MÁSTER UNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES (INTERUNIVERSITARIO: UOC, UAB, URV, UIB)

# EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

**NOMBRE DEL ESTUDIANTE:** ELADIO CORTIZAS DE CASTRO

**NOMBRE DEL PROFESOR/A COLABORADOR/A:** ANTONIO JOSÉ SEGOVIA HENARES

**NOMBRE DEL PROFESOR/A:** CARLES GARRIGUES OLIVELLA


**FECHA:** 5 DE JUNIO DE 2019

# ÍNDICE

- Justificación del TFM
- Alcance
- Objetivos
- Planificación del trabajo
- Metodología de Evaluación de Impacto relativa a la Protección de Datos (EIPD)
  - Identificación del tratamiento
  - Descripción del tratamiento
  - Análisis de la necesidad de realizar una EIPD
  - Descripción sistemática del tratamiento
  - Necesidad y proporcionalidad del tratamiento
  - Legitimación del tratamiento
  - Análisis de Riesgos de los derechos y libertades fundamentales de las personas físicas
  - Informe EIPD
  - Revisión EIPD

# JUSTIFICACIÓN DEL TFM

- Actualmente estamos en una etapa de novedades legales en el ámbito de la protección de datos, donde surgen nuevas obligaciones en la materia. Entre ellas las Evaluaciones de Impacto relativas a la Protección de Datos. Estas buscan garantizar los derechos y libertades de las personas.
- Vemos la necesidad, para los responsables de privacidad en general, de ampliar conocimientos sobre las Evaluaciones de Impacto relativas a la Protección de Datos. Consideramos que hay poca información disponible al ser un campo nuevo en la legislación española.

# ALCANCE

La metodología va a contener una descripción de las actividades que deben desarrollarse, de qué manera (metodología) y con qué resultado (finalidad).

Será de aplicación mayoritariamente para las Pymes españolas.

# OBJETIVOS

Objetivo general.

- Desarrollar una metodología de Evaluaciones de Impacto relativas a la Protección de Datos (EIPD).

Objetivos específicos.

- Transmitir la necesidad de realizar las EIPD.
- Proporcionar instrumentos útiles para implementar la EIPD.
- Facilitar documentación para la realización de Análisis de Riesgos.
- Proponer un listado de riesgos o amenazas.
- Desarrollar la metodología de evaluación de riesgos.
- Ofrecer medidas de mitigación de riesgos.
- Presentar un modelo de informe de EIPD.

# PLANIFICACIÓN DEL TRABAJO

01

Parte 1

Alcance, datos personales, introducción RGPD

02

Parte 2

Desarrollo de la metodología de EIPD

03

Parte 3

Realización de una EIPD

04

Parte 4

Tratamientos de Riesgos. Reducción riesgo

05

Parte 5

Revisión EIPD
Breve auditoría

# EVALUACIÓN DE IMPACTO (EIPD)

- **Evaluación de impacto:** El cálculo o estimación de los efectos que un conjunto de acciones puede provocar antes, durante o después.
- **Evaluación de impacto relativa a la protección de datos:** Antes de ponernos a tratar datos personales hagamos una reflexión sobre sus consecuencias. Esta reflexión será mediante una metodología sistemática, repetible y documentada.

La EIPD también se puede emplear como instrumento de rendición de cuentas para cumplir los requisitos del RGPD.

# METODOLOGÍA DE EIPD

Consultas a las partes interesadas, si es preciso, a lo largo del proceso (DPD, Interesados afectados, AEPD,…)

# IDENTIFICACIÓN DEL TRATAMIENTO

Debemos determinar la denominación del tratamiento (el título)

# DESCRIPCIÓN DEL TRATAMIENTO

Fijar los objetivos perseguidos con el tratamiento. La revisión de dichos objetivos nos permitirá detectar las finalidades que persigue el tratamiento.

# ANÁLISIS DE LA NECESIDAD

Análisis de la necesidad de la EIPD o la evaluación objetiva.

Consisten en precalificar el riesgo en base a criterios planteados por las autoridades de control y el RGPD.

# DESCRIPCIÓN SISTEMÁTICA

Descripción sistemática del tratamiento.

