Desafío - Seguridad física en entornos TIC

En este desafío validaremos nuestros conocimientos en identificar las mejores prácticas de seguridad física en entornos TIC, cubriendo la protección de instalaciones, puntos de presencia y cuartos de servidores.

Lee todo el documento antes de comenzar el desarrollo **individual** para asegurarte de tener el máximo de puntaje y enfocar bien los esfuerzos.

// Tiempo asociado: 1 hora cronológica

Descripción

Leer el siguiente caso y responder las preguntas propuestas en un documento Word o Google Docs.

DataSecure Inc. es una empresa especializada en almacenamiento de datos y servicios en la nube para clientes corporativos. Su infraestructura tecnológica está distribuida en varios puntos clave:

- Un centro de datos principal ubicado en la sede central.
- Dos Puntos de Presencia (POP) en distintas ciudades para mejorar la conectividad y redundancia.
- Un cuarto de servidores dentro de la sede, donde se encuentran los equipos críticos de la compañía.

A pesar de contar con medidas de ciberseguridad avanzadas, la empresa ha experimentado varios incidentes físicos de seguridad que han comprometido la continuidad del negocio.
Entre los incidentes podemos mencionar los siguientes:

1. Acceso no autorizado en un Punto de Presencia (POP)
    - Durante la madrugada, un intruso ingresó a uno de los POP utilizando una tarjeta de acceso clonada.
    - Las cámaras de vigilancia no registraron actividad, ya que el sistema dejó de funcionar por falta de mantenimiento.
    - El intruso desconectó un router de borde, afectando la conectividad con clientes de la región.
    - No había guardias de seguridad o monitoreo en tiempo real, por lo que el problema solo se detectó horas después.

2. Intento de sabotaje en el cuarto de servidores
    - En la sede central, el personal de TI detectó un incremento inusual de temperatura en el cuarto de servidores.
    - Al revisar, encontraron que uno de los sistemas de refrigeración fue apagado manualmente, generando riesgo de sobrecalentamiento en los servidores críticos.
    - Las puertas de acceso al cuarto de servidores no registraron actividad sospechosa, lo que sugiere que alguien con acceso autorizado cometió la acción.
    - La empresa no cuenta con sensores de temperatura en tiempo real ni alarmas para avisar sobre fallos en la refrigeración.

3. Daño físico a la infraestructura por incendio
    - Un incendio en una subestación eléctrica cercana provocó cortes de energía en la sede central.
    - La empresa cuenta con generadores de respaldo, pero estos tardaron en activarse porque no se les había dado mantenimiento en meses.
    - Algunos servidores críticos sufrieron daños por sobrecarga eléctrica debido a la fluctuación de voltaje durante el incidente.
    - No existen protocolos claros para responder a desastres naturales o incendios en la infraestructura de la empresa.

Requerimientos

1. Explicar la importancia de la seguridad física en una empresa de almacenamiento de datos y la relación con la seguridad de la información. Identificar los principales errores de la seguridad física de la organización y describir como estos afectan a la continuidad del negocio. (**2 Puntos**)

2. Clasificar los incidentes en intrusión, sabotaje y desastre naturales. Además de evaluar el impacto de cada riesgo en la infraestructura de la empresa y su relación con la disponibilidad y confidencialidad de los datos. (**2 Puntos**)

3. Proponer tres medidas de protección perimetral para evitar accesos no autorizados en los POP y sede central. Además de explicar que sistema de control de acceso se puede implementar en la organización para garantizar que solo el personal autorizado pueda ingresar a las áreas críticas. (**3 Puntos**)

4. Proponer mejoras para reforzar la seguridad en los puntos de presencia, asegurando que ataques similares no vuelvan a ocurrir. Además de explicar 3 medidas claves para mejorar la seguridad en el cuarto de servidores, considerando refrigeración, incendio y monitoreo. (**3 Puntos**)

 ¡Mucho éxito!

Consideraciones y recomendaciones