TAREA 03

LEGISLACIÓN PARA EL CUMPLIMIENTO DE LA RESPONSABILIDAD PENAL

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 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.
La dirección de la organización es consciente de que es sujeto obligado para multitud de leyes y normativas. Tras el sistema de gestión de compliance desarrollado en semanas anteriores, ahora la preocupación esta enfocada en los riesgos penales, ya que uno de los principales competidores se ha visto envuelto en un escándalo de escuchas y ha sido objeto de sanciones penales considerables.

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

Apartado 1: Cumplimiento de la responsabilidad penal.
¿Podrías identificar 10 delitos en los que pueda incurrir ACME?

1. Estafa y fraude, en caso de que la empresa prometa un servicio que no cumpla, engañando al cliente (por ejemplo, a través de publicidad engañosa).
2. Cohecho: ofrecer sobornos a funcionarios públicos para obtener contratos o ventajas.
3. Delitos contra la Hacienda Pública y la Seguridad Social: no pagar los impuestos correspondientes o falsificar cuentas.
4. Insolvencias punibles: ocultar activos o realizar operaciones fraudulentas para evitar pagar.
5. Blanqueo de capitales: participar en actividades para ocultar el origen ilegal de fondos.
6. Delitos contra los derechos de los trabajadores: no cumplir con las normativas laborales, como el pago de salarios o la seguridad en el trabajo.
7. Tráfico de influencias: utilizar la posición de la empresa para influir en decisiones de funcionarios públicos.
8. Delitos contra la intimidad, allanamiento y otros delitos informáticos: interceptar o escuchar comunicaciones privadas sin autorización (importante al trabajar con embajadas).
9. Delitos contra la propiedad intelectual e industrial, el mercado y los consumidores: Utilizar tecnología o software sin licencia adecuada, podría considerarse una negligencia en la seguridad.
10. Delitos contra el medio ambiente: No gestionar adecuadamente los residuos o contaminar el entorno.

¿Podrías elaborar una matriz de riesgo penal de la organización?

Probabilidad / Impacto	1	2	3	4	5
5		Cohecho Blanqueo capitales		Delitos contra intimidad	
4		Delitos contra Hacienda Pública Insolvencias punibles	Delito contra trabajadores Tráfico de influencias	Estafa y fraude Delito contra propiedad intelectual	
3	Delito contra medio ambiente				
2					
1					

Dado el tipo de empresa que es ACME SA, es probable que ya tenga implantadas las medidas necesarias para que la probabilidad de estos delitos se mantenga en niveles moderados. Por eso, algunos de los delitos tienen una probabilidad moderada de ocurrir, su impacto en la empresa sería alto debido a las graves consecuencias legales y reputacionales.

- Estafa y fraude

  Probabilidad: Alta (4) la empresa maneja una gran cantidad de clientes y servicios, lo que aumenta el riesgo de promesas incumplidas o publicidad engañosa.

  Impacto: Alto (4) las consecuencias pueden incluir sanciones legales, pérdida de reputación y confianza del cliente pero no necesariamente devastadoras.

- Cohecho

  Probabilidad: Media (2) aunque es menos probable, la obtención de contratos con embajadas y multinacionales puede llevar a intentos de soborno.

  Impacto: Alto (5) las sanciones por cohecho son severas y pueden incluir multas significativas y penas de prisión, además de dañar gravemente la reputación de la empresa.

- Delitos contra la Hacienda Pública y la Seguridad Social

  Probabilidad: Baja (2) la empresa debe cumplir con numerosas obligaciones fiscales y aunque es menos probable, cualquier incumplimiento podría ocurrir.

  Impacto: Alto (4) las consecuencias de no pagar impuestos o falsificar cuentas pueden incluir multas, sanciones legales y daños en la reputación.

- Insolvencias punibles

  Probabilidad: Baja (2) la ocultación de activos u operaciones fraudulentas para evitar pagos es un riesgo, aunque menos probable.

  Impacto: Alto (4) las consecuencias son graves, suponiendo sanciones legales y pérdida de credibilidad ante los inversores y clientes.

- Blanqueo de capitales

  Probabilidad: Bajo (2) aunque es poco probable, la empresa podría ser utilizada para ocultar fondos ilegales debido a su presencia internacional.

  Impacto: Muy alto (5) las sanciones que corresponden al blanqueo de capitales son severas y pueden incluir multas significativas y penas de prisión.

- Delitos contra los derechos de los trabajadores

Probabilidad: Media (3) con una gran cantidad de empleados y posibles subcontratados, el riesgo de incumplimientos laborales es significativo.

Impacto: Alto (4) las consecuencias pueden incluir multas, sanciones y daños reputacionales, además afectar a la moral de los empleados.

- Tráfico de influencias

Probabilidad: Media (3) la empresa podría utilizar su posición para influir en decisiones de funcionarios públicos.

Impacto: Alto (4) las sanciones por este tipo de delito pueden ser severas y dañar la reputación de la empresa.

- Delitos contra la intimidad, allanamiento y otros delitos informáticos

Probabilidad: Alta (4) trabajando con embajadas y multinacionales, la interceptación de comunicaciones privadas sin autorización es un riesgo significativo.

