Perfil de la Empresa Simulada

Nombre: TiendaOnlineExpress
Sector: Comercio electrónico
Activos sensibles: Almacena datos personales de clientes, inventarios, y datos de pago.

Paso 1: Identificación de Activos Críticos

Objetivo:

Identificar y priorizar los activos más importantes que se deben proteger.

Actividad:

Activos identificados:

1. **Base de datos de clientes** (información personal y tarjetas de crédito)
2. **Servidor del sitio web** (disponibilidad de la tienda)
3. **Sistema de pagos**
4. **Backups en la nube**
5. **Credenciales de acceso administrativo**

Clasificación de criticidad:

- **Crítica:** BD de clientes, sistema de pagos
- **Alta:** servidor web, backups
- **Media:** credenciales de empleados

Paso 2: Análisis de Amenazas y Riesgos

Objetivo:

Identificar amenazas y evaluar riesgos.

Amenazas identificadas:

- **Phishing** → robo de credenciales de empleados

- **Ransomware** → secuestro de la base de datos
- **Ataques DDoS** → caída del sitio
- **Malware** → robo de datos confidenciales

Impactos:

- Pérdida de confianza del cliente
- Sanciones legales por filtración de datos (Ley Habeas Data)
- Interrupción de las ventas

Paso 3: Formación del Equipo de Respuesta a Incidentes

Roles definidos:

- **Coordinador general**: Encargado de decisiones estratégicas
- **Técnico de sistemas**: Aísla y analiza los sistemas afectados
- **Legal**: Evalúa el impacto legal y prepara comunicados
- **Responsable de comunicación**: Informa a clientes/proveedores
- **Soporte al cliente**: Atiende consultas y gestiona reputación

Listado de contactos de emergencia: Se creó y se guardó en el servidor interno y copia física.

Paso 4: Desarrollo de Procedimientos de Detección

Procedimiento diseñado:

- Monitoreo de logs del servidor web y base de datos
- Configuración de alertas en el firewall
- Revisión diaria de intentos de acceso fallido

Paso 5: Elaboración del Plan de Contención

Plan de contención básico:

1. Identificar sistemas comprometidos

2. Desconectar máquinas afectadas
3. Cambiar credenciales comprometidas
4. Notificar al equipo de respuesta
5. Informar a proveedores de servicios si aplica

Paso 6: Plan de Recuperación y Continuidad del Negocio

Estrategia diseñada:

- Restauración desde copias de seguridad (diarias y semanales)
- Revisión post-restauración con herramientas anti-malware
- Comunicación a clientes en caso de filtración de datos
- Prueba trimestral del plan de recuperación

Paso 7: Conclusiones

Aprendizajes clave:

- Importancia de la planificación antes del incidente
- La detección temprana y la respuesta rápida marcan la diferencia
- Cada activo debe tener su propio plan de protección
- La ciberseguridad no es solo tecnología, también es comunicación y organización

---