## TAREA 05

# NORMATIVA VIGENTE DE CIBERSEGURIDAD DE ÁMBITO NACIONAL E INTERNACIONAL

### 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.**

**En los últimos meses ACME esta de enhorabuena, ha logrado la adjudicación de un contrato mayor para la prestación de servicios de comunicaciones a una institución de las Fuerzas y Cuerpos de Seguridad del Estado. Dado el servicio que provee ha sido designado como proveedor de servicio esencial.**

**Dados los compromisos existentes hasta la fecha y con los nuevos contratos adjudicados, ACME va a abordar el proyecto de despliegue de un Sistema de Gestión de Seguridad de la Información, así como un Sistema de Gestión de Continuidad de Negocio. Asimismo, con el contrato otorgado para Fuerzas y Cuerpos de Seguridad del Estado, debe cumplir con la normativa del Esquema Nacional de Seguridad y con la Directiva NIS.**

**Apartado 1: Normas nacionales e internacionales**

**¿Podrías proponer tres controles de cada proceso de seguridad de la normativa NIST?**

Procesos de seguridad de la normativa NIST

1. Identificación:

Asset Management, inventario y clasificación de activos.
Business Environment, identificar el entorno empresarial y sus dependencias.
Governance, políticas y procedimientos de seguridad.

2. Protección:

Access Control, control de acceso (roles y privilegios mínimos).
Data Security, encriptación de datos.
Maintenance, mantenimiento y actualización de sistemas.

3. Detección:

Anomalies and Events, monitoreo continuo para detectar anomalías.
Security Continuous Monitoring, implementar sistemas de monitoreo continuo.
Detection Processes, procedimientos para detectar y reportar incidentes.

4. Respuesta:

Response Planning, planes de respuesta ante incidentes.
Communications, comunicación interna y externa durante incidentes.
Analysis, análisis forense después de incidentes.

5. Recuperación:

Recovery Planning, planes de recuperación ante desastres.
Improvements, mejora continua en base a las lecciones aprendidas.
Communications, comunicación durante la recuperación.

**Apartado 2: Sistema de gestión de seguridad de la información basado en ISO 27001**

- Contexto descriptivo de la organización alineado con los requisitos del estándar:

ACME S.A. es una empresa dedicada a dar servicios de telecomunicaciones internacionales, con 300,000 clientes en España, localizada en 32 países. La sede central está ubicada en Madrid, con instalaciones modernas que incluyen climatización inteligente, jardines en las azoteas, y paneles solares. ACME ha sido designada como proveedor esencial para las Fuerzas y Cuerpos de Seguridad del Estado, lo que implica cumplir con normativas como el Esquema Nacional de Seguridad y la Directiva NIS.

- Propuesta de tres controles para la mitigación de riesgos identificados:

1. Establecer controles de acceso físicos y lógicos, implementando sistemas biométricos y autenticación multifactor para acceder a áreas críticas y sistemas informáticos o a información sensible.
2. Utilizar encriptación avanzada, utilizar algoritmos robustos para proteger datos sensibles tanto en tránsito como en reposo.
3. Programar auditorías periódicas tanto internas como externas de forma regular para asegurar el cumplimiento continuo con las normativas ISO 27001.

- Desarrollo de tres métricas de seguridad para ACME:

1. Media de incidentes detectados al mes: recopilar el número total de incidentes detectados y dividirlo por el número total de meses y así poder hacer un estudio de cuando hubo más, y donde se debe reforzar la seguridad.
2. Tiempo medio para resolver incidentes: saber el promedio del tiempo que se tarda desde la detección hasta la resolución completa del incidente, para poder mejorar los procedimientos.
3. Porcentaje de sistemas actualizados: calcular los sistemas utilizados por la organización que tienen los últimos parches de seguridad o actualizaciones realizadas y compararlo con el número total de sistemas, para mantener los sistemas actualizados y reducir las posibles vulnerabilidades.

