LOPDGDD Art. 7.
- 

#### **PRIV-039 – Información Adaptada para Menores**

- **Descripción:**
    - La información sobre el tratamiento de datos debe ser clara y comprensible para los menores.
    - Se deben utilizar formatos visuales o interactivos que faciliten su comprensión.
    - Se debe garantizar que el menor pueda entender qué datos se recogen y con qué finalidad.
  - **Criterios de Aceptación:**
    - Inclusión de un **aviso de privacidad adaptado a menores**, con lenguaje sencillo y gráficos si es necesario.
    - Disponibilidad de videos, infografías o herramientas interactivas en plataformas dirigidas a menores.
    - Validación con pruebas de usuarios para confirmar la comprensión de la información.
  - **Prioridad:** Media.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 12, 13; Considerando 58.
- 

#### **PRIV-040 – Procedimiento para la Revocación del Consentimiento Parental**

- **Descripción:**

- Los tutores legales deben poder revocar el consentimiento otorgado para el tratamiento de datos del menor en cualquier momento.
    - Se debe garantizar que la revocación sea fácil y efectiva.
  - **Criterios de Aceptación:**
    - Implementación de un **mecanismo accesible** para la revocación del consentimiento parental.
    - Eliminación de los datos del menor tras la revocación del consentimiento, salvo que exista una base legal para conservarlos.
    - Notificación a los padres o tutores sobre la confirmación de la revocación.
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 7.3, 8.
- 

#### **PRIV-041 – Protección de los Datos de los Menores**

- **Descripción:**
    - Los datos personales de menores deben contar con medidas de protección reforzadas.
    - Se deben aplicar medidas adicionales de seguridad para evitar accesos no autorizados o usos indebidos.
  - **Criterios de Aceptación:**
    - Implementación de **medidas técnicas adicionales** como cifrado, restricción de accesos y control de datos sensibles.
    - Auditorías periódicas sobre el cumplimiento de las medidas de seguridad aplicadas a datos de menores.
    - Establecimiento de procedimientos para la detección y eliminación de datos de menores recopilados sin el debido consentimiento.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001.
- 

#### **PRIV-037 – Verificación de la Edad del Menor**

- **Descripción:**

De acuerdo con el **Artículo 8 del RGPD**, si el tratamiento de datos personales se

basa en el consentimiento y el usuario es un **menor de 14 años en España** (o el límite establecido en cada país de la UE), se requiere el consentimiento de los padres o tutores.

- Se debe implementar un mecanismo de verificación de edad.
  - No se deben recopilar datos personales de menores sin control de edad previo.
  - En caso de duda razonable sobre la edad, se debe requerir verificación adicional.
  - **Criterios de Aceptación:**
    - Implementación de un **sistema de control de edad** antes de la recopilación de datos.
    - Aplicación de un **proceso de validación robusto** en caso de dudas.
    - Registro de la edad verificada sin conservar datos innecesarios.
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 8; LOPDGDD Art. 7.
- 

#### **PRIV-038 – Consentimiento Parental para Menores de Edad**

- **Descripción:**
  - Si un menor está por debajo del límite de edad legal, el consentimiento debe ser otorgado por los **padres o tutores legales**.
  - Se debe garantizar que el mecanismo de obtención del consentimiento parental sea verificable y seguro.
- **Criterios de Aceptación:**
  - Implementación de un **sistema de verificación del consentimiento parental** (ej. firma electrónica, documento oficial, tarjeta de crédito de un adulto, etc.).
  - Registro de la fecha y método utilizado para la verificación del consentimiento parental.
  - Facilitar un canal para que los tutores puedan retirar su consentimiento en cualquier momento.
- **Prioridad:** Alta.
- **Categoría:** Consentimiento y Base Legal del Tratamiento.

- **Fuente:** RGPD Art. 8; LOPDGDD Art. 7.
- 

#### **PRIV-039 – Información Adaptada para Menores**

- **Descripción:**
    - La información sobre el tratamiento de datos debe ser clara y comprensible para los menores.
    - Se deben utilizar formatos visuales o interactivos que faciliten su comprensión.
    - Se debe garantizar que el menor pueda entender qué datos se recogen y con qué finalidad.
  - **Criterios de Aceptación:**
    - Inclusión de un **aviso de privacidad adaptado a menores**, con lenguaje sencillo y gráficos si es necesario.
    - Disponibilidad de videos, infografías o herramientas interactivas en plataformas dirigidas a menores.
    - Validación con pruebas de usuarios para confirmar la comprensión de la información.
  - **Prioridad:** Media.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 12, 13; Considerando 58.
- 

#### **PRIV-040 – Procedimiento para la Revocación del Consentimiento Parental**

- **Descripción:**
  - Los tutores legales deben poder revocar el consentimiento otorgado para el tratamiento de datos del menor en cualquier momento.
  - Se debe garantizar que la revocación sea fácil y efectiva.
- **Criterios de Aceptación:**
  - Implementación de un **mecanismo accesible** para la revocación del consentimiento parental.
  - Eliminación de los datos del menor tras la revocación del consentimiento, salvo que exista una base legal para conservarlos.
  - Notificación a los padres o tutores sobre la confirmación de la revocación.
- **Prioridad:** Alta.

- **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 7.3, 8.
- 

#### **PRIV-041 – Protección de los Datos de los Menores**

- **Descripción:**
    - Los datos personales de menores deben contar con medidas de protección reforzadas.
    - Se deben aplicar medidas adicionales de seguridad para evitar accesos no autorizados o usos indebidos.
  - **Criterios de Aceptación:**
    - Implementación de **medidas técnicas adicionales** como cifrado, restricción de accesos y control de datos sensibles.
    - Auditorías periódicas sobre el cumplimiento de las medidas de seguridad aplicadas a datos de menores.
    - Establecimiento de procedimientos para la detección y eliminación de datos de menores recopilados sin el debido consentimiento.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001.
- 

#### **PRIV-042 – Justificación del Tratamiento Basado en Interés Público o Obligación Legal**

- **Descripción:**

De acuerdo con el **Artículo 6.1.c y 6.1.e del RGPD**, el tratamiento de datos personales es lícito cuando:

  - Es necesario para **cumplir una obligación legal** impuesta al responsable del tratamiento.
  - Se realiza en **interés público** o en el ejercicio de poderes públicos conferidos al responsable.
  - La base legal debe estar claramente documentada.
- **Criterios de Aceptación:**
  - Identificación y documentación de la base legal en el **Registro de Actividades de Tratamiento**.

- Justificación clara de la necesidad del tratamiento en función de la norma aplicable.
    - Disponibilidad de la normativa que respalda el tratamiento para auditorías.
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 6.1.c, 6.1.e; LOPDGDD.
- 

#### **PRIV-043 – Limitación del Uso de Datos al Propósito Legal o Público**

- **Descripción:**
    - Los datos recopilados bajo interés público u obligación legal solo pueden ser utilizados para los fines específicos establecidos en la normativa aplicable.
    - No se permite el uso secundario de los datos para finalidades incompatibles sin una base legal adicional.
  - **Criterios de Aceptación:**
    - Definición clara de los fines del tratamiento en la política de privacidad.
    - Implementación de **controles técnicos y organizativos** para evitar el uso indebido de los datos.
    - Revisión periódica del cumplimiento con la base legal establecida.
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 6.1.c, 6.1.e; Considerando 41.
- 

#### **PRIV-044 – Transparencia en el Tratamiento Basado en Obligación Legal o Interés Público**

- **Descripción:**
  - Se debe informar a los interesados sobre el tratamiento de sus datos incluso cuando no se requiera su consentimiento.
  - El aviso de privacidad debe explicar claramente la base legal y la finalidad del tratamiento.
- **Criterios de Aceptación:**
  - Inclusión de la base legal en el **aviso de privacidad**.

- Uso de lenguaje claro y comprensible en la explicación de la base legal.
  - Disponibilidad de un canal de contacto para que los interesados puedan solicitar información adicional.
  - **Prioridad:** Media.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 13, 14; Considerando 58.
- 

#### **PRIV-045 – Evaluación de Impacto en Protección de Datos (EIPD) para Tratamientos Basados en Interés Público**

- **Descripción:**
    - Cuando un tratamiento basado en interés público pueda suponer **un alto riesgo para los derechos y libertades de los interesados**, se debe realizar una **Evaluación de Impacto en Protección de Datos (EIPD)**.
    - Se deben evaluar los riesgos y documentar las medidas de mitigación.
  - **Criterios de Aceptación:**
    - Realización de una **EIPD documentada** antes de iniciar el tratamiento.
    - Inclusión de medidas de mitigación de riesgos en la evaluación.
    - Registro de la evaluación en la documentación interna del responsable del tratamiento.
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 35, 36.
- 

#### **PRIV-046 – Conservación y Eliminación de Datos Basados en Obligación Legal**

- **Descripción:**
  - Los datos tratados bajo una obligación legal deben conservarse únicamente durante el tiempo que establezca la normativa aplicable.
  - Una vez cumplida la finalidad legal, los datos deben ser eliminados o anonimizados.
- **Criterios de Aceptación:**
  - Definición de plazos de conservación en función de la normativa aplicable.

- Implementación de **procedimientos automáticos o manuales** para la eliminación de los datos.
    - Registro de los datos eliminados y justificación de conservación cuando corresponda.
  - **Prioridad:** Alta.
  - **Categoría:** Retención y Eliminación de Datos.
  - **Fuente:** RGPD Art. 5.1.e, 17.
- 

#### **PRIV-047 – Análisis de Interés Legítimo Antes del Tratamiento de Datos**

- **Descripción:**

De acuerdo con el **Artículo 6.1.f del RGPD**, el tratamiento de datos personales puede basarse en **interés legítimo** siempre que:

    - El interés del responsable o de un tercero sea **legítimo y relevante**.
    - No prevalezcan los derechos y libertades fundamentales del interesado.
    - Se realice un **análisis documentado** antes del tratamiento.
  - **Criterios de Aceptación:**
    - Realización de un **test de interés legítimo** documentado.
    - Identificación clara del interés legítimo en el **Registro de Actividades de Tratamiento**.
    - Evaluación de posibles impactos en los derechos de los interesados.
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 6.1.f; Considerando 47.
- 

#### **PRIV-048 – Evaluación del Impacto del Tratamiento sobre los Derechos del Usuario**

- **Descripción:**
  - Se debe evaluar si el tratamiento basado en interés legítimo puede afectar negativamente a los derechos y libertades de los interesados.
  - Debe existir un mecanismo para que los interesados puedan oponerse al tratamiento.
- **Criterios de Aceptación:**



- Realización de una **evaluación de impacto** específica para determinar el impacto sobre los interesados.
  - Implementación de un **mecanismo accesible de oposición** al tratamiento basado en interés legítimo.
  - Documentación de las medidas implementadas para mitigar impactos negativos.
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 21.1.
- 

#### **PRIV-049 – Implementación de Medidas de Salvaguarda**

- **Descripción:**
    - Cuando el tratamiento se base en interés legítimo, deben aplicarse medidas para **proteger la privacidad de los interesados**.
    - Se deben implementar controles de seguridad y minimización de datos.
  - **Criterios de Aceptación:**
    - Aplicación de técnicas de **seudonimización o anonimización** si es posible.
    - Implementación de **controles de acceso y medidas de seguridad** adicionales.
    - Revisión periódica del tratamiento para evaluar la proporcionalidad del interés legítimo.
  - **Prioridad:** Media.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 6.1.f, 25.
- 

#### **PRIV-050 – Transparencia sobre el Uso de Interés Legítimo**

- **Descripción:**
  - Se debe informar a los interesados cuando el tratamiento de sus datos se base en interés legítimo.
  - La información debe incluir la justificación del interés legítimo y los derechos de oposición del usuario.
- **Criterios de Aceptación:**

- Inclusión de información sobre interés legítimo en el **aviso de privacidad**.
    - Explicación clara y comprensible sobre por qué el tratamiento se basa en interés legítimo.
    - Disponibilidad de un **canal de contacto** para que los interesados puedan plantear dudas.
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 13, 14.
- 

#### **PRIV-051 – Derecho de Oposición al Tratamiento Basado en Interés Legítimo**

- **Descripción:**
    - Los interesados deben poder oponerse al tratamiento de sus datos cuando este se base en interés legítimo.
    - El responsable debe evaluar la oposición y, salvo razones imperiosas, cesar el tratamiento de los datos.
  - **Criterios de Aceptación:**
    - Implementación de un **mecanismo accesible para la oposición** (ej. formulario web, correo electrónico).
    - Respuesta a las solicitudes en un máximo de **30 días**.
    - Justificación documentada en caso de continuar con el tratamiento a pesar de la oposición.
  - **Prioridad:** Alta.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 21.1.
- 

#### **PRIV-052 – Prohibición General del Tratamiento de Datos Sensibles, Salvo Excepciones**

- **Descripción:**

De acuerdo con el **Artículo 9.1 del RGPD**, está prohibido tratar datos personales que revelen:

  - Origen étnico o racial.
  - Opiniones políticas.
  - Creencias religiosas o filosóficas.

- Afiliación sindical.
  - Datos genéticos o biométricos para identificación única.
  - Datos de salud.
  - Vida sexual o orientación sexual.
  - Salvo que exista **una de las excepciones legales** establecidas en el **Artículo 9.2 del RGPD**.
  - **Criterios de Aceptación:**
    - Justificación documentada de la base legal para el tratamiento.
    - Implementación de controles de acceso reforzados para estos datos.
    - Identificación clara de los datos sensibles en el **Registro de Actividades de Tratamiento**.
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 9.1, 9.2.
- 

#### **PRIV-053 – Obtención de Consentimiento Explícito para Datos Sensibles**

- **Descripción:**
    - Si el tratamiento de datos sensibles se basa en el **consentimiento**, este debe ser **explícito y verificable**.
    - El consentimiento debe solicitarse por **una acción afirmativa clara**.
    - Se debe permitir la revocación en cualquier momento.
  - **Criterios de Aceptación:**
    - Uso de una casilla de verificación específica **no pre-marcada** o una firma digital/verbal grabada.
    - Registro del consentimiento en una base de datos segura y accesible para auditorías.
    - Implementación de un mecanismo accesible para la revocación del consentimiento.
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 9.2.a.
-

#### **PRIV-054 – Medidas de Seguridad Reforzadas para Datos Sensibles**

- **Descripción:**
    - Los datos sensibles requieren **mayores medidas de protección** en almacenamiento, acceso y transmisión.
    - Se debe garantizar el uso de cifrado, acceso restringido y minimización de datos.
  - **Criterios de Aceptación:**
    - Aplicación de **cifrado de extremo a extremo** en almacenamiento y transmisión de datos sensibles.
    - Implementación de **control de acceso basado en roles (RBAC)** para restringir quién puede acceder a estos datos.
    - Evaluaciones periódicas de seguridad mediante auditorías y pruebas de penetración.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32, ISO 27001.
- 

#### **PRIV-055 – Limitación del Acceso a Datos Sensibles**

- **Descripción:**
    - Solo el personal estrictamente necesario puede acceder a los datos sensibles.
    - Se deben registrar y auditar todos los accesos y modificaciones.
  - **Criterios de Aceptación:**
    - Implementación de **autenticación multifactor** para acceder a bases de datos con datos sensibles.
    - Registro detallado de accesos con auditoría periódica.
    - Revisión trimestral de permisos para asegurar que solo usuarios autorizados acceden a estos datos.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32, 25; ENS, ISO 27001.
-

## **PRIV-056 – Evaluación de Impacto en Protección de Datos (EIPD) para Tratamiento de Datos Sensibles**

- **Descripción:**
    - Antes de procesar datos sensibles, se debe evaluar el impacto en la privacidad y documentar las medidas de mitigación.
    - Si los riesgos son elevados, se debe consultar a la autoridad de protección de datos antes de iniciar el tratamiento.
  - **Criterios de Aceptación:**
    - Realización de una **Evaluación de Impacto en Protección de Datos (EIPD)** antes del tratamiento de datos sensibles.
    - Documentación de medidas de mitigación para reducir los riesgos identificados.
    - Registro y aprobación interna de la EIPD por parte del Delegado de Protección de Datos (DPO).
  - **Prioridad:** Alta.
  - **Categoría:** Consentimiento y Base Legal del Tratamiento.
  - **Fuente:** RGPD Art. 35, 36.
- 

## **PRIV-057 – Eliminación y Retención Segura de Datos Sensibles**

- **Descripción:**
  - Los datos sensibles solo pueden conservarse durante el tiempo estrictamente necesario para su finalidad.
  - Se debe garantizar su eliminación o anonimización cuando ya no sean requeridos.
- **Criterios de Aceptación:**
  - Definición de **períodos de retención claros** en el Registro de Actividades de Tratamiento.
  - Implementación de **mecanismos seguros de eliminación** (borrado seguro, sobrescritura, destrucción física).
  - Registro y auditoría de las eliminaciones realizadas.
- **Prioridad:** Alta.
- **Categoría:** Retención y Eliminación de Datos.
- **Fuente:** RGPD Art. 5.1.e, 17.

---

#### **PRIV-058 – Restricción del Tratamiento de Datos Relativos a Condenas y Delitos**

- **Descripción:**

Según el **Artículo 10 del RGPD**, los datos sobre condenas penales y delitos solo pueden ser tratados si:

- Es autorizado por **una norma legal o reglamentaria** de la UE o de un Estado miembro.
- Se cumplen **medidas de seguridad reforzadas** para su tratamiento.
- La finalidad del tratamiento está claramente definida y justificada.

- **Criterios de Aceptación:**

- Justificación documentada del tratamiento en función de la norma aplicable.
- Identificación clara de estos datos en el **Registro de Actividades de Tratamiento**.
- Implementación de medidas de seguridad específicas para estos datos.

- **Prioridad:** Alta.

- **Categoría:** Consentimiento y Base Legal del Tratamiento.

- **Fuente:** RGPD Art. 10; LOPDGDD Art. 10.

---

#### **PRIV-059 – Limitación del Acceso a Datos Relativos a Delitos Penales**

- **Descripción:**

- Solo el **personal estrictamente autorizado** puede acceder a los datos penales.
- Se deben registrar y auditar todos los accesos y modificaciones.
- Se debe garantizar que estos datos no sean utilizados para fines incompatibles con su finalidad original.

- **Criterios de Aceptación:**

- Implementación de **autenticación multifactor** para acceder a bases de datos con datos penales.
- Registro detallado de accesos con auditoría periódica.
- Revisión trimestral de permisos para asegurar que solo usuarios autorizados acceden a estos datos.

- **Prioridad:** Alta.

- **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ENS, ISO 27001.
- 

#### **PRIV-060 – Seguridad y Protección de los Datos Relativos a Condenas y Delitos**

- **Descripción:**
    - Los datos penales requieren **medidas de protección reforzadas** en almacenamiento, acceso y transmisión.
    - Se debe garantizar el uso de cifrado, acceso restringido y auditoría continua.
  - **Criterios de Aceptación:**
    - Aplicación de **cifrado de extremo a extremo** en almacenamiento y transmisión de datos penales.
    - Implementación de **controles de acceso y medidas de seguridad** adicionales.
    - Evaluaciones periódicas de seguridad mediante auditorías y pruebas de penetración.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001; ENS.
- 

#### **PRIV-061 – Evaluación de Impacto en Protección de Datos (EIPD) para el Tratamiento de Datos Penales**

- **Descripción:**
  - Antes de procesar datos penales, se debe evaluar el impacto en la privacidad y documentar las medidas de mitigación.
  - Si los riesgos son elevados, se debe consultar a la autoridad de protección de datos antes de iniciar el tratamiento.
- **Criterios de Aceptación:**
  - Realización de una **Evaluación de Impacto en Protección de Datos (EIPD)** antes del tratamiento de datos penales.
  - Documentación de medidas de mitigación para reducir los riesgos identificados.

- Registro y aprobación interna de la EIPD por parte del Delegado de Protección de Datos (DPO).
  - **Prioridad:** Alta.
  - **Categoría:** Evaluación de Impacto en la Privacidad.
  - **Fuente:** RGPD Art. 35, 36.
- 

#### **PRIV-062 – Conservación y Eliminación Segura de Datos Relativos a Condenas y Delitos**

- **Descripción:**
    - Los datos penales solo pueden conservarse durante el tiempo estrictamente necesario para su finalidad.
    - Se debe garantizar su eliminación o anonimización cuando ya no sean requeridos.
  - **Criterios de Aceptación:**
    - Definición de **períodos de retención claros** en el Registro de Actividades de Tratamiento.
    - Implementación de **mecanismos seguros de eliminación** (borrado seguro, sobrescritura, destrucción física).
    - Registro y auditoría de las eliminaciones realizadas.
  - **Prioridad:** Alta.
  - **Categoría:** Retención y Eliminación de Datos.
  - **Fuente:** RGPD Art. 5.1.e, 17.
- 

#### **PRIV-063 – Implementación de un Mecanismo para el Ejercicio del Derecho de Acceso**

- **Descripción:**

Según el **Artículo 15 del RGPD**, los interesados tienen derecho a obtener del responsable del tratamiento:

  - Confirmación sobre si se están tratando o no sus datos personales.
  - Acceso a sus datos personales y a la información relacionada con su tratamiento.
  - Una copia gratuita de los datos en un formato estructurado y de uso común.



- **Criterios de Aceptación:**
    - Disponibilidad de un **mecanismo accesible** (ej. portal web, correo electrónico, oficina física) para presentar solicitudes de acceso.
    - Confirmación al interesado sobre la recepción de la solicitud en un plazo máximo de **48 horas**.
    - Garantía de respuesta en un plazo máximo de **30 días**.
  - **Prioridad:** Alta.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 15.
- 

#### **PRIV-064 – Formato Estandarizado para la Entrega de Datos Personales**

- **Descripción:**
    - Los datos personales deben entregarse en un formato estructurado, de uso común y lectura mecánica.
    - Se deben utilizar formatos como **CSV, JSON, XML o PDF**.
  - **Criterios de Aceptación:**
    - Entrega de los datos en formato estructurado dentro del plazo legal.
    - Uso de **medios electrónicos seguros** para la transferencia de datos.
    - Posibilidad de facilitar una versión en papel si el usuario lo solicita.
  - **Prioridad:** Media.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 15, 20.
- 

#### **PRIV-065 – Identificación del Solicitante Antes de la Entrega de Datos**

- **Descripción:**
  - Se deben establecer mecanismos para **verificar la identidad del solicitante** antes de facilitarle acceso a sus datos personales.
  - No se debe solicitar información excesiva que limite el ejercicio del derecho de acceso.
- **Criterios de Aceptación:**
  - Solicitud de identificación mediante **DNI, pasaporte o identificación digital**.

- No requerir documentación adicional innecesaria.
    - Mantener registros de las verificaciones realizadas.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 12.6.
- 

#### **PRIV-066 – Excepciones y Denegación Justificada del Derecho de Acceso**

- **Descripción:**
    - El derecho de acceso puede denegarse si afecta negativamente los derechos y libertades de terceros o si existe una obligación legal que lo impida.
    - Se debe justificar documentalmente cada denegación de acceso.
  - **Criterios de Aceptación:**
    - Análisis documentado de la denegación con justificación legal.
    - Notificación al interesado explicando los motivos de la denegación.
    - Implementación de un canal de reclamación para los usuarios afectados.
  - **Prioridad:** Media.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 15.4.
- 

#### **PRIV-067 – Registro de Solicitudes de Acceso y Respuestas**

- **Descripción:**
  - Se debe mantener un **registro de todas las solicitudes de acceso recibidas** y sus respuestas.
  - Este registro debe incluir:
    - Fecha de solicitud.
    - Identidad del solicitante.
    - Información proporcionada o motivo de denegación.
- **Criterios de Aceptación:**
  - Implementación de un **sistema de gestión de solicitudes**.
  - Registro actualizado con el estado de cada solicitud.

- Protección de estos registros contra accesos no autorizados.
  - **Prioridad:** Alta.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** RGPD Art. 30.
- 

#### **PRIV-063 – Implementación de un Mecanismo para el Ejercicio del Derecho de Acceso**

- **Descripción:**

Según el **Artículo 15 del RGPD**, los interesados tienen derecho a obtener del responsable del tratamiento:

- Confirmación sobre si se están tratando o no sus datos personales.
  - Acceso a sus datos personales y a la información relacionada con su tratamiento.
  - Una copia gratuita de los datos en un formato estructurado y de uso común.
- **Criterios de Aceptación:**
    - Disponibilidad de un **mecanismo accesible** (ej. portal web, correo electrónico, oficina física) para presentar solicitudes de acceso.
    - Confirmación al interesado sobre la recepción de la solicitud en un plazo máximo de **48 horas**.
    - Garantía de respuesta en un plazo máximo de **30 días**.
  - **Prioridad:** Alta.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 15.
- 

#### **PRIV-064 – Formato Estandarizado para la Entrega de Datos Personales**

- **Descripción:**

- Los datos personales deben entregarse en un formato estructurado, de uso común y lectura mecánica.
- Se deben utilizar formatos como **CSV, JSON, XML o PDF**.

- **Criterios de Aceptación:**

- Entrega de los datos en formato estructurado dentro del plazo legal.

- Uso de **medios electrónicos seguros** para la transferencia de datos.
    - Posibilidad de facilitar una versión en papel si el usuario lo solicita.
  - **Prioridad:** Media.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 15, 20.
- 

#### **PRIV-065 – Identificación del Solicitante Antes de la Entrega de Datos**

- **Descripción:**
    - Se deben establecer mecanismos para **verificar la identidad del solicitante** antes de facilitarle acceso a sus datos personales.
    - No se debe solicitar información excesiva que limite el ejercicio del derecho de acceso.
  - **Criterios de Aceptación:**
    - Solicitud de identificación mediante **DNI, pasaporte o identificación digital**.
    - No requerir documentación adicional innecesaria.
    - Mantener registros de las verificaciones realizadas.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 12.6.
- 

#### **PRIV-066 – Excepciones y Denegación Justificada del Derecho de Acceso**

- **Descripción:**
  - El derecho de acceso puede denegarse si afecta negativamente los derechos y libertades de terceros o si existe una obligación legal que lo impida.
  - Se debe justificar documentalmente cada denegación de acceso.
- **Criterios de Aceptación:**
  - Análisis documentado de la denegación con justificación legal.
  - Notificación al interesado explicando los motivos de la denegación.
  - Implementación de un canal de reclamación para los usuarios afectados.

- **Prioridad:** Media.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 15.4.
- 

#### **PRIV-067 – Registro de Solicitudes de Acceso y Respuestas**

- **Descripción:**
    - Se debe mantener un **registro de todas las solicitudes de acceso recibidas** y sus respuestas.
    - Este registro debe incluir:
      - Fecha de solicitud.
      - Identidad del solicitante.
      - Información proporcionada o motivo de denegación.
  - **Criterios de Aceptación:**
    - Implementación de un **sistema de gestión de solicitudes**.
    - Registro actualizado con el estado de cada solicitud.
    - Protección de estos registros contra accesos no autorizados.
  - **Prioridad:** Alta.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** RGPD Art. 30.
- 

#### **PRIV-068 – Implementación de un Mecanismo para el Ejercicio del Derecho de Rectificación**

- **Descripción:**

Según el **Artículo 16 del RGPD**, los interesados tienen derecho a solicitar la rectificación de sus datos personales si son incorrectos, inexactos o incompletos.

  - El responsable del tratamiento debe permitir la corrección sin demoras injustificadas.
  - En caso de datos incompletos, el interesado puede aportar información adicional para completarlos.
- **Criterios de Aceptación:**
  - Disponibilidad de un **canal accesible** (ej. portal web, correo electrónico, teléfono) para solicitar la rectificación de datos.

