ÍNDICE:

1.- Descripción de la tarea. 2
Caso práctico 2
¿Qué te pedimos que hagas? 3
Apartado 1: Entorno regulatorio de aplicación. 3
Apartado 2: Análisis y gestión de riesgos 4
Apartado 3: Sistema de gestión de cumplimiento. 4
Bibliografía: 7

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.

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.

¿Qué te pedimos que hagas?

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

Apartado 1: Entorno regulatorio de aplicación.

¿Podrías identificar tres leyes de aplicación para ACME?

1. **Reglamento General de Protección de Datos (RGPD**):

    - **Descripción:** Es una ley imprescindible para ACME, ya que la empresa dispone y controla gran cantidad de datos personales de clientes. El RGPD indica las normas de protección de estos datos en la Unión Europea. El incumplimiento de esta daría como resultado la perdida de prestigio si como hacer frente a fuertes sanciones económicas.

    - **Impacto:** La empresa ACME debe poner los medios para asegurar que los datos personales de los clientes estén protegidos adecuadamente y con ello cumplir los requisitos de privacidad y seguridad.

2. **Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE):**

    - **Descripción:** esta Ley es la que regula los intercambios comerciales que son realizados a través de internet. Para la empresa ACME es una ley importante dado que su negocio va enfocado a las telecomunicaciones y muchos de los servicios se prestan on-line.

    - **Impacto:** La empresa ACME debe cumplir con esta ley, proporcionando información a los usuarios e implementando medidas de seguridad.

3. **Ley Orgánica de Protección de Datos (LOPD):**

    - **Descripción:** Esta ley complementa a el RGPD, establece obligaciones específicas para las empresas que gestionan datos personales en España. Es una ley esencial para poder asegurar los datos de los clientes.

- **Impacto:** La empresa debe garantizar el cumplimiento de la LOPD implementando políticas, procesos y procedimientos que garanticen la seguridad de los datos, así como la gestión de consentimientos y la respuesta a las solicitudes de acceso a los datos.

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. **Riesgo de incumplimiento del RGPD:**

- **Descripción:** La falta de las medidas oportunas para conseguir la protección de los datos de los clientes, con el posible resultado de la filtración de datos de estos.
- **Probabilidad:** Alta
- **Impacto:** Alto
- **Consecuencias:** Las consecuencias del incumplimiento son varios como sanciones económicas, pérdida de confianza de los clientes y daño a la reputación de la empresa.

2. **Riesgo de incumplimiento de la LSSI-CE:**

- **Descripción:** Que la empresa no cumpla con las regulaciones de comercio electrónico y servicios de la sociedad de la información.
- **Probabilidad:** Media
- **Impacto:** Medio
- **Consecuencias:** La empresa debería enfrentarse en este caso a sanciones económicas y posibles limites en la operación de servicios en línea.

3. **Riesgo de incumplimiento de la ISO 27001:**

- **Descripción**: El que la empresa no obtenga o no sea capaz de mantener la certificación ISO 27001 la cual es requerida por clientes multinacionales, puede provocar la pérdida de contratos importantes.
- **Probabilidad:** Media
- **Impacto:** Alto
- **Consecuencias**: La empresa se enfrentaría a la pérdida de clientes importantes y con ello a una reducción de ingresos.

Apartado 3: Sistema de gestión de cumplimiento.

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

- **Clientes:** Los clientes esperan que la empresa ACME proteja sus datos y que cumpla con las regulaciones y leyes que son de aplicación en esta materia.
- **Empleados:** Los Empleados deben estar informados y bien formados sobre las políticas de cumplimiento para evitar las posibles sanciones y mantener el buen rumbo de la empresa.
- **Accionistas:** Ellos con el cumplimiento buscan que su inversión sea rentable y protegerla de posibles sanciones que puedan afectar el valor de la empresa.
- **Proveedores:** Esta parte interesada deben cumplir con las políticas de cumplimiento de ACME que las relaciones comerciales que mantienen perduren en el tiempo y con ello evitar posibles riesgos compartidos.
- **Entidades regulatorias:** Estas entidades están interesadas en el cumplimiento y por ello supervisaran y se aseguraran que ACME cumpla con todas las leyes y regulaciones que les sea de aplicación.

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

1. **Riesgo de incumplimiento del RGPD:**
    - **Control:** Establecer e implementar políticas y procedimientos de protección de datos, cabe destacar entre ellos la formación continua de empleados en la materia de privacidad de los datos y realizar auditorías periódicas para confirmar su cumplimiento.
2. **Riesgo de incumplimiento de la LSSI-CE:**
    - **Control:** Realizar auditorías periódicas de cumplimiento, actualizar todas las políticas de comercio electrónico para estar de acuerdo con la regulación vigente. Dedicar un equipo a la gestión de la conformidad con la LSSI-CE.
3. **Riesgo de incumplimiento de la ISO 27001:**
    - **Control:** Establecer un equipo dedicado a la gestión de la seguridad de la información capacitado y capaz de realizar revisiones internas regulares para asegurar el cumplimiento de todos los apartados de la ISO 27001. Crear e Implementar un sistema de gestión de riesgos para realizar un análisis, identificar y mitigar posibles incumplimientos.

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

- **Número de incidentes de seguridad reportados:** Una de las métricas más socorridas, aunque no efectivas ya que puede haber muchos incidentes no reportados por desconocimiento de estos es medir la cantidad de incidentes de seguridad de los que se tiene conocimiento de los que hemos sido objeto para evaluar la efectividad de las medidas de protección de datos.
- **Porcentaje de empleados formados en políticas de cumplimiento:** Es esencial evaluar la proporción de empleados que han completado la formación en políticas de cumplimiento y con ello conseguir también una mayor penetración de ese conocimiento en la empresa.
- **Número de auditorías de cumplimiento realizadas anualmente:** Es esencial para ello medir la cantidad de auditorías realizadas, tanto internas como externas

y con ello comprobar que se está llevando a cabo revisiones regulares del cumplimiento.

- **Tiempo promedio de respuesta a incidentes de cumplimiento:** para comprobar que las medidas son efectivas se puede evaluar la rapidez con la que la empresa responde a incidentes de cumplimiento y con ello minimizar el impacto.
- **Porcentaje de cumplimiento de los requisitos de la ISO 27001:** El equipo dedicado a asegurar el cumplimiento de los estándares de la ISO 27001 deben realizar las auditorías internas y medir el grado de cumplimiento de los requisitos de la ISO 27001 con ello asegurarnos de mantener la certificación y cumple con los estándares de seguridad de la información.

Bibliografía:

Temario de la asignatura.