ÍNDICE:

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.

En los últimos meses ACME está 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.

En esta tarea se requerirá de los conocimientos adquiridos a lo largo de la unidad para desarrollar los contenidos requeridos en el ejercicio.

¿Qué te pedimos que hagas?

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

- Apartado 1: Normas nacionales e internacionales

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

Identificar:

- Inventario de activos de información.
- Evaluación de riesgos de ciberseguridad.
- Establecimiento de políticas de seguridad.

Proteger:

- Implementación de control de accesos.
- Cifrado de datos sensibles.
- Formación en concienciación de seguridad.

Detectar:

- Monitorización continua de la red.

- Análisis de logs de seguridad.
- Pruebas de penetración periódicas.

Responder:

- Plan de respuesta a incidentes.
- Simulacros de ciberataques.
- Procedimientos de comunicación de incidentes.

Recuperar:

- Copias de seguridad y procedimientos de restauración
- Plan de continuidad de negocio
- Análisis post-incidente y lecciones aprendidas

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

- *Desarrolla un contexto descriptivo de la organización alineado con los requisitos de información del estándar.*

  ACME S.A. es un proveedor de servicios de telecomunicaciones internacionales con 300,000 clientes en España y presencia en 32 países. La empresa ofrece servicios a particulares y empresas, incluyendo multinacionales y embajadas. Recientemente, ACME ha obtenido un contrato para prestar servicios a las Fuerzas y Cuerpos de Seguridad del Estado, siendo designada como proveedor de servicio esencial. La sede central está en Madrid, con instalaciones modernas y sostenibles. ACME debe cumplir con la certificación ISO27001, el Esquema Nacional de Seguridad y la Directiva NIS.

  Riesgos que podemos identificar:

  1. Interrupción del servicio de red centralizado.
  2. Fuga de datos sensibles de clientes gubernamentales.
  3. Ciberataque a la infraestructura de telecomunicaciones.

- *Propón al menos tres controles para la mitigación de riesgos identificados.*
  1. Implementación de sistemas redundantes y plan de continuidad de negocio.
  2. Cifrado de datos en tránsito y en reposo, con gestión de claves robusta.
  3. Despliegue de sistemas de detección y prevención de intrusiones (IDS/IPS).

- *Desarrolla tres métricas de seguridad para ACME.*
  1. Tiempo medio de detección de incidentes de seguridad.
  2. Porcentaje de empleados que han completado la formación en ciberseguridad.
  3. Número de vulnerabilidades críticas no parcheadas en sistemas críticos

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

El escenario a utilizar para este análisis de impacto es del 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, provocado por los perjuicios que pudieran ocasionar a las empresas a las que ACME da servicio. Según los contratos firmados con los clientes 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 perdida 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 perdidas mayores a 1,5 millones de €.

- *Realiza un análisis de impacto en continuidad sobre los sistemas asociados al servicio de telecomunicaciones*.
  - Lucro cesante: 100,000 € por hora.
  - Compensaciones: 500,000 € por hora después de la primera hora.
  - Impacto en imagen: 200,000 € por incidencia + 1% pérdida de cartera de clientes.
  - Sanciones: Potenciales en caso de caídas prolongadas y repetidas.

- *Establece un valor justificado para los parámetros MTPD, RPO y RTO.*
  - MTPD (Tiempo Máximo de Interrupción Tolerable): 15 horas.

    Justificación: Con las pérdidas estimadas, ACME alcanzaría el límite de 1.5 millones € en aproximadamente 15 horas.

- RPO (Punto de Recuperación Objetivo): 15 minutos

Justificación: Dada la criticidad de los datos de telecomunicaciones, se requiere una pérdida mínima de datos.

- RTO (Tiempo de Recuperación Objetivo): 30 minutos

Justificación: Para evitar compensaciones y minimizar el impacto en la imagen, el servicio debe restablecerse antes de 30 minutos.

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 sistemas:

Considerando la prestación de servicios a las Fuerzas y Cuerpos de Seguridad del Estado, los sistemas se categorizan como ALTO en las tres dimensiones de seguridad:

- Confidencialidad: ALTO (datos sensibles de seguridad nacional)
- Integridad: ALTO (información crítica para operaciones de seguridad)
- Disponibilidad: ALTO (servicios esenciales para la seguridad del Estado).

- Declaración de aplicabilidad justificada:
- La Declaración de Aplicabilidad (DoA) es un documento clave del SGSI basado en ISO 27001 , y también es un requisito para el cumplimiento del ENS . En ella se enumeran todos los controles del Anexo II del ENS (que a su vez se basan en la ISO 27002) y se justifica cuáles de ellos son aplicables a la organización y cuáles no, o si se aplican de forma diferente.

- Control de acceso: Aplicable. Implementación de autenticación multifactor y gestión de privilegios.
  Justificación: Protección contra accesos no autorizados a información sensible.
- Cifrado: Aplicable. Uso de algoritmos robustos para comunicaciones y almacenamiento.
  Justificación: Asegurar la confidencialidad de datos en tránsito y en reposo.
- Seguridad física: Aplicable. Controles de acceso físico y vigilancia en instalaciones críticas.
  Justificación: Prevenir accesos no autorizados y sabotajes a infraestructuras clave.
- Gestión de incidentes: Aplicable. Establecimiento de un CERT (Computer Emergency Response Team).
  Justificación: Respuesta rápida y efectiva ante posibles ciberataques o interrupciones del servicio.
- Auditorías de seguridad: Aplicable. Realización de auditorías periódicas internas y externas.

Justificación: Verificar el cumplimiento continuo de las medidas de seguridad implementadas.
La DoA debe ser un documento vivo que se revise y actualice periódicamente en función de los cambios en los riesgos, la normativa y la infraestructura de ACME

Bibliografía:

Temario de la asignatura.