- Confirmación de la recepción de la solicitud en un plazo máximo de **48 horas**.
    - Respuesta a la solicitud en un plazo máximo de **30 días**.
  - **Prioridad:** Alta.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 16.
- 

#### **PRIV-069 – Validación de la Identidad Antes de la Modificación de Datos**

- **Descripción:**
    - Antes de modificar los datos personales, se debe verificar la identidad del solicitante para evitar cambios fraudulentos.
    - No se deben solicitar documentos excesivos que dificulten el ejercicio del derecho.
  - **Criterios de Aceptación:**
    - Identificación del solicitante mediante **DNI, pasaporte o identificación digital**.
    - No requerir documentación innecesaria que obstaculice el derecho.
    - Mantener registros de las verificaciones realizadas antes de modificar datos.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 12.6.
- 

#### **PRIV-070 – Registro de Rectificaciones Realizadas**

- **Descripción:**
  - Se debe mantener un **registro de todas las solicitudes de rectificación** y de los cambios realizados.
  - Este registro debe contener:
    - Fecha de solicitud.
    - Datos corregidos o completados.
    - Justificación de la rectificación realizada.
- **Criterios de Aceptación:**

- Implementación de un **sistema de gestión de solicitudes de rectificación**.
    - Documentación de todas las modificaciones en el sistema.
    - Protección de los registros de cambios contra accesos no autorizados.
  - **Prioridad:** Alta.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** RGPD Art. 30.
- 

#### **PRIV-071 – Notificación de Rectificación a Terceros que Posean los Datos**

- **Descripción:**
    - Si los datos rectificados han sido compartidos con terceros, el responsable debe notificarles la modificación para que actualicen su información.
    - Se debe informar al interesado sobre las entidades a las que se ha comunicado la rectificación.
  - **Criterios de Aceptación:**
    - Implementación de un mecanismo para **informar a terceros** sobre las rectificaciones.
    - Registro de las notificaciones enviadas y confirmación de recepción cuando sea posible.
    - Comunicación al interesado sobre las entidades notificadas.
  - **Prioridad:** Media.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 19.
- 

#### **PRIV-072 – Excepciones y Denegación Justificada de la Rectificación**

- **Descripción:**
  - Se puede denegar la rectificación si los datos son correctos y no hay justificación válida para su modificación.
  - Si la rectificación no es posible, el interesado debe recibir una respuesta motivada.
- **Criterios de Aceptación:**

- Análisis documentado de la solicitud y justificación en caso de denegación.
    - Notificación al interesado explicando los motivos de la denegación.
    - Establecimiento de un canal de reclamación para los interesados afectados.
  - **Prioridad:** Media.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 16.
- 

#### **PRIV-073 – Implementación de un Mecanismo para el Ejercicio del Derecho de Supresión**

- **Descripción:**

Según el **Artículo 17 del RGPD**, los interesados tienen derecho a solicitar la eliminación de sus datos personales cuando:

    - Ya no sean necesarios para la finalidad con la que fueron recogidos.
    - Retiren su consentimiento y no haya otra base legal para el tratamiento.
    - Se hayan tratado de forma ilícita.
    - Se deba cumplir una obligación legal.
    - Los datos se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a menores.
  - **Criterios de Aceptación:**
    - Disponibilidad de un **canal accesible** (portal web, correo electrónico, oficina física) para presentar solicitudes de supresión.
    - Confirmación de la recepción de la solicitud en un plazo máximo de **48 horas**.
    - Respuesta y eliminación de datos en un plazo máximo de **30 días**.
  - **Prioridad:** Alta.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 17.
- 

#### **PRIV-074 – Verificación de la Identidad Antes de la Eliminación de Datos**

- **Descripción:**



- Antes de eliminar los datos, se debe verificar la identidad del solicitante para evitar supresiones fraudulentas.
    - No se debe solicitar información innecesaria que dificulte el ejercicio del derecho.
  - **Criterios de Aceptación:**
    - Identificación del solicitante mediante **DNI, pasaporte o identificación digital**.
    - Protección contra solicitudes fraudulentas mediante un procedimiento seguro de validación.
    - Mantener registros de las verificaciones realizadas antes de eliminar los datos.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 12.6.
- 

#### **PRIV-075 – Eliminación Segura de Datos Personales**

- **Descripción:**
    - La supresión de datos debe realizarse mediante técnicas que garanticen su eliminación definitiva y segura.
    - En caso de datos almacenados en copias de seguridad, se deben definir procedimientos para su eliminación en el menor tiempo posible.
  - **Criterios de Aceptación:**
    - Implementación de técnicas de **borrado seguro, sobrescritura o destrucción física** para la eliminación de datos.
    - Eliminación de registros en bases de datos activas y archivos de respaldo según la política de retención.
    - Registro de las eliminaciones realizadas para auditoría.
  - **Prioridad:** Alta.
  - **Categoría:** Retención y Eliminación de Datos.
  - **Fuente:** RGPD Art. 17; ISO 27001.
- 

#### **PRIV-076 – Notificación de Supresión a Terceros que Posean los Datos**

- **Descripción:**

- Si los datos suprimidos han sido compartidos con terceros, el responsable debe notificarles la eliminación para que actualicen su información.
  - Se debe informar al interesado sobre las entidades a las que se ha comunicado la supresión.
  - **Criterios de Aceptación:**
    - Implementación de un mecanismo para **informar a terceros** sobre las eliminaciones de datos.
    - Registro de las notificaciones enviadas y confirmación de recepción cuando sea posible.
    - Comunicación al interesado sobre las entidades notificadas.
  - **Prioridad:** Media.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 19.
- 

#### **PRIV-077 – Excepciones y Denegación Justificada del Derecho de Supresión**

- **Descripción:**
    - El derecho de supresión no se aplica si el tratamiento es necesario para:
      - Ejercer el derecho a la libertad de expresión e información.
      - Cumplir una obligación legal.
      - Razones de interés público en el ámbito de la salud.
      - Archivos históricos, científicos o estadísticos de interés público.
      - Defensa de reclamaciones legales.
  - **Criterios de Aceptación:**
    - Análisis documentado de la solicitud y justificación en caso de denegación.
    - Notificación al interesado explicando los motivos de la denegación.
    - Establecimiento de un canal de reclamación para los interesados afectados.
  - **Prioridad:** Media.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 17.3.
-

## **PRIV-078 – Implementación de un Mecanismo para el Ejercicio del Derecho a la Limitación del Tratamiento**

- **Descripción:**

Según el **Artículo 18 del RGPD**, los interesados tienen derecho a solicitar la limitación del tratamiento de sus datos personales en los siguientes casos:

- Cuando impugnen la exactitud de los datos y se esté verificando su corrección.
- Cuando el tratamiento sea ilícito y el interesado prefiera la limitación en lugar de la supresión.
- Cuando el responsable ya no necesite los datos, pero el interesado los requiera para formular o defender reclamaciones legales.
- Cuando el interesado se haya opuesto al tratamiento en virtud del **Artículo 21 del RGPD** y se esté evaluando la prevalencia de los intereses legítimos del responsable.

- **Criterios de Aceptación:**

- Disponibilidad de un **canal accesible** (portal web, correo electrónico, oficina física) para presentar solicitudes de limitación del tratamiento.
- Confirmación de la recepción de la solicitud en un plazo máximo de **48 horas**.
- Respuesta a la solicitud en un plazo máximo de **30 días**.

- **Prioridad:** Alta.

- **Categoría:** Derechos del Usuario.

- **Fuente:** RGPD Art. 18.

---

## **PRIV-079 – Implementación de Medidas Técnicas para la Limitación del Tratamiento**

- **Descripción:**

- Mientras los datos estén limitados, solo podrán ser almacenados y utilizados para reclamaciones legales, defensa de derechos o protección de intereses de terceros.
- Se deben aplicar medidas para que estos datos no sean modificados ni utilizados en otros tratamientos activos.

- **Criterios de Aceptación:**

- Implementación de un **sistema de bloqueo temporal** en bases de datos para los datos restringidos.

- Señalización clara de los datos afectados por la limitación dentro del sistema.
    - Restricción de acceso a los datos limitados solo a usuarios autorizados.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 18.2; ISO 27001.
- 

#### **PRIV-080 – Notificación de la Limitación a Terceros que Posean los Datos**

- **Descripción:**
    - Si los datos limitados han sido compartidos con terceros, el responsable del tratamiento debe notificarles la restricción para que suspendan su uso.
    - Se debe informar al interesado sobre las entidades a las que se ha comunicado la limitación.
  - **Criterios de Aceptación:**
    - Implementación de un mecanismo para **informar a terceros** sobre la limitación del tratamiento.
    - Registro de las notificaciones enviadas y confirmación de recepción cuando sea posible.
    - Comunicación al interesado sobre las entidades notificadas.
  - **Prioridad:** Media.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 19.
- 

#### **PRIV-081 – Levantamiento de la Limitación del Tratamiento**

- **Descripción:**
  - Si la causa que motivó la limitación deja de existir (por ejemplo, se verifica la exactitud de los datos o se resuelve una reclamación legal), el tratamiento puede reanudarse.
  - Antes de levantar la limitación, el interesado debe ser informado.
- **Criterios de Aceptación:**
  - Notificación al interesado antes de proceder con el levantamiento de la limitación.

- Registro documentado de la eliminación de la restricción y su justificación.
    - Confirmación de que los datos vuelven a estar disponibles para los tratamientos normales solo tras la notificación.
  - **Prioridad:** Media.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 18.3.
- 

#### **PRIV-082 – Registro de Solicitudes de Limitación y Respuestas**

- **Descripción:**
    - Se debe mantener un **registro de todas las solicitudes de limitación del tratamiento** y de las respuestas dadas.
    - Este registro debe contener:
      - Fecha de solicitud.
      - Datos afectados por la limitación.
      - Motivo de la restricción y duración prevista.
      - Justificación en caso de denegación.
  - **Criterios de Aceptación:**
    - Implementación de un **sistema de gestión de solicitudes de limitación**.
    - Documentación de todas las modificaciones en el sistema.
    - Protección de los registros contra accesos no autorizados.
  - **Prioridad:** Alta.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** RGPD Art. 30.
- 

#### **PRIV-083 – Implementación de un Mecanismo para el Ejercicio del Derecho a la Portabilidad**

- **Descripción:**

Según el **Artículo 20 del RGPD**, los interesados tienen derecho a:

  - Recibir sus datos personales en un formato estructurado, de uso común y lectura mecánica.
  - Transmitir sus datos a otro responsable del tratamiento sin impedimentos.

- Solicitar que la transmisión se haga directamente entre responsables cuando sea técnicamente posible.
  - **Criterios de Aceptación:**
    - Disponibilidad de un **canal accesible** (portal web, correo electrónico, oficina física) para presentar solicitudes de portabilidad.
    - Confirmación de la recepción de la solicitud en un plazo máximo de **48 horas**.
    - Respuesta a la solicitud y entrega de los datos en un plazo máximo de **30 días**.
  - **Prioridad:** Alta.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 20.
- 

#### **PRIV-084 – Formato Estandarizado para la Entrega de Datos**

- **Descripción:**
    - Los datos personales deben entregarse en un **formato estructurado, de uso común y de fácil lectura mecánica**, como:
      - **JSON**
      - **CSV**
      - **XML**
      - **PDF estructurado**
    - Se debe garantizar la compatibilidad con sistemas de otros responsables del tratamiento.
  - **Criterios de Aceptación:**
    - Implementación de formatos **interoperables** según los estándares del sector.
    - Uso de **protocolos de transferencia segura** para la entrega de datos.
    - Garantía de que los datos exportados son completos y exactos.
  - **Prioridad:** Alta.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 20.1.
-

## **PRIV-085 – Seguridad en la Transferencia de Datos Portables**

- **Descripción:**
    - Se deben aplicar medidas de seguridad para evitar accesos no autorizados durante la transferencia de datos personales a otros responsables del tratamiento.
    - Se deben utilizar mecanismos de autenticación para verificar la identidad del solicitante antes de la entrega de los datos.
  - **Criterios de Aceptación:**
    - Uso de **cifrado fuerte (AES-256, TLS 1.2+)** en la transferencia de datos.
    - Autenticación del solicitante mediante **doble factor de verificación (2FA)** antes de la entrega de los datos.
    - Implementación de **protocolos seguros de intercambio de datos** (ej. API seguras).
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32, ISO 27001.
- 

## **PRIV-086 – Transferencia Directa de Datos a Otro Responsable del Tratamiento**

- **Descripción:**
  - Si el interesado solicita que sus datos sean transferidos directamente a otro responsable del tratamiento, se debe facilitar la transmisión siempre que sea técnicamente viable.
  - Se debe garantizar que el destinatario tenga la capacidad de recibir los datos en el formato proporcionado.
- **Criterios de Aceptación:**
  - Disponibilidad de una opción de **transferencia directa** entre responsables.
  - Confirmación de que el responsable receptor puede procesar los datos en el formato transferido.
  - Implementación de **protocolos seguros para la transmisión de datos** entre responsables.
- **Prioridad:** Media.
- **Categoría:** Derechos del Usuario.

- **Fuente:** RGPD Art. 20.2.
- 

#### **PRIV-087 – Registro de Solicitudes y Entregas de Datos Portables**

- **Descripción:**
    - Se debe mantener un **registro de todas las solicitudes de portabilidad de datos personales** y de las respuestas dadas.
    - Este registro debe contener:
      - Fecha de solicitud.
      - Datos entregados y formato utilizado.
      - Método de transferencia y destinatario.
      - Justificación en caso de denegación.
  - **Criterios de Aceptación:**
    - Implementación de un **sistema de gestión de solicitudes de portabilidad**.
    - Documentación de todas las transferencias de datos realizadas.
    - Protección de los registros contra accesos no autorizados.
  - **Prioridad:** Alta.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** RGPD Art. 30.
- 

#### **PRIV-088 – Excepciones y Denegación Justificada del Derecho a la Portabilidad**

- **Descripción:**
  - El derecho a la portabilidad solo aplica cuando el tratamiento se basa en el **consentimiento** o en la **ejecución de un contrato**, y el tratamiento se realiza por medios automatizados.
  - Se puede denegar la portabilidad si afecta negativamente los derechos y libertades de terceros.
- **Criterios de Aceptación:**
  - Análisis documentado de la solicitud y justificación en caso de denegación.
  - Notificación al interesado explicando los motivos de la denegación.



- Establecimiento de un canal de reclamación para los interesados afectados.
  - **Prioridad:** Media.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 20.3.
- 

#### **PRIV-089 – Implementación de un Mecanismo para el Ejercicio del Derecho de Oposición**

- **Descripción:**

Según el **Artículo 21 del RGPD**, los interesados tienen derecho a oponerse al tratamiento de sus datos personales cuando:

    - El tratamiento se base en **interés legítimo** o en el **cumplimiento de una misión de interés público**, salvo que el responsable pueda demostrar **motivos legítimos imperiosos** que prevalezcan sobre los derechos del interesado.
    - Los datos sean utilizados con fines de **marketing directo**, en cuyo caso debe cesar inmediatamente el tratamiento.
    - Se utilicen para **decisiones automatizadas o elaboración de perfiles** con efectos jurídicos o significativos.
  - **Criterios de Aceptación:**
    - Disponibilidad de un **canal accesible** (portal web, correo electrónico, oficina física) para presentar solicitudes de oposición.
    - Confirmación de la recepción de la solicitud en un plazo máximo de **48 horas**.
    - Respuesta y cese del tratamiento en un plazo máximo de **30 días** (salvo excepciones justificadas).
  - **Prioridad:** Alta.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 21.
- 

#### **PRIV-090 – Oposición al Tratamiento Basado en Interés Legítimo o Interés Público**

- **Descripción:**
  - Si el tratamiento se basa en **interés legítimo o misión de interés público**, el responsable puede continuar con el tratamiento solo si demuestra

**motivos legítimos imperiosos** que prevalezcan sobre los derechos del interesado.

- En caso de que no existan estos motivos, se debe cesar el tratamiento de los datos personales del interesado.

- **Criterios de Aceptación:**

- Evaluación y documentación de la justificación del interés legítimo en caso de continuar el tratamiento.
- Notificación al interesado sobre la aceptación o denegación de su solicitud.
- Implementación de mecanismos para cesar el tratamiento en caso de aceptación de la oposición.

- **Prioridad:** Alta.

- **Categoría:** Consentimiento y Base Legal del Tratamiento.

- **Fuente:** RGPD Art. 21.1.

---

#### **PRIV-091 – Oposición al Uso de Datos para Marketing Directo**

- **Descripción:**

- El interesado tiene **derecho absoluto a oponerse** al tratamiento de sus datos con fines de marketing directo, incluyendo la elaboración de perfiles relacionados con dicho marketing.
- El responsable debe cesar el tratamiento inmediatamente tras recibir la solicitud.

- **Criterios de Aceptación:**

- Implementación de un **mecanismo de exclusión rápida** en bases de datos de marketing.
- Confirmación al interesado del cese del tratamiento en un plazo máximo de **48 horas**.
- No reutilización de los datos con fines comerciales una vez recibida la oposición.

- **Prioridad:** Alta.

- **Categoría:** Derechos del Usuario.

- **Fuente:** RGPD Art. 21.2.

---

## PRIV-092 – Oposición a la Elaboración de Perfiles y Decisiones Automatizadas

- **Descripción:**
    - El interesado tiene derecho a oponerse a que sus datos sean utilizados para la **toma de decisiones automatizadas**, incluida la elaboración de perfiles que produzcan efectos jurídicos o significativos sobre él.
    - Si la oposición es válida, se debe garantizar que la decisión sea revisada manualmente.
  - **Criterios de Aceptación:**
    - Implementación de un **mecanismo para la revisión humana** de decisiones automatizadas en caso de oposición.
    - Notificación al interesado sobre la resolución de su solicitud.
    - Documentación de la oposición y las medidas adoptadas en el sistema.
  - **Prioridad:** Media.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 22.
- 

## PRIV-093 – Registro de Solicitudes de Oposición y Respuestas

- **Descripción:**
  - Se debe mantener un **registro de todas las solicitudes de oposición** y sus respuestas.
  - Este registro debe contener:
    - Fecha de solicitud.
    - Motivo de la oposición.
    - Estado de la solicitud y resolución.
- **Criterios de Aceptación:**
  - Implementación de un **sistema de gestión de solicitudes de oposición**.
  - Documentación de todas las modificaciones en el sistema tras la oposición.
  - Protección de los registros contra accesos no autorizados.
- **Prioridad:** Alta.
- **Categoría:** Auditoría y Cumplimiento.
- **Fuente:** RGPD Art. 30.

---

#### **PRIV-094 – Protección del Derecho a la Privacidad en el Entorno Digital**

- **Descripción:**

Según la **LOPDGDD (Artículo 79-97)**, los ciudadanos tienen derecho a la privacidad en sus comunicaciones digitales y al uso de dispositivos electrónicos.

- Se debe garantizar que las comunicaciones electrónicas sean **confidenciales y seguras**.
- Los datos generados en el uso de dispositivos electrónicos solo podrán ser tratados con base legal adecuada.

- **Criterios de Aceptación:**

- Implementación de **protocolos de cifrado** en comunicaciones digitales.
- Restricción del acceso a los datos generados por el uso de dispositivos electrónicos.
- Inclusión de medidas de seguridad en aplicaciones y plataformas digitales.

- **Prioridad:** Alta.

- **Categoría:** Derechos Digitales.

- **Fuente:** LOPDGDD Art. 79-80.

---

#### **PRIV-095 – Derecho a la Neutralidad en Internet**

- **Descripción:**

- Los usuarios deben poder acceder y distribuir información en internet sin bloqueos, restricciones o discriminación injustificada por parte de los proveedores de servicios.
- No se pueden aplicar prácticas de discriminación o priorización de tráfico sin una justificación legal o técnica.

- **Criterios de Aceptación:**

- Garantía de **igualdad de acceso** a todos los contenidos y servicios en internet sin restricciones arbitrarias.
- Monitorización para evitar bloqueos o ralentización de servicios sin causa justificada.
- Información transparente sobre la gestión del tráfico de red por parte de los proveedores de servicios.

- **Prioridad:** Alta.

- **Categoría:** Derechos Digitales.
  - **Fuente:** LOPDGDD Art. 80; Reglamento UE 2015/2120.
- 

#### **PRIV-096 – Derecho al Olvido en Búsquedas en Internet**

- **Descripción:**
    - Los interesados pueden solicitar la eliminación de enlaces a información personal en buscadores cuando estos datos sean inexactos, inadecuados o ya no sean relevantes.
    - El responsable del buscador debe analizar cada solicitud y determinar si procede la eliminación.
  - **Criterios de Aceptación:**
    - Disponibilidad de un **mecanismo accesible** para solicitar la eliminación de enlaces.
    - Evaluación de cada solicitud según el **interés público** y la relevancia de la información.
    - Implementación de procedimientos para comunicar la eliminación al usuario.
  - **Prioridad:** Media.
  - **Categoría:** Derechos Digitales.
  - **Fuente:** RGPD Art. 17; LOPDGDD Art. 93.
- 

#### **PRIV-097 – Derecho al Olvido en Redes Sociales y Plataformas Digitales**

- **Descripción:**
  - Los usuarios pueden solicitar la eliminación de su información personal publicada en redes sociales o plataformas digitales.
  - Se debe garantizar la eliminación efectiva de la información y la imposibilidad de su indexación posterior.
- **Criterios de Aceptación:**
  - Implementación de un **mecanismo accesible** para la solicitud de eliminación de contenido.
  - Confirmación de la eliminación efectiva en un plazo razonable.
  - Medidas para evitar que la información siga accesible tras su eliminación.
- **Prioridad:** Alta.

- **Categoría:** Derechos Digitales.
  - **Fuente:** LOPDGDD Art. 94.
- 

#### **PRIV-098 – Protección de la Identidad Digital y el Uso de Pseudónimos**

- **Descripción:**
    - Los ciudadanos tienen derecho a utilizar pseudónimos en plataformas digitales y redes sociales para proteger su identidad.
    - Se debe evitar la recopilación innecesaria de información personal en servicios digitales.
  - **Criterios de Aceptación:**
    - Posibilidad de registro y uso de pseudónimos en plataformas digitales.
    - Restricción de la solicitud de datos personales salvo cuando sea estrictamente necesario.
    - Protección contra la vinculación de pseudónimos con la identidad real sin consentimiento.
  - **Prioridad:** Media.
  - **Categoría:** Derechos Digitales.
  - **Fuente:** LOPDGDD Art. 96.
- 

#### **PRIV-099 – Derecho de Desconexión Digital en el Ámbito Laboral**

- **Descripción:**
  - Los trabajadores tienen derecho a no ser contactados fuera del horario laboral mediante medios digitales.
  - Las empresas deben implementar políticas que garanticen la desconexión digital y eviten la sobrecarga digital.
- **Criterios de Aceptación:**
  - Definición de una **política de desconexión digital** en la organización.
  - Garantía de que no se enviarán correos electrónicos o mensajes fuera del horario laboral sin justificación.
  - Establecimiento de canales de reclamación en caso de incumplimiento del derecho de desconexión.
- **Prioridad:** Alta.

- **Categoría:** Derechos Digitales.
  - **Fuente:** LOPDGDD Art. 88.
- 

#### **PRIV-100 – Protección de Menores en Internet**

- **Descripción:**
    - Se deben implementar medidas para proteger a los menores frente a contenido inadecuado en plataformas digitales.
    - Se debe garantizar que los servicios en línea dirigidos a menores respeten la normativa sobre privacidad infantil.
  - **Criterios de Aceptación:**
    - Implementación de **controles parentales y filtros de contenido** en plataformas digitales.
    - Revisión de términos y condiciones de servicios dirigidos a menores.
    - Medidas para evitar la recopilación de datos de menores sin el consentimiento de sus tutores legales.
  - **Prioridad:** Alta.
  - **Categoría:** Protección de Menores.
  - **Fuente:** LOPDGDD Art. 92; RGPD Art. 8.
- 

#### **PRIV-101 – Implementación de una Política de Desconexión Digital**

- **Descripción:**

Según la **LOPDGDD (Artículo 88)**, los trabajadores tienen derecho a la desconexión digital fuera de su jornada laboral para garantizar su descanso, permisos y conciliación de la vida personal y profesional.

  - Las empresas deben definir una **política de desconexión digital**.
  - Se deben establecer medidas para evitar el contacto fuera del horario laboral sin justificación.
- **Criterios de Aceptación:**
  - Creación y difusión de una **política interna de desconexión digital**.
  - Garantía de que no se envíen comunicaciones fuera del horario laboral, salvo excepciones justificadas.
  - Implementación de **protocolos de reclamación** en caso de incumplimiento.

- **Prioridad:** Alta.
  - **Categoría:** Derechos Digitales.
  - **Fuente:** LOPDGDD Art. 88.
- 

#### **PRIV-102 – Regulación del Uso de Herramientas Digitales para la Comunicación Laboral**

- **Descripción:**
    - Se deben establecer reglas claras sobre el uso de correos electrónicos, mensajería instantánea y otras herramientas digitales fuera del horario laboral.
    - Se debe definir un horario de disponibilidad laboral digital y evitar interrupciones innecesarias.
  - **Criterios de Aceptación:**
    - Definición de **frangas horarias de disponibilidad digital**.
    - Configuración de sistemas para **bloquear notificaciones fuera del horario laboral** en herramientas corporativas.
    - Formación a empleados y directivos sobre el respeto a la desconexión digital.
  - **Prioridad:** Media.
  - **Categoría:** Derechos Digitales.
  - **Fuente:** LOPDGDD Art. 88.
- 

#### **PRIV-103 – Excepciones Justificadas para Contacto Fuera del Horario Laboral**

- **Descripción:**
  - Se deben definir claramente las situaciones en las que se permite contactar a un empleado fuera del horario laboral (ej. emergencias, crisis operativas).
  - Estas excepciones deben ser **documentadas y justificadas**.
- **Criterios de Aceptación:**
  - Establecimiento de **criterios objetivos** para casos excepcionales.
  - Registro de comunicaciones realizadas fuera del horario laboral y su justificación.



- Implementación de **medidas de compensación** si el trabajador debe responder fuera de su jornada.
  - **Prioridad:** Media.
  - **Categoría:** Derechos Digitales.
  - **Fuente:** LOPDGDD Art. 88.
- 

#### **PRIV-104 – Derecho del Trabajador a Denunciar Incumplimientos**

- **Descripción:**
    - Los empleados deben contar con **canales internos de denuncia** si consideran que su derecho a la desconexión digital no se respeta.
    - Se debe garantizar la confidencialidad de las denuncias y evitar represalias.
  - **Criterios de Aceptación:**
    - Creación de un **canal seguro y confidencial** para reportar incumplimientos.
    - Definición de plazos y procedimientos para la gestión de reclamaciones.
    - Medidas disciplinarias en caso de violación reiterada de la desconexión digital.
  - **Prioridad:** Alta.
  - **Categoría:** Derechos Digitales.
  - **Fuente:** LOPDGDD Art. 88.
- 

#### **PRIV-105 – Formación y Sensibilización sobre Desconexión Digital**

- **Descripción:**
  - Se debe capacitar a empleados y directivos sobre la importancia de la desconexión digital y su impacto en la salud mental y el rendimiento laboral.
  - Las organizaciones deben promover buenas prácticas en el uso de herramientas digitales.
- **Criterios de Aceptación:**
  - Realización de sesiones formativas sobre el derecho a la desconexión digital.

- Difusión de materiales educativos sobre el equilibrio entre vida laboral y personal.
    - Implementación de **campañas internas de concienciación**.
  - **Prioridad:** Media.
  - **Categoría:** Derechos Digitales.
  - **Fuente:** LOPDGDD Art. 88.
- 

#### **PRIV-106 – Implementación de una Política de Seguridad de la Información**

- **Descripción:**

Según el **Artículo 32 del RGPD**, el responsable del tratamiento debe aplicar medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado, teniendo en cuenta los riesgos asociados al tratamiento de datos personales.

    - Se debe contar con una **Política de Seguridad de la Información** alineada con normativas como ISO 27001 y ENS.
    - La política debe definir roles, responsabilidades y procedimientos de seguridad.
  - **Criterios de Aceptación:**
    - Redacción y aprobación de una **Política de Seguridad** aplicable a toda la organización.
    - Identificación y asignación de responsables de seguridad de la información.
    - Revisión y actualización periódica de la política de seguridad (mínimo anual).
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ENS; ISO 27001.
- 

#### **PRIV-107 – Gestión de Accesos y Control de Privilegios**

- **Descripción:**
  - Solo el personal autorizado debe acceder a los datos personales según el principio de **privilegios mínimos** y **necesidad de conocer**.
  - Se deben implementar controles de autenticación segura y auditoría de accesos.

- **Criterios de Aceptación:**
    - Uso de **autenticación multifactor (MFA)** para accesos a información sensible.
    - Implementación de un **sistema de control de accesos basado en roles (RBAC)**.
    - Registro y auditoría de accesos con revisiones periódicas.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001; ENS.
- 

#### **PRIV-108 – Protección contra Amenazas y Ataques Cibernéticos**

- **Descripción:**
    - Se deben implementar **medidas de seguridad perimetral**, como firewalls, sistemas de detección de intrusos (IDS/IPS) y herramientas de monitoreo de seguridad.
    - Se debe contar con un **plan de respuesta ante incidentes**.
  - **Criterios de Aceptación:**
    - Instalación de firewalls y sistemas de detección de intrusos.
    - Monitorización en tiempo real de eventos de seguridad.
    - Implementación de un **procedimiento de respuesta a incidentes** con tiempos de actuación definidos.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ENS; ISO 27001.
- 

#### **PRIV-109 – Cifrado de Datos Personales**

- **Descripción:**
  - Los datos personales deben cifrarse tanto en tránsito como en reposo para evitar accesos no autorizados.
  - Se deben utilizar algoritmos de cifrado robustos y claves de acceso seguras.
- **Criterios de Aceptación:**

- Uso de cifrado **AES-256** para datos almacenados.
    - Implementación de cifrado en tránsito mediante **TLS 1.2 o superior**.
    - Revisión periódica de claves y algoritmos de cifrado.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001; ENS.
- 

#### **PRIV-110 – Copias de Seguridad y Recuperación ante Desastres**

- **Descripción:**
    - Se deben realizar **copias de seguridad periódicas** de los datos personales para garantizar su recuperación en caso de incidentes.
    - Las copias deben estar cifradas y almacenadas en ubicaciones seguras.
  - **Criterios de Aceptación:**
    - Realización de **copias de seguridad automáticas** con periodicidad definida (diaria/semanal/mensual según criticidad).
    - Pruebas de recuperación periódicas para garantizar la integridad de los respaldos.
    - Almacenamiento de copias en ubicaciones seguras con cifrado.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001; ENS.
- 

#### **PRIV-111 – Registro y Auditoría de Actividades sobre Datos Personales**

- **Descripción:**
  - Se deben registrar todas las actividades que afecten a los datos personales, incluyendo accesos, modificaciones y transferencias.
  - Los registros deben permitir detectar accesos no autorizados o usos indebidos.
- **Criterios de Aceptación:**
  - Implementación de **logs de auditoría** para todas las operaciones sobre datos personales.
  - Almacenamiento de registros en sistemas protegidos contra alteraciones.

- Análisis periódico de los logs para detectar anomalías.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 30, 32; ENS; ISO 27001.
- 

#### **PRIV-112 – Evaluaciones de Riesgos y Seguridad de la Información**

- **Descripción:**
    - Se deben realizar evaluaciones periódicas para identificar vulnerabilidades y amenazas en los sistemas que tratan datos personales.
    - Los resultados deben utilizarse para implementar mejoras en la seguridad.
  - **Criterios de Aceptación:**
    - Realización de **evaluaciones de riesgo** al menos una vez al año.
    - Implementación de **medidas correctivas** basadas en los hallazgos.
    - Documentación y actualización de los riesgos identificados.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ENS; ISO 27001.
- 

#### **PRIV-113 – Plan de Concienciación y Formación en Seguridad**

- **Descripción:**
  - Se debe capacitar a los empleados en **buenas prácticas de seguridad de la información** y protección de datos.
  - Se deben realizar campañas periódicas de concienciación para prevenir ataques como phishing o ingeniería social.
- **Criterios de Aceptación:**
  - Formación obligatoria en seguridad para todos los empleados con acceso a datos personales.
  - Simulación de ataques de phishing y evaluación de la respuesta de los empleados.
  - Evaluación anual de la efectividad de las campañas de concienciación.
- **Prioridad:** Media.

- **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ENS; ISO 27001.
- 

#### **PRIV-114 – Implementación de un Sistema de Control de Accesos Basado en Roles (RBAC)**

- **Descripción:**

Según el **Artículo 32 del RGPD**, el acceso a datos personales debe ser limitado al personal autorizado bajo el principio de **mínimos privilegios y necesidad de conocer**.

