# ÍNDICE:

## 1.- Descripción de la tarea.

# Caso práctico

isftic. *Antena de Telecomunicaciones* (CC BY-NC-SA)

La compañía ACME S.A. se encarga de proveer servicios de telecomunicaciones enfocados en comunicaciones internacionales tanto a particulares como a empresas.

ACME tiene una cartera de 300.000 clientes en España a los que ofrece estos servicios y por los cuales cobra una tarifa media de 23,5 € mensuales.

ACME está presente en 32 países, y se aprovecha de esta situación para dar servicio a multinacionales. Durante el año 2022 ACME ha logrado adjudicarse el servicio de telecomunicaciones de todas las embajadas en España.

Uno de sus clientes multinacionales es una entidad bancaria, con un nivel de madurez en seguridad elevado, uno de los requisitos que establece es la certificación ISO27001 en los servicios de comunicaciones.

La sede central de ACME se encuentra en Madrid, fue abierta en el año 2020, sus oficinas cuentan con climatización inteligente, jardines en las azoteas para mejorar la climatización y aprovechar el agua de la lluvia para los riegos de sus zonas verdes y paneles solares para mejorar la eficiencia energética.

Además, parte de los terrenos de la organización, han sido convertidos en parques públicos que pueden ser utilizados por los residentes de la zona, y los accesos por carretera a la zona han sido acondicionados, mejorados y reasfaltados.

Dada su cartera de clientes, ACME es responsable de la información de su cartera de 300.000 clientes, de los cuales maneja diversos datos como pueden ser, datos identificativos, de residencia, bancarios, de trafico de llamadas, etc... con diferentes sensibilidades. Existen dos regulaciones cuyo objetivo es la protección de los datos personales de los individuales, la Regulación General de Protección de Datos (GDPR) y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPD- GDD).

# ¿Qué te pedimos que hagas?

**Teniendo en cuenta la compañía descrita en el escenario anterior, da respuesta a las siguientes preguntas:**

**Apartado 1: Principios de protección de datos.**

*Enumera 10 datos de carácter personal que trate ACME en la prestación de sus servicios.*

Los datos personales son según hemos visto en el temario "cualquier información relativa a una persona física identificada o identificable". Y por ello ACME trata los siguientes datos:

1. Nombre y Apellidos: Para identificación, facturación y personalización del servicio.
2. Domicilio: Necesario para la prestación del servicio, facturación y cumplimiento legal.
3. Dirección de Correo Electrónico (personal): Comunicación, gestión de cuenta y marketing (si hay consentimiento) Hay que tener en cuenta que una dirección genérica como info@acme.com no se considera dato personal.
4. El Documento Nacional de Identidad (DNI): Se utilizará para la identificación del cliente y cumplimiento de obligaciones legales.
5. El número de teléfono personal: el cual se usa para la prestación del servicio de telecomunicaciones y soporte al cliente.
6. Datos Bancarios (Número de Cuenta, IBAN): Procesamiento de pagos por los servicios.
7. Datos de Tráfico de Llamadas (Duración, Origen, Destino): Facturación, optimización de la red y cumplimiento legal (ej: registros de llamadas).
8. Dirección IP: Seguridad de la red, resolución de problemas y, con consentimiento, publicidad dirigida.
9. Datos de Geolocalización (si ofrece servicios basados en ubicación): Servicios basados en la ubicación y marketing.
10. Identificador de Cookie: Seguimiento de la actividad online del usuario (con consentimiento).

### *¿Alguno de los datos enumerados es sensible?*

Los datos sensibles son origen racial, ideología política, religión o creencias, afiliación sindical, datos relativos a la salud, datos relativos a la vida sexual u orientaciones sexuales, datos genéticos y biométricos.

Aunque ACME no trata estos datos directamente, a partir de los datos de tráfico de llamadas o geolocalización podría revelar información sensible. Por ejemplo, si un cliente llama con frecuencia a un centro de salud mental, podría inferirse información sobre su salud.

