



TAREA 04

**LEGISLACIÓN Y
JURISPRUDENCIA EN
MATERIA DE
PROTECCIÓN DE DATOS**

NORMATIVA DE CIBERSEGURIDAD

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

Caso práctico

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 riego 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 tráfico 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).

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.

Datos de carácter personal que trata ACME:

1. Nombre y apellidos
2. Dirección de residencia del cliente
3. Número de teléfono
4. Dirección de correo electrónico
5. Número de identificación (DNI / NIE)
6. Datos bancarios
7. Datos de localización
8. Datos de facturación
9. Dirección IP
10. Historial de llamadas realizadas

¿Alguno de los datos enumerados es sensible?

Algunos de los datos anteriormente enumerados son de carácter sensible, como los datos bancarios o los datos de localización, debido a su naturaleza y el potencial impacto en la privacidad de los individuos si se divulgan o se utilizan de manera indebida. Estos requerirán de protección adicional debido a ser datos con mayor sensibilidad que el resto.

Apartado 2: Regulación General de Protección de Datos.

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

La empresa ACME puede legitimar el tratamiento de datos de sus clientes bajo varios escenarios, de acuerdo con el Reglamento General de Protección de Datos (RGPD).

1. ACME puede tratar los datos personales si obtiene el consentimiento explícito de los clientes para fines específicos. Este consentimiento debe ser libre, específico e informado.

2. El tratamiento de esos datos es legítimo si es necesario para la ejecución de un contrato en el que el cliente es parte, como por ejemplo para poder proporcionarles la prestación de servicios de telecomunicaciones.

3. La empresa puede tratar datos personales para cumplir con las obligaciones legales, como la facturación y el pago de impuestos.

4. Puede tratar datos personales si tiene un interés legítimo que no prevalezca sobre los derechos y libertades del cliente, como los datos de navegación en su sitio web.

5. En situaciones de emergencia, ACME puede tratar datos personales para proteger los intereses vitales (vida) del cliente o de otra persona física.

6. La empresa puede tratar los datos de forma legítima cuando es necesario para el cumplimiento de alguna actividad de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (ACME).

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

- Responsable del tratamiento de datos o controlador: es la entidad que decide los fines y los medios de tratamiento de los datos personales de sus clientes.

La empresa ACME S.A., decide recopilar y almacenar datos de contacto de sus clientes para gestionar sus cuentas y proporcionar soporte técnico.

La organización determina cómo se utilizarán los datos de tráfico de llamadas para analizar patrones de uso y mejorar sus servicios.

- Encargado de tratamiento o procesador: en la entidad que trata los datos personales por cuenta del responsable del tratamiento.

Una empresa de call center contratada por ACME que se dedica a gestionar las llamadas de atención al cliente y dar soporte.

Una empresa de servicios de facturación contratada por ACME para procesar los pagos de los clientes.

- Propietario de los datos / Interesado: la persona física titular de los datos personales.

Un cliente de la empresa que proporciona sus datos personales para obtener los servicios de telecomunicaciones.

Un empleado de ACME que comparte sus datos para la gestión de su contrato laboral.

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

1. Gestión de contratos y facturación,

ACME recopila y almacena datos personales de facturación y datos bancarios para emitir y gestionar correctamente las facturas mensuales de los clientes. Al suscribirse a los servicios de la organización, los clientes facilitan sus datos bancarios y de contacto, que son almacenados y utilizados para enviar las facturas mensuales.

2. Atención al cliente,

La empresa utiliza datos personales, como datos de contacto e historial de llamadas para resolver consultas y problemas técnicos de los clientes. Cuando un cliente contacta con el servicio de atención al cliente de ACME para resolver un problema técnico, la empresa accede al historial de llamadas y datos del cliente para ofrecer una solución adecuada.

3. Marketing y promociones,

ACME trata datos personales, como datos de contacto y preferencias del cliente, para enviar ofertas promocionales y campañas de marketing. Se envían correos electrónicos a los clientes con ofertas especiales basadas en sus preferencias y patrones de uso de los servicios.

Apartado 3: Análisis de impacto en privacidad.

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

- Gestión de facturación,

Riesgos: la recopilación y almacenamiento de datos bancarios y de facturación conlleva riesgos significativos, como los posibles accesos no autorizados, la pérdida de datos y el uso indebido de la información financiera. Estos riesgos pueden resultar en fraudes financieros y pérdida de confianza por parte de los clientes.

Medidas de mitigación: para minimizar estos riesgos, ACME debe implementar medidas de seguridad robustas, como la encriptación de datos, controles de acceso estrictos (doble autenticación) y auditorías regulares. Además, es crucial que la empresa cumpla con las normativas de protección de datos, con el RGPD y que informe a los clientes sobre cómo utilizar y proteger sus datos personales.

- Atención al cliente,

Riesgos: el tratamiento de datos de contacto e historial de llamadas puede exponer información sensible sobre las comunicaciones y preferencias de los clientes. Existe el riesgo de que estos datos sean accedidos por personas no autorizadas o utilizados de manera indebida lo que podría comprometer la privacidad de los clientes.

Medidas de mitigación: debe asegurar que sólo el personal autorizado tenga acceso a estos datos y que se utilicen únicamente para los fines previstos. La implementación de políticas de privacidad claras, la capacitación del personal empleado en protección de datos y el uso de tecnologías de seguridad, como la encriptación y el monitoreo continuo, son esenciales para proteger la privacidad de los clientes.

- Marketing y promociones,

Riesgos: el uso de datos personales para marketing puede ser intrusivo si no se gestiona adecuadamente. Los clientes pueden sentirse invadidos si reciben comunicaciones no deseadas o si sus datos se utilizan sin su consentimiento. Además, existe el riesgo de que los datos sean compartidos con terceros sin el conocimiento o consentimiento de los clientes.

Medidas de mitigación: me debe obtener el consentimiento explícito de los clientes antes de utilizar sus datos para fines de marketing. Es importante que las políticas de privacidad sean transparentes y que los clientes tengan la opción de optar por no recibir comunicaciones promocionales. Además, la empresa debe garantizar que los datos se almacenen de forma segura y que no se compartan con terceros sin el consentimiento del cliente.