    - Se debe establecer un **sistema de control de accesos basado en roles (RBAC)**.
    - Solo los empleados con funciones específicas deben poder acceder a los datos personales.
  - **Criterios de Aceptación:**
    - Definición de **roles de acceso** con permisos diferenciados según funciones.
    - Implementación de un **sistema de gestión de identidades y accesos (IAM)**.
    - Auditoría periódica de los permisos asignados a cada usuario.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ENS; ISO 27001.
- 

#### **PRIV-115 – Autenticación Multifactor para el Acceso a Datos Sensibles**

- **Descripción:**
  - Para acceder a datos personales de **alta sensibilidad** (salud, financieros, biométricos, etc.), se debe implementar **autenticación multifactor (MFA)**.
  - Se deben utilizar credenciales robustas y medidas adicionales de autenticación.
- **Criterios de Aceptación:**
  - Uso de **MFA obligatorio** para accesos a bases de datos con información sensible.
  - Implementación de **contraseñas seguras** con requisitos de complejidad.

- Revisión periódica de credenciales y autenticaciones.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ENS; ISO 27001.
- 

#### **PRIV-116 – Registro y Auditoría de Accesos a Datos Personales**

- **Descripción:**
    - Se debe registrar toda actividad de acceso, modificación o eliminación de datos personales.
    - Los registros deben permitir detectar accesos indebidos o sospechosos.
  - **Criterios de Aceptación:**
    - Implementación de **logs de auditoría** para todas las operaciones sobre datos personales.
    - Almacenamiento seguro de los registros de acceso sin posibilidad de alteración.
    - Análisis periódico de logs para detectar accesos inusuales.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 30, 32; ENS; ISO 27001.
- 

#### **PRIV-117 – Revisión y Revocación de Permisos de Acceso**

- **Descripción:**
  - Se deben revisar periódicamente los permisos de acceso a datos personales para evitar accesos innecesarios.
  - Cuando un empleado cambie de rol o abandone la organización, sus accesos deben revocarse inmediatamente.
- **Criterios de Aceptación:**
  - Auditoría de permisos de acceso al menos cada **6 meses**.
  - Implementación de un **proceso automatizado** de revocación de accesos cuando un usuario deje la organización.
  - Registro de los cambios de permisos en el sistema de control de accesos.
- **Prioridad:** Alta.

- **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ENS; ISO 27001.
- 

#### **PRIV-118 – Segmentación de Datos para Minimizar Exposición**

- **Descripción:**
    - Se debe segmentar la información para que los usuarios solo accedan a los datos estrictamente necesarios.
    - Se debe aplicar la separación entre **entornos de producción y prueba** para evitar accesos indebidos.
  - **Criterios de Aceptación:**
    - Implementación de **perfiles de usuario con acceso restringido** a información específica.
    - Separación de **bases de datos de producción y prueba** para evitar exposición innecesaria.
    - Monitorización de accesos para detectar intentos de acceso a datos no autorizados.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001.
- 

#### **PRIV-119 – Protección de Accesos a Datos en Dispositivos Móviles**

- **Descripción:**
  - Se deben aplicar medidas para evitar accesos no autorizados a datos personales desde dispositivos móviles (smartphones, tablets, portátiles).
  - Se debe garantizar el uso de conexiones seguras y control de dispositivos corporativos.
- **Criterios de Aceptación:**
  - Implementación de **cifrado en dispositivos móviles** que accedan a datos personales.
  - Restricción de acceso a datos personales desde redes no seguras.
  - Uso de **gestión de dispositivos móviles (MDM)** para proteger información corporativa.
- **Prioridad:** Media.



- **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ENS; ISO 27001.
- 

#### **PRIV-120 – Restricción del Acceso a Datos por Ubicación y Dispositivo**

- **Descripción:**
    - Se deben establecer restricciones de acceso a datos personales basadas en la ubicación y el tipo de dispositivo.
    - Se debe bloquear el acceso desde ubicaciones o dispositivos no autorizados.
  - **Criterios de Aceptación:**
    - Implementación de **geolocalización para accesos restringidos** (ej. solo desde la UE).
    - Bloqueo de accesos desde **dispositivos no registrados o desconocidos**.
    - Monitorización y alertas en caso de accesos desde ubicaciones inusuales.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001.
- 

#### **PRIV-121 – Implementación de un Sistema de Gestión de Identidades y Accesos (IAM)**

- **Descripción:**

Según el **Artículo 32 del RGPD**, se deben aplicar controles de acceso adecuados para evitar accesos no autorizados a los datos personales.

  - Se debe contar con un **Sistema de Gestión de Identidades y Accesos (IAM)** para gestionar usuarios y permisos.
  - Los accesos deben basarse en el **principio de mínimo privilegio y necesidad de conocer**.
- **Criterios de Aceptación:**
  - Implementación de un **sistema IAM** para la gestión centralizada de accesos.
  - Creación de perfiles de usuario con permisos diferenciados.
  - Auditoría periódica de accesos y permisos.
- **Prioridad:** Alta.

- **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ENS; ISO 27001.
- 

#### **PRIV-122 – Autenticación Multifactor (MFA) para Accesos a Datos Sensibles**

- **Descripción:**
    - Todo acceso a sistemas con datos personales sensibles debe requerir **autenticación multifactor (MFA)** para prevenir accesos no autorizados.
    - Se deben aplicar métodos de autenticación robustos, como OTP, biometría o certificados digitales.
  - **Criterios de Aceptación:**
    - Implementación de **MFA obligatorio** en sistemas con datos personales críticos.
    - Uso de métodos de autenticación seguros como OTP o biometría.
    - Registro y auditoría de cada autenticación en los sistemas.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ENS; ISO 27001.
- 

#### **PRIV-123 – Políticas de Contraseñas Seguras y Renovación Periódica**

- **Descripción:**
  - Las contraseñas utilizadas en los sistemas de información deben cumplir con requisitos de **seguridad y complejidad**.
  - Se deben establecer mecanismos para **cambio y expiración periódica** de contraseñas.
- **Criterios de Aceptación:**
  - Uso de contraseñas con **mínimo 12 caracteres, combinando letras, números y símbolos**.
  - Implementación de **cambio obligatorio de contraseña cada 90 días**.
  - Aplicación de medidas contra ataques de fuerza bruta y reutilización de contraseñas.
- **Prioridad:** Alta.
- **Categoría:** Seguridad de la Información.

- **Fuente:** RGPD Art. 32; ISO 27001; ENS.
- 

#### **PRIV-124 – Restricción del Uso de Cuentas Compartidas**

- **Descripción:**
    - Se debe evitar el uso de cuentas de usuario compartidas en los sistemas que gestionan datos personales.
    - Cada usuario debe tener credenciales individuales para garantizar la trazabilidad.
  - **Criterios de Aceptación:**
    - Implementación de **cuentas individuales para cada usuario** en los sistemas.
    - Eliminación de cuentas genéricas o compartidas en entornos con datos personales.
    - Registro y auditoría de todos los accesos individuales.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001; ENS.
- 

#### **PRIV-125 – Bloqueo de Cuentas tras Intentos Fallidos de Autenticación**

- **Descripción:**
  - Se debe configurar un límite de intentos fallidos de autenticación para evitar ataques de fuerza bruta.
  - El sistema debe bloquear temporalmente la cuenta y notificar al usuario tras múltiples intentos fallidos.
- **Criterios de Aceptación:**
  - Implementación de bloqueo de cuenta tras **5 intentos fallidos** de autenticación.
  - Notificación al usuario sobre intentos de acceso no autorizados.
  - Revisión de accesos sospechosos en los logs de seguridad.
- **Prioridad:** Media.
- **Categoría:** Seguridad de la Información.
- **Fuente:** RGPD Art. 32; ISO 27001.

---

## PRIV-126 – Eliminación y Desactivación de Cuentas Inactivas

- **Descripción:**
  - Las cuentas de usuario que no se utilicen durante un período prolongado deben ser **desactivadas o eliminadas** para reducir riesgos de accesos no autorizados.
- **Criterios de Aceptación:**
  - Implementación de un **proceso automático de inactivación** para cuentas sin uso en **90 días**.
  - Notificación previa al usuario antes de la desactivación de su cuenta.
  - Registro de cuentas inactivas y revisiones periódicas para su eliminación.
- **Prioridad:** Media.
- **Categoría:** Seguridad de la Información.
- **Fuente:** RGPD Art. 32; ISO 27001.

---

## PRIV-127 – Control de Dispositivos y Ubicación para la Autenticación

- **Descripción:**
  - Se deben aplicar controles para restringir accesos a datos personales desde dispositivos no autorizados o ubicaciones sospechosas.
  - Se debe alertar al usuario si se detecta un intento de acceso desde una nueva ubicación o dispositivo.
- **Criterios de Aceptación:**
  - Implementación de **restricciones de acceso basadas en ubicación (ej. solo desde la UE)**.
  - Bloqueo de accesos desde **dispositivos no registrados o desconocidos**.
  - Alertas de seguridad en caso de intentos de acceso sospechosos.
- **Prioridad:** Media.
- **Categoría:** Seguridad de la Información.
- **Fuente:** RGPD Art. 32; ISO 27001.

---

## PRIV-128 – Cifrado Obligatorio de Datos Personales en Reposo

- **Descripción:**

Según el **Artículo 32 del RGPD**, se deben aplicar medidas de seguridad para proteger los datos personales contra accesos no autorizados, incluyendo el cifrado de datos almacenados.

- Se debe garantizar el uso de **cifrado robusto (AES-256 o superior)** para datos personales almacenados en bases de datos, servidores y dispositivos.

- **Criterios de Aceptación:**

- Implementación de cifrado **AES-256 o equivalente** para almacenamiento de datos personales.
- Protección de claves de cifrado mediante módulos de seguridad de hardware (HSM).
- Auditoría periódica del uso y efectividad del cifrado.

- **Prioridad:** Alta.

- **Categoría:** Seguridad de la Información.

- **Fuente:** RGPD Art. 32; ISO 27001; ENS.

---

#### **PRIV-129 – Cifrado de Datos en Tránsito mediante Protocolos Seguros**

- **Descripción:**

- Se debe garantizar que los datos personales transmitidos a través de redes internas o externas se encuentren cifrados para evitar su interceptación.
- Se deben utilizar **protocolos de comunicación seguros como TLS 1.2 o superior**.

- **Criterios de Aceptación:**

- Implementación de **cifrado de extremo a extremo** en transmisiones de datos personales.
- Uso obligatorio de **TLS 1.2+ en sitios web, APIs y servicios en la nube**.
- Deshabilitación de protocolos obsoletos (SSL, TLS 1.0, TLS 1.1).

- **Prioridad:** Alta.

- **Categoría:** Seguridad de la Información.

- **Fuente:** RGPD Art. 32; ISO 27001; ENS.

---

#### **PRIV-130 – Anonimización de Datos Personales en Análisis y Estadísticas**

- **Descripción:**
    - Para el uso de datos personales en fines estadísticos, científicos o de investigación, se debe aplicar técnicas de anonimización que imposibiliten la reidentificación del individuo.
    - Se debe garantizar que la anonimización sea irreversible.
  - **Criterios de Aceptación:**
    - Aplicación de **técnicas de anonimización como agregación, enmascaramiento o generalización**.
    - Evaluación periódica para verificar la irreversibilidad del proceso.
    - Implementación de mecanismos de anonimización en bases de datos y archivos con datos personales.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 89; ISO 20889; ENS.
- 

#### **PRIV-131 – Seudonimización de Datos para Minimizar Riesgos**

- **Descripción:**
    - Se debe aplicar **seudonimización** en los datos personales cuando sea posible para reducir el riesgo de exposición en caso de incidentes de seguridad.
    - Laseudonimización debe ser reversible solo por usuarios autorizados con claves de descryptación.
  - **Criterios de Aceptación:**
    - Uso de técnicas como **tokenización, hashing o cifrado reversible** con claves seguras.
    - Separación de datosseudonimizados y claves de reasignación en entornos diferentes.
    - Control estricto de accesos a los datos originales yseudonimizados.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 25, 32; ISO 20889.
- 

#### **PRIV-132 – Almacenamiento Seguro de Claves de Cifrado**

- **Descripción:**
    - Las claves utilizadas para el cifrado y la seudonimización deben ser protegidas contra accesos no autorizados.
    - Se deben utilizar mecanismos de almacenamiento seguros como módulos de seguridad de hardware (**HSM**) o bóvedas de claves.
  - **Criterios de Aceptación:**
    - Uso de **HSM o bóvedas de claves seguras** para almacenamiento de claves.
    - Implementación de **rotación periódica de claves** y control de acceso estricto.
    - Registro de acceso y uso de claves de cifrado.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001.
- 

#### **PRIV-133 – Evaluación de la Resistencia de Algoritmos de Cifrado y Anonimización**

- **Descripción:**
    - Se deben realizar auditorías y pruebas de seguridad periódicas para evaluar la resistencia de los algoritmos de cifrado y anonimización frente a ataques de reidentificación.
  - **Criterios de Aceptación:**
    - Pruebas de seguridad anuales sobre los algoritmos de cifrado y anonimización.
    - Implementación de medidas correctivas en caso de vulnerabilidades detectadas.
    - Evaluación de nuevos estándares y algoritmos de cifrado recomendados.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 20889; ENS.
- 

#### **PRIV-134 – Implementación de un Sistema de Registro de Actividad sobre Datos Personales**

- **Descripción:**  
Según el **Artículo 30 del RGPD**, el responsable del tratamiento debe llevar un **registro de todas las actividades de tratamiento**, especificando:
    - Categorías de datos tratados.
    - Finalidad del tratamiento.
    - Responsable y encargados del tratamiento.
    - Transferencias internacionales realizadas.
  - **Criterios de Aceptación:**
    - Implementación de un **sistema automatizado de registro de actividades de tratamiento**.
    - Actualización periódica de los registros con información precisa.
    - Acceso restringido a los registros a personal autorizado.
  - **Prioridad:** Alta.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** RGPD Art. 30; ENS; ISO 27001.
- 

#### **PRIV-135 – Registro y Monitorización de Accesos a Datos Personales**

- **Descripción:**
    - Se deben registrar todas las operaciones de **lectura, escritura, modificación y eliminación** de datos personales.
    - Se debe garantizar que estos registros sean inalterables y accesibles solo para auditoría.
  - **Criterios de Aceptación:**
    - Implementación de **logs de auditoría** que registren accesos a datos personales.
    - Almacenamiento seguro de los registros, evitando alteraciones.
    - Revisión periódica de accesos para detectar posibles accesos indebidos.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 30, 32; ENS; ISO 27001.
- 

#### **PRIV-136 – Registro de Modificaciones y Eliminaciones de Datos**



- **Descripción:**
    - Se deben mantener registros detallados de **quién, cuándo y cómo** se modificaron o eliminaron datos personales.
    - Se debe garantizar la reversibilidad o trazabilidad de los cambios realizados.
  - **Criterios de Aceptación:**
    - Implementación de **versionado y logs de cambios** en bases de datos con datos personales.
    - Notificación automática en caso de modificación o eliminación masiva de datos.
    - Protección de los registros de cambios contra alteraciones malintencionadas.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 30, 32; ENS; ISO 27001.
- 

#### **PRIV-137 – Trazabilidad de Transferencias de Datos Personales**

- **Descripción:**
  - Se deben registrar y documentar todas las transferencias de datos personales, incluyendo:
    - Origen y destino de los datos.
    - Motivo de la transferencia.
    - Medidas de seguridad aplicadas.
- **Criterios de Aceptación:**
  - Registro de transferencias de datos en **sistemas centralizados de auditoría**.
  - Verificación de que las transferencias cumplen con las bases legales del RGPD.
  - Aplicación de cifrado en las transferencias y firma digital en documentos de autorización.
- **Prioridad:** Alta.
- **Categoría:** Seguridad de la Información.
- **Fuente:** RGPD Art. 30, 44; ISO 27001.

---

### **PRIV-138 – Protección de los Registros contra Manipulación y Accesos No Autorizados**

- **Descripción:**
    - Los registros de actividad y trazabilidad deben ser **inalterables** y accesibles solo por personal autorizado.
    - Se deben implementar mecanismos de detección de intentos de alteración.
  - **Criterios de Aceptación:**
    - Implementación de **sistemas de almacenamiento inmutable** para logs y auditorías.
    - Monitorización en tiempo real de intentos de acceso o manipulación de registros.
    - Realización de copias de seguridad de registros críticos.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 30, 32; ISO 27001.
- 

### **PRIV-139 – Análisis Periódico de los Registros y Reporte de Incidentes**

- **Descripción:**
  - Se deben revisar regularmente los registros de actividad para detectar accesos indebidos o actividades sospechosas.
  - Los incidentes detectados deben ser documentados y gestionados conforme a los procedimientos internos de seguridad.
- **Criterios de Aceptación:**
  - Implementación de **alertas automáticas** en caso de actividad anómala sobre datos personales.
  - Realización de revisiones periódicas de logs de acceso y cambios.
  - Registro de incidentes de seguridad y generación de informes para revisión interna.
- **Prioridad:** Media.
- **Categoría:** Auditoría y Cumplimiento.
- **Fuente:** RGPD Art. 32; ISO 27001

---

#### **PRIV-140 – Implementación de un Sistema de Prevención y Detección de Intrusos (IDS/IPS)**

- **Descripción:**

Según el **Artículo 32 del RGPD**, se deben aplicar medidas técnicas para garantizar la seguridad de los datos personales ante accesos no autorizados.

- Se debe contar con sistemas de **detección y prevención de intrusos (IDS/IPS)** para monitorizar y bloquear actividades sospechosas.

- **Criterios de Aceptación:**

- Instalación de **IDS/IPS en redes y servidores críticos**.
- Generación de alertas en tiempo real ante intentos de intrusión.
- Revisión periódica de eventos de seguridad detectados.

- **Prioridad:** Alta.

- **Categoría:** Seguridad de la Información.

- **Fuente:** RGPD Art. 32; ISO 27001; ENS.

---

#### **PRIV-141 – Implementación de Firewalls para la Protección Perimetral**

- **Descripción:**

- Se deben utilizar **firewalls de nueva generación (NGFW)** para proteger la infraestructura contra accesos no autorizados y ciberataques.
- Se debe filtrar y controlar el tráfico entrante y saliente.

- **Criterios de Aceptación:**

- Configuración de **firewalls perimetrales y host-based** en redes y servidores críticos.
- Implementación de reglas para bloquear tráfico sospechoso o no autorizado.
- Auditorías periódicas de la configuración del firewall.

- **Prioridad:** Alta.

- **Categoría:** Seguridad de la Información.

- **Fuente:** RGPD Art. 32; ISO 27001; ENS.

---

#### **PRIV-142 – Protección contra Ataques de Ingeniería Social y Phishing**

- **Descripción:**
    - Se deben establecer medidas para prevenir **ataques de phishing, spoofing e ingeniería social** que puedan comprometer la seguridad de los datos personales.
    - Se deben realizar campañas de concienciación para empleados y usuarios.
  - **Criterios de Aceptación:**
    - Implementación de **filtros anti-phishing** en correos electrónicos.
    - Simulación periódica de ataques de phishing y evaluación de la respuesta de empleados.
    - Formación anual en ciberseguridad para todo el personal.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ENS; ISO 27001.
- 

#### **PRIV-143 – Protección contra Malware y Ransomware**

- **Descripción:**
    - Se deben implementar soluciones de seguridad para prevenir infecciones por **malware, ransomware y otros ataques cibernéticos**.
    - Se deben utilizar herramientas de **detección de comportamiento anómalo** en dispositivos y servidores.
  - **Criterios de Aceptación:**
    - Instalación de **antivirus y EDR (Endpoint Detection & Response)** en todos los dispositivos.
    - Configuración de **políticas de restricción de ejecución de software no autorizado**.
    - Monitorización y respuesta rápida ante incidentes de seguridad.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ENS; ISO 27001.
- 

#### **PRIV-144 – Seguridad en Servicios Cloud y Terceros Proveedores**

- **Descripción:**
    - Se deben establecer medidas de control para garantizar la seguridad en servicios de **computación en la nube y proveedores externos**.
    - Se deben evaluar periódicamente los riesgos asociados a estos proveedores.
  - **Criterios de Aceptación:**
    - Uso de **cifrado de datos en la nube** para garantizar su privacidad.
    - Evaluación de proveedores de nube según normativas como **ISO 27017 y ENS**.
    - Contratos de procesamiento de datos que establezcan medidas de seguridad adecuadas.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 28, 32; ISO 27001; ENS.
- 

#### **PRIV-145 – Protección contra Ataques de Denegación de Servicio (DDoS)**

- **Descripción:**
    - Se deben implementar medidas para **prevenir y mitigar ataques de denegación de servicio (DDoS)** que puedan afectar la disponibilidad de los sistemas que gestionan datos personales.
    - Se deben utilizar soluciones de protección en la red y en la infraestructura.
  - **Criterios de Aceptación:**
    - Implementación de **mitigación automática de DDoS** en redes y servidores.
    - Uso de **CDN (Content Delivery Networks)** para minimizar el impacto de ataques volumétricos.
    - Monitorización constante del tráfico para detectar patrones de ataque.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ENS; ISO 27001.
- 

#### **PRIV-146 – Gestión de Parches y Actualizaciones de Seguridad**

- **Descripción:**
    - Se debe contar con un proceso de **gestión de actualizaciones y parches de seguridad** para prevenir vulnerabilidades explotables por amenazas externas.
    - Se debe garantizar que los sistemas críticos sean actualizados con prioridad.
  - **Criterios de Aceptación:**
    - Implementación de un **plan de gestión de parches** con actualización periódica.
    - Aplicación de **actualizaciones críticas en un plazo máximo de 7 días** desde su publicación.
    - Monitorización de vulnerabilidades y aplicación de mitigaciones temporales si no hay parches disponibles.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001; ENS.
- 

#### **PRIV-147 – Auditoría Periódica de Seguridad frente a Amenazas Externas**

- **Descripción:**
    - Se deben realizar auditorías de seguridad y **pruebas de penetración (pentesting)** para identificar vulnerabilidades explotables desde el exterior.
    - Los resultados deben utilizarse para mejorar continuamente la seguridad.
  - **Criterios de Aceptación:**
    - Realización de **pentesting y auditorías de seguridad al menos una vez al año**.
    - Implementación de **planes de acción correctivos** en base a los hallazgos.
    - Evaluación de la resiliencia ante ataques cibernéticos mediante simulaciones.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ENS; ISO 27001.
-

## **PRIV-148 – Implementación de un Plan de Gestión de Incidentes de Seguridad**

- **Descripción:**

Según el **Artículo 32 del RGPD**, las organizaciones deben contar con un **plan de gestión de incidentes de seguridad** que permita la identificación, respuesta y mitigación de ataques o accesos no autorizados.

- Se debe definir un **protocolo claro** para la gestión de incidentes, con roles y responsabilidades.
- Debe incluir procedimientos de notificación y recuperación.

- **Criterios de Aceptación:**

- Creación y difusión de un **Plan de Gestión de Incidentes** en la organización.
- Definición de un **equipo de respuesta a incidentes (CSIRT o SOC)**.
- Evaluación periódica de la efectividad del plan mediante simulaciones de ataques.

- **Prioridad:** Alta.

- **Categoría:** Seguridad de la Información.

- **Fuente:** RGPD Art. 32, 33; ENS; ISO 27001.

---

## **PRIV-149 – Sistema de Detección y Notificación de Incidentes de Seguridad**

- **Descripción:**

- Se debe implementar un **sistema de monitoreo continuo** para detectar incidentes de seguridad.
- Debe contar con alertas automatizadas y notificación en tiempo real.

- **Criterios de Aceptación:**

- Implementación de herramientas **SIEM (Security Information and Event Management)** para la detección de anomalías.
- Configuración de **alertas automáticas** ante eventos sospechosos.
- Definición de un procedimiento de escalamiento y resolución de incidentes.

- **Prioridad:** Alta.

- **Categoría:** Seguridad de la Información.

- **Fuente:** RGPD Art. 32; ENS; ISO 27001.

---

## **PRIV-150 – Notificación de Brechas de Seguridad a la Autoridad de Protección de Datos**

- **Descripción:**

Según el **Artículo 33 del RGPD**, en caso de una **brecha de seguridad** que afecte datos personales, se debe notificar a la autoridad de control en un plazo máximo de **72 horas** desde su detección.

- Se debe documentar el incidente, su impacto y las medidas adoptadas.

- **Criterios de Aceptación:**

- Procedimiento formalizado para la **notificación de brechas de seguridad** a la autoridad competente.
- Registro detallado del incidente con evaluación del impacto.
- Envío de la notificación a la autoridad en un **máximo de 72 horas**.

- **Prioridad:** Alta.

- **Categoría:** Seguridad de la Información.

- **Fuente:** RGPD Art. 33; ENS.

---

## **PRIV-151 – Notificación de Brechas de Seguridad a los Afectados**

- **Descripción:**

Según el **Artículo 34 del RGPD**, si una brecha de seguridad supone un **alto riesgo para los derechos y libertades de los afectados**, se debe notificar individualmente a los interesados.

- La notificación debe ser clara y contener recomendaciones para mitigar riesgos.

- **Criterios de Aceptación:**

- Implementación de un **protocolo de comunicación con los afectados** en caso de brecha.
- Envío de notificaciones en **plazo razonable** con instrucciones para mitigar daños.
- Documentación de todas las comunicaciones realizadas.

- **Prioridad:** Alta.

- **Categoría:** Seguridad de la Información.

- **Fuente:** RGPD Art. 34; ENS.

---



## **PRIV-152 – Registro y Documentación de Incidentes de Seguridad**

- **Descripción:**
    - Se debe mantener un registro de **todos los incidentes de seguridad** relacionados con datos personales, incluyendo:
      - Fecha y hora del incidente.
      - Naturaleza y alcance del incidente.
      - Medidas adoptadas para su mitigación.
    - Este registro debe estar disponible para auditorías internas y externas.
  - **Criterios de Aceptación:**
    - Implementación de un **sistema de gestión de incidentes** con registros detallados.
    - Documentación de las acciones tomadas en respuesta a cada incidente.
    - Revisión periódica de registros para identificar tendencias y mejorar la seguridad.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 33, 34; ISO 27001; ENS.
- 

## **PRIV-153 – Simulación y Análisis de Respuesta ante Incidentes**

- **Descripción:**
  - Se deben realizar simulaciones periódicas de incidentes de seguridad para evaluar la respuesta de la organización.
  - Se deben analizar los resultados y aplicar mejoras en los procedimientos.
- **Criterios de Aceptación:**
  - Realización de **simulacros de brechas de seguridad al menos una vez al año**.
  - Análisis de **fallos detectados en los simulacros** y aplicación de mejoras.
  - Formación del personal para mejorar la respuesta ante incidentes.
- **Prioridad:** Media.
- **Categoría:** Seguridad de la Información.
- **Fuente:** RGPD Art. 32; ISO 27001; ENS.

---

#### **PRIV-154 – Plan de Recuperación y Continuidad ante Incidentes de Seguridad**

- **Descripción:**
    - Se debe contar con un **Plan de Continuidad del Negocio (BCP)** que contemple medidas para garantizar la operatividad tras un incidente de seguridad.
    - Debe incluir la restauración de datos y sistemas afectados.
  - **Criterios de Aceptación:**
    - Definición de un **plan de continuidad y recuperación ante desastres (DRP)**.
    - Pruebas periódicas de la efectividad del plan.
    - Garantía de recuperación en **tiempos mínimos aceptables (RTO/RPO)**.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001; ENS.
- 

#### **PRIV-155 – Creación de un Plan de Respuesta ante Brechas de Seguridad**

- **Descripción:**

Según el **Artículo 32 del RGPD**, las organizaciones deben contar con un **Plan de Respuesta ante Brechas de Seguridad**, que establezca:

  - Procedimientos de detección, análisis y contención de incidentes.
  - Roles y responsabilidades en la respuesta a incidentes.
  - Métodos de notificación interna y externa.
- **Criterios de Aceptación:**
  - Implementación de un **Plan de Respuesta ante Brechas de Seguridad** aprobado por la dirección.
  - Definición de un **equipo de respuesta a incidentes de seguridad (CSIRT/SOC)**.
  - Revisión anual y pruebas del plan mediante simulaciones.
- **Prioridad:** Alta.
- **Categoría:** Seguridad de la Información.
- **Fuente:** RGPD Art. 32, 33; ISO 27001; ENS.

---

#### **PRIV-156 – Procedimientos de Contención y Mitigación de Brechas de Seguridad**

- **Descripción:**
    - Se deben establecer **procedimientos de contención inmediata** para reducir el impacto de una brecha de seguridad.
    - Deben existir protocolos para mitigar los efectos y evitar su propagación.
  - **Criterios de Aceptación:**
    - Implementación de un **protocolo de contención rápida**.
    - Procedimientos documentados para **aislar sistemas comprometidos**.
    - Evaluación de los efectos de la brecha y aplicación de medidas de mitigación.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32, 33; ISO 27001.
- 

#### **PRIV-157 – Evaluación del Impacto de la Brecha de Seguridad**

- **Descripción:**
    - Se debe realizar una **evaluación del impacto** de cada brecha de seguridad para determinar su gravedad y afectación a los datos personales.
    - Se debe clasificar la brecha según su riesgo (bajo, medio, alto).
  - **Criterios de Aceptación:**
    - Implementación de un **mecanismo de clasificación de impacto** basado en criterios objetivos.
    - Registro detallado del número de afectados y la criticidad de los datos expuestos.
    - Procedimiento de escalado en caso de incidentes de alto impacto.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32, 33; ENS.
- 

#### **PRIV-158 – Notificación a la Autoridad de Protección de Datos**

- **Descripción:**  
Según el **Artículo 33 del RGPD**, si una brecha de seguridad supone un **riesgo para los derechos y libertades de los afectados**, se debe notificar a la autoridad competente en un **plazo máximo de 72 horas**.
    - Se debe documentar la brecha y justificar las medidas adoptadas.
  - **Criterios de Aceptación:**
    - Procedimiento documentado para **notificar la brecha en menos de 72 horas**.
    - Registro detallado del incidente, medidas tomadas y mitigaciones futuras.
    - Confirmación de recepción de la notificación por la autoridad de control.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 33.
- 

#### **PRIV-159 – Notificación a los Afectados en Caso de Riesgo Alto**

- **Descripción:**  
Según el **Artículo 34 del RGPD**, si la brecha de seguridad **supone un alto riesgo** para los afectados, se debe informar directamente a cada uno de ellos.
    - La notificación debe incluir recomendaciones para mitigar posibles consecuencias.
  - **Criterios de Aceptación:**
    - Implementación de un **protocolo de comunicación con los afectados**.
    - Envío de notificación de manera clara y accesible.
    - Registro de las comunicaciones enviadas y recepción de confirmación por los usuarios.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 34.
- 

#### **PRIV-160 – Registro y Documentación de Brechas de Seguridad**

- **Descripción:**

- Se debe mantener un **registro detallado** de todas las brechas de seguridad, independientemente de si se notifican o no a la autoridad de control.
- Este registro debe contener:
  - Fecha y hora del incidente.
  - Naturaleza de la brecha.
  - Datos afectados y número de usuarios impactados.
  - Acciones tomadas y medidas preventivas futuras.
- **Criterios de Aceptación:**
  - Implementación de un **sistema de gestión de incidentes** con registro de brechas.
  - Documentación clara de las respuestas a cada incidente.
  - Evaluación periódica del registro para identificar patrones y prevenir futuras brechas.
- **Prioridad:** Media.
- **Categoría:** Seguridad de la Información.
- **Fuente:** RGPD Art. 33, 34; ISO 27001; ENS.

