Actividad 12. Ejemplos de determinación de costes de un incidente

Ejemplo 1:

Contexto:

El proceso crítico de una empresa es la venta por internet. El BIA determina que el impacto de una parada es de 100€ a la hora. El personal de seguridad considera tres posibles estrategias para restablecer el servicio:

a) Con un plazo de puesta en marcha de 7 días, disponer un servidor nuevo en el que montar las copias de seguridad. El importe es de 2000€.

b) Con un plazo de 3 días, alquilar un servidor alojado por terceros para montar las copias de seguridad. El contrato mínimo es por un mes, con un importe de 1000€.

c) Con un plazo de 5 días, arreglar el servidor averiado. El importe de la reparación es de 100€.

1. Seleccionar la mejor opción para restablecer el servicio.
2. Restablecido el servicio, la empresa dispone de un mes para restablecerlo por completo, entendiendo como tal volver a disponer de un servidor en propiedad. ¿Cuál sería el coste?

Ejemplo 1:

Solución:

1. Es necesario evaluar el coste de cada solución.

Coste solución A:

Coste parada = 24x7x100 = 16.800 €.

Coste recuperación = 2.000 €.

Coste total = 18.800 €.

Coste solución B:

Coste parada = 24x3x100 = 7.200 €.

Coste recuperación = 1.000 €.

Coste total = 8.200 €

Coste solución C:

Coste parada = 24x5x100 = 12.000 €

Coste recuperación = 100 €.

Coste total = 12.100 €.

La solución de coste mínimo para restablecer el servicio es la solución B, que además es la que proporciona el menor RTO.

2. Para restablecer el servidor, hay varias opciones:

Con la **solución A,** comprar uno nuevo:

coste solución total = 8.200 + 2.000 = 10.200

Con la **solución B**, alquilar servidor y arreglar el servidor averiado:

coste solución total = 7.200 + 1.000 = 8.200 €

Con la **solución B**, alquilar servidor y comprar uno nuevo:

coste solución total = 7.200 + 1.000 +2000= 10.200 €

Con la **solución C**, arreglar el servidor averiado:

coste solución total = 8.200 + 100 = 8.300 €

Ejemplo 2:

Pasos a realizar para el cálculo de costes de un incidente de seguridad informática:

1. **Cálculo del costo directo:**
   - **Objetivo:** Determinar los gastos inmediatos incurridos tras un incidente de seguridad.
   - **Descripción:** Identificar y cuantificar los recursos utilizados para responder al incidente, como:
     - Horas de personal de TI y respuesta a incidentes.
     - Costos de herramientas y software especializados.
     - Gastos de servicios externos (forenses, legales, etc.).
     - Costos de comunicación y notificación a los afectados.
     - Daños físicos a equipos o infraestructura.

     Ejemplo: Suponga que un ataque de ransomware obliga a contratar a un equipo forense por 20.000 € y la pérdida de productividad del personal de TI representa 30.000 €. El costo directo sería 50.000 €.
2. **Cálculo del costo indirecto:**
   - **Objetivo:** Evaluar las pérdidas financieras a mediano y largo plazo derivadas del incidente.
   - **Descripción:** Considerar factores como:
     - Pérdida de ingresos por interrupción del negocio.
     - Daño a la reputación y pérdida de clientes.
     - Costos legales y regulatorios por incumplimiento de normativas.
     - Disminución de la productividad por cambios en procesos y medidas de seguridad.
     - Aumento de las primas de seguros.

Ejemplo: Si un ataque de phishing ocasiona la pérdida de datos confidenciales de clientes, la empresa podría enfrentar multas por incumplimiento de GDPR y una caída en las ventas del 10%, lo que se traduce en un costo indirecto significativo.

3. **Cálculo del costo de oportunidad:**
   - **Objetivo:** Estimar los beneficios potenciales que se han dejado de percibir debido al incidente.
   - **Descripción:** Evaluar:
     - Oportunidades de negocio perdidas por la indisponibilidad de sistemas o datos.
     - Retrasos en el lanzamiento de nuevos productos o servicios.
     - Pérdida de ventaja competitiva en el mercado.
     - Disminución de la inversión y el crecimiento empresarial.

   Ejemplo: Si un ataque cibernético retrasa la implementación de un nuevo sistema de gestión de pedidos, la empresa podría perder la oportunidad de aumentar sus ventas en un 15%, lo que representa un costo de oportunidad considerable.
4. **Cálculo del costo reputacional:**
   - **Objetivo:** Cuantificar el impacto negativo del incidente en la imagen y la credibilidad de la organización.
   - **Descripción:** Considerar:
     - Daño a la confianza de los clientes, socios e inversores.
     - Disminución del valor de la marca.
     - Mayor dificultad para atraer y retener talento.
     - Aumento del escrutinio público y la presión regulatoria.

Ejemplo: Una filtración de datos de información personal de clientes puede dañar gravemente la reputación de una empresa, lo que se traduce en pérdidas de ingresos a largo plazo y dificultades para mantener su posición en el mercado.

5. Cálculo del costo total:

- **Objetivo:** Obtener una visión global del impacto financiero total del incidente de seguridad.
- **Descripción:** Sumar los costos directos, indirectos, de oportunidad y reputacionales para obtener una cifra completa del impacto del incidente.

Ejemplo: Costo directo (50.000 €) + Costo indirecto (200.000 €) + Costo de oportunidad (150.000€) + Costo reputacional 300.000 €) = Costo total (700.000 €).

Consideraciones adicionales:

- La complejidad del ejercicio dependerá del tamaño y tipo de organización, la gravedad del incidente y la disponibilidad de datos.
- Es importante utilizar metodologías de cálculo reconocidas y adaptarlas a las características específicas de cada caso.
- Los resultados obtenidos servirán para comprender mejor el impacto financiero de los incidentes de seguridad y tomar decisiones informadas sobre la inversión en medidas de prevención y respuesta.

Ejercicio ejemplo: Ataque de Ransomware

Escenario: Un hospital sufre un ataque de ransomware que cifra sus sistemas informáticos durante 3 días. Las operaciones se ven gravemente afectadas, incluyendo la cancelación de cirugías y la demora en la atención a pacientes.

Solución:

Costos directos:

- Horas de personal de TI y respuesta a incidentes: 20 técnicos * 8 horas/día * 3 días * 100 €/hora = 48.000 €
- Costo del software de descifrado: 20.000 €
- Pérdida de ingresos por cancelaciones: 50.000 €

Costo total: 118.000 €

Costos indirectos:

- Daño a la reputación: Pérdida del 10% de pacientes en los próximos 6 meses: 200.000 €
- Aumento de las primas de seguros: 10.000 €

Costo total: 210.000 €

Costo de oportunidad:

- Retraso en la implementación de un nuevo sistema de registros médicos electrónicos: 150.000 €

Costo total: 150.000 €

Costo total del incidente: 118.000 e (costos directos) + 210.000 € (costos indirectos) + 150.000 € (costo de oportunidad) = 478.000 €