Impacto: Muy alto (5) las consecuencias pueden ser devastadoras, incluyendo sanciones legales, pérdida de confianza y daños en la reputación de la empresa

- Delitos contra la propiedad intelectual e industrial, el mercado y los consumidores

Probabilidad: Alto (4) el uso de tecnologías sin licencia adecuada o la seguridad necesaria, puede ocurrir, sobre todo en entornos tecnológicos avanzados.

Impacto: Alto (4) las consecuencias pueden incluir multas, sanciones y puede desembocar en posibles ciberataques y pérdida de datos, especialmente al trabajar con embajadas y organismos importantes.

- Delito contra el medio ambiente

Probabilidad: Media (1) la empresa tiene prácticas sostenibles, pero siempre existe el riesgo de incumplimientos ambientales.

Impacto: Medio (3) las consecuencias pueden incluir multas y sanciones, aunque el impacto será menor en comparación con otros delitos.

Aunque la probabilidad de que ocurran alguno de estos delitos sea moderada. ACME S.A. debe continuar fortaleciendo las medidas preventivas para mitigar los riesgos y proteger su reputación y estabilidad en el mercado.

Apartado 2: Sistema de gestión de compliance penal. Propón al menos una acción mitigante por cada riesgo identificado.

1. Estafa y fraude

Implementar controles internos rigurosos y auditorías periódicas para asegurar que los servicios prometidos se cumplan y que la publicidad sea acorde con lo que ofrece la empresa. Además, añadir un buzón de denuncias para que empleados y clientes reporten las irregularidades.

2. Cohecho

Desarrollar un código ético y de conducta que prohíba este tipo de acciones (sobornos). Realizar conferencias sobre ética y cumplimiento, para que los empleados se conciencien sobre el tema.

3. Delitos contra la Hacienda Pública y la Seguridad Social

Implementar un sistema de gestión fiscal que asegure el cumplimiento de las obligaciones tributarias y de seguridad social. Realizar auditorías fiscales internas y externas periódicamente.

4. Insolvencias punibles

Mantener una contabilidad transparente y precisa. realizar auditorías financieras regulares y establecer políticas claras para la gestión de ingresos (activos y pasivos).

5. Blanqueo de capitales

Implementar un programa de cumplimiento para evitar el lavado de dinero que incluya el debido cuidado del cliente (KYC: Know your customer), monitorear las transacciones y reportar las actividades sospechosas

6. Delitos contra los derechos de los trabajadores

Asegurar el cumplimiento de todas las normativas laborales mediante auditorías regulares y hacer a los empleados conscientes de sus derechos laborales. Establecer un buzón de denuncias para que puedan reportar violaciones de sus derechos.

7. Tráfico de influencias

Implementar políticas de transparencia en los procesos de contratación y toma de decisiones. Realizar capacitaciones sobre ética y conflictos de interés para los empleados.

8. Delitos contra la intimidad, allanamiento y otros delitos informáticos

Implementar medidas de seguridad cibernética, incluyendo encriptación de datos y monitoreo de redes. Enseñar a los usuarios sobre protección de datos y privacidad.

9. Delitos contra la propiedad intelectual e industrial, el mercado y los consumidores

Asegurar que todos los softwares y tecnologías utilizadas estén debidamente licenciados, realizar auditorías de cumplimiento y de seguridad, capacitar a los empleados sobre la importancia de respetar la propiedad intelectual para evitar este delito.

10. Delitos contra el medio ambiente

Implementar un sistema de gestión ambiental que incluya la evaluación del impacto ambiental de la empresa, la gestión adecuada de residuos. Realizar auditorías ambientales para hacer un seguimiento.

Apartado 3: Sistema de gestión antisoborno y anticorrupción.

Identifica al menos 3 riesgos en el entorno de ACME relacionados con el soborno y la corrupción.

- Sobornos para obtener contratos gubernamentales, ACME podría verse tentada a ofrecer sobornos a funcionarios públicos para asegurar contratos lucrativos, especialmente al trabajar con embajadas y organismos gubernamentales. Un ejemplo podría ser ofrecer pagos a funcionarios para ganar contratos de telecomunicaciones con embajadas.

La obtención de contratos gubernamentales es altamente competitiva y lucrativa, lo que puede incentivar prácticas corruptas para asegurar estos contratos.

- Corrupción a través de intermediarios, los intermediarios o agentes contratados por ACME podrían involucrarse en prácticas corruptas, como pagar sobornos en nombre de la empresa para obtener algún tipo de ventaja comercial.

El uso de intermediarios puede dificultar el control directo de las prácticas comerciales, aumentando el riesgo de corrupción.

- Fondos de soborno ocultos, la creación de fondos de soborno que no están registrados (cajas negras) para financiar sobornos y pagos indebidos a empleados de otras empresas o funcionarios.

La existencia de fondos no registrados facilita la realización de pagos corruptos sin ser detectados por los controles internos.

- Pagos o regalos para la facilitación, ofrecer favores, regalos, pagos u hospitalidad a clientes o funcionarios para acelerar o influir en sus decisiones y procesos administrativos.

Los pagos de facilitación son una forma común de corrupción que puede ser difícil de detectar pero que puede tener graves consecuencias legales y reputacionales.

Estos riesgos pueden tener graves consecuencias legales y reputacionales para la organización. Es crucial que la empresa implante un sistema de gestión antisoborno y anticorrupción robusto.