Ciclo de vida de los datos

- Partes que intervienen: interesados, responsables del tratamiento, encargados del tratamiento, trabajadores, y terceras partes
- Tipos de datos
- Operaciones de tratamiento
- Medios tecnológicos

# NECESIDAD Y PROPORCIONALIDAD

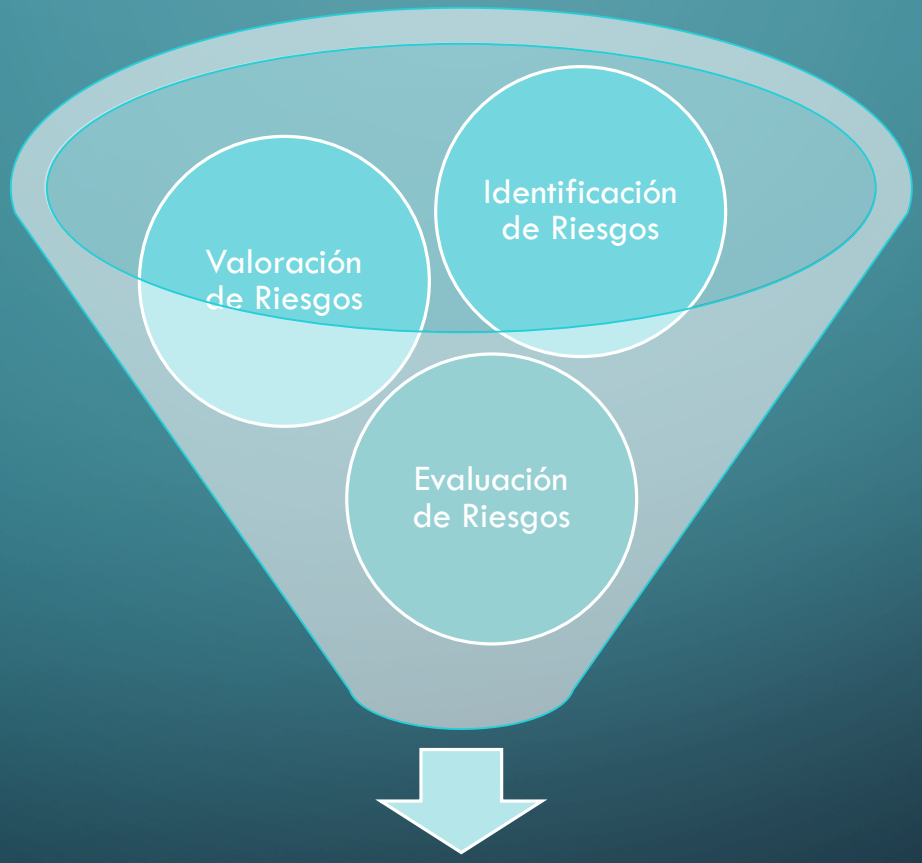
- **Necesidad del tratamiento:** solo se tratarán datos personales si su finalidad no puede alcanzarse “razonablemente” por otros medios.

- **Proporcionalidad del tratamiento:** La finalidad no pueda obtenerse mediante otros medios que resulten menos intrusivos.

# LEGITIMACIÓN DEL TRATAMIENTO

- Supuestos de licitud o bases legitimadoras del artículo 6.1 del RGPD
- Excepciones de las previstas en el artículo 9.2 del RGPD

