[logo de la organización]

[nombre de la organización]

**PLAN DE PROYECTO**  
 **para Cumplir con el Reglamento General de Protección de Datos Europeo**

|  |  |
| --- | --- |
| Código: |  |
| Versión: |  |
| Fecha de la versión: |  |
| Creado por: |  |
| Aprobado por: |  |
| Nivel de confidencialidad: |  |

**Historial de cambios**

|  |  |  |  |
| --- | --- | --- | --- |
| **Fecha** | **Versión** | **Creado por** | **Descripción del cambio** |
| dd.mm.aaaa | 0.1 | EUGDPRAcademy | Descripción básica del documento |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Tabla de contenido**

[1. Propósito, alcance y usuarios 3](#_Toc503766271)

[2. Documentos de referencia 3](#_Toc503766272)

[3. Proyecto de implementación del RGPD UE 3](#_Toc503766273)

[3.1. Objetivo del proyecto 3](#_Toc503766274)

[3.2. Resultados del proyecto 3](#_Toc503766275)

[3.3. Plazos 5](#_Toc503766276)

[3.4. Organización del proyecto 5](#_Toc503766277)

[3.4.1. Promotor del proyecto 5](#_Toc503766278)

[3.4.2. Gerente del proyecto 6](#_Toc503766279)

[3.4.3. Equipo del proyecto 6](#_Toc503766280)

[3.5. Principales riesgos del proyecto 6](#_Toc503766281)

[3.6. Herramientas para la implementación del proyecto y realización de informes 6](#_Toc503766282)

[4. Gestión de registros guardados en base a este documento 7](#_Toc503766283)

[5. Validez y gestión de documentos 7](#_Toc503766284)

# Propósito, alcance y usuarios

El propósito del Plan de Proyecto es definir de manera clara los objetivos de implementación del proyecto del Reglamento General de Protección de Datos Europeo, los documentos que necesitan redactarse, los plazos, y las funciones y responsabilidades del proyecto.

El Plan de Proyecto es aplicable a todas las actividades realizadas en el proyecto de implementación del RGPD UE.

Los usuarios de este documento son los miembros de [alta dirección] y los miembros del equipo del proyecto.

# Documentos de referencia

* El RGPD UE 2016/679 (Reglamento (EU) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE)
* [legislación nacional o reglamento pertinente para la implementación del RGPD ]
* [otras leyes y reglamentos locales]

# Proyecto de implementación del RGPD UE

## Objetivo del proyecto

El objetivo del proyecto es implementar el sistema de gestión RGPD UE de acuerdo con el Reglamento General de Protección de Datos (RGPD UE 2016/679) del Parlamento Europeo y del Consejo antes de [fecha].

## Resultados del proyecto

Con el fin de asegurar una planificación más eficiente, la empresa debe de utilizar el Cuestionario de Evaluación para determinar en qué áreas necesita trabajar más para cumplir con el RGPD.

Durante el proyecto de implementación del RGPD UE, lo siguientes documentos (algunos de los cuales contienen apéndices que no expresamente indicados aquí) se escribirá:

