TAREA 02

DISEÑO DE SISTEMAS DE GESTIÓN DE CUMPLIMIENTO NORMATIVO

NORMATIVA DE CIBERSEGURIDAD

ALBA MOREJÓN GARCÍA

2024/2025

CETI - 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. Además de un código ético recientemente desarrollado, y compromisos adquiridos con sus últimos clientes. Todos estos requerimientos hacen que la mejor opción de gestionar la situación y satisfacer a todas las partes interesadas sea el despliegue de un sistema de gestión de compliance.

Un sistema de gestión compliance es un conjunto de medidas y procesos que una organización implementa para garantizar que sus operaciones cumplen todas las leyes, regulaciones y estándares éticos. Está basado en la norma internacional ISO 37301, este sistema ayuda a estructurar y gestionar el programa de cumplimiento de las empresas. Consta de varios elementos esenciales como las políticas y procedimientos, evaluación de riesgos, controles internos, capacitación y concienciación, monitoreo…
Objetivos:

- Garantizar que la empresa cumple con todas las normativas y leyes aplicables, evitando sanciones legales o multas.
- Ayudar a identificar, evaluar y mitigar riesgos en diferentes áreas de la organización.
- Reforzar la reputación de la empresa y generar confianza en los clientes, inversores y socios comerciales.
- Permitir que los empleados conozcan y cumplan sus responsabilidades de manera clara y eficiente.
- Ayudar a establecer una cultura organizacional basada en la ética y la integridad.

Este sistema no solo asegura el cumplimiento legal, sino que también promueve una cultura ética y responsable dentro de la organización.

Apartado 1: Entorno regulatorio de aplicación. ¿Podrías identificar tres leyes de aplicación para ACME?

1. Ley General de Telecomunicaciones (Ley 11/2022): Esta ley es fundamental para asegurar que la empresa ACME cumpla con los requisitos legales y técnicos necesarios para operar en el sector de las telecomunicaciones en España. Regula la prestación de servicios y el despliegue de redes lo cual es esencial para su operación.
2. Reglamento General de Protección de Datos (RGPD): Es una normativa europea de aplicación directa en España, regula la protección de los datos personales de los usuarios. ACME debe asegurarse de cumplir con los requisitos para proteger la privacidad de sus clientes y evitar sanciones, manteniendo así su confianza.
3. Ley de Seguridad de las Redes y Sistemas de Información (Ley 12/2018): Esta ley transpone la Directiva NIS(Network and Information Systems) de la Unión Europea. Establece medidas para garantizar un alto del nivel de seguridad de las redes y sistemas de información utilizados en la

prestación de servicios esenciales, como los de telecomunicación. Dado que ACME provee servicios a embajadas y otras entidades sensibles, esta ley es particularmente relevante para asegurar el alto nivel de seguridad

Otras leyes importantes:

- Ley de Protección de Infraestructuras Físicas (ley 8/2011): Esta ley establece medidas para la protección de infraestructuras críticas. Es relevante debido a que las telecomunicaciones son consideradas infraestructuras críticas, asegura que ACME implemente medidas para proteger estas infraestructuras de posibles amenazas.
- ISO 27001: Es un estándar internacional que exige que las empresas gestionen bien los riesgos relacionados con la seguridad de la información. Esta certificación es relevante para ACME porque uno de los clientes lo exige.
- Esquema Nacional de Seguridad (ENS): Aplicable si la empresa provee servicios a organismos públicos, como las embajadas. Asegura la protección de la información que gestiona y es cruzar para cumplir con los requisitos de seguridad del sector público.

Estas leyes son esenciales para que la empresa ACME opere de manera legal y ética garantizando la seguridad y privacidad de sus servicios de telecomunicaciones. Cada una de estas normativas tiene su importancia y puede ser prioritaria dependiendo del contexto específico de los servicios y clientes de la empresa ACME. La elección de cual aplicar primero puede depender de los riesgos específicos y las exigencias de sus clientes.

Fuentes: Boletín Oficial del Estado (BOE), Agencia Española de Protección de Datos (AEPD), Ministerio de Asuntos Económicos y Transformación Digital y Centro Criptológico Nacional (CNN).

Apartado 2: Análisis y gestión de riesgos

¿Podrías identificar tres riesgos de cumplimiento en el escenario de ACME, indicando una descripción del mismo, junto con su probabilidad e impacto?

1. Incumplimiento del Reglamento General de Protección de Datos RGPD.

La empresa gestiona datos personales de 300.000 clientes en España y posiblemente datos sensibles de embajadas y multinacionales. Existe el riesgo de no cumplir con las normas del RGPD, como no obtener el consentimiento, exponer datos a ciberatacantes o no informar de brechas de seguridad.

La probabilidad de incumplimiento es alta, debido a la gran cantidad de datos gestionados la posibilidad de cometer un error es elevada.

El impacto sería muy alto, las sanciones pueden llegar a ser muy severas, incluyendo multas significativas (hasta el 4% de los ingresos o 20 millones) y daños en la reputación de la empresa.

2. Falta de certificación ISO 27001.

Uno de los clientes importantes de ACME, requiere que la organización tenga dicha certificación para sus servicios de comunicaciones, que asegura que los sistemas de información estén protegidos frente a riesgos. No contar con la certificación podría poner en riesgo el mantenimiento de ese cliente y que se exijan otros estándares de seguridad.

La probabilidad de que se dé es media, la certificación es alcanzable pero requiere tiempo, recursos y esfuerzo por parte de la empresa para implementarla correctamente.

El impacto es muy alto, la pérdida de clientes grandes como el banco afectaría significativamente a los ingresos y a su reputación en el mercado.