---

## PRIV-161 – Simulación y Evaluación de Respuesta ante Brechas de Seguridad

- **Descripción:**
  - Se deben realizar **simulaciones periódicas de brechas de seguridad** para evaluar la capacidad de respuesta de la organización.
  - Los resultados deben utilizarse para mejorar los procedimientos y tiempos de reacción.
- **Criterios de Aceptación:**
  - Ejecución de **pruebas de respuesta a incidentes al menos una vez al año**.
  - Evaluación de los tiempos de detección, contención y notificación.
  - Ajuste del Plan de Respuesta basado en los resultados de las simulaciones.
- **Prioridad:** Media.
- **Categoría:** Seguridad de la Información.

- **Fuente:** RGPD Art. 32; ISO 27001; ENS.
- 

#### **PRIV-162 – Plan de Recuperación de Datos y Sistemas tras una Brecha de Seguridad**

- **Descripción:**
    - Se debe contar con un **Plan de Recuperación ante Incidentes de Seguridad** que permita restablecer los datos y sistemas afectados por la brecha.
    - Debe incluir medidas de continuidad del negocio y recuperación de datos.
  - **Criterios de Aceptación:**
    - Implementación de un **Plan de Recuperación de Datos y Sistemas (DRP)**.
    - Pruebas periódicas de la efectividad del plan mediante simulaciones.
    - Garantía de recuperación en **tiempos mínimos aceptables (RTO/RPO)**.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001; ENS.
- 

#### **PRIV-163 – Evaluación de la Base Legal para la Transferencia Internacional de Datos**

- **Descripción:**

Según el **Artículo 44 del RGPD**, cualquier transferencia de datos personales fuera de la UE debe cumplir con una base legal válida, como:

  - **Decisiones de adecuación de la Comisión Europea.**
  - **Cláusulas contractuales tipo (SCCs).**
  - **Normas corporativas vinculantes (BCRs).**
  - **Excepciones específicas del Artículo 49 del RGPD.**
- **Criterios de Aceptación:**
  - Evaluación y documentación de la base legal para la transferencia.
  - Uso de SCCs o BCRs si el país destinatario no tiene una decisión de adecuación.
  - Revisión legal antes de establecer cualquier transferencia de datos fuera de la UE.

- **Prioridad:** Alta.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 44-49.
- 

#### **PRIV-164 – Uso de Decisiones de Adecuación de la Comisión Europea**

- **Descripción:**
    - Se permite la transferencia de datos personales a países que la **Comisión Europea haya declarado adecuados** en materia de protección de datos.
    - No es necesario aplicar medidas adicionales si existe una decisión de adecuación válida.
  - **Criterios de Aceptación:**
    - Verificación de que el país de destino cuenta con una **decisión de adecuación vigente**.
    - Registro y documentación de la justificación de la transferencia basada en adecuación.
    - Monitoreo de actualizaciones de la Comisión Europea sobre países adecuados.
  - **Prioridad:** Alta.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 45.
- 

#### **PRIV-165 – Aplicación de Cláusulas Contractuales Tipo (SCCs) para Transferencias**

- **Descripción:**
  - En ausencia de una decisión de adecuación, la transferencia debe estar basada en **Cláusulas Contractuales Tipo (SCCs)** aprobadas por la Comisión Europea.
  - Se deben incluir garantías adicionales para la seguridad de los datos.
- **Criterios de Aceptación:**
  - Uso de **SCCs actualizadas** en contratos con entidades fuera de la UE.
  - Evaluación de impacto en la protección de datos antes de la transferencia (Transfer Impact Assessment, TIA).

- Aplicación de medidas técnicas adicionales si el país receptor tiene normativas que puedan afectar la privacidad de los datos.
  - **Prioridad:** Alta.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 46; Recomendaciones del EDPB.
- 

#### **PRIV-166 – Implementación de Normas Corporativas Vinculantes (BCRs) para Empresas Multinacionales**

- **Descripción:**
    - Las organizaciones multinacionales pueden transferir datos entre sus filiales fuera de la UE si cuentan con **Normas Corporativas Vinculantes (BCRs)** aprobadas por una autoridad de protección de datos.
  - **Criterios de Aceptación:**
    - Aprobación de las BCRs por una autoridad de control de la UE.
    - Garantía de que las filiales aplican medidas de seguridad y privacidad equivalentes a las del RGPD.
    - Actualización y auditoría periódica de las BCRs.
  - **Prioridad:** Media.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 47.
- 

#### **PRIV-167 – Aplicación de Salvaguardas Adicionales en Transferencias de Datos**

- **Descripción:**
  - Si la transferencia de datos implica riesgos para la privacidad de los usuarios, se deben aplicar **medidas técnicas y organizativas adicionales** para garantizar la seguridad de los datos.
  - Esto incluye cifrado fuerte, anonimización o restricciones de acceso.
- **Criterios de Aceptación:**
  - Implementación de **cifrado extremo a extremo (E2EE)** en la transmisión de datos.
  - Evaluación de riesgos de acceso gubernamental en el país receptor.
  - Aplicación de políticas de minimización de datos en transferencias internacionales.



- **Prioridad:** Alta.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 46; Recomendaciones del EDPB.
- 

#### **PRIV-168 – Excepciones para la Transferencia de Datos en Casos Específicos**

- **Descripción:**
    - En circunstancias excepcionales, los datos personales pueden ser transferidos fuera de la UE sin SCCs ni decisión de adecuación, si se cumple una de las **excepciones del Artículo 49 del RGPD**, tales como:
      - Consentimiento explícito del interesado.
      - Ejecución de un contrato.
      - Interés público.
      - Defensa de reclamaciones legales.
  - **Criterios de Aceptación:**
    - Evaluación y documentación de la excepción aplicada a la transferencia.
    - Obtención de **consentimiento explícito e informado** cuando sea la base utilizada.
    - Garantía de que la transferencia es puntual y no sistemática.
  - **Prioridad:** Media.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 49.
- 

#### **PRIV-169 – Supervisión y Auditoría de Transferencias Internacionales de Datos**

- **Descripción:**
  - Se deben realizar auditorías periódicas para garantizar que las transferencias de datos cumplen con los requisitos del RGPD.
  - Se debe contar con registros detallados de todas las transferencias internacionales.
- **Criterios de Aceptación:**
  - Implementación de un **sistema de registro de transferencias de datos**.
  - Auditoría interna anual de los procedimientos de transferencia.

- Evaluación de cumplimiento con las últimas regulaciones y recomendaciones del EDPB.
  - **Prioridad:** Media.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 44-49.
- 

#### **PRIV-170 – Plan de Contingencia ante Cambios Regulatorios sobre Transferencias**

- **Descripción:**
    - Dado que la normativa sobre transferencias internacionales puede cambiar, se debe contar con un plan de contingencia para adaptarse a nuevas regulaciones.
    - Debe incluir procedimientos en caso de que un país pierda su decisión de adecuación o se modifiquen las SCCs.
  - **Criterios de Aceptación:**
    - Seguimiento constante de actualizaciones regulatorias.
    - Implementación de estrategias de migración de datos en caso de cambios en la legalidad de las transferencias.
    - Coordinación con equipos legales para adaptar contratos y medidas de seguridad.
  - **Prioridad:** Media.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 44-49.
- 

#### **PRIV-171 – Implementación de Cláusulas Contractuales Tipo (SCCs) en Transferencias Internacionales**

- **Descripción:**

Según el **Artículo 46 del RGPD**, en ausencia de una **decisión de adecuación**, las organizaciones deben utilizar **Cláusulas Contractuales Tipo (SCCs)** aprobadas por la Comisión Europea para garantizar la seguridad de las transferencias de datos fuera de la UE.

  - Las SCCs deben reflejar los requisitos de privacidad y seguridad del RGPD.
  - Se deben evaluar los riesgos antes de su aplicación.
- **Criterios de Aceptación:**

- Inclusión de **SCCs actualizadas (versión 2021 de la Comisión Europea)** en contratos con proveedores fuera de la UE.
  - Evaluación de impacto en protección de datos (TIA) antes de cada transferencia.
  - Aplicación de **medidas adicionales** si la legislación del país receptor afecta la privacidad de los datos.
  - **Prioridad:** Alta.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 46; Recomendaciones del EDPB.
- 

#### **PRIV-172 – Evaluación de Riesgos en Transferencias Basadas en SCCs (Transfer Impact Assessment – TIA)**

- **Descripción:**
    - Antes de utilizar SCCs, las organizaciones deben realizar una **Evaluación de Impacto en Transferencias (TIA)** para analizar los riesgos que puedan surgir debido a las leyes de vigilancia del país de destino.
    - Si el análisis revela riesgos elevados, se deben aplicar **salvaguardas adicionales**.
  - **Criterios de Aceptación:**
    - Realización de una **TIA documentada** antes de cada transferencia basada en SCCs.
    - Identificación de riesgos regulatorios y aplicación de medidas de mitigación.
    - Revisión periódica de las TIA para asegurar su vigencia.
  - **Prioridad:** Alta.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 46; Recomendaciones del EDPB.
- 

#### **PRIV-173 – Uso de Normas Corporativas Vinculantes (BCRs) para Transferencias dentro de un Grupo Empresarial**

- **Descripción:**
  - Las **Normas Corporativas Vinculantes (BCRs)** permiten la transferencia de datos personales entre entidades de un mismo grupo empresarial fuera de la UE, garantizando el cumplimiento del RGPD en todas las filiales.

- Las BCRs deben ser aprobadas por una autoridad de control de la UE.
  - **Criterios de Aceptación:**
    - Obtención de la **aprobación de las BCRs** por una autoridad de protección de datos.
    - Garantía de que todas las filiales aplican los mismos estándares de protección de datos.
    - Auditoría y actualización periódica de las BCRs.
  - **Prioridad:** Media.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 47.
- 

#### **PRIV-174 – Salvaguardas Adicionales en Transferencias con SCCs y BCRs**

- **Descripción:**
    - Cuando las SCCs o BCRs no sean suficientes para garantizar la privacidad, se deben aplicar **medidas técnicas y organizativas adicionales** como:
      - **Cifrado de extremo a extremo (E2EE).**
      - **Minimización de datos antes de la transferencia.**
      - **Limitación del acceso a los datos en el país de destino.**
  - **Criterios de Aceptación:**
    - Implementación de **cifrado de datos con claves controladas dentro de la UE.**
    - Restricción de acceso solo a personal autorizado.
    - Evaluación continua de la eficacia de las salvaguardas adicionales.
  - **Prioridad:** Alta.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 46; Recomendaciones del EDPB.
- 

#### **PRIV-175 – Incorporación de Obligaciones Contractuales en Acuerdos con Proveedores**

- **Descripción:**
  - En contratos con proveedores fuera de la UE, se deben incluir cláusulas que obliguen a la empresa receptora a:

- Cumplir con las disposiciones del RGPD.
    - Cooperar con las auditorías de cumplimiento.
    - Implementar medidas de seguridad adecuadas.
  - **Criterios de Aceptación:**
    - Inclusión de cláusulas sobre **seguridad y confidencialidad** en contratos de proveedores.
    - Implementación de un **proceso de auditoría periódica** de cumplimiento.
    - Documentación de las evaluaciones de seguridad de los proveedores.
  - **Prioridad:** Alta.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 28, 46.
- 

#### **PRIV-176 – Auditoría y Revisión Periódica del Cumplimiento de SCCs y BCRs**

- **Descripción:**
    - Se deben realizar auditorías periódicas para garantizar que las SCCs y BCRs se aplican correctamente y que los datos personales están protegidos.
  - **Criterios de Aceptación:**
    - Auditoría anual del cumplimiento de **SCCs y BCRs** en transferencias internacionales.
    - Revisión de la **vigencia de contratos y salvaguardas aplicadas**.
    - Corrección inmediata de incumplimientos detectados en auditorías.
  - **Prioridad:** Media.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 46, 47.
- 

#### **PRIV-177 – Registro y Documentación de Transferencias con SCCs y BCRs**

- **Descripción:**
  - Se debe mantener un **registro actualizado** de todas las transferencias realizadas bajo SCCs y BCRs, incluyendo:
    - Fecha de la transferencia.

- Tipo de datos transferidos.
    - Base legal utilizada.
    - Salvaguardas adicionales aplicadas.
  - **Criterios de Aceptación:**
    - Implementación de un **sistema de registro de transferencias**.
    - Actualización periódica del registro con detalles de cada transferencia.
    - Accesibilidad del registro para auditorías internas y externas.
  - **Prioridad:** Media.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 30, 46.
- 

#### **PRIV-177 – Implementación de Certificaciones de Protección de Datos**

- **Descripción:**

Según los **Artículos 42 y 43 del RGPD**, las organizaciones pueden obtener **certificaciones** en protección de datos como una forma de demostrar conformidad con la normativa.

    - Las certificaciones deben ser emitidas por organismos acreditados y reconocidos en la UE.
    - Deben ser revisadas periódicamente para asegurar su vigencia.
  - **Criterios de Aceptación:**
    - Identificación de certificaciones aplicables (ej. **EuroPrivacy, ISO/IEC 27701**).
    - Implementación de controles y procesos para cumplir con los estándares requeridos.
    - Mantenimiento y auditoría periódica de la certificación obtenida.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** RGPD Art. 42.
- 

#### **PRIV-178 – Selección de Organismos de Certificación Acreditados**

- **Descripción:**

- Solo se pueden obtener certificaciones de **entidades acreditadas** por las autoridades de protección de datos de la UE o por organismos reconocidos a nivel internacional.
  - **Criterios de Aceptación:**
    - Verificación de que el organismo emisor está acreditado según el **RGPD y ISO/IEC 17065**.
    - Revisión de los criterios de certificación exigidos por cada organismo.
    - Documentación de la elección del organismo certificador.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 43.
- 

#### **PRIV-179 – Implementación de un Sistema de Gestión de Privacidad Basado en Certificación**

- **Descripción:**
    - La organización debe adaptar su **Sistema de Gestión de Privacidad (SGP)** para cumplir con los requisitos de la certificación seleccionada.
    - Debe integrar procedimientos documentados para garantizar la continuidad del cumplimiento.
  - **Criterios de Aceptación:**
    - Definición y documentación de un **SGP basado en estándares de certificación**.
    - Inclusión de auditorías internas para evaluar el cumplimiento con los requisitos de certificación.
    - Mantenimiento de registros sobre la implementación y supervisión del SGP.
  - **Prioridad:** Alta.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** RGPD Art. 42; ISO/IEC 27701.
- 

#### **PRIV-180 – Verificación de Cumplimiento Periódico con los Estándares de Certificación**

- **Descripción:**

- Una vez obtenida la certificación, se deben realizar **evaluaciones regulares** para confirmar que los estándares siguen cumpliéndose.
  - **Criterios de Aceptación:**
    - Implementación de revisiones anuales o conforme al período establecido por el certificado.
    - Realización de auditorías internas o externas para evaluar el mantenimiento del cumplimiento.
    - Documentación de medidas correctivas ante hallazgos de auditoría.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** RGPD Art. 42-43.
- 

#### **PRIV-181 – Integración de Certificaciones en Contratos con Encargados del Tratamiento**

- **Descripción:**
    - Se debe garantizar que los encargados del tratamiento con los que se contrata posean certificaciones reconocidas en protección de datos o apliquen medidas equivalentes.
  - **Criterios de Aceptación:**
    - Verificación de la certificación o medidas de cumplimiento de los encargados del tratamiento.
    - Inclusión de cláusulas en los contratos que exijan el mantenimiento de certificaciones o auditorías externas.
    - Revisión periódica del estado de certificación de los proveedores.
  - **Prioridad:** Media.
  - **Categoría:** Transferencias Internacionales y Gobernanza.
  - **Fuente:** RGPD Art. 28, 42.
- 

#### **PRIV-182 – Publicación y Transparencia de la Certificación Obtenida**

- **Descripción:**
  - Las organizaciones certificadas pueden hacer público su **sello de certificación** para demostrar su compromiso con la protección de datos.



- Se debe asegurar que la certificación se usa de manera transparente y sin generar confusión en los interesados.
  - **Criterios de Aceptación:**
    - Publicación de la certificación en la web corporativa y documentos relevantes.
    - Inclusión de información sobre el alcance y validez de la certificación.
    - Garantía de que la certificación se presenta de manera clara y no engañosa.
  - **Prioridad:** Baja.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 42.
- 

#### **PRIV-183 – Mantenimiento de un Registro de Certificaciones y Evaluaciones de Cumplimiento**

- **Descripción:**
    - Se debe mantener un **registro interno** de todas las certificaciones obtenidas, así como de las evaluaciones y auditorías realizadas para su mantenimiento.
  - **Criterios de Aceptación:**
    - Creación de un **registro de certificaciones y auditorías de cumplimiento**.
    - Documentación de fechas de renovación y revisión de certificaciones.
    - Protección del registro contra accesos no autorizados y alteraciones.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 42-43.
- 

#### **PRIV-184 – Evaluación de Beneficios y Costes de la Certificación**

- **Descripción:**
  - Antes de optar por una certificación, la organización debe analizar los **beneficios, costes y exigencias** para determinar su viabilidad y rentabilidad.
- **Criterios de Aceptación:**

- Realización de un análisis de **coste-beneficio de la certificación**.
    - Evaluación de los recursos necesarios para la implementación y mantenimiento.
    - Aprobación de la certificación por la alta dirección en función del análisis realizado.
  - **Prioridad:** Baja.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 42.
- 

#### **PRIV-185 – Verificación de Países con Decisión de Adecuación Vigente**

- **Descripción:**

Según el **Artículo 45 del RGPD**, los datos personales pueden transferirse a un país fuera de la UE si la **Comisión Europea ha emitido una decisión de adecuación**, confirmando que el país ofrece un nivel de protección equivalente al del RGPD.

    - Se debe garantizar que la transferencia solo se realice a países con decisión de adecuación vigente.
  - **Criterios de Aceptación:**
    - Revisión periódica de la **lista de países adecuados** publicada por la Comisión Europea.
    - Documentación de la base legal para cada transferencia basada en adecuación.
    - Implementación de un sistema de monitoreo para detectar cambios en la adecuación de países.
  - **Prioridad:** Alta.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 45.
- 

#### **PRIV-186 – Documentación de Transferencias Basadas en Decisiones de Adecuación**

- **Descripción:**
  - Se debe mantener un **registro detallado** de todas las transferencias de datos personales a países con decisión de adecuación.
- **Criterios de Aceptación:**

- Implementación de un **sistema de registro de transferencias internacionales**.
    - Documentación de la justificación de la transferencia y su base legal.
    - Verificación de la adecuación vigente antes de cada nueva transferencia.
  - **Prioridad:** Alta.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 30, 45.
- 

#### **PRIV-187 – Seguimiento de Cambios en la Lista de Países Adecuados**

- **Descripción:**
    - La Comisión Europea puede revocar o modificar decisiones de adecuación, por lo que las organizaciones deben estar preparadas para adaptarse a estos cambios.
  - **Criterios de Aceptación:**
    - Implementación de un **proceso de monitoreo** para identificar cambios en la lista de países adecuados.
    - Definición de un **plan de contingencia** en caso de revocación de una decisión de adecuación.
    - Notificación interna a los responsables del tratamiento cuando haya cambios en la lista de países adecuados.
  - **Prioridad:** Alta.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 45.
- 

#### **PRIV-188 – Uso del Marco de Privacidad de Datos UE-EE.UU. (Privacy Shield 2.0)**

- **Descripción:**
  - En julio de 2023, la Comisión Europea adoptó la decisión de adecuación para el **Marco de Privacidad de Datos UE-EE.UU. (Data Privacy Framework - DPF)**, permitiendo transferencias a empresas certificadas en EE.UU.
- **Criterios de Aceptación:**
  - Verificación de que el destinatario en EE.UU. está **certificado en el DPF**.
  - Documentación de la certificación y su validez antes de la transferencia.

- Supervisión de cualquier cambio en la legalidad del **Privacy Shield 2.0**.
  - **Prioridad:** Alta.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 45; Decisión de la Comisión Europea sobre el DPF.
- 

#### **PRIV-189 – Revisión de Obligaciones de los Destinatarios en Países Adecuados**

- **Descripción:**
    - Aunque un país tenga una decisión de adecuación, los destinatarios de los datos deben cumplir con sus **obligaciones contractuales y de seguridad**.
  - **Criterios de Aceptación:**
    - Inclusión de cláusulas en contratos con destinatarios en países adecuados que refuercen el cumplimiento del RGPD.
    - Evaluación de medidas de seguridad y control en el país de destino.
    - Revisión de la continuidad del nivel de protección ofrecido por el destinatario.
  - **Prioridad:** Media.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 45.
- 

#### **PRIV-190 – Alternativas en Caso de Falta de Decisión de Adecuación**

- **Descripción:**
  - Si un país no tiene una decisión de adecuación, se deben evaluar alternativas como:
    - **Cláusulas Contractuales Tipo (SCCs).**
    - **Normas Corporativas Vinculantes (BCRs).**
    - **Excepciones del Artículo 49 del RGPD.**
- **Criterios de Aceptación:**
  - Análisis de la viabilidad de SCCs o BCRs cuando no haya adecuación.
  - Implementación de salvaguardas adicionales si se usa una alternativa.
  - Documentación de la justificación de la transferencia en el registro de actividades.

- **Prioridad:** Alta.
  - **Categoría:** Transferencias Internacionales.
  - **Fuente:** RGPD Art. 46-49.
- 

#### **PRIV-191 – Registro y Auditoría de Transferencias a Países Adecuados**

- **Descripción:**
    - Se debe realizar una auditoría periódica de las transferencias de datos a países adecuados para asegurar su conformidad con la normativa.
  - **Criterios de Aceptación:**
    - Revisión y actualización del **registro de transferencias internacionales**.
    - Evaluación de la legalidad de cada transferencia en función de los cambios normativos.
    - Corrección de cualquier irregularidad detectada en la auditoría.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** RGPD Art. 45.
- 

#### **PRIV-192 – Publicación y Transparencia sobre Transferencias Internacionales**

- **Descripción:**
    - La organización debe informar a los interesados sobre las transferencias de datos a países adecuados en su política de privacidad.
  - **Criterios de Aceptación:**
    - Inclusión de información clara en la **política de privacidad** sobre transferencias internacionales.
    - Explicación de la base legal utilizada para cada transferencia en el aviso de privacidad.
    - Transparencia sobre los mecanismos de protección aplicados a los datos transferidos.
  - **Prioridad:** Media.
  - **Categoría:** Transparencia y Derechos del Usuario.
  - **Fuente:** RGPD Art. 13-14.
-

### **PRIV-193 – Identificación de Tratamientos que Requieren una Evaluación de Impacto en Protección de Datos (EIPD)**

- **Descripción:**

Según el **Artículo 35 del RGPD**, una **Evaluación de Impacto en Protección de Datos (EIPD)** es obligatoria cuando un tratamiento puede implicar un **alto riesgo** para los derechos y libertades de las personas, especialmente en los siguientes casos:

- Uso de **tecnologías innovadoras** como IA o biometría.
- **Monitoreo sistemático de personas** a gran escala.
- Tratamiento masivo de **datos sensibles** o de **menores**.
- Elaboración de **perfiles con impacto significativo en los derechos de los interesados**.

- **Criterios de Aceptación:**

- Identificación de tratamientos que requieren una **EIPD obligatoria** antes de su implementación.
- Registro y documentación de la justificación cuando se determine que no es necesaria una EIPD.
- Aplicación de un procedimiento estandarizado para la detección de tratamientos de alto riesgo.

- **Prioridad:** Alta.

- **Categoría:** Evaluaciones de Seguridad.

- **Fuente:** RGPD Art. 35; LOPDGDD.

---

### **PRIV-194 – Definición de una Metodología Estandarizada para la Realización de una EIPD**

- **Descripción:**

- La organización debe establecer una **metodología estructurada** para realizar Evaluaciones de Impacto en Protección de Datos (EIPD), que incluya:
  - **Descripción detallada del tratamiento y su finalidad.**
  - **Evaluación de la necesidad y proporcionalidad del tratamiento.**
  - **Identificación y análisis de riesgos potenciales.**
  - **Medidas de mitigación y seguridad aplicadas.**

- **Criterios de Aceptación:**

- Desarrollo de una **guía interna de EIPD** con metodología clara y aplicable.
  - Uso de formatos estandarizados para realizar evaluaciones.
  - Validación de la metodología por el **Delegado de Protección de Datos (DPO)**.
  - **Prioridad:** Alta.
  - **Categoría:** Evaluaciones de Seguridad.
  - **Fuente:** RGPD Art. 35; LOPDGDD.
- 

#### **PRIV-195 – Evaluación de Necesidad y Proporcionalidad del Tratamiento**

- **Descripción:**
    - La EIPD debe justificar la necesidad del tratamiento en relación con su finalidad y evaluar si existen **alternativas menos invasivas**.
  - **Criterios de Aceptación:**
    - Análisis de si el tratamiento es esencial para su finalidad declarada.
    - Comparación con **métodos alternativos menos intrusivos**.
    - Documentación de la justificación de necesidad y proporcionalidad en la EIPD.
  - **Prioridad:** Alta.
  - **Categoría:** Evaluaciones de Seguridad.
  - **Fuente:** RGPD Art. 35.
- 

#### **PRIV-196 – Identificación y Evaluación de Riesgos para los Derechos de los Interesados**

- **Descripción:**
  - Se deben identificar y documentar los **riesgos potenciales** que el tratamiento pueda suponer para los derechos de los interesados, clasificándolos en **bajo, medio o alto**.
- **Criterios de Aceptación:**
  - Identificación de **riesgos de acceso no autorizado, filtración o alteración de datos**.
  - Evaluación del impacto sobre la privacidad y derechos de los interesados.
  - Priorización de los riesgos en función de su **probabilidad y gravedad**.

- **Prioridad:** Alta.
  - **Categoría:** Evaluaciones de Seguridad.
  - **Fuente:** RGPD Art. 35; LOPDGDD.
- 

#### **PRIV-197 – Implementación de Medidas para Mitigar Riesgos en la EIPD**

- **Descripción:**
    - Se deben proponer y aplicar **medidas técnicas y organizativas** para reducir los riesgos identificados en la evaluación, incluyendo:
      - **Seudonimización o anonimización de datos.**
      - **Control de accesos basado en roles (RBAC) y autenticación multifactor (MFA).**
      - **Cifrado de información sensible.**
      - **Limitación de la retención de datos y mecanismos de supresión segura.**
  - **Criterios de Aceptación:**
    - Aplicación de medidas de seguridad adecuadas según el **riesgo identificado**.
    - Documentación de cada medida adoptada en la EIPD.
    - Revisión y validación de medidas por el **DPO y el equipo de seguridad**.
  - **Prioridad:** Alta.
  - **Categoría:** Evaluaciones de Seguridad.
  - **Fuente:** RGPD Art. 32, 35.
- 

#### **PRIV-198 – Consulta Obligatoria a la Autoridad de Control en Caso de Riesgo Elevado**

- **Descripción:**
  - Si la EIPD revela un **riesgo elevado que no puede ser mitigado adecuadamente**, la organización debe **consultar a la autoridad de control** antes de proceder con el tratamiento.
- **Criterios de Aceptación:**
  - Identificación de tratamientos que requieren consulta previa a la autoridad.



- Envío de documentación completa a la autoridad competente.
    - Espera de la evaluación y recomendaciones de la autoridad antes de iniciar el tratamiento.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 36.
- 

#### **PRIV-199 – Registro y Mantenimiento de un Archivo de EIPD Realizadas**

- **Descripción:**
    - Se debe mantener un **registro centralizado** de todas las EIPD realizadas, con información sobre:
      - Fecha de la evaluación.
      - Descripción del tratamiento analizado.
      - Medidas de mitigación adoptadas.
  - **Criterios de Aceptación:**
    - Implementación de un **sistema de registro de EIPD** accesible para auditorías.
    - Protección contra accesos no autorizados a las evaluaciones registradas.
    - Actualización periódica del registro con nuevas EIPD realizadas.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 35.
- 

#### **PRIV-200 – Revisión Periódica de EIPD para Tratamientos en Curso**

- **Descripción:**
  - Se deben revisar periódicamente las EIPD realizadas para asegurar que las medidas implementadas siguen siendo efectivas y adecuadas.
- **Criterios de Aceptación:**
  - Revisión de cada EIPD al menos **una vez cada dos años** o cuando se realicen cambios en el tratamiento.
  - Evaluación de la vigencia de las medidas de mitigación aplicadas.

- Registro de cambios o mejoras en la gestión de riesgos.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 35; LOPDGDD.
- 

#### **PRIV-201 – Implementación de un Proceso de Análisis de Riesgos en Protección de Datos**

- **Descripción:**

Según el **Artículo 32 del RGPD**, las organizaciones deben realizar análisis de riesgos para determinar las amenazas que pueden afectar la seguridad de los datos personales y definir medidas de mitigación adecuadas.

