Normativa de ciberseguridad

Sistemas de Gestión de Cumplimiento

### 

### 

| Índice |
| --- |
| 1. Entorno regulatorio de aplicación. 2. Análisis y gestión de riesgos, mapa de riesgos. 3. Documentación del sistema de cumplimiento normativo diseñado. |

| Enunciado |
| --- |
| 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. |
| ¿Podrías identificar tres riesgos de cumplimiento en el escenario de ACME, indicando una descripción del mismo, junto con su Probabilidad Cualitativa e impacto? Recuerda las leyes de aplicación de ACME de la tarea de anterior unidad, pueden servir para orientar el riesgo de cumplimiento en base a ellas.  Sigue este formato de tabla para presentar la información: |
|  |
| 1. **Riesgo: Incumplimiento de Requisitos de Seguridad para Clientes Corporativos:**    * **Descripción:** Existe un riesgo moderado de no cumplir con los estándares de seguridad ISO27001 exigidos por el cliente bancario. Este incumplimiento podría resultar en la pérdida del cliente, daño significativo a la reputación y posibles consecuencias legales.    * **Probabilidad Cualitativa:** Moderada.    * **Impacto:** Alto.    * **Riesgo:** Moderado a Alto. 2. **Riesgo: Violaciones Ambientales en Operaciones y Proyectos de Infraestructura:**    * **Descripción:** Existe un riesgo moderado a bajo de violar normativas ambientales en relación con las instalaciones ecológicas y parques públicos de ACME. Tales violaciones podrían traducirse en multas sustanciales, pérdida de licencias y un impacto negativo en la imagen corporativa.    * **Probabilidad Cualitativa:** Baja a Moderada.    * **Impacto:** Moderado a Alto.    * **Riesgo:** Moderado. 3. **Riesgo: Incumplimiento de Normativas Internacionales en Operaciones Multinacionales:**    * **Descripción:** Existe un riesgo moderado de no cumplir con las diversas regulaciones locales en los 32 países donde ACME opera. Este incumplimiento podría resultar en sanciones internacionales, pérdida de licencias y disputas legales, afectando negativamente la capacidad de operar globalmente.    * **Probabilidad Cualitativa:** Moderada.    * **Impacto:** Alto.    * **Riesgo:** Moderado a Alto. |
| 2. Propón al menos un control por cada riesgo identificado. |

| 1. **Riesgo: Incumplimiento de Requisitos de Seguridad para Clientes Corporativos:**    * **Control Propuesto:** Implementar auditorías de seguridad regulares y revisiones internas para asegurar el cumplimiento continuo con los estándares de seguridad ISO27001. Además, establecer un programa de formación constante para el personal con acceso a sistemas críticos de seguridad. 2. **Riesgo: Violaciones Ambientales en Operaciones y Proyectos de Infraestructura:**    * **Control Propuesto:** Establecer un equipo de gestión ambiental dedicado para supervisar y evaluar regularmente el cumplimiento de las normativas ambientales. Además, realizar auditorías ambientales periódicas para identificar y abordar cualquier área de no conformidad, y garantizar la capacitación constante del personal en prácticas ambientalmente sostenibles. 3. **Riesgo: Incumplimiento de Normativas Internacionales en Operaciones Multinacionales:**    * **Control Propuesto:** Mantener un equipo de expertos legales que monitoree y actualice constantemente las regulaciones de telecomunicaciones y comercio en los países donde opera ACME. Establecer un sistema de gestión de compliance global que asegure la alineación con las normativas locales, incluyendo revisiones regulares y actualizaciones de políticas y procedimientos. |
| --- |