* **Política de Protección de Datos Personales** – una política creada para establecer los principios de protección de datos generales así como para probar el compromiso de la empresa con esos principios;
* **Política de Protección de Datos de los Empleados –**  una política que establece las condiciones bajo las cuales la empresa trata datos personales de sus empleados ;
* **Aviso de Privacidad –**  un aviso que establece las condiciones bajo las cuales la empresa trata los datos personales de sus clientes/visitantes del sitio web;
* **Registro de Avisos de Privacidad** – un documento donde se necesita hacer un listado de todos los avisos de privacidad;
* **Política de retención de Datos –** una política que establece el periodo por el cual los datos personales deben ser guardados por la empresa;
* **Descripción del Trabajo del Delegado de Protección de Datos–** un documento que describe las responsabilidades del delegado de protección de datos;
* **Directrices para la elaboración del Inventario de Datos y las Actividades de Tratamiento –** un documento que explica cómo hacer una lista de todas las actividades de tratamiento de los datos;
* **Inventario de Actividades de Tratamiento –** un documento que se realiza con el fin de ser utilizado por la empresa para probar que cumple con los requisitos del art.30 del RGPD UE;
* **Formulario de Consentimiento del Interesado –**  un documento utilizado por la empresa para obtener el consentimiento de los interesados para el tratamiento de datos personales con fines específicos;
* **Formulario de Retirada del Consentimiento del Interesado –** un documento utilizado por los interesados para retirar su consentimiento;
* **Formulario de Consentimiento Paterno –**  un documento utilizado por la empresa para obtener el consentimiento del padre/tutor legal/representante de un menor para tratar datos personales con un fin específico;
* **Formulario de Retirada del Consentimiento Paterno** **–** un documento utilizado por el padre/tutor legal/representante de un menor para retirar el consentimiento del tratamiento de datos personales con un fin específico;
* **Procedimiento de solicitud de Acceso del Interesado –**  un documento que establece el proceso por el cual la empresa responde a las solicitudes de los interesados;
* **Metodología de Evaluación del Impacto de Protección de Datos** – un documento que describe cómo evaluar la necesidad y proporcionalidad de una determinada actividad de tratamiento y facilita medidas para mitigar los riesgos potenciales de los derechos y libertades de los interesados;
* **Registro de EIPDs –** un documento utilizado por la empresa para documentar el proceso de EIPD. Incluye el cuestionario de Umbral y el cuestionario de EIPD;
* **Procedimiento de transferencia de datos Transfronterizos –** un documento que establece las condiciones bajo las cuales una transferencia de datos transfronteriza puede ser llevada a cabo;
* **Cláusulas Contractuales –** cláusulas modelo emitidas por la Comisión de la UE para proporcionar garantías adecuadas con respecto a la protección de la privacidad y los derechos y libertades fundamentales de las personas y en relación con el ejercicio de los derechos correspondientes
* **Cuestionario de Cumplimiento del Encargado del RGPD –** un cuestionario destinado a evaluar el cumplimiento del proveedor con el RGPD de la UE;
* **Acuerdo de Tratamiento del Datos del Proveedor –**  un documento contractual destinado a establecer los límites y condiciones bajo las cuales un proveedor (encargado) puede tratar datos personales en nombre de la empresa (responsable);
* **Política de Seguridad TI**– describe las reglas básica s de seguridad para todos los empleados;
* **Política de Control de Acceso** – define cómo la dirección aprueba los derechos de acceso a usuarios particulares de sistemas de información;
* **Procedimientos de Seguridad para Departamentos TI** – describe las reglas de seguridad que deben ser empleadas para la infraestructura TI;
* **Política de Trae Tu Propio Dispositivo (BYOD)**  – describe las reglas para utilizar los teléfonos móviles y otros dispositivos que no pertenecen a la empresa con fines de negocio;
* **Política de Teletrabajo y Dispositivos Móviles** – describe las reglas de seguridad para usar ordenadores portátiles, teléfonos móviles y otros dispositivos fuera de las instalaciones de la empresa ;
* **Política de Escritorio Limpio y Pantalla Limpia** – define cómo proteger la información que se encuentra en el lugar de trabajo y en la pantalla del ordenador;
* **Política de Clasificación de la Información** – describe cómo clasificar los datos de acuerdo a la confidencialidad, y cómo proteger los datos debidamente;
* **Política de Anonimización y Seudonimización** – define cómo utilizar estas técnica para proteger el tratamiento de datos personales;
* **Política sobre el Uso del Encriptado** – define cómo utilizar los controles criptográficos y las claves para proteger la confidencialidad y la integridad de los datos;
* **Plan de Recuperación de Desastres** – define cómo recuperar la infraestructura y los datos después de un incidente perturbador;
* **Procedimiento de Auditoria Interna** – define cómo probar, analizar y evaluar las garantías organizativas y técnicas de una empresa;
* **Apéndice** **– Lista de Verificación de Auditoria Interna ISO 27001** proporciona una serie de preguntas basadas en 114 controles que están enumerados en el Anexo A de ISO 27001;
* **Procedimiento de Respuesta y Notificación ante una Violación de Seguridad de Datos –** un procedimiento que establece las obligaciones de la empresa en caso de una violación de información de datos personales;
* **Registro de Violación de Seguridad de Datos –**  registro interno de la empresa de violación de seguridad de datos;
* **Notificación de Violación de Seguridad de Datos a la Autoridad de Control**  – el documento para ser utilizado en caso de una violación de seguridad de datos;
* **Notificación de Violación de Seguridad de Datos a los Interesados** – el documento para ser utilizado en caso de una violación de datos

