GRUPOTECNOLÓGICOUNIVERSITARIO

TECNOLÓGICO UNIVERSITARIO AGUASCALIENTES

VALORES · CULTURA · VANGUARDIA EDUCATIVA

ALUMNO: JONATHAN ALEJANDRO RAMIREZ GONZALEZ

MATRÍCULA: 1954

CUATRIMESTRE: NOVENO

CARRERA: LICENCIATURA EN INGENIERIA SISTEMAS COMPUTACIONALES

ASIGNATURA: AUDITORIA DE LA INFORMACIÓN

DOCENTE: ING. MORALES TERRONES JOSÉ CARLOS

FECHA DE ENTREGA: 20/05/2025

Parte 1: Análisis de Impacto al Negocio (BIA)

Escenario:

La empresa *ServiTech*, especializada en servicios de TI, sufre un ataque de ransomware que cifra todos sus servidores y paraliza las operaciones por 48 horas.

Procesos críticos y análisis de impacto:

Proceso	Impacto financiero	Impacto reputacional	Tiempo máximo tolerable (MTD)
Soporte técnico	$5,000/hr en penalizaciones por SLA	Alta (clientes insatisfechos, pérdida de contratos)	2 horas
Gestión de infraestructura	$3,000/hr (interrupción de servicios de hosting y redes)	Media (percepción de inestabilidad)	4 horas
Atención al cliente	$1,500/hr (cancelaciones, quejas)	Alta (mala imagen en redes sociales)	6 horas

Parte 2: Diseño de Planes

A. Plan de Respaldo (Backup)

Estrategia 3-2-1:

Realizar respaldo diario de datos críticos (base de datos de clientes, tickets, configuraciones de red).

- **3** copias de seguridad:
  - Copia 1: en servidor local
  - Copia 2: en disco externo cifrado en oficina
  - Copia 3: en nube (Google Cloud Storage o AWS S3)
- **2** tipos de soporte: almacenamiento en disco físico + almacenamiento en la nube
- **1** copia fuera del sitio: sede alterna segura

B. Plan de Recuperación

Pasos prioritarios de recuperación:

1. Activar protocolo de contingencia y notificar al equipo de TI.
2. Aislar los sistemas afectados para contener el ransomware.
3. Restaurar respaldos más recientes desde la nube/sede alterna.
4. Verificar la integridad de los datos restaurados.
5. Reanudar progresivamente los servicios críticos.
6. Monitorear sistemas y aplicar parches de seguridad.
7. Realizar informe post-incidente.

C. Plan de Emergencia

Protocolo de comunicación durante la crisis:

- **Interno (empleados):**
  - Notificación vía SMS y app de comunicación interna (ej. Microsoft Teams alternativo o WhatsApp).
  - Usar correos alternos personales si el sistema de correo corporativo está afectado.
  - Reunión virtual de emergencia por Zoom (con cuenta externa).
- **Externo (clientes):**
  - Comunicado oficial por redes sociales (Twitter, Facebook).
  - Página web de respaldo con banner de estado del servicio.
  - Email informativo desde cuenta secundaria (ej: continuidad_servitech@gmail.com).

Parte 3: Simulación de Pruebas

Escenario de prueba:

Simular un corte total de acceso al servidor principal durante 1 hora, incluyendo la caída de la base de datos de clientes y la gestión de tickets.

Métricas para evaluar el éxito:

1. **Tiempo de recuperación (RTO):** objetivo menor a 2 horas.
2. **Porcentaje de datos restaurados:** mínimo 95% de integridad.
3. **Comunicación efectiva:** confirmación del 100% del personal sobre el plan de emergencia.

Parte 4: Comparación de Estrategias de Continuidad

Estrategia	Ventajas	Desventajas
Recuperación en la nube	Escalabilidad, acceso desde cualquier lugar, rápida recuperación	Dependencia del proveedor, costos por uso
Centro de datos propio	Control total, personalización de seguridad	Requiere inversión inicial alta, mantenimiento constante

Reflexión Final: ¿Qué estrategia es mejor para ServiTech?

Recomendaría la **recuperación en la nube** para *ServiTech*, ya que su giro (servicios de TI) requiere alta disponibilidad, flexibilidad y recuperación rápida. Además, una empresa mediana como esta puede evitar los altos costos de infraestructura física, delegando la disponibilidad y redundancia a un proveedor confiable como AWS, Azure o Google Cloud. No obstante, es importante mantener al menos una copia local cifrada como respaldo adicional.

Anexos:

Flujo resumido de recuperación:

Ataque → Aislamiento → Restauración → Verificación → Comunicación → Reanudación

Riesgos adicionales:

- Falta de personal capacitado en ciberseguridad.
- Caídas eléctricas que afecten respaldos locales.
- Errores humanos al restaurar sistemas o manejar comunicaciones.