    - Se debe establecer un **proceso estructurado de identificación y gestión de riesgos** basado en estándares internacionales como **ISO/IEC 27005** o **ENS (Esquema Nacional de Seguridad)**.
  - **Criterios de Aceptación:**
    - Definición de un **procedimiento formal de análisis de riesgos**.
    - Aplicación de metodologías reconocidas para evaluar la probabilidad e impacto de los riesgos.
    - Documentación y actualización periódica del análisis de riesgos.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001; ENS.
- 

#### **PRIV-202 – Identificación y Clasificación de Activos de Información**

- **Descripción:**
  - Se deben identificar y clasificar los activos de información que contienen datos personales, determinando su criticidad y nivel de protección necesario.
- **Criterios de Aceptación:**
  - Elaboración de un **inventario de activos de información**, incluyendo bases de datos, sistemas, servidores y dispositivos.
  - Asignación de una categoría de riesgo a cada activo según su impacto en la privacidad.

- Implementación de medidas de protección adecuadas para cada categoría de activo.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-203 – Evaluación de Amenazas y Vulnerabilidades en los Sistemas de Información**

- **Descripción:**
    - Se debe analizar periódicamente la exposición de los sistemas a amenazas internas y externas que puedan comprometer la seguridad de los datos personales.
  - **Criterios de Aceptación:**
    - Realización de **pruebas de vulnerabilidad y auditorías de seguridad** al menos una vez al año.
    - Identificación de **amenazas internas y externas** que puedan afectar los sistemas.
    - Implementación de controles y medidas para mitigar las vulnerabilidades detectadas.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-204 – Aplicación de Controles de Seguridad según ISO 27001 y ENS**

- **Descripción:**
  - Se deben establecer **controles de seguridad** adecuados para proteger los datos personales, en conformidad con los requisitos de **ISO 27001** y el **Esquema Nacional de Seguridad (ENS)** en caso de administraciones públicas.
- **Criterios de Aceptación:**
  - Implementación de **medidas de seguridad organizativas, técnicas y operativas** según estándares internacionales.
  - Evaluación periódica de la **efectividad de los controles** aplicados.

- Documentación de las medidas adoptadas y justificación de su idoneidad.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-205 – Gestión de Accesos y Control de Privilegios en Sistemas de Información**

- **Descripción:**
    - Se deben establecer controles estrictos de acceso a los sistemas que contienen datos personales, aplicando el principio de **mínimos privilegios y necesidad de conocer**.
  - **Criterios de Aceptación:**
    - Implementación de **autenticación multifactor (MFA)** para accesos a datos sensibles.
    - Uso de **roles de acceso basados en funciones (RBAC)** para limitar privilegios.
    - Auditoría y revisión periódica de accesos para detectar usos indebidos.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001; ENS.
- 

#### **PRIV-206 – Implementación de un Plan de Continuidad del Negocio y Recuperación ante Desastres (BCP/DRP)**

- **Descripción:**
  - Se debe garantizar la continuidad operativa en caso de incidentes de seguridad mediante un **Plan de Continuidad del Negocio (BCP)** y un **Plan de Recuperación ante Desastres (DRP)**.
- **Criterios de Aceptación:**
  - Definición de un **BCP y DRP alineado con ISO 27001 y ENS**.
  - Realización de **pruebas periódicas de recuperación** de datos y sistemas.
  - Documentación de procedimientos y tiempos de recuperación (RTO/RPO).
- **Prioridad:** Alta.

- **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-207 – Monitorización y Detección de Incidentes de Seguridad**

- **Descripción:**
    - Se deben establecer mecanismos de **monitorización continua** para detectar incidentes de seguridad que puedan afectar los datos personales.
  - **Criterios de Aceptación:**
    - Implementación de **Sistemas de Gestión de Eventos e Información de Seguridad (SIEM)**.
    - Configuración de **alertas automáticas ante eventos sospechosos**.
    - Revisión periódica de logs y actividades sospechosas en los sistemas.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-208 – Gestión de Incidentes de Seguridad y Respuesta a Brechas de Datos**

- **Descripción:**
    - Se debe contar con un **procedimiento documentado** para la gestión de incidentes de seguridad y brechas de datos personales.
  - **Criterios de Aceptación:**
    - Definición de un **plan de respuesta a incidentes** en conformidad con ISO 27035.
    - Establecimiento de plazos y responsables para la gestión de incidentes.
    - Registro de incidentes detectados y medidas correctivas aplicadas.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001; ENS.
- 

#### **PRIV-209 – Auditorías y Evaluaciones Periódicas de Seguridad**

- **Descripción:**
    - Se deben realizar auditorías regulares para garantizar la efectividad de las medidas de seguridad aplicadas en el tratamiento de datos personales.
  - **Criterios de Aceptación:**
    - Realización de auditorías internas de seguridad al menos **una vez al año**.
    - Identificación y corrección de vulnerabilidades detectadas en auditorías.
    - Documentación y seguimiento de acciones correctivas.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-210 – Implementación de un Programa de Auditoría de Cumplimiento en Protección de Datos**

- **Descripción:**

Según el **Artículo 32 del RGPD** y el **Artículo 28 de la LOPDGDD**, las organizaciones deben realizar auditorías periódicas para evaluar su grado de cumplimiento en materia de protección de datos y seguridad.

    - Se debe establecer un **plan de auditoría estructurado** que cubra todas las áreas de cumplimiento.
    - Las auditorías deben incluir revisiones de procesos, medidas de seguridad y registros de tratamiento.
  - **Criterios de Aceptación:**
    - Definición y ejecución de un **plan anual de auditoría de cumplimiento**.
    - Revisión de la aplicación de medidas de seguridad, minimización de datos y derechos de los interesados.
    - Implementación de medidas correctivas basadas en los resultados de la auditoría.
  - **Prioridad:** Alta.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** RGPD Art. 32; LOPDGDD Art. 28; ENS.
- 

#### **PRIV-211 – Evaluación de Cumplimiento con el Esquema Nacional de Seguridad (ENS)**

- **Descripción:**
    - Las entidades que operan en el ámbito público o gestionan servicios esenciales deben cumplir con el **Esquema Nacional de Seguridad (ENS)**.
    - Se deben realizar auditorías para verificar el cumplimiento de los niveles de seguridad exigidos.
  - **Criterios de Aceptación:**
    - Revisión de la conformidad con los **requisitos del ENS (básico, medio o alto)**.
    - Evaluación del cumplimiento con los **principios de seguridad, integridad y disponibilidad**.
    - Implementación de medidas correctivas en caso de incumplimiento.
  - **Prioridad:** Alta.
  - **Categoría:** Auditoría y Seguridad.
  - **Fuente:** ENS; RGPD Art. 32.
- 

#### **PRIV-212 – Auditoría de Medidas Técnicas y Organizativas de Seguridad**

- **Descripción:**
    - Se deben auditar periódicamente las **medidas técnicas y organizativas** implementadas para garantizar la seguridad de los datos personales.
  - **Criterios de Aceptación:**
    - Evaluación de medidas como **cifrado, control de accesos, autenticación y monitorización**.
    - Pruebas de resistencia a ataques (pentesting) y auditorías de logs de seguridad.
    - Aplicación de planes de mejora según hallazgos de auditoría.
  - **Prioridad:** Alta.
  - **Categoría:** Auditoría y Seguridad.
  - **Fuente:** RGPD Art. 32; ENS; ISO 27001.
- 

#### **PRIV-213 – Auditoría del Registro de Actividades de Tratamiento**

- **Descripción:**

- Se debe verificar que el **Registro de Actividades de Tratamiento** está actualizado y refleja con precisión los tratamientos de datos personales en la organización.
  - **Criterios de Aceptación:**
    - Auditoría anual del **Registro de Actividades de Tratamiento**.
    - Identificación y corrección de inconsistencias o registros desactualizados.
    - Garantía de que todos los tratamientos cumplen con los principios del RGPD.
  - **Prioridad:** Alta.
  - **Categoría:** Auditoría y Gobernanza.
  - **Fuente:** RGPD Art. 30; LOPDGDD.
- 

#### **PRIV-214 – Verificación del Cumplimiento de los Derechos de los Interesados**

- **Descripción:**
    - Se debe auditar la capacidad de la organización para gestionar las solicitudes de derechos de los interesados (acceso, rectificación, supresión, oposición, portabilidad, limitación del tratamiento).
  - **Criterios de Aceptación:**
    - Pruebas de gestión de solicitudes de derechos de los interesados.
    - Evaluación de los **plazos de respuesta y justificación de denegaciones**.
    - Documentación de todas las solicitudes y sus respuestas en un registro centralizado.
  - **Prioridad:** Alta.
  - **Categoría:** Auditoría y Gobernanza.
  - **Fuente:** RGPD Art. 12-22; LOPDGDD.
- 

#### **PRIV-215 – Auditoría de Transferencias Internacionales de Datos**

- **Descripción:**
  - Se deben revisar las transferencias internacionales de datos para verificar que cumplen con las bases legales aplicables (**SCCs, BCRs, decisiones de adecuación o excepciones del Artículo 49**).
- **Criterios de Aceptación:**



- Revisión de contratos que contengan **Cláusulas Contractuales Tipo (SCCs)**.
  - Evaluación de la documentación de las **Evaluaciones de Impacto en Transferencias (TIA)**.
  - Verificación de que las transferencias cumplen con las normas del RGPD y la LOPDGDD.
  - **Prioridad:** Alta.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** RGPD Art. 44-49; LOPDGDD.
- 

#### **PRIV-216 – Auditoría de Encargados del Tratamiento y Proveedores**

- **Descripción:**
    - Se debe evaluar el cumplimiento de los encargados del tratamiento y proveedores externos que gestionan datos personales en nombre de la organización.
    - Se deben revisar contratos, medidas de seguridad y cumplimiento de obligaciones legales.
  - **Criterios de Aceptación:**
    - Auditoría de proveedores al menos **una vez al año**.
    - Revisión de contratos para verificar cláusulas de protección de datos.
    - Evaluación del cumplimiento de medidas de seguridad en proveedores.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Gobernanza.
  - **Fuente:** RGPD Art. 28; LOPDGDD.
- 

#### **PRIV-217 – Evaluación de Brechas de Seguridad y Planes de Mitigación**

- **Descripción:**
  - Se debe auditar la gestión de incidentes y brechas de seguridad para verificar que los procedimientos de respuesta sean efectivos y conformes con la normativa.
- **Criterios de Aceptación:**
  - Revisión del **registro de incidentes de seguridad y notificaciones**.

- Evaluación de la efectividad del **plan de respuesta ante incidentes**.
    - Implementación de mejoras en función de los resultados de la auditoría.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Seguridad.
  - **Fuente:** RGPD Art. 33-34; ENS.
- 

#### **PRIV-218 – Documentación y Seguimiento de No Conformidades y Planes de Mejora**

- **Descripción:**
    - Se debe mantener un registro de las auditorías realizadas, las no conformidades detectadas y los planes de mejora implementados.
  - **Criterios de Aceptación:**
    - Registro de **hallazgos de auditoría y planes de acción correctivos**.
    - Seguimiento del cumplimiento de los planes de mejora.
    - Validación de que las no conformidades han sido corregidas en las revisiones posteriores.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Gobernanza.
  - **Fuente:** RGPD Art. 24, 32; ENS.
- 

#### **PRIV-219 – Implementación de un Registro de Actividades de Tratamiento**

- **Descripción:**

Según el **Artículo 30 del RGPD**, los responsables y encargados del tratamiento deben llevar un **Registro de Actividades de Tratamiento (RAT)** que documente de forma estructurada todos los tratamientos de datos personales.

  - Se debe incluir información clave sobre cada tratamiento, como su finalidad, base legal y medidas de seguridad aplicadas.
- **Criterios de Aceptación:**
  - Creación y mantenimiento de un **Registro de Actividades de Tratamiento** accesible.
  - Inclusión de **todos los tratamientos activos** dentro de la organización.
  - Disponibilidad del RAT para auditorías y requerimientos de la autoridad de control.

- **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 30.
- 

#### **PRIV-220 – Identificación y Clasificación de Tratamientos de Datos Personales**

- **Descripción:**
    - Se debe garantizar que todos los tratamientos de datos personales estén correctamente identificados y clasificados en el Registro de Actividades de Tratamiento.
  - **Criterios de Aceptación:**
    - Clasificación de tratamientos según **su finalidad y base legal**.
    - Identificación de tratamientos de **alto riesgo** o que requieran Evaluación de Impacto en Protección de Datos (EIPD).
    - Documentación del responsable y encargado del tratamiento en cada actividad.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 30.
- 

#### **PRIV-221 – Contenido Mínimo del Registro de Actividades de Tratamiento**

- **Descripción:**
  - El Registro de Actividades de Tratamiento debe incluir al menos la siguiente información:
    - Nombre y datos del responsable y, en su caso, del representante y DPO.
    - **Finalidad del tratamiento.**
    - **Base legal** y categorías de interesados y datos tratados.
    - **Destinatarios de los datos**, incluyendo transferencias internacionales.
    - **Plazos de conservación** de los datos.
    - **Medidas de seguridad aplicadas.**
- **Criterios de Aceptación:**

- Verificación de que el RAT contiene todos los elementos obligatorios del **Artículo 30 del RGPD**.
    - Implementación de un formato estructurado y accesible.
    - Actualización periódica del contenido del registro.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 30.
- 

#### **PRIV-222 – Actualización y Mantenimiento del Registro de Actividades de Tratamiento**

- **Descripción:**
    - El RAT debe ser actualizado periódicamente para reflejar con precisión los tratamientos de datos personales dentro de la organización.
    - Se deben definir **responsables de la actualización** y procedimientos de revisión periódica.
  - **Criterios de Aceptación:**
    - Revisión y actualización del **RAT al menos una vez al año** o cuando haya cambios en los tratamientos.
    - Implementación de un **procedimiento interno de actualización del RAT**.
    - Registro de cambios realizados en los tratamientos documentados.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 30.
- 

#### **PRIV-223 – Digitalización y Centralización del Registro de Actividades de Tratamiento**

- **Descripción:**
  - Se recomienda que el RAT esté digitalizado y centralizado en una plataforma de gestión accesible por los responsables de privacidad.
- **Criterios de Aceptación:**
  - Implementación de una **plataforma digital** o software para gestionar el RAT.

- Accesibilidad del registro a los equipos legales, de seguridad y al DPO.
    - Protección del RAT contra modificaciones no autorizadas.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 30.
- 

#### **PRIV-224 – Inclusión del Registro de Transferencias Internacionales en el RAT**

- **Descripción:**
    - Se deben documentar todas las **transferencias internacionales de datos personales** en el RAT, indicando la base legal utilizada para cada transferencia.
  - **Criterios de Aceptación:**
    - Registro de **todas las transferencias fuera del EEE** en el RAT.
    - Identificación de la **base legal de la transferencia** (Decisión de Adecuación, SCCs, BCRs, excepciones).
    - Revisión periódica de la legalidad de las transferencias registradas.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 30, 44-49.
- 

#### **PRIV-225 – Auditoría del Registro de Actividades de Tratamiento**

- **Descripción:**
  - Se debe realizar una auditoría anual del RAT para verificar su **actualización, coherencia y cumplimiento con la normativa**.
- **Criterios de Aceptación:**
  - Revisión del RAT en auditorías internas y externas.
  - Evaluación de la coherencia del RAT con la realidad operativa de la organización.
  - Implementación de medidas correctivas en caso de inconsistencias.
- **Prioridad:** Media.
- **Categoría:** Auditoría y Cumplimiento.

- **Fuente:** RGPD Art. 30.
- 

#### **PRIV-226 – Inclusión de Evaluaciones de Impacto en Protección de Datos (EIPD) en el RAT**

- **Descripción:**
    - Se debe reflejar en el RAT qué tratamientos han requerido una **Evaluación de Impacto en Protección de Datos (EIPD)** y la fecha en que se realizó.
  - **Criterios de Aceptación:**
    - Registro en el RAT de **tratamientos de alto riesgo** que requieran EIPD.
    - Documentación de la fecha y medidas implementadas en la EIPD.
    - Supervisión del DPO en la actualización del RAT con EIPD.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 30, 35.
- 

#### **PRIV-227 – Accesibilidad del RAT para la Autoridad de Control**

- **Descripción:**
    - El Registro de Actividades de Tratamiento debe estar disponible en todo momento para su revisión por parte de la autoridad de control en caso de inspección o requerimiento.
  - **Criterios de Aceptación:**
    - Disponibilidad del RAT en caso de solicitud por la autoridad competente.
    - Garantía de que el RAT está completo y actualizado antes de una inspección.
    - Registro de accesos y modificaciones realizadas en el RAT.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 30.
- 

#### **PRIV-228 – Definición de una Política de Conservación de Datos**

- **Descripción:**

Según el **Artículo 5.1.e del RGPD**, los datos personales deben conservarse

**únicamente durante el tiempo necesario** para cumplir con los fines del tratamiento.

- Se debe establecer una **política documentada** que defina los períodos de retención y eliminación de datos personales.
  - **Criterios de Aceptación:**
    - Creación de una **Política de Conservación de Datos** clara y accesible.
    - Inclusión de plazos de retención específicos para cada categoría de datos.
    - Definición de procesos seguros para la eliminación de datos una vez cumplidos los plazos.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 5.1.e.
- 

#### **PRIV-229 – Determinación de Plazos de Retención Basados en Finalidades Legítimas**

- **Descripción:**
    - Se deben establecer plazos de retención para cada tipo de datos personales en función de su finalidad, asegurando que no se conserven más tiempo del necesario.
  - **Criterios de Aceptación:**
    - Definición de **plazos de conservación diferenciados** según la base legal del tratamiento.
    - Verificación de que la retención no excede los requisitos legales aplicables.
    - Aplicación de medidas técnicas para la eliminación automática o manual de datos tras el plazo de retención.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** RGPD Art. 5, 6.
- 

#### **PRIV-230 – Eliminación Segura de Datos Personales Tras la Finalización del Plazo de Retención**

- **Descripción:**

- Se deben definir y aplicar mecanismos de **eliminación segura de datos**, evitando que puedan ser recuperados o utilizados indebidamente tras el cumplimiento del plazo de retención.
  - **Criterios de Aceptación:**
    - Implementación de **métodos seguros de eliminación**, como el borrado criptográfico o la sobrescritura de datos.
    - Registro de todas las eliminaciones realizadas, asegurando trazabilidad.
    - Realización de auditorías para verificar que los procesos de eliminación cumplen con la normativa.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 17; ISO 27001.
- 

#### **PRIV-231 – Revisión Periódica de la Necesidad de Conservación de Datos**

- **Descripción:**
    - Se deben realizar **revisiones periódicas** para evaluar si los datos almacenados siguen siendo necesarios para la finalidad original del tratamiento.
  - **Criterios de Aceptación:**
    - Definición de un **proceso de revisión de datos cada 12 meses** o en función del ciclo de vida del tratamiento.
    - Eliminación o anonimización de datos que hayan excedido su plazo de retención.
    - Registro de las revisiones y decisiones tomadas sobre los datos conservados.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 5.
- 

#### **PRIV-232 – Anonimización de Datos para Extender su Uso sin Impactar la Privacidad**

- **Descripción:**



- En algunos casos, los datos pueden ser **anonimizados** en lugar de eliminados para su uso en estudios estadísticos o de investigación sin riesgo para la privacidad.
  - **Criterios de Aceptación:**
    - Aplicación de técnicas de **anonimización irreversibles**.
    - Garantía de que los datos anonimizados no pueden ser reidentificados.
    - Documentación de la justificación y el procedimiento de anonimización aplicado.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 5, 89.
- 

#### **PRIV-233 – Eliminación de Datos Personales a Solicitud del Interesado (Derecho al Olvido)**

- **Descripción:**

Según el **Artículo 17 del RGPD**, los interesados tienen derecho a solicitar la eliminación de sus datos personales en determinadas circunstancias.
  - **Criterios de Aceptación:**
    - Implementación de un **proceso para gestionar solicitudes de eliminación** de datos.
    - Verificación de la elegibilidad de la solicitud conforme al **Artículo 17 del RGPD**.
    - Eliminación efectiva de los datos dentro de los plazos legales establecidos.
  - **Prioridad:** Alta.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 17.
- 

#### **PRIV-234 – Documentación y Registro de Eliminaciones de Datos**

- **Descripción:**
  - Se debe mantener un **registro de eliminación de datos** para demostrar el cumplimiento con la política de conservación y eliminación de datos.
- **Criterios de Aceptación:**

- Registro de todas las eliminaciones realizadas, con fecha, responsable y método utilizado.
    - Protección del registro contra alteraciones o accesos no autorizados.
    - Disponibilidad del registro en caso de auditoría o requerimiento de la autoridad de control.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** RGPD Art. 5.
- 

#### **PRIV-235 – Gestión de Excepciones en la Eliminación de Datos**

- **Descripción:**
    - En algunos casos, los datos no pueden eliminarse inmediatamente debido a **obligaciones legales, regulatorias o contractuales**.
  - **Criterios de Aceptación:**
    - Identificación de excepciones legales a la eliminación de datos.
    - Implementación de **medidas de bloqueo o restricción de acceso** en lugar de eliminación cuando corresponda.
    - Documentación de la justificación de conservación en cada caso.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 17.
- 

#### **PRIV-236 – Inclusión de Plazos de Conservación en la Política de Privacidad**

- **Descripción:**
  - Los interesados deben ser informados sobre **los plazos de retención de sus datos** en la política de privacidad de la organización.
- **Criterios de Aceptación:**
  - Inclusión de información sobre **conservación y eliminación** en la política de privacidad.
  - Transparencia sobre los derechos de los interesados en relación con la conservación de sus datos.

- Actualización de la política de privacidad cuando haya cambios en la política de conservación.
  - **Prioridad:** Media.
  - **Categoría:** Transparencia y Derechos del Usuario.
  - **Fuente:** RGPD Art. 13, 14.
- 

#### **PRIV-237 – Auditoría de Cumplimiento de la Política de Conservación de Datos**

- **Descripción:**
    - Se debe auditar periódicamente el cumplimiento de la política de conservación de datos para asegurar que se aplican correctamente los plazos de retención y eliminación.
  - **Criterios de Aceptación:**
    - Realización de auditorías al menos **una vez al año** sobre la aplicación de la política de conservación.
    - Identificación y corrección de posibles incumplimientos en la eliminación de datos.
    - Documentación de los hallazgos de la auditoría y las acciones correctivas aplicadas.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Gobernanza.
  - **Fuente:** RGPD Art. 5.
- 

#### **PRIV-238 – Definición de un Procedimiento de Supresión Segura de Datos Personales**

- **Descripción:**

Según el **Artículo 5.1.e del RGPD**, los datos personales deben eliminarse cuando ya no sean necesarios para los fines del tratamiento.

  - Se debe establecer un **procedimiento formal y documentado** que especifique cómo se eliminarán los datos de manera segura.
- **Criterios de Aceptación:**
  - Creación de un **protocolo interno de supresión segura** de datos personales.
  - Identificación de **responsables del proceso de eliminación** dentro de la organización.

- Aseguramiento de que la supresión cumple con los requisitos de **ISO 27001 y ENS**.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 5.1.e; ISO 27001; ENS.
- 

#### **PRIV-239 – Aplicación de Métodos de Eliminación Irreversible de Datos**

- **Descripción:**
    - Se deben implementar técnicas de **supresión definitiva** de datos personales para garantizar que no puedan ser recuperados.
  - **Criterios de Aceptación:**
    - Uso de **borrado criptográfico (crypto-shredding)** para la eliminación segura de datos en sistemas digitales.
    - Aplicación de **sobrescritura múltiple de datos (DoD 5220.22-M, NIST 800-88)** en almacenamiento magnético y SSD.
    - Verificación de la efectividad de los métodos de eliminación aplicados.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-240 – Eliminación Segura de Datos en Dispositivos Físicos**

- **Descripción:**
  - Los dispositivos físicos que contienen datos personales deben ser destruidos o limpiados de forma segura antes de su reutilización o eliminación.
- **Criterios de Aceptación:**
  - Aplicación de **desmagnetización (degaussing)** en discos duros HDD.
  - Trituración de dispositivos físicos que contengan datos sensibles.
  - Registro y trazabilidad de la destrucción de dispositivos en inventarios de TI.
- **Prioridad:** Alta.
- **Categoría:** Seguridad de la Información.

- **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-241 – Automatización del Proceso de Eliminación de Datos en Sistemas**

- **Descripción:**
    - Se deben automatizar procesos de eliminación de datos para minimizar errores humanos y garantizar el cumplimiento de los plazos de retención.
  - **Criterios de Aceptación:**
    - Implementación de **reglas de eliminación automática** según la Política de Conservación de Datos.
    - Verificación de que los sistemas aplican borrado seguro conforme a estándares internacionales.
    - Auditoría de los logs de eliminación para validar la efectividad del proceso.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-242 – Registro de Supresión de Datos y Trazabilidad de Eliminaciones**

- **Descripción:**
    - Se debe mantener un **registro de supresión de datos** donde se documente la eliminación de datos personales con detalles sobre el método utilizado y la fecha de eliminación.
  - **Criterios de Aceptación:**
    - Implementación de un **sistema de trazabilidad de eliminaciones**.
    - Registro de **responsables, método de supresión y datos eliminados**.
    - Protección del registro contra accesos no autorizados o modificaciones.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** RGPD Art. 5.1.e; ISO 27001; ENS.
- 

#### **PRIV-243 – Auditoría del Proceso de Eliminación de Datos**

- **Descripción:**

- Se deben realizar auditorías periódicas para verificar que la eliminación de datos personales cumple con la normativa y las políticas internas.
  - **Criterios de Aceptación:**
    - Realización de **auditorías anuales** del proceso de supresión segura.
    - Identificación de mejoras en los métodos de eliminación de datos.
    - Documentación y aplicación de medidas correctivas en caso de incumplimientos.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Seguridad.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-244 – Eliminación de Copias de Seguridad con Datos Personales**

- **Descripción:**
    - Las copias de seguridad deben eliminarse conforme a la política de conservación de datos y con métodos seguros para evitar su recuperación.
  - **Criterios de Aceptación:**
    - Aplicación de **cifrado en copias de seguridad** para facilitar su eliminación segura.
    - Borrado de copias de seguridad tras la finalización del periodo de retención.
    - Registro de la eliminación de copias en el sistema de trazabilidad.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-245 – Destrucción Física de Documentación en Papel**

- **Descripción:**
  - Los documentos físicos que contengan datos personales deben ser destruidos de manera segura para evitar accesos no autorizados.
- **Criterios de Aceptación:**
  - Uso de **tritadoras de nivel P-4 o superior** para documentos con información sensible.

- Contratación de empresas certificadas para la destrucción segura de documentos.
    - Registro de la eliminación de documentos en un **sistema de trazabilidad**.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-246 – Capacitación del Personal en Supresión Segura de Datos**

- **Descripción:**
    - Se debe formar al personal en los procedimientos de supresión segura de datos para evitar errores o incumplimientos normativos.
  - **Criterios de Aceptación:**
    - Inclusión de módulos sobre eliminación segura en el **plan de formación de protección de datos**.
    - Pruebas de conocimiento sobre técnicas de supresión de datos en formaciones periódicas.
    - Supervisión del cumplimiento de los procedimientos por parte del DPO.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** RGPD Art. 5.1.e; ISO 27001.
- 

#### **PRIV-247 – Inclusión de los Procedimientos de Supresión en la Política de Seguridad**

- **Descripción:**
  - La organización debe integrar los procedimientos de eliminación segura dentro de su **Política de Seguridad de la Información**.
- **Criterios de Aceptación:**
  - Documentación de las técnicas de eliminación en la **Política de Seguridad**.
  - Definición de roles y responsabilidades en la gestión de eliminación de datos.
  - Revisión periódica de la política para adaptarla a cambios normativos o tecnológicos.

- **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-248 – Implementación de un Procedimiento de Bloqueo de Datos**

- **Descripción:**

Según el **Artículo 32 de la LOPDGDD**, cuando se solicite la supresión de datos, pero exista una **obligación legal o un procedimiento administrativo o judicial en curso**, los datos deben ser bloqueados en lugar de eliminados.

    - El bloqueo impide su tratamiento salvo para su conservación y acceso por autoridades competentes.
  - **Criterios de Aceptación:**
    - Creación de un **procedimiento formal de bloqueo de datos**.
    - Garantía de que los datos bloqueados no son accesibles ni reutilizables para otros fines.
    - Definición de **responsables del proceso de bloqueo** dentro de la organización.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información y Gobernanza.
  - **Fuente:** LOPDGDD Art. 32.
- 

#### **PRIV-249 – Identificación de Datos Sujetos a Bloqueo**

- **Descripción:**
  - Se debe identificar qué datos deben ser bloqueados cuando un interesado solicita la supresión y se determine que hay una causa legal que obliga a su retención temporal.
- **Criterios de Aceptación:**
  - Determinación de **criterios claros para identificar datos bloqueables**.
  - Aplicación del bloqueo solo a los **datos estrictamente necesarios** para la finalidad legal.
  - Registro de los datos bloqueados en un **sistema de trazabilidad**.
- **Prioridad:** Alta.
- **Categoría:** Gobernanza y Seguridad.



