Exámen práctico Modulo III

Daniel Stix Soto

Según las especificaciones y características empresariales, vamos a realizar un análisis de riesgo correspondiente a sus activos.

Caracterización cualitativa de las amenazas:

1. Corte de comunicaciones: conexión por cobre y respaldo 4G, sin interrupción en los últimos 3 años.

2. Corte de suministro eléctrico: recurrentes durante la época de lluvia

3. Ataque por ransomware: servidor no dedicado (utilizado para múltiples funciones), sin mención de medidas de ciberseguridad.

Análisis cualitativo:

Amenaza	Probabilidad
Corte de comunicaciones	Baja
Corte de suministro	Alta
Ataque por ransomware	Alta

Mátriz de riesgo (impacto*probabilidad):

Asumiendo que todas las amenzas producen una degradación del 100% del activo, asignamos valores númericos a la escala cualitativa. En una escala del 1 al 10, 1 siendo baja, 5 siendo media y 10 siendo alta.

| Amenaza | Impacto (10) | Probabilidad | Riesgo (10 × P)

| Corte de comunicaciones | 10 | 1 (Baja) | 10
| Corte de suministro | 10 | 10 (Alta) | 100
| Ataque por ransomware | 10 | 10 (Alta) | 100

Análisis por activos:

1. Base de datos: al contener las URL´s extraídas y datos de clientes, si el servicio se pierde o no está accesible no puede generar los correos
Riesgo: Total
Impacto: Servicio inutilizable sin acceso e integridad a la BDD

2. Servidor: ejecuta programa de búsquedas, guarda URL´s y genera correo. También usado para tareas no controladas
Riesgo: Muy alto
Impacto: Caída del servicio, corrupción de datos, malware

3. Electricidad: cortes frecuentes durante época de lluvias. Sin energía, no funcona ni el servidor ni la red.
Riesgo: Crítico
Impacto: Servicio detenido

4. Comunicaciones: utilizado para búsqueda online de noticias y envío de correos. Cierta estabilidad proporcionada mediante el respaldo 4G. Posible degradación
Riesgo: Bajo
Impacto: Servicio con funcionalidad lenta pero no inutilizado

| Activo | Dependencia | Riesgo | Impacto en Disponibilidad
| BBDD | Total | Alto | Crítico (sin datos no hay servicio)
| Servidor | Total | Muy Alto | Crítico (centro del proceso)
| Electricidad | Total | Crítico | Crítico (caída total del sistema)
| Comunicaciones | Total | Bajo | Bajo (posible lentitud, no interrupción completa) |

Posibles contramedidas por activo:

1. Electricidad (cortes frecuentes)
Contramedida:

Instalación de un SAI (Sistema de Alimentación Ininterrumpida) o batería de respaldo.

Opción más avanzada: Generador eléctrico automático.

Beneficio:

Mantiene el servidor encendido durante cortes breves.

Da tiempo para apagados seguros o continuidad limitada del servicio.

2. Servidor (uso compartido, sin seguridad)
Contramedida:

Separar el servidor en un entorno dedicado solo para el servicio de noticias.

Instalar software antivirus/antimalware, restringir la navegación y uso recreativo.

Crear usuarios separados con permisos limitados.

Beneficio:

Reduce drásticamente el riesgo de infección o mal uso.

Mejora la disponibilidad y estabilidad del sistema.

3. Ransomware (alta probabilidad)
Contramedida:

Copias de seguridad automatizadas y versionadas de la BBDD y configuraciones del sistema.

Guardarlas en un sistema externo o en la nube, desconectado del servidor.

Beneficio:

Recuperación rápida tras un ataque.

Reducción del impacto del secuestro de datos.

4. Comunicaciones (riesgo bajo, pero dependiente)
Contramedida:

Optimizar el uso del respaldo 4G, usando un sistema de conmutación automática.

Monitorización de la red para detectar fallos y cambiar al canal alternativo.

Beneficio:

Asegura el envío del correo diario incluso ante cortes del canal principal.

Conclusión:
La implementación de medidas de redundancia (energía y red), junto con una mejora en la ciberseguridad y gestión del servidor, reducirá significativamente los riesgos identificados y garantizará la disponibilidad y continuidad del servicio.