## Apartado 2: Regulación General de Protección de Datos.

### *¿Bajo qué escenarios se podría legitimar ACME en el tratamiento de datos de sus clientes?*

ACME solo se podrá realizar un tratamiento legitimo de los datos de sus clientes bajo los siguientes escenarios:

1. **Consentimiento explícito**:
   - Ejemplo: ACME pide autorización para usar datos de geolocalización para optimizar la cobertura de red.
2. **Ejecución de un contrato**:
   - Ejemplo: Procesar datos bancarios para cobrar la tarifa mensual acordada en el contrato de servicios.
3. **Cumplimiento de una obligación legal**:
   - Ejemplo: Conservar registros de tráfico de llamadas durante 12 meses, como exige la Ley de Telecomunicaciones.
4. **Intereses legítimos del responsable**:
   - Ejemplo: Analizar patrones de uso para detectar fraudes (siempre que se prioricen los derechos del cliente).
5. **Protección de intereses vitales**:
   - Ejemplo: Usar datos de ubicación para localizar a un cliente en una emergencia (ej: llamada al 112).
6. **Interés público o ejercicio de poderes oficiales**:
   - Ejemplo: Compartir datos con autoridades judiciales bajo una orden legal (ej: investigación de delitos).

### *Indica al menos un ejemplo de cada figura de tratamiento de datos.*

Para ilustrar las diferentes figuras en el tratamiento de datos, y en el contexto de ACME:

1. **Interesado (Propietario de los datos):**

Un cliente individual, como Laura Martínez, que contrata el servicio y proporciona su DNI y dirección.

2. **Responsable del Tratamiento (Controlador):**

ACME S.A., quien decide qué datos recopilar, cómo usarlos y con qué finalidad (ej: facturación, soporte técnico)..

3. **Encargado del Tratamiento (Procesador):**

Empresa externalizada de call center en Valladolid, que gestiona consultas de clientes siguiendo instrucciones de ACME.

*Indica tres actividades de tratamiento que estén llevadas a cabo por ACME.*

ACME realiza numerosas actividades de tratamiento de datos personales. Aquí hay tres ejemplos clave:

1. **Recopilación y almacenamiento de datos identificativos** (nombre, DNI, dirección) para crear perfiles de cliente.
2. **Procesamiento de datos bancarios** para cobros mensuales automatizados.
3. **Transferencia de datos de tráfico de llamadas** a autoridades, bajo requerimiento legal.

## Apartado 3: Análisis de impacto en privacidad.

*Realiza un análisis de impacto de las tres actividades de tratamiento descritas en el apartado anterior.*

ACME, dada la naturaleza de sus actividades de tratamiento de datos, debería realizar un Análisis de Impacto en la Privacidad (AIP) para evaluar y mitigar los riesgos para la privacidad asociados con estas actividades. A continuación, se presenta un análisis de impacto para cada una de las tres actividades identificadas anteriormente:

### 1. Actividad: Procesamiento de datos bancarios para cobros mensuales

- **Riesgos identificados**:
  - **Acceso no autorizado**: Hackers podrían robar datos bancarios y realizar cargos fraudulentos.
  - **Error en el procesamiento**: Fallos técnicos podrían generar cobros erróneos.

- **Medidas de mitigación**:
  - **Cifrado de extremo a extremo** en transacciones financieras.
  - **Autenticación multifactor** para acceder a sistemas de pago.
  - **Auditorías mensuales** para verificar la exactitud de los cobros.

**2. Actividad: Almacenamiento de registros de tráfico de llamadas**

- **Riesgos identificados**:
  - **Vigilancia masiva**: Los registros podrían usarse para perfilar hábitos de comunicación de clientes.
  - **Fuga de datos**: Empleados internos podrían acceder a registros sin autorización.
- **Medidas de mitigación**:
  - **Anonimización** de datos después de 6 meses (cumpliendo el mínimo legal).
  - **Control de acceso basado en roles**: Solo el departamento legal puede acceder a registros completos.
  - **Monitorización en tiempo real** con herramientas SIEM para detectar accesos sospechosos.

**3. Actividad: Transferencia de datos a la entidad bancaria cliente (multinacional)**

- **Riesgos identificados**:
  - **Transferencia insegura**: Si la entidad bancaria opera en un país sin adecuación al RGPD (ej: Estados Unidos), hay riesgo de exposición.
  - **Uso indebido**: La entidad bancaria podría usar los datos para fines no autorizados (ej: publicidad).
- **Medidas de mitigación**:
  - **Cláusulas Contractuales Tipo (CCT)** para garantizar cumplimiento del RGPD en transferencias internacionales.
  - **Evaluación previa de seguridad** de la entidad bancaria (ej: verificar certificación ISO27001).
  - **Acuerdos de confidencialidad** que limiten el uso de datos a lo estrictamente necesario.

# Bibliografía:

Temario de la asignatura.