# ANÁLISIS DE RIESGOS

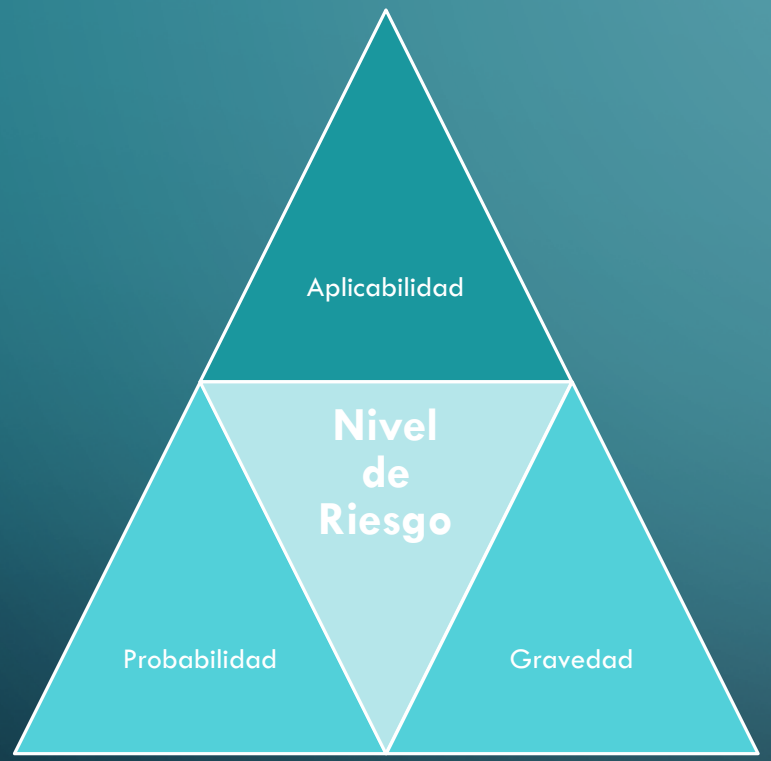



Tratamiento de Riesgos

# IDENTIFICACIÓN DE RIESGOS

- Listado de riesgos ya establecidos.
- Lista de comprobación

# VALORACIÓN DE RIESGOS



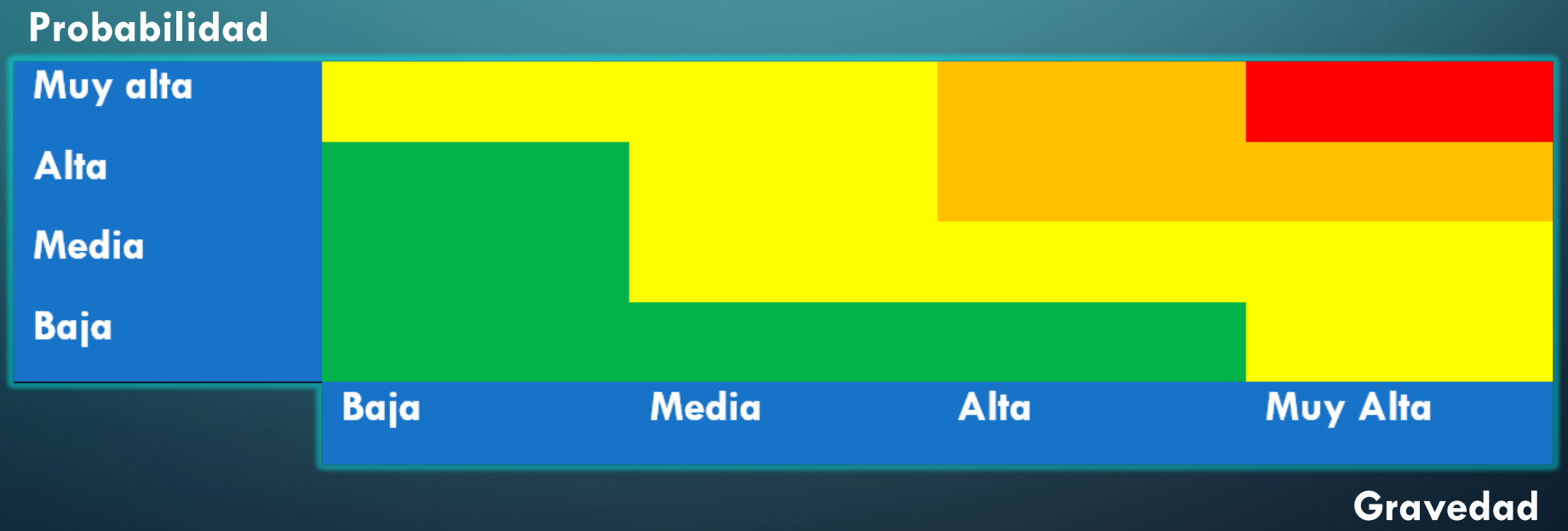

