Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Normativa de Ciberseguridad

UD02. Sistemas de Gestión de compliance.
Tarea Online 02.

JUAN ANTONIO GARCIA MUELAS

INDICE

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?

- Reglamento General de Recaudación de la Seguridad Social (RGRSS), que establece las normas y procedimientos de recaudación de contribuciones a la Seguridad Social, así como los plazos y sanciones por incumplimiento.
- La Ley Orgánica de Protección de Datos (LOPD) y su Reglamento de desarrollo (RGPD), que establecen las obligaciones de las empresas en lo referente al tratamiento de los datos personales de sus clientes, debiendo garantizar la privacidad y seguridad de estos datos y estableciendo sanciones para quienes incumplan estas normas.
- La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) que regula los servicios de la sociedad de la información, correo electrónico, páginas web o mensajería instantánea.
- La Ley de Régimen Jurídico del Sector Público (LRJSP), que regula el régimen jurídico del sector público español. La empresa debe cumplir con esta ley en todos sus procesos de comunicación con las administraciones públicas.

✓ 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?

Analizando las actividades de ACME, así como su entorno regulatorio, destacaría:

- Riesgo por incumplimiento de la normativa de protección de datos: La empresa puede incumplir dicha normativa por no cumplir con los requisitos establecidos en la LOPD, el RGPD, la LSSI-CE o la LSSI, pudiendo provocar sanciones económicas, multas, la pérdida de clientes y de reputación de la empresa.
  - Probabilidad: Alta.
  - Impacto: Alto.
- Riesgo por incumplimiento de la normativa de seguridad de la información: Está asociado al anterior riesgo. Sino implementa las medidas de seguridad adecuadas para proteger sus datos y sistemas, ACME podría estar incumpliendo esta norma, provocando la pérdida de datos, interrupción de los servicios, y posibilitando ataques cibernéticos.
  - Probabilidad: Alta.
  - Impacto: Medio.
- Riesgo de incumplimiento de la normativa de prevención del blanqueo de capitales: ACME puede incumplir con la normativa de prevención del blanqueo de capitales sino realiza los controles adecuados para identificar y prevenir las operaciones de blanqueo de capitales. Esto puede provocar sanciones económicas, administrativas y penales.
  - Probabilidad: Media.
  - Impacto: Alto.
- Riesgo de incumplimiento de la normativa de competencia: Puede incumplir la normativa de competencia mediante prácticas anticompetitivas como, por ejemplo, el abuso de posición de dominio, la colusión (pacto ilícito) o el dumping (fiscal o

financiero). Todo ello puede provocar sanciones económicas, administrativas y penales.

- Probabilidad: Media.
- Impacto: Alto.

✓ Apartado 3: Sistema de gestión de cumplimiento.

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

- La dirección: La dirección de ACME es la responsable de definir el sistema de gestión de cumplimiento y de garantizar su implantación y mantenimiento.
- Los empleados: Los empleados son, por un lado, responsables de cumplir con los requisitos del sistema de gestión de cumplimiento, pero, además, se ven amparados por este, porque debe garantizar un ambiente laboral y regulatorio seguro.
- Los clientes: Los clientes pueden verse afectados por el incumplimiento de ACME de normativas y regulación.
- Los proveedores: Son parte interesada en la prevención de blanqueo, transparencia en las relaciones comerciales...
- Los accionistas: Los accionistas pueden verse afectados por el impacto financiero del incumplimiento de la empresa y su pérdida de valor.
- Los sindicatos: que pueden representar a los empleados en la implementación y mantenimiento del sistema de gestión de cumplimiento.
- Otras organizaciones de la sociedad civil: No solo los sindicatos son parte interesada en el sistema de gestión de cumplimiento de ACME. Otros tipos de organizaciones de la sociedad civil (desde colegios del entorno, hasta Bomberos, pasando por ONG o asociaciones vecinales) pueden tener interés en el correcto cumplimiento de ACME de las leyes y normativas vigentes.

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

- Riesgo por incumplimiento de la normativa de protección de datos:
  Desarrollar un procedimiento que garantice el cumplimiento de los requisitos establecidos en la norma, como:
  - La identificación de los datos personales que se tratan.
  - Los fines para los que se tratan los datos personales.
  - Las bases legales para el tratamiento de los datos personales.
  - Los derechos de los titulares de los datos personales.
  - Los mecanismos para garantizar la seguridad de los datos personales.
- Riesgo por incumplimiento de la normativa de seguridad de la información: Implementar un plan de seguridad que incluya medidas como:
  - La evaluación de los riesgos de seguridad de la información.
  - La implementación de medidas de seguridad para mitigar los riesgos identificados.
  - La formación del personal en materia de seguridad de la información.
  - La realización de auditorías de seguridad de la información.
- Riesgo de incumplimiento de la normativa de prevención del blanqueo de capitales: Necesitará de un programa de prevención ante el blanqueo de capitales con:
  - La identificación de los clientes y de sus actividades.
  - La realización de comprobaciones de los clientes.
  - La implementación de medidas de control para prevenir las operaciones de blanqueo de capitales.

- Riesgo de incumplimiento de la normativa de competencia:
  Implementar una política de competencia con principios como:
  - La competencia leal.
  - La no discriminación de los clientes.
  - La transparencia en las relaciones comerciales.
  - La cooperación entre competidores.

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

1. Porcentaje de cumplimiento de los requisitos normativos.
   Esta métrica mide el porcentaje de requisitos normativos que la empresa cumple y muestra el grado de adherencia de ACME respecto a normativa y legislación. Precisa para su cálculo conocer de forma clara el total de requisitos normativos que sean aplicables, para poder dividirlos con el número de requisitos normativos cumplidos.
2. Número de incumplimientos detectados.
   Esta métrica detallada, mide el número de incumplimientos de los requisitos normativos detectados en ACME. Podemos calcularla mediante el conteo de incumplimientos que se han detectado en un periodo de tiempo determinado.
3. Tiempo medio para la resolución de los incumplimientos.
   Esta métrica nos mide el tiempo que tarda la empresa en resolver los incumplimientos de requisitos normativos detectados. Se calcula entonces dividiendo el tiempo total que se ha empleado en resolver los incumplimientos detectados por ese mismo número de incumplimientos detectados.
4. Nivel de satisfacción de las partes interesadas.
   Con esta métrica podremos evaluar el nivel de satisfacción de las partes interesadas con nuestro sistema y su repercusión directa. Para ello se debe recopilar información de las partes interesadas, mediante encuestas, entrevistas o grupos de discusión.
5. Coste del cumplimiento normativo.
   Esta métrica mide el coste que supone para la empresa cumplir con los requisitos normativos. Podemos calcularla mediante la suma de costes directos e indirectos asociados al cumplimiento normativo.