- **Fuente:** LOPDGDD Art. 32.
- 

#### **PRIV-250 – Restricción de Acceso y Tratamiento de Datos Bloqueados**

- **Descripción:**
    - Los datos bloqueados solo deben ser accesibles por autoridades competentes o en caso de reclamaciones, garantizando que no sean utilizados para otros fines.
  - **Criterios de Aceptación:**
    - Configuración de **controles de acceso restringidos** a los datos bloqueados.
    - Implementación de medidas técnicas para evitar su procesamiento activo.
    - Auditoría del acceso a los datos bloqueados para verificar su correcto uso.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** LOPDGDD Art. 32.
- 

#### **PRIV-251 – Definición del Plazo de Bloqueo y Eliminación Final**

- **Descripción:**
    - Una vez finalizado el motivo legal que justifica el bloqueo, los datos deben ser eliminados de forma segura y definitiva.
  - **Criterios de Aceptación:**
    - Definición de un **plazo máximo de bloqueo** en función de la normativa aplicable.
    - Implementación de un mecanismo de **eliminación segura** tras el plazo de bloqueo.
    - Registro de la fecha de eliminación y validación del proceso.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información y Gobernanza.
  - **Fuente:** LOPDGDD Art. 32.
- 

#### **PRIV-252 – Registro y Trazabilidad de Datos Bloqueados**

- **Descripción:**

- Se debe mantener un **registro centralizado** de todos los datos bloqueados, con información sobre su motivo, plazo y responsables del bloqueo.
  - **Criterios de Aceptación:**
    - Implementación de un **sistema de registro de bloqueos de datos**.
    - Protección del registro contra accesos no autorizados o modificaciones.
    - Disponibilidad del registro para auditorías internas o requerimientos de la autoridad de control.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** LOPDGDD Art. 32.
- 

#### **PRIV-253 – Automatización del Bloqueo de Datos en los Sistemas de Información**

- **Descripción:**
    - Se recomienda la implementación de **mecanismos automatizados** para aplicar el bloqueo de datos en bases de datos y sistemas de gestión documental.
  - **Criterios de Aceptación:**
    - Configuración de reglas automáticas de **bloqueo en bases de datos**.
    - Verificación de que los datos bloqueados no puedan ser modificados o procesados.
    - Generación de alertas cuando se alcance el plazo de eliminación de los datos bloqueados.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** LOPDGDD Art. 32.
- 

#### **PRIV-254 – Auditoría del Cumplimiento del Bloqueo de Datos**

- **Descripción:**
  - Se deben realizar auditorías periódicas para garantizar que el procedimiento de bloqueo se está aplicando correctamente y que no hay datos bloqueados siendo procesados indebidamente.
- **Criterios de Aceptación:**

- Realización de **auditorías anuales** sobre los procedimientos de bloqueo.
  - Verificación del cumplimiento de los plazos de retención y eliminación final.
  - Implementación de medidas correctivas ante incumplimientos detectados.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Seguridad.
  - **Fuente:** LOPDGDD Art. 32.
- 

#### **PRIV-255 – Capacitación del Personal en el Procedimiento de Bloqueo de Datos**

- **Descripción:**
    - Los empleados deben recibir formación sobre la aplicación del **bloqueo de datos personales** y la gestión de reclamaciones.
  - **Criterios de Aceptación:**
    - Inclusión de módulos sobre **bloqueo de datos y reclamaciones** en la formación interna.
    - Evaluación del conocimiento del personal sobre cuándo y cómo aplicar el bloqueo.
    - Supervisión del cumplimiento de los procedimientos por parte del DPO.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** LOPDGDD Art. 32.
- 

#### **PRIV-256 – Inclusión del Procedimiento de Bloqueo en la Política de Protección de Datos**

- **Descripción:**
  - Se debe integrar el procedimiento de bloqueo dentro de la **Política de Protección de Datos** de la organización para garantizar su cumplimiento y coherencia con el resto de normativas.
- **Criterios de Aceptación:**
  - Documentación del procedimiento de bloqueo en la **Política de Protección de Datos**.
  - Definición de roles y responsabilidades en la gestión de datos bloqueados.

- Revisión periódica de la política para adaptarla a cambios normativos.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** LOPDGDD Art. 32.
- 

#### **PRIV-257 – Implementación de un Proceso de Identificación de Riesgos en Protección de Datos**

- **Descripción:**

Según el **Artículo 35 del RGPD**, se deben identificar y evaluar los **riesgos potenciales** que puedan afectar la seguridad y privacidad de los datos personales.

    - Se debe establecer un **proceso formal** para detectar amenazas en los tratamientos de datos.
    - Los riesgos deben clasificarse según su impacto y probabilidad.
  - **Criterios de Aceptación:**
    - Definición de una **metodología estándar para la identificación de riesgos**.
    - Identificación de **riesgos técnicos, organizativos y regulatorios** en cada tratamiento.
    - Registro de los riesgos detectados en un **sistema de gestión de riesgos**.
  - **Prioridad:** Alta.
  - **Categoría:** Evaluaciones de Seguridad y Gobernanza.
  - **Fuente:** RGPD Art. 35.
- 

#### **PRIV-258 – Análisis de Categorías de Riesgo en el Tratamiento de Datos**

- **Descripción:**
  - Se deben clasificar los riesgos identificados en categorías para facilitar su evaluación y mitigación.
  - Las categorías pueden incluir:
    - **Acceso no autorizado.**
    - **Pérdida o alteración de datos.**
    - **Uso indebido o excesivo de datos personales.**

- **Transferencias ilegales de datos.**
  - **Criterios de Aceptación:**
    - Aplicación de una **clasificación estructurada de riesgos**.
    - Identificación de impactos específicos sobre los derechos y libertades de los interesados.
    - Priorización de los riesgos en función de su criticidad.
  - **Prioridad:** Alta.
  - **Categoría:** Evaluaciones de Seguridad y Gobernanza.
  - **Fuente:** RGPD Art. 35.
- 

#### **PRIV-259 – Evaluación de la Probabilidad e Impacto de los Riesgos Detectados**

- **Descripción:**
    - Cada riesgo identificado debe ser evaluado en función de su **probabilidad de ocurrencia** y su **impacto potencial** sobre la privacidad.
  - **Criterios de Aceptación:**
    - Uso de una **matriz de riesgos** que combine probabilidad e impacto.
    - Evaluación de **escenarios de ataque o vulnerabilidad** en cada tratamiento.
    - Registro de los resultados de la evaluación en un **documento de gestión de riesgos**.
  - **Prioridad:** Alta.
  - **Categoría:** Evaluaciones de Seguridad y Gobernanza.
  - **Fuente:** RGPD Art. 35.
- 

#### **PRIV-260 – Identificación de Riesgos en el Uso de Nuevas Tecnologías**

- **Descripción:**
  - Se debe evaluar el impacto de la introducción de **tecnologías innovadoras** que puedan implicar un **alto riesgo para la privacidad**.
- **Criterios de Aceptación:**
  - Evaluación de **IA, biometría, Big Data o blockchain** en los tratamientos de datos.
  - Análisis de los riesgos específicos asociados a cada tecnología.

- Implementación de salvaguardas antes de desplegar nuevas tecnologías.
  - **Prioridad:** Alta.
  - **Categoría:** Evaluaciones de Seguridad.
  - **Fuente:** RGPD Art. 35.
- 

#### **PRIV-261 – Identificación de Riesgos en el Tratamiento de Datos Sensibles**

- **Descripción:**
    - Se deben identificar **riesgos adicionales** en el tratamiento de **datos sensibles** como:
      - **Datos de salud.**
      - **Datos biométricos y genéticos.**
      - **Datos de menores.**
      - **Datos de origen étnico o religión.**
  - **Criterios de Aceptación:**
    - Identificación de tratamientos con datos sensibles y sus riesgos asociados.
    - Aplicación de medidas de seguridad reforzadas en estos tratamientos.
    - Documentación de los resultados en el **Registro de Actividades de Tratamiento (RAT)**.
  - **Prioridad:** Alta.
  - **Categoría:** Evaluaciones de Seguridad.
  - **Fuente:** RGPD Art. 9, 35.
- 

#### **PRIV-262 – Identificación de Riesgos en Transferencias Internacionales de Datos**

- **Descripción:**
  - Se deben analizar los riesgos asociados a **transferencias de datos fuera del Espacio Económico Europeo (EEE)** y aplicar medidas de mitigación adecuadas.
- **Criterios de Aceptación:**
  - Verificación de la existencia de una **base legal válida** para la transferencia.
  - Evaluación del nivel de protección del país de destino.

- Implementación de medidas de seguridad adicionales en caso de riesgo elevado.
  - **Prioridad:** Alta.
  - **Categoría:** Evaluaciones de Seguridad y Gobernanza.
  - **Fuente:** RGPD Art. 44-49.
- 

#### **PRIV-263 – Implementación de un Registro de Riesgos Detectados**

- **Descripción:**
    - Se debe mantener un **registro actualizado de riesgos** que contenga detalles sobre los riesgos identificados, su evaluación y las medidas de mitigación aplicadas.
  - **Criterios de Aceptación:**
    - Creación de un **documento centralizado de riesgos en protección de datos**.
    - Revisión periódica y actualización del registro según cambios en los tratamientos.
    - Accesibilidad del registro para auditorías internas y externas.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 35.
- 

#### **PRIV-264 – Auditoría del Proceso de Identificación de Riesgos**

- **Descripción:**
  - Se deben realizar auditorías periódicas para evaluar la eficacia del proceso de identificación de riesgos y la aplicación de medidas de mitigación.
- **Criterios de Aceptación:**
  - Realización de auditorías internas sobre la **identificación y gestión de riesgos** al menos una vez al año.
  - Implementación de mejoras en la metodología de identificación de riesgos.
  - Documentación y seguimiento de las acciones correctivas derivadas de la auditoría.
- **Prioridad:** Media.

- **Categoría:** Auditoría y Seguridad.
  - **Fuente:** RGPD Art. 35.
- 

#### **PRIV-265 – Capacitación del Personal en Identificación de Riesgos**

- **Descripción:**
    - Se debe capacitar al personal en la **identificación de riesgos** en los tratamientos de datos personales, especialmente a aquellos que gestionan información sensible.
  - **Criterios de Aceptación:**
    - Inclusión de módulos de identificación de riesgos en los programas de formación.
    - Evaluación del conocimiento del personal sobre la gestión de riesgos.
    - Supervisión del cumplimiento de las buenas prácticas en la identificación de riesgos.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** RGPD Art. 35.
- 

#### **PRIV-266 – Integración de la Gestión de Riesgos en la Estrategia de Seguridad de la Organización**

- **Descripción:**
  - La identificación de riesgos debe estar alineada con la estrategia general de **seguridad de la información y cumplimiento normativo** de la organización.
- **Criterios de Aceptación:**
  - Incorporación del proceso de identificación de riesgos en la **Política de Seguridad de la Información**.
  - Definición de roles y responsabilidades en la gestión de riesgos de protección de datos.
  - Revisión periódica de la alineación con normativas y estándares como **ISO 27001 y ENS**.
- **Prioridad:** Media.
- **Categoría:** Gobernanza y Seguridad.



- **Fuente:** RGPD Art. 35; ISO 27001; ENS.
- 

#### **PRIV-267 – Implementación de un Plan de Mitigación de Riesgos en Protección de Datos**

- **Descripción:**

Según el **Artículo 32 del RGPD** y los estándares de **ISO 27001 y ENS**, se deben implementar **medidas técnicas y organizativas** para reducir los riesgos identificados en el tratamiento de datos personales.

- Se debe documentar un **plan de mitigación** que establezca controles específicos según el nivel de riesgo detectado.

- **Criterios de Aceptación:**

- Definición de un **plan de mitigación estructurado** basado en el análisis de riesgos.
- Implementación de controles de seguridad según la criticidad del riesgo.
- Seguimiento y auditoría periódica de las medidas de mitigación aplicadas.

- **Prioridad:** Alta.

- **Categoría:** Seguridad de la Información y Gobernanza.

- **Fuente:** RGPD Art. 32; ISO 27001; ENS.

---

#### **PRIV-268 – Aplicación de Controles de Acceso Basados en Roles (RBAC) y Mínimos Privilegios**

- **Descripción:**

- Se deben implementar **controles de acceso** para restringir el tratamiento de datos personales solo a usuarios autorizados.
- Se debe aplicar el principio de **mínimos privilegios y necesidad de conocer**.

- **Criterios de Aceptación:**

- Implementación de **autenticación multifactor (MFA)** en accesos críticos.
- Aplicación de **controles de acceso basados en roles (RBAC)** en todos los sistemas de datos personales.
- Revisión periódica de los accesos y eliminación de permisos innecesarios.

- **Prioridad:** Alta.

- **Categoría:** Seguridad de la Información.

- **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-269 – Cifrado de Datos en Reposo y en Tránsito**

- **Descripción:**
    - Se deben implementar mecanismos de **cifrado fuerte** para garantizar la confidencialidad de los datos personales almacenados y transmitidos.
  - **Criterios de Aceptación:**
    - Uso de **cifrado AES-256** para datos en reposo.
    - Implementación de **TLS 1.2 o superior** para datos en tránsito.
    - Revisión y auditoría de los controles de cifrado de forma periódica.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS; RGPD Art. 32.
- 

#### **PRIV-270 – Implementación de Técnicas de Seudonimización y Anonimización**

- **Descripción:**
    - Cuando sea posible, se deben aplicar técnicas de **seudonimización** o **anonimización** para reducir los riesgos en caso de acceso no autorizado a los datos personales.
  - **Criterios de Aceptación:**
    - Uso de técnicas de **hashing, enmascaramiento y tokenización** en bases de datos.
    - Evaluación de la irreversibilidad de los procesos de anonimización.
    - Documentación de las técnicas aplicadas en el plan de mitigación de riesgos.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001; ENS.
- 

#### **PRIV-271 – Implementación de Auditoría y Monitorización de Seguridad (SIEM)**

- **Descripción:**

- Se deben establecer sistemas de **monitorización continua y detección de incidentes** para identificar amenazas en tiempo real.
  - **Criterios de Aceptación:**
    - Implementación de **Sistemas de Gestión de Eventos e Información de Seguridad (SIEM)**.
    - Configuración de **alertas automáticas ante eventos sospechosos**.
    - Revisión periódica de logs de acceso y eventos de seguridad.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-272 – Implementación de un Plan de Respuesta a Incidentes y Brechas de Seguridad**

- **Descripción:**
    - Se debe definir un **protocolo de respuesta** ante incidentes de seguridad que puedan afectar la confidencialidad, integridad o disponibilidad de los datos personales.
  - **Criterios de Aceptación:**
    - Creación de un **Plan de Respuesta a Incidentes** basado en ISO 27035.
    - Establecimiento de plazos y responsables para la gestión de incidentes.
    - Registro y documentación de todas las brechas de seguridad detectadas.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001; ENS.
- 

#### **PRIV-273 – Implementación de un Plan de Continuidad del Negocio y Recuperación ante Desastres (BCP/DRP)**

- **Descripción:**
  - Se debe garantizar la continuidad operativa y recuperación de datos en caso de incidentes graves mediante un **Plan de Continuidad del Negocio (BCP)** y un **Plan de Recuperación ante Desastres (DRP)**.
- **Criterios de Aceptación:**

- Definición de un **BCP y DRP alineado con ISO 27001 y ENS**.
  - Realización de **pruebas periódicas de recuperación** de datos y sistemas.
  - Documentación de procedimientos y tiempos de recuperación (RTO/RPO).
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-274 – Auditoría del Cumplimiento de las Medidas de Mitigación**

- **Descripción:**
    - Se deben realizar auditorías periódicas para evaluar la eficacia de las medidas de mitigación aplicadas y su adecuación a los riesgos identificados.
  - **Criterios de Aceptación:**
    - Realización de auditorías de seguridad al menos **una vez al año**.
    - Evaluación del cumplimiento de las medidas establecidas en el plan de mitigación.
    - Documentación de las auditorías y aplicación de acciones correctivas.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Seguridad.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-275 – Capacitación del Personal en Medidas de Mitigación de Riesgos**

- **Descripción:**
  - Se debe capacitar al personal en la **aplicación de medidas de mitigación de riesgos** para garantizar su correcta implementación.
- **Criterios de Aceptación:**
  - Inclusión de módulos sobre **medidas de mitigación de riesgos** en la formación del personal.
  - Evaluación del conocimiento del personal sobre la aplicación de controles de seguridad.
  - Supervisión del cumplimiento de buenas prácticas en mitigación de riesgos.

- **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-276 – Implementación de un Proceso de Revisión Periódica de Seguridad**

- **Descripción:**

Según el **Esquema Nacional de Seguridad (ENS)**, se deben realizar revisiones periódicas para evaluar la efectividad de las **medidas de seguridad y mitigación de riesgos** en el tratamiento de datos personales.

    - Se debe definir un proceso de revisión que incluya **frecuencia, responsables y criterios de evaluación**.
  - **Criterios de Aceptación:**
    - Creación de un **procedimiento formal de revisión de seguridad**.
    - Realización de revisiones periódicas conforme a los criterios establecidos en el ENS.
    - Registro de hallazgos y aplicación de mejoras en base a las revisiones realizadas.
  - **Prioridad:** Alta.
  - **Categoría:** Auditoría y Seguridad.
  - **Fuente:** ENS.
- 

#### **PRIV-277 – Evaluación de Cumplimiento con el ENS y Normativas de Seguridad**

- **Descripción:**
  - Se debe verificar periódicamente que las **medidas de seguridad implementadas** cumplen con los requisitos del ENS y otras normativas aplicables como **ISO 27001 y RGPD**.
- **Criterios de Aceptación:**
  - Revisión de la **adecuación de las medidas de seguridad** a los requisitos del ENS.
  - Evaluación del cumplimiento con principios de **integridad, confidencialidad y disponibilidad**.
  - Implementación de acciones correctivas en caso de no conformidades detectadas.

- **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información y Gobernanza.
  - **Fuente:** ENS; ISO 27001.
- 

#### **PRIV-278 – Auditorías de Seguridad de la Información Basadas en el ENS**

- **Descripción:**
    - Se deben realizar **auditorías periódicas** para evaluar la efectividad de las medidas de seguridad y detectar vulnerabilidades en los sistemas de información.
  - **Criterios de Aceptación:**
    - Realización de auditorías de seguridad al menos **una vez al año**.
    - Identificación y corrección de vulnerabilidades detectadas en auditorías.
    - Registro de las auditorías y seguimiento de medidas correctivas aplicadas.
  - **Prioridad:** Alta.
  - **Categoría:** Auditoría y Seguridad.
  - **Fuente:** ENS.
- 

#### **PRIV-279 – Pruebas de Estrés y Evaluaciones de Resiliencia de Seguridad**

- **Descripción:**
    - Se deben realizar **pruebas de estrés y simulaciones** para evaluar la resiliencia de los sistemas de información ante ciberataques o fallos críticos.
  - **Criterios de Aceptación:**
    - Ejecución de **pruebas de penetración (pentesting)** periódicas.
    - Simulación de escenarios de **incidentes de seguridad y recuperación de datos**.
    - Documentación de resultados y aplicación de mejoras en seguridad.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ENS; ISO 27001.
-

## **PRIV-280 – Supervisión de Incidentes de Seguridad y Evaluación de Respuesta**

- **Descripción:**
    - Se debe supervisar continuamente los **incidentes de seguridad** registrados y evaluar la **efectividad de la respuesta** aplicada en cada caso.
  - **Criterios de Aceptación:**
    - Revisión de **registros de incidentes** y medidas de mitigación adoptadas.
    - Evaluación de la eficacia del **Plan de Respuesta a Incidentes** basado en ISO 27035.
    - Implementación de mejoras en protocolos de respuesta y detección de amenazas.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ENS; ISO 27001.
- 

## **PRIV-281 – Evaluación de Controles de Acceso y Gestión de Identidades**

- **Descripción:**
    - Se debe revisar periódicamente la **gestión de accesos y privilegios** en los sistemas de información, garantizando la aplicación del principio de mínimos privilegios.
  - **Criterios de Aceptación:**
    - Auditoría de permisos y accesos al menos **una vez al año**.
    - Identificación y revocación de accesos innecesarios o no autorizados.
    - Validación de la efectividad de los controles de acceso implementados.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ENS; ISO 27001.
- 

## **PRIV-282 – Análisis y Validación de Medidas de Protección de Datos en la Nube**

- **Descripción:**

- Se debe evaluar la seguridad y cumplimiento normativo de los servicios de almacenamiento y procesamiento en la nube, asegurando que cumplen con los estándares del ENS.
  - **Criterios de Aceptación:**
    - Revisión de **medidas de seguridad en entornos cloud** como cifrado, controles de acceso y auditoría de actividad.
    - Validación del **cumplimiento del proveedor cloud con ENS, ISO 27017 y RGPD**.
    - Evaluación de mecanismos de **resiliencia y recuperación ante fallos** en la nube.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información y Gobernanza.
  - **Fuente:** ENS; ISO 27017; RGPD.
- 

#### **PRIV-283 – Actualización y Mejora Continua del ENS en la Organización**

- **Descripción:**
    - La organización debe actualizar periódicamente sus políticas y procedimientos de seguridad para garantizar la **mejora continua** en el cumplimiento del ENS.
  - **Criterios de Aceptación:**
    - Revisión de la **Política de Seguridad** al menos una vez al año.
    - Implementación de mejoras derivadas de auditorías y cambios regulatorios.
    - Formación continua del personal en nuevas amenazas y mejores prácticas de seguridad.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** ENS; ISO 27001.
-



#### **PRIV-284 – Capacitación del Personal en Evaluación y Validación de Seguridad ENS**

- **Descripción:**
    - Se debe formar al personal encargado de la seguridad en los criterios de evaluación, validación y cumplimiento del ENS.
  - **Criterios de Aceptación:**
    - Inclusión de módulos sobre **revisión de seguridad y ENS** en el plan de formación.
    - Evaluación periódica del conocimiento del personal en seguridad ENS.
    - Implementación de ejercicios prácticos y simulaciones en la formación.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** ENS.
- 

#### **PRIV-285 – Implementación de un Sistema de Monitoreo de Actividades de Tratamiento**

- **Descripción:**

Según el **Artículo 87 de la LOPDGDD**, se deben establecer mecanismos para supervisar y controlar el **uso de los datos personales**, garantizando la detección de accesos indebidos o usos no autorizados.

    - Se debe contar con un **sistema de monitoreo** que permita registrar y auditar el acceso y tratamiento de los datos personales.
  - **Criterios de Aceptación:**
    - Implementación de un **sistema de registro de eventos y accesos** en los tratamientos de datos.
    - Supervisión periódica de los registros generados para detectar anomalías.
    - Aplicación de medidas correctivas ante detección de actividades sospechosas.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información y Gobernanza.
  - **Fuente:** LOPDGDD Art. 87.
- 

#### **PRIV-286 – Registro de Actividades Críticas sobre Datos Personales**

- **Descripción:**
    - Se deben identificar y registrar las **actividades críticas** relacionadas con el tratamiento de datos personales, tales como:
      - Accesos y modificaciones a bases de datos.
      - Extracción o copia de información sensible.
      - Transferencias de datos fuera de la organización.
  - **Criterios de Aceptación:**
    - Implementación de registros de auditoría para actividades sensibles.
    - Configuración de alertas automáticas ante operaciones sospechosas.
    - Evaluación periódica de los registros para garantizar la integridad de los datos.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información y Gobernanza.
  - **Fuente:** LOPDGDD Art. 87; ISO 27001.
- 

#### **PRIV-287 – Supervisión de Accesos a Datos Sensibles**

- **Descripción:**
    - Se deben establecer controles para monitorear el acceso a **datos sensibles**, garantizando que solo personal autorizado pueda interactuar con la información.
  - **Criterios de Aceptación:**
    - Aplicación de **autenticación multifactor (MFA)** en accesos a datos críticos.
    - Revisión periódica de los permisos asignados a usuarios con acceso privilegiado.
    - Registro de accesos e intentos fallidos a bases de datos sensibles.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** LOPDGDD Art. 87; ISO 27001.
- 

#### **PRIV-288 – Implementación de Políticas de Control de Actividades en Entornos de Trabajo**

- **Descripción:**
    - Se deben definir **políticas y procedimientos** que regulen el uso de los datos personales en los entornos de trabajo, evitando el acceso o uso indebido de información.
  - **Criterios de Aceptación:**
    - Redacción de una **Política de Uso de Datos en el Entorno Laboral**.
    - Implementación de restricciones de acceso a datos según la función del usuario.
    - Comunicación de las políticas a los empleados y responsables de tratamiento.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** LOPDGDD Art. 87.
- 

#### **PRIV-289 – Configuración de Alertas y Detección de Comportamientos Anómalos**

- **Descripción:**
    - Se deben implementar herramientas de **detección de amenazas internas**, que permitan identificar usos indebidos de los datos personales.
  - **Criterios de Aceptación:**
    - Configuración de alertas en **sistemas de monitorización (SIEM)** para detectar anomalías.
    - Análisis de patrones de comportamiento de usuarios con acceso a datos sensibles.
    - Aplicación de medidas preventivas en caso de detección de actividades sospechosas.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** LOPDGDD Art. 87; ISO 27001.
- 

#### **PRIV-290 – Control de Dispositivos y Canales de Comunicación**

- **Descripción:**

- Se debe establecer un control sobre **dispositivos y medios de comunicación** utilizados para el acceso y tratamiento de datos personales.
  - **Criterios de Aceptación:**
    - Restricción del uso de dispositivos externos (USB, discos duros, almacenamiento en la nube).
    - Control de la transferencia de datos a través de correos electrónicos o sistemas de mensajería.
    - Configuración de cifrado obligatorio en dispositivos que almacenen datos personales.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** LOPDGDD Art. 87; ENS.
- 

#### **PRIV-291 – Auditoría del Monitoreo y Control de Actividades**

- **Descripción:**
    - Se deben realizar auditorías periódicas para verificar la efectividad del **monitoreo y control de actividades**, asegurando que los mecanismos de supervisión son efectivos.
  - **Criterios de Aceptación:**
    - Realización de auditorías anuales sobre **sistemas de monitoreo y control de accesos**.
    - Identificación y corrección de fallos en los mecanismos de supervisión.
    - Aplicación de medidas correctivas derivadas de las auditorías realizadas.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Seguridad.
  - **Fuente:** LOPDGDD Art. 87; ISO 27001; ENS.
- 

#### **PRIV-292 – Mantenimiento de un Registro de Monitoreo y Control de Actividades**

- **Descripción:**
  - Se debe mantener un **registro actualizado de todas las actividades de supervisión y control**, con información sobre accesos, modificaciones y alertas generadas.

- **Criterios de Aceptación:**
    - Creación de un **sistema de registro de eventos** en bases de datos y sistemas de información.
    - Protección del registro contra modificaciones no autorizadas.
    - Disponibilidad del registro para auditorías y revisiones internas.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** LOPDGDD Art. 87; ISO 27001.
- 

#### **PRIV-293 – Capacitación del Personal en Políticas de Control y Supervisión**

- **Descripción:**
    - Se debe formar al personal en **prácticas de control de acceso, supervisión y monitoreo**, asegurando el cumplimiento de las normas de seguridad.
  - **Criterios de Aceptación:**
    - Inclusión de módulos sobre **control y supervisión de actividades** en la formación interna.
    - Evaluación del conocimiento del personal en gestión de accesos y uso adecuado de los datos personales.
    - Implementación de ejercicios prácticos y simulaciones en la formación.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** LOPDGDD Art. 87.
- 

#### **PRIV-294 – Implementación de un Procedimiento para el Uso de Videovigilancia**

- **Descripción:**

Según el **Artículo 22 de la LOPDGDD**, el uso de sistemas de videovigilancia debe cumplir con el principio de **proporcionalidad**, limitándose a la finalidad de **seguridad y prevención de delitos**.

  - Se debe definir un procedimiento formal para la gestión de imágenes captadas por cámaras de seguridad.
- **Criterios de Aceptación:**

- Creación de un **procedimiento interno para la gestión de videovigilancia**.
  - Uso de cámaras solo en **zonas necesarias** sin afectar la intimidad de las personas.
  - Implementación de **carteles informativos** sobre la existencia del sistema de videovigilancia.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad y Cumplimiento Normativo.
  - **Fuente:** LOPDGDD Art. 22.
- 

#### **PRIV-295 – Identificación de la Finalidad de la Videovigilancia**

- **Descripción:**
    - Se debe justificar el uso de sistemas de videovigilancia y documentar su finalidad para evitar un tratamiento excesivo de imágenes.
  - **Criterios de Aceptación:**
    - Definición clara de la finalidad del tratamiento (seguridad, protección de bienes, control de accesos).
    - Garantía de que las cámaras no graban zonas privadas o espacios donde se vulnere la intimidad.
    - Documentación de la justificación legal del uso de videovigilancia.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad y Cumplimiento Normativo.
  - **Fuente:** LOPDGDD Art. 22; RGPD Art. 5.
- 

#### **PRIV-296 – Señalización Obligatoria del Uso de Cámaras de Videovigilancia**

- **Descripción:**
  - Se deben colocar **carteles informativos visibles** en los lugares donde se encuentren instaladas cámaras de videovigilancia, informando a las personas sobre la grabación de imágenes.
- **Criterios de Aceptación:**
  - Instalación de **señalización clara y visible** con información sobre la videovigilancia.
  - Inclusión en los carteles de los **datos del responsable del tratamiento**.

- Disponibilidad de información adicional sobre el uso de las imágenes a solicitud de los interesados.
  - **Prioridad:** Alta.
  - **Categoría:** Transparencia y Cumplimiento.
  - **Fuente:** LOPDGDD Art. 22; RGPD Art. 13.
- 

#### **PRIV-297 – Limitación del Acceso a las Imágenes Captadas por Videovigilancia**

- **Descripción:**
    - Solo personas autorizadas deben poder acceder a las imágenes grabadas, asegurando que no se usen para fines distintos a la seguridad.
  - **Criterios de Aceptación:**
    - Aplicación de **controles de acceso restringidos** a las grabaciones.
    - Registro de accesos a las imágenes con fecha, hora y motivo.
    - Prohibición del uso de cámaras para fines distintos a los autorizados (ej. supervisión laboral no justificada).
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad y Gobernanza.
  - **Fuente:** LOPDGDD Art. 22; RGPD Art. 32.
- 

#### **PRIV-298 – Periodo de Conservación y Eliminación de Imágenes de Videovigilancia**

- **Descripción:**
  - Las imágenes captadas por videovigilancia deben conservarse por un periodo máximo de **30 días**, salvo que sean necesarias para una investigación legal.
- **Criterios de Aceptación:**
  - Eliminación automática de imágenes transcurridos **30 días** salvo excepciones justificadas.
  - Implementación de **sistemas automatizados de borrado seguro** de imágenes.
  - Registro de casos en los que se conserven imágenes más allá del periodo estándar.
- **Prioridad:** Alta.