Para cada riesgo determinaremos

- Aplicabilidad
- Probabilidad
- Gravedad

Obteniendo su nivel de riesgo

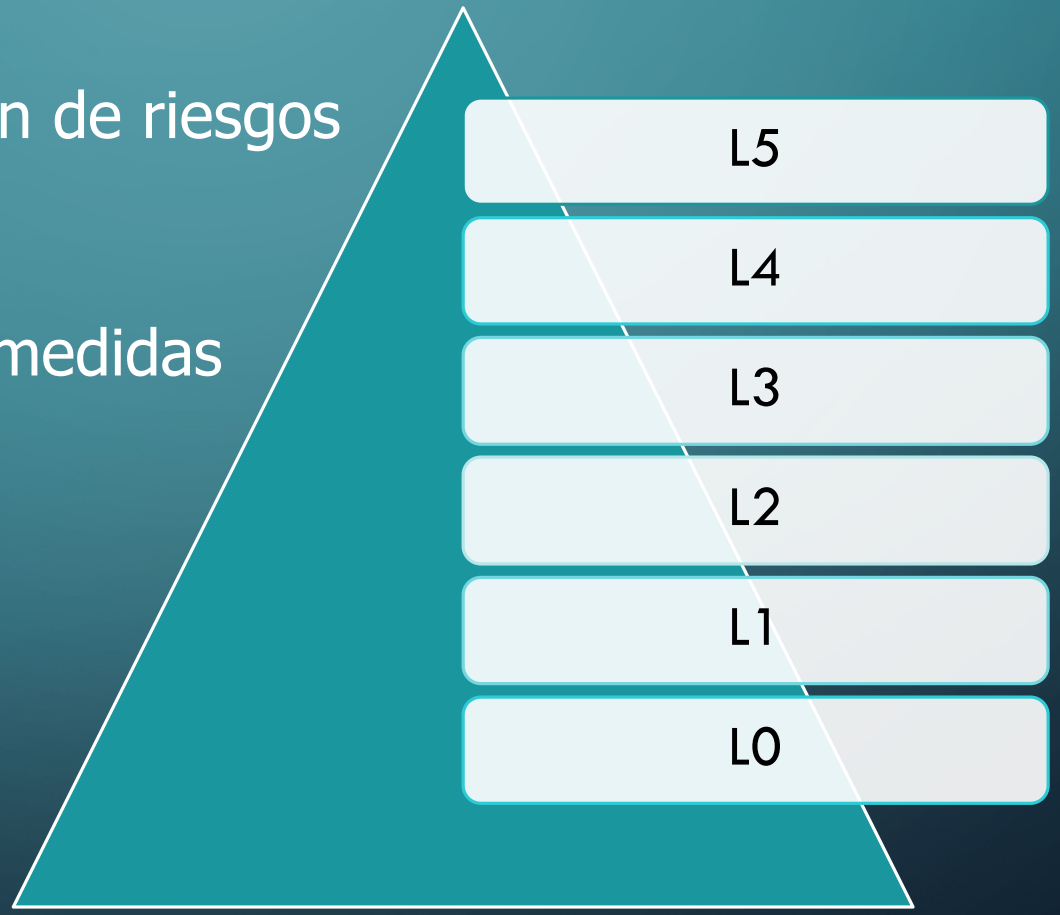
# EVALUACIÓN DE RIESGOS

Estimación del nivel de riesgo y priorización de riesgos a través de un mapa de calor