## Plazos

Los plazos para la aceptación de documentos individuales en el curso de la implementación del RGPD UE son los siguientes:

|  |  |
| --- | --- |
| ***Documento*** | ***Plazos para la aceptación del documento*** |
| \* |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

La presentación final de los resultados del proyecto está planificada para [fecha].

## Organización del proyecto

### Promotor del proyecto

A todos los proyectos se les asigna un "promotor" que no participa activamente en el proyecto. El patrocinador del proyecto debe ser informado regularmente por el responsable sobre el estado del proyecto, e intervenir su el proyecto es interrumpido.

[Nombre, cargo] ha sido nombrado patrocinador.

### Gerente del proyecto

La función del gerente del proyecto es asegurar los recursos necesarios para llevar a cabo la implementación del proyecto, coordinar el proyecto, informar al promotor del progreso, y realizar el trabajo administrativo relacionado con el proyecto. El responsable del proyecto debe asegurar la implementación ininterrumpida del proyecto dentro de los plazos establecidos.

[Nombre, cargo] ha sido nombrado responsable del proyecto.

### Equipo del proyecto

La función del equipo del proyecto es ayudar en diversos aspectos de la implementación del proyecto, realizar las tareas que se especifican en el proyecto y tomar decisiones sobre diversos asuntos que requieren un enfoque multidisciplinario. El equipo del proyecto se reúne siempre antes de que se complete la versión final de un documento de la sección 2 de este Plan del Proyecto, y en todos los demás casos, cuando el gerente del proyecto lo considere necesario

*Tabla de participantes en el proyecto*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Nombre* | *Unidad de la organización* | *Puesto* | *Teléfono* | *E-mail* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Principales riesgos del proyecto

Los principales riesgos en la implementación del proyecto son los siguientes:

1. Extensión de los plazos.
2. Realización de actividades que incurran en costes innecesarios y pérdida de tiempo.
3. Escasez o falta de empleados competentes (ej. un DPO).

Algunas medidas para reducir los riesgos mencionados anteriormente son las siguientes:

* El gerente del proyecto supervisa que todas las actividades del proyecto sean realizadas dentro de los plazos definidos y solicita a tiempo la intervención del promotor del proyecto.
* Contratación de un consultor que asegure que los tiempos y los recursos no sean utilizados en actividades que no son importantes para el proyecto y que las actividades individuales no sean encaminadas en una dirección incorrecta.
* Contratación de un experto en protección de datos que proponga las actividades más apropiadas.

## Herramientas para la implementación del proyecto y realización de informes

Se creará, en la red local, una carpeta compartida que incluya todos los documentos generados durante el proyecto. Todos los miembros del equipo del proyecto tendrán acceso a esos documentos. Sólo el gerente del proyecto [y miembros del equipo del proyecto] estarán autorizados a realizar modificaciones y a borrar archivos.

El gerente del proyecto preparará un informe de implementación del proyecto mensualmente y lo enviará al promotor del proyecto.

# Gestión de registros guardados en base a este documento

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nombre del registro | Ubicación | Persona responsable de su almacenamiento | Control para la protección del registro | Tiempo de retención |
| Informe del proyecto de implementación (en formato electrónico) | Carpeta compartida para actividades relacionadas con el proyecto | Gerente del proyecto | Sólo el gerente del proyecto está autorizado a editar datos | El informe es almacenado durante un periodo de 3 años |

# Validez y gestión de documentos

Este documento es válido a partir de [fecha].

El propietario de este documento es [cargo].

[cargo]

[nombre]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[firma]