3. Incumplimiento de la Ley de Protección de Infraestructuras Críticas (Ley 8/2011)

ACME podría no implementar medidas de protección adecuadas contra posibles amenazas, para garantizar la seguridad de sus telecomunicaciones (consideradas infraestructuras críticas). Esto incluye la falta de planes de seguridad, no colaborar con las autoridades y no responder eficazmente ante incidentes de seguridad. Dado que la empresa proporciona servicios a embajadas y otras entidades importantes, podría entrar en serios problemas si no cumpliera con esta ley.

La probabilidad de que ocurra es media, si ya tiene algunas medidas de seguridad es menos probable que incumpla esta ley, pero el riesgo existe por la complejidad de los requisitos legales.
El impacto sería muy alto, un fallo en la protección de las infraestructuras tendría consecuencias graves, como obtener sanciones legales, pérdida de confianza o contratos e incluso afectaciones a la seguridad nacional

Apartado 3: Sistema de gestión de cumplimiento.

Enumera al menos 5 partes interesadas en el sistema de gestión de cumplimiento de ACME.

1. Cliente

Las empresas y embajadas que contratan los servicios de ACME, tienen necesidades específicas relacionadas con la seguridad, la confidencialidad y la continuidad de la prestación de servicio. Estas entidades están interesadas en que la empresa cumpla con los estándares internacionales y las normativas aplicables, además de garantizar un servicio fiable y enfrentarse a los incidentes de manera rápida y efectiva.

2. Empleados

Las personas que trabajan en la empresa son una parte fundamental para implementar las políticas y procedimientos del sistema de cumplimiento. Están interesados en trabajar en un entorno estable, con políticas claras, herramientas y formación adecuada para cumplir con las normativas legales y los valores éticos de la organización. También les interesa la estabilidad y el éxito de la empresa, así como oportunidades de desarrollo profesional.

3. Proveedores y socios

Las empresas y entidades que colaboran con ACME para proporcionar servicios o productos, buscan mantener una relación sólida y transparente, cumpliendo con los estándares y regulaciones necesarias. También están interesados en la estabilidad y fiabilidad de sus asociaciones, así como en oportunidades de crecimiento conjunto.

4. Inversores

Los inversores tienen interés en que la empresa ACME opere de manera legal y ética, asegurándose de que cumpla con todas las normativas legales para evitar riesgos financieros y reputacionales, protegiendo sus inversiones. Buscan garantizar confianza y reducir la probabilidad de pérdidas operativas, afianzando la estabilidad y el crecimiento de la empresa así como en la gestión adecuada de riesgos.

5. Organismos gubernamentales

Las entidades gubernamentales, como la Agencia Española de Protección de Datos y Comisión Nacional de los Mercados y la Competencia, supervisan que se cumpla con las leyes y regulaciones aplicables.
Estas entidades están interesadas en la implementación de las medidas adecuadas para garantizar la privacidad de los usuarios, la seguridad de los servicios y colaborar ante incidentes de ciberseguridad.

Propón al menos un control por cada riesgo identificado en el apartado 2.

Incumplimiento del Reglamento General de Protección de Datos RGPD.

- Implementar un sistema de gestión de datos personales que incluya la obtención de consentimiento y encriptar los datos personales almacenados. Esto asegura que los datos se manejen de forma segura.
- Establecer un protocolo de respuesta a incidentes de seguridad que incluya la notificación inmediata a las autoridades. Esto ayudará a minimizar el impacto de cualquier incidente de seguridad.

Falta de certificación ISO 27001.

- Desarrollar un plan de acción para obtener la certificación ISO 27001, que incluya la asignación de recursos necesarios y la formación del personal. Además, diseñar un sistema que incluya políticas, procedimientos y controles que se deban llevar a cabo. Esto asegurará que la empresa cumpla con los requisitos de la norma.
- Realizar auditorías periódicas para asegurar el cumplimiento continuo de los requisitos. Esto ayudará a identificar y corregir cualquier deficiencia previamente.

Incumplimiento de la Ley de Protección de Infraestructuras Críticas (Ley 8/2011)

- Establecer un plan de seguridad que incluya el análisis de riesgos, la identificación y protección de las infraestructuras críticas así como la colaboración con las autoridades pertinentes. Esto asegurará que las infraestructuras estén protegidas contra posibles amenazas.
- Implementar medidas de respuesta rápida ante incidentes de seguridad y realizar simulacros para evaluar y mejorar la capacidad de respuesta de la empresa. Esto ayudará a garantizar una respuesta eficaz ante cualquier incidente.

Define 5 métricas de evaluación del sistema de gestión de cumplimiento normativo.

1. Número de incidentes de incumplimiento, contar la cantidad de incidentes se han registrado en un periodo determinado. Ayuda a medir la efectividad del sistema en prevención de violaciones de las normativas.
2. Tiempo de respuesta a incidentes, medir el tiempo promedio que tarda la empresa en responder a un incidente de cumplimiento, desde su detección hasta su resolución.
3. Nivel de formación de empleados, calcular el porcentaje de empleados que han completado la formación en cumplimiento normativo. Asegura que los empleados estén informados y preparados para afrontar los incidentes.
4. Número de auditorías internas realizadas, contar la cantidad de auditorías internas de cumplimiento realizadas en un periodo determinado, para evaluar la proactividad de la empresa en identificar y corregir posibles incumplimientos.
5. Satisfacción de las partes interesadas, medir la satisfacción de clientes, empleados, inversores y otros interesados, con el sistema de cumplimiento normativo a través de encuestas o feedback. Asegura que el sistema de cumplimiento no sólo sea efectivo sino, valorado por quienes interactúan con él.