- **Categoría:** Seguridad y Cumplimiento.
  - **Fuente:** LOPDGDD Art. 22.
- 

#### **PRIV-299 – Gestión de Solicitudes de Acceso a Imágenes por Parte de Interesados**

- **Descripción:**
    - Los interesados pueden solicitar el acceso a sus imágenes siempre que no afecte a derechos de terceros o a una investigación en curso.
  - **Criterios de Aceptación:**
    - Definición de un **procedimiento para gestionar solicitudes de acceso** a imágenes.
    - Respuesta a las solicitudes dentro del **plazo máximo de un mes**.
    - Garantía de que la entrega de imágenes no compromete la privacidad de otras personas.
  - **Prioridad:** Media.
  - **Categoría:** Derechos del Usuario y Cumplimiento.
  - **Fuente:** RGPD Art. 15; LOPDGDD Art. 22.
- 

#### **PRIV-300 – Evaluación de Impacto en Protección de Datos (EIPD) para Videovigilancia**

- **Descripción:**
  - Si el uso de videovigilancia puede generar un **riesgo elevado** para los derechos de las personas, se debe realizar una **Evaluación de Impacto en Protección de Datos (EIPD)**.
- **Criterios de Aceptación:**
  - Identificación de si la videovigilancia puede afectar derechos fundamentales.
  - Documentación de los riesgos asociados y medidas de mitigación.
  - Aprobación de la evaluación por parte del **Delegado de Protección de Datos (DPO)**.
- **Prioridad:** Media.
- **Categoría:** Evaluaciones de Seguridad.
- **Fuente:** RGPD Art. 35.



---

### **PRIV-301 – Supervisión y Auditoría del Uso de Videovigilancia**

- **Descripción:**
    - Se deben realizar auditorías periódicas para evaluar el cumplimiento normativo en el uso de sistemas de videovigilancia.
  - **Criterios de Aceptación:**
    - Realización de **auditorías anuales sobre videovigilancia**.
    - Identificación y corrección de deficiencias en el uso de las cámaras.
    - Registro de las auditorías y aplicación de mejoras en el procedimiento.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Seguridad.
  - **Fuente:** LOPDGDD Art. 22; ENS.
- 

### **PRIV-302 – Capacitación del Personal en el Uso de Sistemas de Videovigilancia**

- **Descripción:**
    - Se debe formar al personal que gestiona sistemas de videovigilancia en los aspectos legales y técnicos relacionados con la protección de datos.
  - **Criterios de Aceptación:**
    - Inclusión de módulos sobre **uso adecuado de videovigilancia y privacidad** en las formaciones internas.
    - Evaluación del conocimiento del personal sobre el tratamiento de imágenes.
    - Implementación de medidas disciplinarias en caso de incumplimiento de las normativas.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** LOPDGDD Art. 22.
- 

### **PRIV-303 – Implementación de una Política de Uso de Dispositivos Digitales**

- **Descripción:**

Según el **Artículo 87 de la LOPDGDD**, las organizaciones pueden establecer

normas para el uso de **dispositivos digitales corporativos** con fines profesionales, garantizando la seguridad y privacidad de los datos personales.

- Se debe definir una **Política de Uso de Dispositivos** que contemple el acceso, almacenamiento y uso de información en ordenadores, móviles y otros equipos.
  - **Criterios de Aceptación:**
    - Redacción y comunicación de la **Política de Uso de Dispositivos Digitales**.
    - Aplicación de controles de acceso y medidas de seguridad en dispositivos corporativos.
    - Supervisión del cumplimiento de la política mediante auditorías y revisiones periódicas.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** LOPDGDD Art. 87; ISO 27001.
- 

#### **PRIV-304 – Separación de Uso Profesional y Personal en Dispositivos Corporativos**

- **Descripción:**
    - Se debe garantizar que los **dispositivos corporativos sean utilizados exclusivamente para fines laborales**, evitando el almacenamiento o acceso a información personal.
  - **Criterios de Aceptación:**
    - Configuración de **perfiles separados (sandboxing)** para uso personal y profesional en dispositivos.
    - Prohibición del uso de dispositivos corporativos para almacenar información privada.
    - Aplicación de software de gestión de dispositivos móviles (**MDM – Mobile Device Management**).
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** LOPDGDD Art. 87; ISO 27001.
- 

#### **PRIV-305 – Implementación de Controles de Acceso y Autenticación Segura**

- **Descripción:**
    - Se deben establecer medidas de **autenticación segura** para el acceso a dispositivos digitales que gestionen datos personales.
  - **Criterios de Aceptación:**
    - Uso obligatorio de **autenticación multifactor (MFA)** en accesos críticos.
    - Configuración de **políticas de contraseñas seguras y rotación periódica**.
    - Aplicación de **bloqueo automático de sesión tras inactividad**.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** LOPDGDD Art. 87; ISO 27001.
- 

#### **PRIV-306 – Control de Transferencias de Datos desde Dispositivos Digitales**

- **Descripción:**
    - Se debe establecer un **control de transferencia de datos personales** en dispositivos digitales para evitar fugas de información.
  - **Criterios de Aceptación:**
    - Restricción del uso de **dispositivos de almacenamiento USB no autorizados**.
    - Implementación de **controles en transferencias de archivos por correo o nube**.
    - Monitorización del tráfico de datos para detectar posibles exfiltraciones.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** LOPDGDD Art. 87; ISO 27001.
- 

#### **PRIV-307 – Protección de Datos en Dispositivos Móviles y Portátiles**

- **Descripción:**
  - Se deben aplicar medidas de **protección de datos en portátiles, móviles y tabletas** para evitar pérdidas o accesos no autorizados.
- **Criterios de Aceptación:**
  - Configuración de **cifrado de disco completo** en dispositivos móviles.

- Implementación de **herramientas de borrado remoto** en caso de pérdida o robo.
    - Aplicación de restricciones en la instalación de software no autorizado.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** LOPDGDD Art. 87; ISO 27001.
- 

#### **PRIV-308 – Monitorización del Uso de Dispositivos Digitales en la Empresa**

- **Descripción:**
    - Se debe supervisar el uso de dispositivos digitales en la empresa para detectar posibles accesos no autorizados o incumplimientos de la normativa.
  - **Criterios de Aceptación:**
    - Configuración de **sistemas de monitorización (SIEM) para registro de accesos**.
    - Implementación de alertas ante comportamientos sospechosos en dispositivos.
    - Análisis periódico de logs de actividad en equipos corporativos.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad y Gobernanza.
  - **Fuente:** LOPDGDD Art. 87; ISO 27001.
- 

#### **PRIV-309 – Gestión de Incidentes Relacionados con Dispositivos Digitales**

- **Descripción:**
  - Se debe definir un **protocolo de actuación en caso de incidentes** relacionados con el uso indebido o la pérdida de dispositivos digitales.
- **Criterios de Aceptación:**
  - Registro de incidentes relacionados con accesos no autorizados o pérdidas de dispositivos.
  - Aplicación de medidas correctivas ante vulneraciones detectadas.
  - Notificación a la autoridad de control en caso de brechas de seguridad graves.

- **Prioridad:** Media.
  - **Categoría:** Seguridad y Cumplimiento.
  - **Fuente:** LOPDGDD Art. 87; RGPD Art. 33.
- 

#### **PRIV-310 – Auditoría Periódica del Uso de Dispositivos Digitales**

- **Descripción:**
    - Se deben realizar auditorías periódicas para verificar el **cumplimiento de la normativa en el uso de dispositivos digitales** dentro de la organización.
  - **Criterios de Aceptación:**
    - Realización de **auditorías anuales** sobre el uso de dispositivos.
    - Identificación de posibles vulnerabilidades y aplicación de mejoras.
    - Registro de las auditorías y aplicación de acciones correctivas.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Seguridad.
  - **Fuente:** LOPDGDD Art. 87; ENS.
- 

#### **PRIV-311 – Capacitación del Personal en el Uso Seguro de Dispositivos Digitales**

- **Descripción:**
    - Se debe formar al personal sobre las **buenas prácticas en el uso de dispositivos digitales**, minimizando riesgos de fuga de datos o accesos no autorizados.
  - **Criterios de Aceptación:**
    - Inclusión de módulos sobre **uso seguro de dispositivos digitales** en formaciones internas.
    - Simulación de ataques de phishing y malware en entornos controlados.
    - Evaluación del conocimiento del personal en **gestión segura de dispositivos**.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** LOPDGDD Art. 87; ISO 27001.
-

---

## PRIV-312 – Justificación del Uso de Sistemas de Geolocalización en el Ámbito Laboral

- **Descripción:**

Según el **Artículo 90 de la LOPDGDD**, las empresas pueden utilizar sistemas de **geolocalización** en dispositivos de trabajo solo cuando sea **estrictamente necesario** para fines laborales y con el conocimiento del trabajador.

- Se debe justificar documentalmente la necesidad de geolocalizar a los empleados.

- **Criterios de Aceptación:**

- Definición de la **finalidad específica y proporcional** del uso de geolocalización.
- Garantía de que el sistema no recoja información personal fuera del horario laboral.
- Inclusión de la geolocalización en la **evaluación de impacto en privacidad (EIPD)** si es necesaria.

- **Prioridad:** Alta.

- **Categoría:** Gobernanza y Derechos del Usuario.

- **Fuente:** LOPDGDD Art. 90; RGPD Art. 6.

---

## PRIV-313 – Información y Transparencia sobre el Uso de Geolocalización

- **Descripción:**

- Se debe informar a los empleados **de forma clara y transparente** sobre la existencia y funcionamiento del sistema de geolocalización, así como de sus derechos al respecto.

- **Criterios de Aceptación:**

- Comunicación previa a los trabajadores sobre el uso de geolocalización.
- Inclusión en el **aviso de privacidad** de información detallada sobre el sistema.
- Explicación del mecanismo para ejercer derechos de acceso, rectificación y oposición.

- **Prioridad:** Alta.

- **Categoría:** Transparencia y Derechos del Usuario.

- **Fuente:** LOPDGDD Art. 90; RGPD Art. 13.
- 

#### **PRIV-314 – Consentimiento y Base Legal para la Geolocalización de Trabajadores**

- **Descripción:**
    - El tratamiento de datos de geolocalización debe basarse en una **base legal válida**, como el **interés legítimo** o el **cumplimiento de una obligación contractual**, sin exigir el consentimiento del trabajador.
  - **Criterios de Aceptación:**
    - Evaluación de la **base legal** más adecuada para la geolocalización.
    - Prohibición de obtener la ubicación del trabajador fuera del horario laboral sin su consentimiento.
    - Garantía de que los datos de geolocalización no se usan con fines distintos a los declarados.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Cumplimiento Normativo.
  - **Fuente:** LOPDGDD Art. 90; RGPD Art. 6.
- 

#### **PRIV-315 – Limitación del Acceso y Uso de Datos de Geolocalización**

- **Descripción:**
    - Solo el **personal autorizado** debe tener acceso a los datos de geolocalización de los trabajadores, garantizando que no se utilicen con fines ajenos a la relación laboral.
  - **Criterios de Aceptación:**
    - Implementación de **controles de acceso restringidos** a los datos de ubicación.
    - Registro y supervisión de accesos a la información de geolocalización.
    - Prohibición de uso de los datos para vigilancia no autorizada o discriminación laboral.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad y Gobernanza.
  - **Fuente:** LOPDGDD Art. 90; RGPD Art. 32.
-

#### **PRIV-316 – Definición de Períodos de Conservación y Eliminación de Datos de Ubicación**

- **Descripción:**
    - Los datos de geolocalización deben conservarse solo durante el **tiempo estrictamente necesario** y eliminarse cuando ya no sean requeridos para la finalidad declarada.
  - **Criterios de Aceptación:**
    - Definición de **plazos de retención razonables** para los datos de ubicación.
    - Implementación de **mecanismos de eliminación automática** de datos antiguos.
    - Registro de accesos y uso de los datos de geolocalización.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad y Cumplimiento Normativo.
  - **Fuente:** LOPDGDD Art. 90; RGPD Art. 5.
- 

#### **PRIV-317 – Gestión de Solicitudes de Acceso, Rectificación y Oposición a la Geolocalización**

- **Descripción:**
    - Se debe garantizar que los trabajadores puedan **ejercer sus derechos** en relación con la geolocalización, incluyendo la solicitud de acceso a sus datos o la oposición a su tratamiento en determinados casos.
  - **Criterios de Aceptación:**
    - Definición de un **procedimiento para gestionar solicitudes de derechos**.
    - Garantía de respuesta a solicitudes en un plazo máximo de **30 días**.
    - Evaluación de la viabilidad de la oposición en función de la base legal aplicada.
  - **Prioridad:** Media.
  - **Categoría:** Derechos del Usuario y Cumplimiento.
  - **Fuente:** RGPD Art. 15-21.
- 

#### **PRIV-318 – Evaluación de Impacto en Protección de Datos (EIPD) para Sistemas de Geolocalización**



- **Descripción:**
    - Si el uso de geolocalización puede implicar un **riesgo elevado para la privacidad**, se debe realizar una **Evaluación de Impacto en Protección de Datos (EIPD)** antes de su implementación.
  - **Criterios de Aceptación:**
    - Análisis del impacto de la geolocalización en la privacidad de los empleados.
    - Implementación de medidas de mitigación si se detectan riesgos.
    - Supervisión del DPO en la evaluación del sistema de geolocalización.
  - **Prioridad:** Media.
  - **Categoría:** Evaluaciones de Seguridad.
  - **Fuente:** RGPD Art. 35.
- 

#### **PRIV-319 – Auditoría y Supervisión del Uso de Sistemas de Geolocalización**

- **Descripción:**
    - Se deben realizar **auditorías periódicas** para verificar el correcto uso de los sistemas de geolocalización y el cumplimiento de la normativa.
  - **Criterios de Aceptación:**
    - Realización de auditorías internas al menos **una vez al año**.
    - Identificación de incumplimientos y aplicación de medidas correctivas.
    - Registro y documentación de las auditorías realizadas.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** LOPDGDD Art. 90.
- 

#### **PRIV-320 – Capacitación del Personal en el Uso Responsable de la Geolocalización**

- **Descripción:**
  - Se debe formar a los empleados sobre sus **derechos y obligaciones** en relación con la geolocalización en el ámbito laboral.
- **Criterios de Aceptación:**

- Inclusión de módulos sobre **geolocalización y privacidad** en las formaciones internas.
    - Evaluación del conocimiento del personal sobre el tratamiento de datos de ubicación.
    - Implementación de medidas disciplinarias en caso de uso indebido de los sistemas.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** LOPDGDD Art. 90.
- 

#### **PRIV-321 – Evaluación de Riesgos en el Tratamiento de Datos en la Nube**

- **Descripción:**

Según **ISO 27001 y ENS**, antes de utilizar servicios en la nube, se debe realizar una **evaluación de riesgos** para determinar las amenazas y vulnerabilidades asociadas al procesamiento de datos personales.
  - **Criterios de Aceptación:**
    - Análisis de los **riesgos de seguridad, acceso no autorizado y pérdida de datos**.
    - Evaluación del **cumplimiento normativo del proveedor cloud (ISO 27017, RGPD, ENS)**.
    - Definición de **medidas de mitigación** para reducir los riesgos identificados.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información y Gobernanza.
  - **Fuente:** ISO 27001; ENS; RGPD Art. 32.
- 

#### **PRIV-322 – Selección de Proveedores Cloud con Garantías de Seguridad y Cumplimiento**

- **Descripción:**
  - Se debe seleccionar proveedores de servicios en la nube que **cumplan con estándares de seguridad reconocidos** y garanticen un nivel adecuado de protección de datos personales.
- **Criterios de Aceptación:**

- Verificación de certificaciones como **ISO 27001, ISO 27017, ISO 27701, SOC 2 o ENS**.
  - Evaluación de la **ubicación de los servidores** y cumplimiento del RGPD en transferencias internacionales.
  - Inclusión de **cláusulas contractuales tipo (SCCs) o acuerdos de procesamiento de datos (DPA)** en contratos con proveedores.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información y Cumplimiento.
  - **Fuente:** ISO 27001; ENS; RGPD Art. 28.
- 

#### **PRIV-323 – Cifrado de Datos en la Nube en Reposo y en Tránsito**

- **Descripción:**
    - Se deben aplicar **mecanismos de cifrado** en los datos personales almacenados y transmitidos en la nube para prevenir accesos no autorizados.
  - **Criterios de Aceptación:**
    - Implementación de **cifrado AES-256 para datos en reposo**.
    - Uso de **protocolos seguros como TLS 1.2 o superior para datos en tránsito**.
    - Revisión periódica de las **políticas de cifrado y almacenamiento seguro**.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS; RGPD Art. 32.
- 

#### **PRIV-324 – Control de Accesos y Gestión de Identidades en Entornos Cloud**

- **Descripción:**
  - Se deben establecer **controles de acceso estrictos** para garantizar que solo personal autorizado pueda acceder a los datos en la nube.
- **Criterios de Aceptación:**
  - Implementación de **gestión de identidades y accesos (IAM)** con autenticación multifactor (MFA).
  - Configuración de permisos con el principio de **mínimos privilegios y necesidad de conocer**.

- Auditoría periódica de accesos y eliminación de cuentas inactivas o sin uso.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS; RGPD Art. 32.
- 

#### **PRIV-325 – Monitorización y Registro de Actividades en la Nube**

- **Descripción:**
    - Se deben **monitorear las actividades y accesos** a los datos en la nube para detectar anomalías y prevenir incidentes de seguridad.
  - **Criterios de Aceptación:**
    - Implementación de **sistemas de monitorización de logs (SIEM)** en los entornos cloud.
    - Configuración de **alertas en tiempo real** ante accesos sospechosos o cambios en la configuración.
    - Revisión periódica de los registros y reportes de seguridad generados.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS; RGPD Art. 32.
- 

#### **PRIV-326 – Gestión de Copias de Seguridad en Entornos Cloud**

- **Descripción:**
  - Se debe garantizar la existencia de **copias de seguridad cifradas y accesibles** para la recuperación de datos en caso de fallos o incidentes de seguridad.
- **Criterios de Aceptación:**
  - Implementación de **backups automáticos** con versiones de recuperación.
  - Almacenamiento de copias de seguridad en **ubicaciones seguras y georredundantes**.
  - Pruebas periódicas de restauración para validar la integridad de los backups.
- **Prioridad:** Media.

- **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-327 – Evaluación de Impacto en Protección de Datos (EIPD) para Tratamientos en la Nube**

- **Descripción:**
    - Se debe realizar una **Evaluación de Impacto en Protección de Datos (EIPD)** si el tratamiento en la nube implica **riesgos elevados para los derechos y libertades de los interesados**.
  - **Criterios de Aceptación:**
    - Análisis de **riesgos específicos del proveedor cloud y medidas de mitigación**.
    - Revisión de **garantías contractuales y auditorías de seguridad del proveedor**.
    - Validación de la EIPD por el **Delegado de Protección de Datos (DPO)**.
  - **Prioridad:** Media.
  - **Categoría:** Evaluaciones de Seguridad.
  - **Fuente:** RGPD Art. 35; ISO 27001.
- 

#### **PRIV-328 – Auditoría y Supervisión del Tratamiento de Datos en la Nube**

- **Descripción:**
    - Se deben realizar auditorías periódicas para verificar la **conformidad con normativas de seguridad y protección de datos en entornos cloud**.
  - **Criterios de Aceptación:**
    - Ejecución de auditorías internas y externas sobre la seguridad en la nube.
    - Evaluación del **cumplimiento del proveedor cloud con estándares de seguridad**.
    - Aplicación de mejoras derivadas de hallazgos de auditoría.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** ISO 27001; ENS.
-

## PRIV-329 – Capacitación del Personal en Seguridad y Protección de Datos en la Nube

- **Descripción:**
    - Se debe formar al personal en **buenas prácticas de seguridad en entornos cloud**, asegurando el uso adecuado de las plataformas de almacenamiento y tratamiento de datos.
  - **Criterios de Aceptación:**
    - Inclusión de formación sobre **seguridad en la nube y riesgos asociados**.
    - Simulación de ataques y escenarios de fuga de información en entornos cloud.
    - Evaluación del conocimiento del personal en materia de seguridad cloud.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** ISO 27001; ENS.
- 

## PRIV-330 – Identificación de Procesos con Decisiones Automatizadas

- **Descripción:**

Según el **Artículo 22 del RGPD**, los interesados tienen derecho a no ser **sometidos a decisiones automatizadas sin intervención humana** cuando estas produzcan efectos jurídicos o significativos en su persona.

  - Se debe identificar **todos los procesos que utilicen inteligencia artificial (IA), machine learning o algoritmos** para la toma de decisiones automatizadas.
- **Criterios de Aceptación:**
  - Registro de los **procesos automatizados** en el **Registro de Actividades de Tratamiento (RAT)**.
  - Documentación de la **finalidad y base legal** del uso de la decisión automatizada.
  - Definición de **criterios de impacto** en los derechos de los interesados.
- **Prioridad:** Alta.
- **Categoría:** Gobernanza y Transparencia.
- **Fuente:** RGPD Art. 22.

---

### PRIV-331 – Garantía de Transparencia en el Uso de Algoritmos

- **Descripción:**
  - Se debe garantizar la **transparencia en el uso de algoritmos**, explicando a los interesados cómo se procesan sus datos y en qué medida afectan a sus derechos.
- **Criterios de Aceptación:**
  - Redacción de una **política de explicabilidad** para los algoritmos utilizados.
  - Inclusión de información sobre decisiones automatizadas en la **política de privacidad**.
  - Implementación de mecanismos para que los interesados puedan solicitar explicaciones sobre las decisiones tomadas por un sistema automatizado.
- **Prioridad:** Alta.
- **Categoría:** Transparencia y Derechos del Usuario.
- **Fuente:** RGPD Art. 13, 22.

---

### PRIV-332 – Derecho a la Intervención Humana en Decisiones Automatizadas

- **Descripción:**
    - Los interesados tienen derecho a **obtener intervención humana** en decisiones automatizadas que les afecten significativamente.
  - **Criterios de Aceptación:**
    - Implementación de **procedimientos para la revisión humana de decisiones automatizadas**.
    - Garantía de un canal accesible para que los interesados puedan **solicitar una revisión manual**.
    - Definición de plazos máximos para la respuesta a solicitudes de intervención humana.
  - **Prioridad:** Alta.
  - **Categoría:** Derechos del Usuario.
  - **Fuente:** RGPD Art. 22.
-

### PRIV-333 – Evaluación de la Equidad y No Discriminación en Algoritmos

- **Descripción:**
    - Se deben implementar controles para evitar **sesgos y discriminación** en la toma de decisiones automatizadas.
  - **Criterios de Aceptación:**
    - Realización de auditorías para detectar **sesgos algorítmicos**.
    - Pruebas periódicas de equidad en los modelos de IA y machine learning.
    - Implementación de medidas correctivas en caso de detectar sesgos en el algoritmo.
  - **Prioridad:** Alta.
  - **Categoría:** Ética en la IA y Seguridad.
  - **Fuente:** RGPD Art. 22; ISO 42001.
- 

### PRIV-334 – Aplicación de Técnicas de Explicabilidad y Auditabilidad de Algoritmos

- **Descripción:**
    - Se deben aplicar técnicas de **explicabilidad** en algoritmos que tomen decisiones automatizadas, garantizando que los resultados sean comprensibles para los afectados.
  - **Criterios de Aceptación:**
    - Uso de herramientas de **explicabilidad de IA** como SHAP o LIME.
    - Documentación de los criterios utilizados por el algoritmo para tomar decisiones.
    - Revisión periódica de los modelos para asegurar su fiabilidad y auditabilidad.
  - **Prioridad:** Media.
  - **Categoría:** Transparencia y Cumplimiento.
  - **Fuente:** RGPD Art. 22; ISO 42001.
- 

### PRIV-335 – Medidas de Seguridad para la Protección de Datos en Sistemas Automatizados

- **Descripción:**



- Se deben implementar medidas de **seguridad avanzadas** para evitar accesos no autorizados o manipulación de datos en sistemas que utilicen algoritmos de decisión automatizada.
  - **Criterios de Aceptación:**
    - Aplicación de **cifrado fuerte en reposo y en tránsito** para datos utilizados por algoritmos.
    - Control de accesos basado en roles (**RBAC**) para los sistemas automatizados.
    - Monitorización de accesos y actividades en los modelos de IA.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-336 – Evaluación de Impacto en Protección de Datos (EIPD) para Decisiones Automatizadas**

- **Descripción:**
    - Si el uso de un algoritmo puede implicar **riesgos elevados para los derechos y libertades de los interesados**, se debe realizar una **Evaluación de Impacto en Protección de Datos (EIPD)**.
  - **Criterios de Aceptación:**
    - Análisis de **riesgos potenciales asociados a la toma de decisiones automatizadas**.
    - Implementación de salvaguardas y medidas de mitigación del impacto.
    - Validación de la evaluación por el **Delegado de Protección de Datos (DPO)**.
  - **Prioridad:** Media.
  - **Categoría:** Evaluaciones de Seguridad.
  - **Fuente:** RGPD Art. 35.
- 

#### **PRIV-337 – Auditoría y Supervisión del Uso de Algoritmos y Decisiones Automatizadas**

- **Descripción:**

- Se deben realizar **auditorías periódicas** para evaluar el correcto funcionamiento de los algoritmos y el cumplimiento de las normativas de protección de datos.
  - **Criterios de Aceptación:**
    - Realización de auditorías internas al menos **una vez al año**.
    - Identificación de sesgos o errores en los algoritmos utilizados.
    - Implementación de mejoras en los modelos tras la auditoría.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** RGPD Art. 22.
- 

#### **PRIV-338 – Capacitación del Personal en Uso Ético de Algoritmos y Decisiones Automatizadas**

- **Descripción:**
    - Se debe formar a los empleados sobre el **uso responsable y transparente de algoritmos**, asegurando que comprenden los riesgos y limitaciones de la IA y machine learning.
  - **Criterios de Aceptación:**
    - Inclusión de formación sobre **ética y equidad en algoritmos** en los programas de capacitación.
    - Simulación de casos prácticos de toma de decisiones automatizadas.
    - Evaluación del conocimiento del personal sobre el impacto de los algoritmos en la privacidad.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** RGPD Art. 22; ISO 42001.
- 

#### **PRIV-339 – Identificación de Riesgos en el Uso de Dispositivos IoT**

- **Descripción:**
  - Los dispositivos IoT pueden procesar **datos personales y sensibles**, lo que genera riesgos de seguridad y privacidad.
  - Se debe realizar una evaluación de **riesgos específicos** del uso de IoT en la organización.

- **Criterios de Aceptación:**
    - Identificación de **dispositivos IoT utilizados** en la organización.
    - Evaluación de **vulnerabilidades** asociadas a la recopilación, almacenamiento y transmisión de datos.
    - Implementación de **controles de mitigación** ante riesgos detectados.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001.
- 

#### **PRIV-340 – Minimización de Datos en IoT**

- **Descripción:**
    - Se debe garantizar que los dispositivos IoT recojan **solo los datos personales estrictamente necesarios** para la finalidad del tratamiento.
  - **Criterios de Aceptación:**
    - Configuración de **opciones de privacidad por defecto** en los dispositivos IoT.
    - Aplicación del principio de **minimización de datos**, evitando la recolección excesiva de información.
    - Revisión y actualización de configuraciones de privacidad periódicamente.
  - **Prioridad:** Alta.
  - **Categoría:** Privacidad por Diseño.
  - **Fuente:** RGPD Art. 5, 25.
- 

#### **PRIV-341 – Cifrado de Datos en Dispositivos IoT**

- **Descripción:**
  - Se deben implementar **mecanismos de cifrado** en la transmisión y almacenamiento de datos recopilados por dispositivos IoT para evitar accesos no autorizados.
- **Criterios de Aceptación:**
  - Uso de **TLS 1.2 o superior** para la comunicación de dispositivos IoT.
  - Implementación de **cifrado AES-256 en datos en reposo**.

- Revisión periódica de los certificados de seguridad y configuraciones de cifrado.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS; RGPD Art. 32.
- 

#### **PRIV-342 – Control de Accesos y Autenticación Segura en IoT**

- **Descripción:**
    - Se deben aplicar controles de acceso estrictos para **limitar el acceso a datos personales** recopilados por dispositivos IoT.
  - **Criterios de Aceptación:**
    - Uso de **autenticación multifactor (MFA)** en dispositivos IoT críticos.
    - Implementación de **control de acceso basado en roles (RBAC)**.
    - Monitorización y auditoría de accesos a la información generada por IoT.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; RGPD Art. 32.
- 

#### **PRIV-343 – Garantía de Transparencia en la Recolección de Datos IoT**

- **Descripción:**
  - Se debe informar a los usuarios sobre el tipo de datos que recopilan los dispositivos IoT y su finalidad.
- **Criterios de Aceptación:**
  - Inclusión de información sobre el uso de IoT en la **política de privacidad**.
  - Posibilidad de que los usuarios configuren sus **preferencias de privacidad** en los dispositivos.
  - Implementación de opciones para que los interesados puedan **revocar su consentimiento** si corresponde.
- **Prioridad:** Alta.
- **Categoría:** Transparencia y Cumplimiento.
- **Fuente:** RGPD Art. 12, 13.