**Apartado 3: Sistema de gestión de continuidad de negocio basado en ISO 22301**

**El escenario a utilizar para este análisis de impacto es el de los sistemas centralizados que dan servicio a la red de comunicaciones de manera centralizada. En caso de indisponibilidad de estos sistemas, la red completa no podría funcionar.**

**Lucro cesante, provocado por la incapacidad de facturación ocasionada por la parada de los servicios de red. Se estima que la organización factura 100.000 € por hora.**

**Compensaciones, provocadas por los perjuicios que pudieran ocasionar a las empresas a las que ACME da servicio. Según los contratos firmados con los clientes de la empresa, se garantiza un 99% de servicio, y únicamente se debe compensar en caso de que la caída dure más de 30 minutos, y si el cliente corporativo lo reclama. Se ha estimado que, a partir de la primera hora, las compensaciones supondrían 500.000€ por cada hora de caída.**

**Imagen, la confianza en la organización y en los servicios que provee se vería afectada. Esto supondría una pérdida de un 1% de la cartera de clientes por cada incidencia. Además, se estima que habría una caída de altas nuevas. Este tipo de perjuicios se ha cuantificado en 200.000€ por incidencia.**

**Sanciones, la comisión del mercado de las telecomunicaciones puede actuar en caso de una pérdida de servicio elevada, además al haber un designio de operador de servicio esencial, una caída prolongada podría ocasionar pérdidas económicas por sanciones.**

**Se estima que esta situación se daría únicamente en caso de caídas repetidas y de larga duración.**

**La organización no está dispuesta a asumir pérdidas mayores a 1,5 millones de €.**

- Análisis de impacto en continuidad sobre los sistemas asociados al servicio de telecomunicaciones:

El análisis de impacto en la continuidad del negocio es crucial para identificar y evaluar los efectos de una interrupción en las actividades críticas de la organización. Para ACME, los sistemas centralizados que dan

servicio a la red de comunicaciones son esenciales. En caso de indisponibilidad, la red completa podría no funcionar y enfrentar pérdidas significativas debido a:

- Lucro cesante, se perderían ingresos por la incapacidad de facturar, la empresa factura alrededor de 100,000 € por hora, si se da una interrupción prolongada podría resultar en pérdidas importantes.
- Compensaciones, se deberán dar compensaciones a los clientes por perjuicios tras la caída del servicio. Debido a los contratos se garantiza el 99% de servicio, si la caída dura más de 30 minutos y es reclamada, serían de 500,000 € por hora.
- Pérdida de confianza, los clientes podrían perder la confianza en la organización y en sus servicios, se estima que un 1% de clientes se pierden por cada incidencia, además de un descenso en las nuevas altas. El daño se aproxima a 200,000 € por incidencia.
- Sanciones regulatorias, por parte de la comisión del mercado de las telecomunicaciones se pueden recibir sanciones económicas debido a que ACME es considerada proveedora de servicio esencial.

- Establecimiento del valor justificado para los parámetros MTPD, RPO Y RTO:

1. MTPD (Maximum Tolerable Period of Disruption): 24 horas, considerando el impacto financiero y reputacional. Una interrupción más prolongada podría resultar en pérdidas significativas y daños en la imagen de la empresa.
2. RPO (Recovery Point Objective): 1 hora, minimizar la pérdida de datos críticos es esencial para mantener la continuidad del negocio y la confianza de los clientes. Se asegura que la información perdida sea mínima..
3. RTO (Recovery Time Objective): 5 horas, para asegurar una rápida restauración del servicio. Este valor permite una rápida restauración del servicio minimizando el impacto en los clientes y las operaciones.

**Apartado 4: Esquema nacional de seguridad**
**Categoriza los sistemas asociados al servicio de telecomunicaciones en función al escenario definido en el caso práctico, por la prestación de servicios a FCSEs.**
**Desarrolla una declaración de aplicabilidad justificada.**

- Categorización de los sistemas asociados al servicio de telecomunicaciones:

Los sistemas asociados al servicio de telecomunicaciones de ACME deben ser categorizados como críticos debido a su rol esencial en las comunicaciones para las Fuerzas y Cuerpos de Seguridad del Estado (FCSE). La declaración se basa en el impacto de un incidente en términos de disponibilidad, autenticidad, integridad, confidencialidad…

- Debe incluir controles específicos:

- Autenticación robusta, implementar sistemas de autenticación Multifactor, protege contra accesos no autorizados y asegura que solo las personas que autorizadas puedan acceder a la información sensible
- Monitoreo continuo, implementar sistemas de monitoreo continuo para vigilar de forma constante los sistemas, detectando anomalías y amenazas en tiempo real.
- Planes detallados de respuesta ante incidentes, desarrollar planes de respuesta ante incidentes que incluyan procedimientos y roles bien definidos y claros, para asegurar respuestas rápidas y efectivas ante cualquier incidente, minimizando el impacto en las operaciones.

Para desarrollar las respuestas de manera clara y detallada es importante seguir una estructura, primero se realiza una introducción describiendo el problema y los objetivos de la respuesta, en el segundo paso analizamos los elementos involucrados, las propuestas de solución y cada una de sus justificaciones, por último en la conclusión hacemos un resumen de los puntos clave y las recomendaciones finales .