# TRATAMIENTO DE RIESGOS

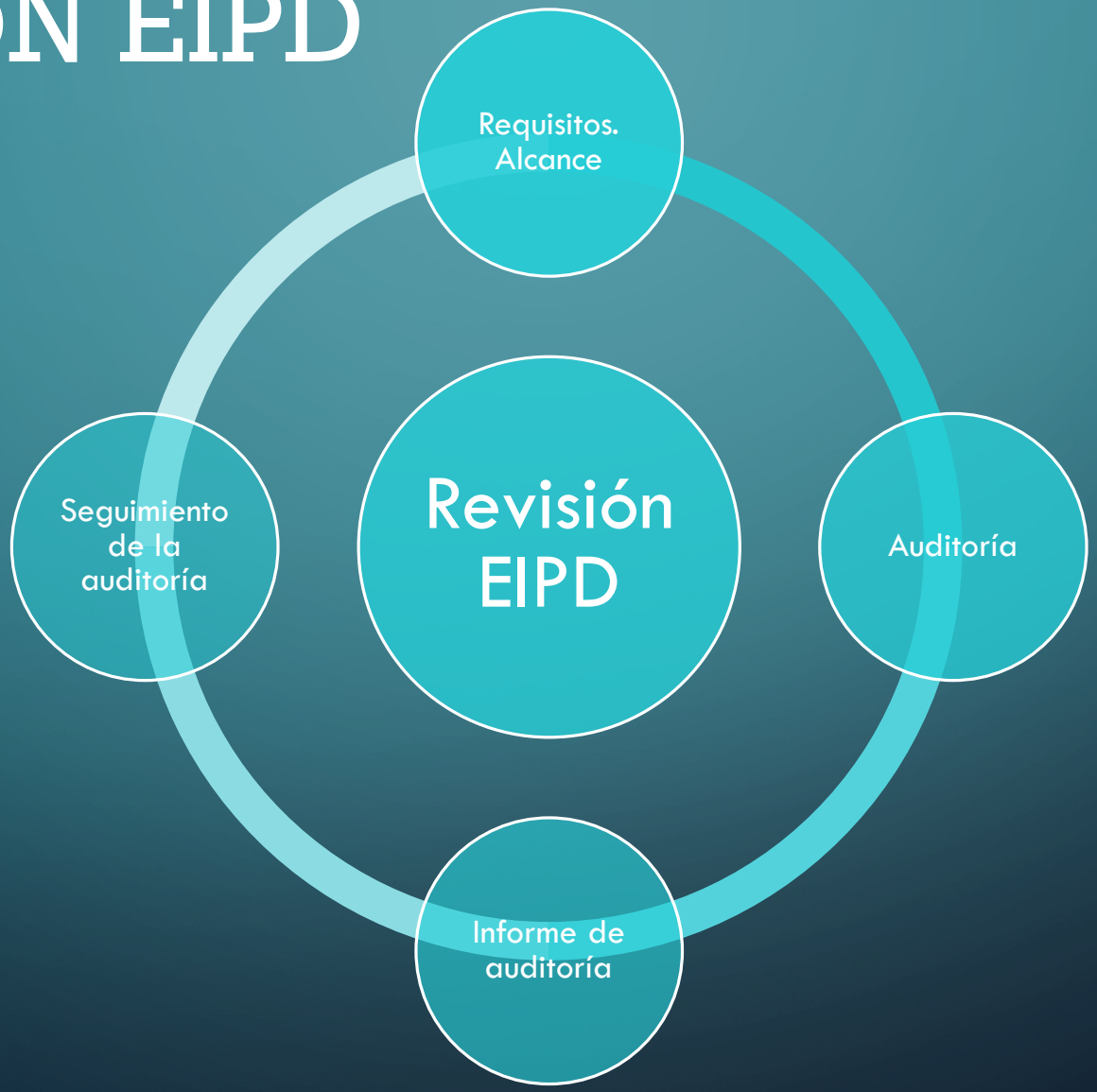
- Plan de acción de mitigación de riesgos
- Niveles de madurez de las medidas
- Riesgo Residual



# INFORME EIPD

**Documentación de todo el proceso**

# REVISIÓN EIPD



# CASO PRÁCTICO

| Tratamiento recursos humanos | |
|---|---|
| Riesgo residual bajo | No conformidad subsanable |

| Tratamientos gestión de pacientes | |
|---|---|
| Riesgo residual medio | No conformidad subsanable |

| Tratamiento formación | |
|---|---|
| Riesgo residual bajo | No conformidad subsanable |

# CONCLUSIONES

Esta metodología de Evaluación de Impacto relativa a la Protección de Datos podrá servir de ejemplo ilustrativo y didáctico para pequeñas y medianas empresas, a modo de guía o recomendación para todo el proceso.

El objetivo general que nos propusimos consistió en desarrollar una metodología sencilla de Evaluaciones de Impacto relativas a la Protección de Datos (EIPD). Creemos que lo hemos conseguido.

# MUCHAS GRACIAS