Análisis de caso

Desafío – Seguridad en entornos TIC

José Miguel Rivera

Empresa “Data Secure INC”

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)

La seguridad física en Data Secure INC es de suma importancia, para poder proveer de un servicio confiable y de calidad la empresa necesita contar con una infraestructura física que permita la disponibilidad 24/7 del servicio, y además, que las medidas de seguridad y protección de los equipamientos estén en óptimas condiciones, estos problemas se han encontrado en Data Secure Inc:

- Falta de mantenimiento de equipamiento de refrigeración, esto resulta crítico en el control de temperaturas del data center.
- No hay un monitoreo de equipos o un lugar donde el software de control se reporte a alguna oficina o puesto de control, generándose alarmas cuando hay movimientos inusuales en los servidores.
- no hay evidencia de cámaras de seguridad.
- No hay pruebas de equipos de respaldo.
- No están definidos los procedimientos y protocolos en caso de problemas.
- Los accesos no están debidamente controlados.

Todas estas fallas provocan problemas han afectado de sobre manera a esta empresa y su continuidad no está garantizada.

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 Punto)

Incidente	Impacto	Evaluación de disponibilidad
Intrusión	Grave, acceso a instalaciones mediante tarjeta clonada	Alta, la desconexión de equipos de la red provocó que una porción de clientes no tuviera acceso al servicio.
Sabotaje	Peligroso, existe personal interno que atenta contra la empresa por lo que se debe alertar a las jefaturas que puedan	Importante, se filtrará a los clientes que la empresa sufre ataques internos lo que bajará la

	identificar este tipo de trabajadores a fin de evitar que circule en lugares donde no debe encontrarse.	aprobación de los clientes hacia la empresa y pone en riesgo la confidencialidad.
Desastres naturales	Grave, no existen protocolos ni procedimientos ante desastres. Los generadores tardan en levantar el servicio y se dañan los servidores por sobrecargas eléctricas.	Alto, la seguridad de los servidores debe aumentar y los planes de respaldo ante fallos deben estar verificados

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)

a) Debe existir control de guardias en sectores determinados de la empresa.
b) Los pórticos deben contar con un control de huella y el personal debidamente enrolado
c) Debe ser de conocimiento quienes o qué personal puede entrar a que lugares, además de que los ingresos y manipulaciones deben quedar registradas, los trabajos documentados y los reportes informados.

Se sugiere cambiar las tarjetas de acceso por credenciales simples, cada persona debe portar su credencial con foto, nombre y cargo, y si es externo debe indicar que es visita.

Los pórticos de acceso deben tener un control de huella y los data center cámaras operativas.

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)

Es clave que en los puntos de presencia exista rotación de guardias en todo horario y la implementación de un libro de incidentes o bitácora que el personal de seguridad informe posteriormente en cada apertura o cierre.

- Los equipos de aire acondicionado deben tener un plan de mantenimiento visible y registrado.
- Deben existir sensores de humo.
- El sistema de vigilancia debe estar operativo y en la sala de cámaras deben haber monitores y una comunicación fluida que pueda ser por radio.