---

#### **PRIV-344 – Evaluación de Impacto en Protección de Datos (EIPD) para IoT**

- **Descripción:**
    - Se debe realizar una **Evaluación de Impacto en Protección de Datos (EIPD)** si el uso de dispositivos IoT implica un **riesgo elevado para la privacidad**.
  - **Criterios de Aceptación:**
    - Análisis de los riesgos y **posibles impactos en los derechos de los usuarios**.
    - Identificación de **medidas de mitigación de riesgos** antes de la implementación.
    - Aprobación de la evaluación por el **Delegado de Protección de Datos (DPO)**.
  - **Prioridad:** Media.
  - **Categoría:** Evaluaciones de Seguridad.
  - **Fuente:** RGPD Art. 35.
- 

#### **PRIV-345 – Monitorización y Supervisión de Dispositivos IoT**

- **Descripción:**
    - Se deben implementar mecanismos de **supervisión y control** para detectar actividades anómalas en dispositivos IoT.
  - **Criterios de Aceptación:**
    - Implementación de **sistemas de monitorización de logs (SIEM)** en dispositivos IoT.
    - Configuración de alertas ante **accesos no autorizados o anomalías** en el comportamiento de los dispositivos.
    - Auditoría periódica de los dispositivos y su configuración de seguridad.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-346 – Gestión del Ciclo de Vida de Dispositivos IoT**

- **Descripción:**
    - Se debe garantizar que los dispositivos IoT tengan una **gestión segura desde su instalación hasta su eliminación**, evitando riesgos por dispositivos desactualizados o comprometidos.
  - **Criterios de Aceptación:**
    - Aplicación de **políticas de actualización de firmware y software** en dispositivos IoT.
    - Definición de procedimientos de **desmantelamiento y eliminación segura de dispositivos**.
    - Eliminación de datos almacenados en dispositivos IoT antes de su baja o reciclaje.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-347 – Auditoría y Evaluación de Seguridad en Dispositivos IoT**

- **Descripción:**
    - Se deben realizar auditorías periódicas para verificar la **conformidad de los dispositivos IoT con las normativas de seguridad y protección de datos**.
  - **Criterios de Aceptación:**
    - Realización de auditorías internas al menos **una vez al año**.
    - Evaluación del cumplimiento de **normas ISO 27001, ENS y RGPD** en dispositivos IoT.
    - Aplicación de mejoras tras las auditorías y pruebas de seguridad.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-348 – Capacitación del Personal en Seguridad y Privacidad de IoT**

- **Descripción:**
  - Se debe capacitar a los empleados sobre **los riesgos de privacidad en dispositivos IoT y las mejores prácticas de seguridad**.

- **Criterios de Aceptación:**
    - Inclusión de módulos sobre **privacidad y seguridad en IoT** en la formación interna.
    - Simulación de ataques y vulnerabilidades en entornos controlados.
    - Evaluación del conocimiento del personal en **protección de datos en IoT**.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-349 – Identificación de Finalidades Legítimas para el Uso de Datos Biométricos y de Salud**

- **Descripción:**
    - El tratamiento de datos biométricos y de salud solo es legítimo si se basa en **una de las excepciones del Artículo 9 del RGPD**, como el **consentimiento explícito**, el **interés público en salud** o el **cumplimiento de obligaciones legales**.
  - **Criterios de Aceptación:**
    - Identificación y justificación documental de la **finalidad específica del tratamiento**.
    - Garantía de que los datos biométricos o de salud **no se usen para finalidades secundarias no autorizadas**.
    - Inclusión de la base legal en el **Registro de Actividades de Tratamiento (RAT)**.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 9; LOPDGDD.
- 

#### **PRIV-350 – Obtención de Consentimiento Explícito cuando sea Requerido**

- **Descripción:**
  - Cuando el tratamiento de datos biométricos o de salud no se base en otra excepción del **Artículo 9 del RGPD**, se debe obtener el **consentimiento explícito** del interesado antes de la recopilación.
- **Criterios de Aceptación:**

- Implementación de un **formulario de consentimiento explícito** antes de la recopilación de datos.
    - Registro seguro de los consentimientos obtenidos.
    - Garantía de que el consentimiento puede ser **revocado en cualquier momento**.
  - **Prioridad:** Alta.
  - **Categoría:** Derechos del Usuario y Cumplimiento.
  - **Fuente:** RGPD Art. 9; LOPDGDD.
- 

#### **PRIV-351 – Minimización y Limitación del Tratamiento de Datos Biométricos y de Salud**

- **Descripción:**
    - Se debe aplicar el principio de **minimización de datos**, garantizando que solo se recojan y almacenen los datos biométricos y de salud estrictamente necesarios para la finalidad declarada.
  - **Criterios de Aceptación:**
    - Evaluación de **si el uso de biometría o datos de salud es imprescindible**.
    - Implementación de **técnicas de anonimización o seudonimización** cuando sea posible.
    - Definición de **plazos de retención mínimos** y mecanismos de eliminación segura.
  - **Prioridad:** Alta.
  - **Categoría:** Privacidad por Diseño y Seguridad de la Información.
  - **Fuente:** RGPD Art. 5, 9.
- 

#### **PRIV-352 – Cifrado y Protección Avanzada de Datos Biométricos y de Salud**

- **Descripción:**
  - Se deben aplicar **medidas de seguridad reforzadas** para proteger los datos biométricos y de salud contra accesos no autorizados.
- **Criterios de Aceptación:**
  - Implementación de **cifrado AES-256 para almacenamiento de datos biométricos y de salud**.



- Uso de **TLS 1.2 o superior para transmisión de datos**.
  - Aplicación de **medidas de seguridad física** para servidores que almacenen datos de salud.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** RGPD Art. 32; ISO 27001.
- 

#### **PRIV-353 – Control de Accesos y Auditoría del Uso de Datos Biométricos y de Salud**

- **Descripción:**
    - Solo el **personal estrictamente autorizado** debe acceder a datos biométricos y de salud, con mecanismos de auditoría para supervisar su uso.
  - **Criterios de Aceptación:**
    - Implementación de **autenticación multifactor (MFA) en accesos a bases de datos de salud y biometría**.
    - Registro de **logs de acceso y modificaciones** en los datos biométricos y de salud.
    - Auditoría periódica de accesos y **eliminación de cuentas inactivas o sin uso justificado**.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información y Cumplimiento.
  - **Fuente:** RGPD Art. 32; ENS; ISO 27001.
- 

#### **PRIV-354 – Garantía de Derechos de los Interesados en el Tratamiento de Biometría y Salud**

- **Descripción:**
  - Se debe garantizar que los interesados puedan **ejercer sus derechos** en relación con el tratamiento de sus datos biométricos o de salud, incluyendo el acceso, rectificación, supresión y oposición.
- **Criterios de Aceptación:**
  - Definición de un **procedimiento para gestionar solicitudes de derechos** en relación con la biometría y datos de salud.

- Respuesta a las solicitudes dentro del **plazo máximo de un mes**.
  - Garantía de que la supresión de datos se realice mediante **métodos seguros**.
  - **Prioridad:** Media.
  - **Categoría:** Derechos del Usuario y Cumplimiento.
  - **Fuente:** RGPD Art. 15-22.
- 

#### **PRIV-355 – Evaluación de Impacto en Protección de Datos (EIPD) para Datos Biométricos y de Salud**

- **Descripción:**
    - Se debe realizar una **Evaluación de Impacto en Protección de Datos (EIPD)** antes de implementar tratamientos que utilicen datos biométricos o de salud, dada su sensibilidad.
  - **Criterios de Aceptación:**
    - Análisis de **riesgos asociados** al tratamiento de datos biométricos y de salud.
    - Implementación de **medidas de mitigación** si se detectan riesgos elevados.
    - Validación de la evaluación por el **Delegado de Protección de Datos (DPO)**.
  - **Prioridad:** Media.
  - **Categoría:** Evaluaciones de Seguridad.
  - **Fuente:** RGPD Art. 35.
- 

#### **PRIV-356 – Auditoría y Supervisión del Uso de Datos Biométricos y de Salud**

- **Descripción:**
  - Se deben realizar auditorías periódicas para garantizar que los datos biométricos y de salud se están tratando de acuerdo con la normativa y las mejores prácticas de seguridad.
- **Criterios de Aceptación:**
  - Realización de auditorías internas al menos **una vez al año**.
  - Identificación de accesos indebidos o tratamientos irregulares.
  - Aplicación de mejoras en los procedimientos de seguridad y privacidad.

- **Prioridad:** Media.
  - **Categoría:** Auditoría y Seguridad.
  - **Fuente:** RGPD Art. 32; ENS.
- 

#### **PRIV-357 – Capacitación del Personal en el Uso Seguro de Datos Biométricos y de Salud**

- **Descripción:**
    - Se debe formar a los empleados que gestionen datos biométricos y de salud sobre **las obligaciones normativas y las mejores prácticas de seguridad**.
  - **Criterios de Aceptación:**
    - Inclusión de formación sobre **protección de datos sensibles y seguridad en biometría**.
    - Evaluación del conocimiento del personal sobre riesgos y medidas de mitigación.
    - Implementación de controles para evitar accesos no autorizados o mal uso de los datos.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** RGPD Art. 9; ISO 27001.
- 

#### **PRIV-358 – Designación Obligatoria del Delegado de Protección de Datos (DPO)**

- **Descripción:**
  - Según el **Artículo 37 del RGPD**, la designación de un **Delegado de Protección de Datos (DPO)** es obligatoria en los siguientes casos:
    - Cuando el tratamiento lo realiza una autoridad u organismo público.
    - Cuando las actividades principales del responsable o encargado implican **tratamientos a gran escala de datos sensibles o vigilancia sistemática**.
    - Cuando lo exige la normativa nacional aplicable.
- **Criterios de Aceptación:**
  - Identificación de si la organización está obligada a nombrar un DPO.

- Designación formal y comunicación del DPO a la autoridad de control.
    - Publicación de los datos de contacto del DPO en la organización y en la política de privacidad.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 37; LOPDGDD.
- 

#### **PRIV-359 – Independencia y Autonomía del Delegado de Protección de Datos**

- **Descripción:**
    - El DPO debe actuar con **independencia y sin recibir instrucciones** sobre el ejercicio de sus funciones, garantizando que no exista conflicto de intereses.
  - **Criterios de Aceptación:**
    - Garantía de que el DPO no desempeña funciones incompatibles con su rol.
    - Inclusión de cláusulas en el contrato que aseguren su autonomía.
    - Acceso directo del DPO a la **alta dirección** y recursos adecuados para desempeñar sus funciones.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza.
  - **Fuente:** RGPD Art. 38.
- 

#### **PRIV-360 – Funciones y Responsabilidades del Delegado de Protección de Datos**

- **Descripción:**
  - Según el **Artículo 39 del RGPD**, el DPO debe desempeñar las siguientes funciones:
    - Informar y asesorar al responsable y empleados sobre sus obligaciones en materia de protección de datos.
    - Supervisar el cumplimiento normativo en la organización.
    - Asesorar en la realización de **Evaluaciones de Impacto en Protección de Datos (EIPD)**.
    - Actuar como **punto de contacto** con la autoridad de control.

- **Criterios de Aceptación:**
    - Definición clara de las funciones del DPO en un documento oficial.
    - Garantía de que el DPO tiene acceso a toda la información relevante.
    - Participación del DPO en todas las cuestiones relacionadas con la protección de datos.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 39.
- 

#### **PRIV-361 – Supervisión del Cumplimiento Normativo por parte del DPO**

- **Descripción:**
    - El DPO debe supervisar el cumplimiento del **RGPD, LOPDGDD y otras normativas aplicables**, incluyendo auditorías y revisiones periódicas.
  - **Criterios de Aceptación:**
    - Elaboración de un **plan de supervisión del cumplimiento normativo**.
    - Revisión periódica de **políticas de privacidad, contratos y medidas de seguridad**.
    - Informes anuales sobre el estado de cumplimiento en la organización.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 39.
- 

#### **PRIV-362 – Participación del DPO en Evaluaciones de Impacto en Protección de Datos (EIPD)**

- **Descripción:**
  - El DPO debe participar y asesorar en la realización de **Evaluaciones de Impacto en Protección de Datos (EIPD)** para tratamientos que presenten **riesgos elevados**.
- **Criterios de Aceptación:**
  - Definición de un procedimiento en el que el DPO asesore en las EIPD.
  - Registro de la opinión del DPO en cada EIPD realizada.
  - Supervisión de las medidas de mitigación recomendadas en la evaluación.

- **Prioridad:** Media.
  - **Categoría:** Evaluaciones de Seguridad.
  - **Fuente:** RGPD Art. 35-39.
- 

#### **PRIV-363 – Canal de Comunicación entre el DPO y la Autoridad de Control**

- **Descripción:**
    - El DPO debe actuar como **interlocutor** entre la organización y la autoridad de control en materia de protección de datos.
  - **Criterios de Aceptación:**
    - Definición de un **procedimiento de comunicación con la autoridad de control**.
    - Registro de consultas y notificaciones realizadas a la autoridad de control.
    - Disponibilidad del DPO para responder a requerimientos normativos.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 39.
- 

#### **PRIV-364 – Formación Continua del Delegado de Protección de Datos**

- **Descripción:**
    - El DPO debe recibir formación continua en **normativa de protección de datos, seguridad de la información y gestión de riesgos** para mantenerse actualizado.
  - **Criterios de Aceptación:**
    - Participación del DPO en **cursos, seminarios y certificaciones** en protección de datos.
    - Registro de la formación recibida en un **expediente de actualización profesional**.
    - Evaluación periódica del nivel de conocimiento del DPO.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** RGPD Art. 37-39.
-

#### **PRIV-365 – Accesibilidad del DPO para los Interesados**

- **Descripción:**
    - Los interesados deben poder contactar con el **DPO** para ejercer sus derechos o plantear consultas sobre el tratamiento de sus datos personales.
  - **Criterios de Aceptación:**
    - Publicación de los datos de contacto del DPO en la **política de privacidad**.
    - Implementación de un canal de comunicación para **consultas y reclamaciones**.
    - Garantía de que las solicitudes recibidas por el DPO sean gestionadas dentro del plazo legal.
  - **Prioridad:** Media.
  - **Categoría:** Derechos del Usuario y Transparencia.
  - **Fuente:** RGPD Art. 37.
- 

#### **PRIV-366 – Auditoría del Funcionamiento del DPO y su Rol en la Organización**

- **Descripción:**
    - Se deben realizar auditorías para garantizar que el DPO cumple con sus funciones de manera eficaz e independiente.
  - **Criterios de Aceptación:**
    - Evaluación anual de la **efectividad del DPO en la supervisión del cumplimiento normativo**.
    - Identificación de mejoras en la operativa del DPO dentro de la organización.
    - Registro de auditorías y aplicación de acciones correctivas si es necesario.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Gobernanza.
  - **Fuente:** RGPD Art. 37-39.
- 

#### **PRIV-367 – Adopción de Códigos de Conducta para la Protección de Datos**

- **Descripción:**

- Según el **Artículo 40 del RGPD**, los códigos de conducta permiten a las organizaciones demostrar el cumplimiento normativo mediante **normas específicas** establecidas por asociaciones representativas o autoridades competentes.
  - **Criterios de Aceptación:**
    - Evaluación de **códigos de conducta aplicables al sector** y su compatibilidad con la organización.
    - Adhesión formal a un código de conducta reconocido.
    - Inclusión de la adhesión en la política de privacidad y documentación de cumplimiento.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 40.
- 

#### **PRIV-368 – Implementación de Medidas Derivadas de Códigos de Conducta**

- **Descripción:**
    - Las organizaciones que se adhieran a un código de conducta deben **implementar sus directrices** en los procesos internos y garantizar su cumplimiento.
  - **Criterios de Aceptación:**
    - Integración de los **requisitos del código de conducta** en las políticas de protección de datos.
    - Asignación de responsabilidades dentro de la organización para supervisar el cumplimiento.
    - Revisión periódica de la aplicación del código y ajustes en función de cambios normativos.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 40.
- 

#### **PRIV-369 – Supervisión y Control del Cumplimiento del Código de Conducta**

- **Descripción:**



- Se debe establecer un mecanismo de **supervisión interna** para garantizar el cumplimiento del código de conducta.
  - **Criterios de Aceptación:**
    - Definición de un **plan de supervisión** de cumplimiento del código de conducta.
    - Auditorías internas periódicas para verificar el seguimiento del código.
    - Comunicación con el organismo certificador o asociación responsable del código.
  - **Prioridad:** Media.
  - **Categoría:** Auditoría y Cumplimiento.
  - **Fuente:** RGPD Art. 40.
- 

#### **PRIV-370 – Obtención de Certificaciones en Protección de Datos**

- **Descripción:**
    - Según el **Artículo 42 del RGPD**, las organizaciones pueden obtener **certificaciones** en protección de datos como una garantía adicional de cumplimiento.
  - **Criterios de Aceptación:**
    - Evaluación de **certificaciones aplicables**, como **ISO/IEC 27701**, **EuroPrivacy**, o **Esquema Nacional de Seguridad (ENS)**.
    - Implementación de controles y procesos para cumplir con los estándares requeridos.
    - Mantenimiento y auditoría periódica de la certificación obtenida.
  - **Prioridad:** Media.
  - **Categoría:** Cumplimiento y Gobernanza.
  - **Fuente:** RGPD Art. 42.
- 

#### **PRIV-371 – Selección de Organismos de Certificación Acreditados**

- **Descripción:**
  - Las certificaciones deben ser emitidas por **organismos acreditados** por las autoridades de protección de datos de la UE o por entidades de certificación reconocidas.
- **Criterios de Aceptación:**

- Verificación de que el organismo certificador está **acreditado según el RGPD**.
    - Revisión de los criterios y auditorías requeridas para la certificación.
    - Documentación de la elección del organismo certificador y sus requisitos.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 42.
- 

#### **PRIV-372 – Implementación de un Sistema de Gestión de Privacidad Basado en Certificación**

- **Descripción:**
    - La organización debe adaptar su **Sistema de Gestión de Privacidad (SGP)** para cumplir con los requisitos de la certificación seleccionada.
  - **Criterios de Aceptación:**
    - Definición y documentación de un **SGP basado en estándares de certificación**.
    - Inclusión de auditorías internas para evaluar el cumplimiento de los requisitos.
    - Mantenimiento de registros sobre la implementación y supervisión del SGP.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 42; ISO/IEC 27701.
- 

#### **PRIV-373 – Evaluación Periódica del Cumplimiento con la Certificación Obtenida**

- **Descripción:**
  - Una vez obtenida la certificación, se deben realizar **evaluaciones regulares** para confirmar que los estándares siguen cumpliéndose.
- **Criterios de Aceptación:**
  - Implementación de revisiones anuales o conforme al período establecido por el certificado.
  - Realización de auditorías internas o externas para evaluar el mantenimiento del cumplimiento.

- Documentación de medidas correctivas ante hallazgos de auditoría.
  - **Prioridad:** Media.
  - **Categoría:** Cumplimiento y Auditoría.
  - **Fuente:** RGPD Art. 42.
- 

#### **PRIV-374 – Publicación y Transparencia sobre Certificaciones Obtenidas**

- **Descripción:**
    - Las organizaciones certificadas pueden hacer público su **sello de certificación** para demostrar su compromiso con la protección de datos.
  - **Criterios de Aceptación:**
    - Publicación de la certificación en la web corporativa y documentos relevantes.
    - Inclusión de información sobre el alcance y validez de la certificación.
    - Garantía de que la certificación se presenta de manera clara y no engañosa.
  - **Prioridad:** Baja.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 42.
- 

#### **PRIV-375 – Capacitación del Personal en Códigos de Conducta y Certificaciones**

- **Descripción:**
  - Se debe formar al personal en los **requisitos de los códigos de conducta y certificaciones** a los que se haya adherido la organización.
- **Criterios de Aceptación:**
  - Inclusión de módulos sobre **códigos de conducta y certificaciones** en el plan de formación interna.
  - Pruebas de conocimiento sobre las normas de certificación y buenas prácticas.
  - Supervisión del cumplimiento de los requisitos por parte del **DPO o equipo de cumplimiento**.
- **Prioridad:** Baja.
- **Categoría:** Gobernanza y Seguridad.

- **Fuente:** RGPD Art. 40-42.
- 

#### **PRIV-376 – Implementación de un Plan de Formación en Protección de Datos**

- **Descripción:**
    - Según el **Esquema Nacional de Seguridad (ENS)** y **ISO 27001**, las organizaciones deben garantizar que los empleados y terceros que acceden a datos personales **reciban formación periódica** en materia de protección de datos y seguridad.
  - **Criterios de Aceptación:**
    - Creación de un **programa de formación estructurado** en protección de datos.
    - Definición de **contenidos adaptados a cada perfil dentro de la organización**.
    - Revisión y actualización del plan de formación de forma periódica.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** ENS; ISO 27001.
- 

#### **PRIV-377 – Formación Obligatoria para Todo el Personal que Trate Datos Personales**

- **Descripción:**
    - Todos los empleados y terceros que tengan acceso a datos personales deben recibir formación en **principios del RGPD, medidas de seguridad y gestión de incidentes**.
  - **Criterios de Aceptación:**
    - Realización de **formaciones obligatorias** al menos una vez al año.
    - Registro de la asistencia a la formación y evaluación de conocimientos.
    - Inclusión de formación específica para **empleados con acceso a datos sensibles**.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** RGPD Art. 39; ENS.
-

### **PRIV-378 – Capacitación del Delegado de Protección de Datos (DPO) y Responsables de Seguridad**

- **Descripción:**
    - El **DPO y los responsables de seguridad** deben recibir formación continua en **normativa, auditoría, seguridad y gestión de riesgos**.
  - **Criterios de Aceptación:**
    - Participación en **cursos de actualización y certificaciones** en protección de datos y ciberseguridad.
    - Registro de las certificaciones obtenidas por el DPO.
    - Evaluación anual de conocimientos y competencias del DPO.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 37-39; ENS.
- 

### **PRIV-379 – Simulaciones de Incidentes de Seguridad y Brechas de Datos**

- **Descripción:**
    - Se deben realizar **simulaciones periódicas** de incidentes de seguridad y brechas de datos para evaluar la capacidad de respuesta del personal.
  - **Criterios de Aceptación:**
    - Realización de **ejercicios de simulación de ataques de phishing, ransomware y filtración de datos**.
    - Evaluación de la reacción del personal y detección de **fallos en la respuesta**.
    - Implementación de medidas correctivas tras cada simulacro.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

### **PRIV-380 – Sensibilización sobre Privacidad por Diseño y por Defecto**

- **Descripción:**

- Se debe formar al personal en el **principio de Privacidad por Diseño y por Defecto**, garantizando que los sistemas y procesos incorporen la protección de datos desde su fase inicial.
  - **Criterios de Aceptación:**
    - Inclusión de formación sobre **diseño seguro y minimización de datos**.
    - Aplicación de **técnicas de anonimización y seudonimización** en el desarrollo de sistemas.
    - Evaluación de la efectividad de la implementación de estos principios en nuevos proyectos.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** RGPD Art. 25; ISO 27001.
- 

#### **PRIV-381 – Formación Específica para Desarrolladores y Administradores de Sistemas**

- **Descripción:**
    - Se debe formar a los **desarrolladores de software y administradores de sistemas** en buenas prácticas de seguridad, codificación segura y gestión de accesos.
  - **Criterios de Aceptación:**
    - Inclusión de cursos sobre **OWASP Top 10, cifrado y control de accesos**.
    - Evaluación de conocimientos mediante pruebas técnicas.
    - Implementación de revisiones de código con enfoque en seguridad y protección de datos.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; RGPD Art. 32.
- 

#### **PRIV-382 – Concienciación sobre Phishing, Ingeniería Social y Ciberataques**

- **Descripción:**
  - Se debe concienciar a los empleados sobre los riesgos de **phishing, ingeniería social y ciberataques** que puedan comprometer la seguridad de los datos personales.

- **Criterios de Aceptación:**
    - Ejecución de **simulaciones de ataques de phishing y malware**.
    - Evaluación del comportamiento del personal ante intentos de fraude digital.
    - Revisión y refuerzo de las políticas de seguridad en función de los resultados.
  - **Prioridad:** Media.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-383 – Evaluación Periódica de Conocimientos sobre Protección de Datos**

- **Descripción:**
    - Se deben realizar **evaluaciones periódicas** para comprobar el nivel de conocimiento del personal en protección de datos y seguridad de la información.
  - **Criterios de Aceptación:**
    - Implementación de **pruebas de conocimiento** tras las formaciones.
    - Identificación de **áreas de mejora en la formación del personal**.
    - Revisión de resultados y actualización de contenidos formativos según necesidades detectadas.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** ENS; ISO 27001.
- 

#### **PRIV-384 – Registro y Seguimiento de la Formación Recibida por el Personal**

- **Descripción:**
  - Se debe mantener un **registro actualizado de la formación recibida** por cada empleado en materia de protección de datos y seguridad.
- **Criterios de Aceptación:**
  - Creación de un **expediente formativo** para cada empleado con las formaciones realizadas.
  - Actualización periódica del estado de formación de cada trabajador.

- Supervisión por parte del **DPO o equipo de cumplimiento** del grado de capacitación del personal.
  - **Prioridad:** Baja.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** ENS; ISO 27001.
- 

#### **PRIV-385 – Implementación de un Proceso de Mejora Continua en Protección de Datos**

- **Descripción:**
    - Según **ISO 27001** y el **Esquema Nacional de Seguridad (ENS)**, las organizaciones deben adoptar un **enfoque de mejora continua** en sus prácticas de protección de datos.
    - Se debe establecer un ciclo de **planificación, ejecución, revisión y corrección (PDCA)** en la gestión de la seguridad de la información y la privacidad.
  - **Criterios de Aceptación:**
    - Definición de un **proceso formal de mejora continua** en protección de datos.
    - Documentación y revisión periódica de **políticas y procedimientos**.
    - Identificación y aplicación de **acciones correctivas** basadas en auditorías y análisis de incidentes.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-386 – Auditorías Internas Periódicas en Protección de Datos**

- **Descripción:**
  - Se deben realizar auditorías internas con **frecuencia regular** para evaluar la eficacia de las medidas de protección de datos y seguridad de la información.
- **Criterios de Aceptación:**
  - Planificación de **auditorías internas al menos una vez al año**.



- Evaluación de **cumplimiento normativo, políticas y controles de seguridad**.
    - Implementación de **medidas correctivas y seguimiento de su aplicación**.
  - **Prioridad:** Alta.
  - **Categoría:** Auditoría y Seguridad.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-387 – Evaluación y Actualización Periódica de Políticas de Privacidad y Seguridad**

- **Descripción:**
    - Las políticas de privacidad, seguridad y cumplimiento deben **revisarse y actualizarse periódicamente** para garantizar su vigencia y alineación con cambios normativos.
  - **Criterios de Aceptación:**
    - Definición de un **calendario de revisión y actualización de políticas**.
    - Implementación de **mecanismos de actualización ante cambios legislativos**.
    - Registro de todas las modificaciones realizadas en las políticas.
  - **Prioridad:** Alta.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** ISO 27001; ENS; RGPD.
- 

#### **PRIV-388 – Supervisión de Incidentes de Seguridad y Aplicación de Medidas Correctivas**

- **Descripción:**
  - Se debe llevar un **registro de incidentes de seguridad** y aplicar medidas correctivas para evitar su repetición y mejorar las prácticas de protección de datos.
- **Criterios de Aceptación:**
  - Implementación de un **registro centralizado de incidentes**.
  - Análisis forense de incidentes y **determinación de causas raíz**.

- Aplicación de **acciones correctivas y planes de mejora** en función de los incidentes reportados.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-389 – Monitorización y Análisis de Vulnerabilidades en los Sistemas**

- **Descripción:**
    - Se deben realizar **pruebas de seguridad periódicas** para detectar vulnerabilidades en los sistemas que manejen datos personales.
  - **Criterios de Aceptación:**
    - Realización de **pruebas de penetración (pentesting) y análisis de vulnerabilidades** al menos una vez al año.
    - Implementación de **herramientas de detección de intrusos (IDS/IPS)**.
    - Aplicación de **parches y actualizaciones de seguridad de manera proactiva**.
  - **Prioridad:** Alta.
  - **Categoría:** Seguridad de la Información.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-390 – Análisis de Impacto ante Cambios Tecnológicos y Normativos**

- **Descripción:**
  - Se debe realizar un **análisis de impacto** cuando haya **cambios normativos, tecnológicos o estructurales** en la organización que afecten la protección de datos.
- **Criterios de Aceptación:**
  - Evaluación de impacto ante **nuevas normativas de protección de datos**.
  - Revisión de seguridad ante **implementación de nuevas tecnologías** en la organización.
  - Inclusión de medidas de mitigación en función del impacto identificado.
- **Prioridad:** Media.
- **Categoría:** Gobernanza y Seguridad.

- **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-391 – Revisión del Cumplimiento de los Acuerdos con Encargados del Tratamiento**

- **Descripción:**
    - Se deben **auditar periódicamente** los acuerdos con **proveedores y encargados del tratamiento** para garantizar su cumplimiento con el RGPD y la seguridad de los datos personales.
  - **Criterios de Aceptación:**
    - Verificación de que los contratos incluyen **cláusulas de protección de datos**.
    - Evaluación del cumplimiento del **RGPD y estándares de seguridad** por parte de los proveedores.
    - Implementación de medidas correctivas ante incumplimientos detectados.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** RGPD Art. 28; ISO 27001.
- 

#### **PRIV-392 – Indicadores de Desempeño y Métricas de Seguridad en Protección de Datos**

- **Descripción:**
  - Se deben definir **indicadores clave de desempeño (KPIs)** para medir la efectividad de las medidas de seguridad y privacidad.
- **Criterios de Aceptación:**
  - Definición de **métricas e indicadores sobre seguridad y cumplimiento**.
  - Análisis trimestral de **tendencias en incidentes de seguridad y auditorías**.
  - Uso de los resultados para **ajustar estrategias de seguridad** y mejorar la protección de datos.
- **Prioridad:** Media.
- **Categoría:** Gobernanza y Seguridad.
- **Fuente:** ISO 27001; ENS.

---

#### **PRIV-393 – Evaluación del Nivel de Madurez en Protección de Datos**

- **Descripción:**
    - Se debe realizar una evaluación periódica del **nivel de madurez en protección de datos** en la organización.
  - **Criterios de Aceptación:**
    - Uso de modelos de **madurez de privacidad y seguridad (CMMI, NIST, ENS)**.
    - Identificación de **áreas de mejora y estrategias de desarrollo**.
    - Documentación de los resultados y planificación de **acciones de mejora**.
  - **Prioridad:** Media.
  - **Categoría:** Gobernanza y Cumplimiento.
  - **Fuente:** ISO 27001; ENS.
- 

#### **PRIV-394 – Capacitación en Mejora Continua en Protección de Datos**

- **Descripción:**
    - Se debe capacitar a los responsables de privacidad y seguridad en **mejora continua, análisis de riesgos y actualización de normativas**.
  - **Criterios de Aceptación:**
    - Inclusión de módulos sobre **gestión de riesgos y mejora continua** en los planes de formación.
    - Evaluaciones periódicas sobre **nuevas amenazas y estrategias de seguridad**.
    - Actualización de conocimientos en función de cambios en el ENS y RGPD.
  - **Prioridad:** Baja.
  - **Categoría:** Gobernanza y Seguridad.
  - **Fuente:** ISO 27001; ENS.
-

