Carlos Alberto Rasgo Solano

Paso 1: Identificación de Activos Críticos
Como responsable de seguridad, mi primera accion fue identificar los activos más importantes de la empresa. Estos activos son los recursos que, si se ven comprometidos, podrían afectar gravemente la operación, la reputación o las finanzas del negocio.

Acciones realizadas:
Reuní al equipo técnico y al equipo administrativo en una breve reunión. Hicimos un listado conjunto de todos los activos relevantes, entre ellos:

- **Base de datos de clientes y transacciones** (incluye información de tarjetas).
- **Servidor web de la tienda online**.
- **Sistema de pagos** integrado con pasarelas externas.
- **Backups automáticos** de la plataforma y datos.
- **Cuentas de correo corporativo** y sus accesos.
- **Acceso administrativo al panel de control del e-commerce**.

Clasificación de criticidad:

Activo	**Nivel de Criticidad**	**Justificación**
Base de datos de clientes	Crítico	Contiene datos personales y financieros.
Servidor web	Crítico	Si cae, no se pueden realizar ventas.
Sistema de pagos	Crítico	Afecta ingresos y experiencia del cliente.
Backups	Alto	Necesarios para recuperación.
Cuentas de correo	Medio	Riesgo de phishing o fuga de información.
Panel administrativo	Alto	Acceso a configuración y gestión interna.

Paso 2: Análisis de Amenazas y Riesgos

Evaluación:
Analizamos los riesgos más comunes que podrían afectar nuestros activos. Durante esta fase se identificaron las siguientes amenazas relevantes:

- **Phishing a empleados** para robar credenciales.

- **Malware o troyanos** instalados desde archivos o plugins de terceros.
- **Ataques DDoS** que afecten la disponibilidad de la tienda.
- **Ransomware** que cifre nuestra base de datos.
- **Acceso no autorizado al sistema de pagos**.

Ejemplo realista:
Uno de nuestros desarrolladores descargó recientemente un plugin para el sitio web desde una fuente no verificada. Afortunadamente fue revisado antes de instalarse, pero demuestra una potencial vía de entrada para malware.

Priorización de riesgos:

Amenaza	Probabilidad	Impacto	Riesgo total
Phishing	Alta	Alto	Alto
Malware externo	Media	Alto	Alto
DDoS	Media	Medio	Medio
Ransomware	Baja	Crítico	Alto
Acceso a pagos	Media	Crítico	Alto

Paso 3: Formación del Equipo de Respuesta a Incidentes

Acción:
Conformamos un pequeño equipo para actuar en caso de incidentes, asignando roles claros:

- **Líder del equipo (Carlos)**: Coordino la respuesta y superviso las decisiones.
- **Técnico de sistemas (Hector)**: Encargado del análisis de logs y bloqueo de amenazas.
- **Encargada de comunicación (Laura)**: Gestiona comunicación interna y con clientes.
- **Asesor legal (Nehemias)**: En caso de compromisos legales o notificación a entidades.

Listado de contactos de emergencia:
Creamos una lista actualizada con los números de cada uno, incluyendo alternativas si alguno no está disponible.

Carlos Alberto Rasgo Solano

Paso 4: Desarrollo de Procedimientos de Detección

Medidas tomadas:
Implementamos herramientas básicas de monitoreo:

Procedimiento interno básico:

1. Revisar logs de acceso al sistema web diariamente.
2. Validar actividad inusual con el IDS.
3. Analizar peticiones con carga anómala o errores repetitivos.
4. Documentar cualquier comportamiento irregular.

Paso 5: Elaboración del Plan de Contención

Simulación y preparación:
Desarrollamos un plan de contención en caso de que uno de nuestros activos críticos se vea comprometido:

- **Aislar el sistema afectado** inmediatamente del resto de la red.
- Notificar al equipo de respuesta para que inicie el análisis.
- Cambiar todas las contraseñas administrativas del sistema.
- Detener procesos sospechosos o no autorizados.
- Si hay indicios de ransomware, no apagar los sistemas hasta análisis.

Protocolo activado en caso de clonación del sitio:

- Notificar de inmediato a hosting y registrar el sitio falso ante la autoridad competente.
- Enviar solicitud a Google para marcación como phishing.
- Publicar alerta en nuestras redes oficiales indicando que **no es nuestro sitio**.

Protocolo ante firma digital robada o falsificada:

- Revocar de inmediato el certificado comprometido.
- Generar uno nuevo y redistribuir por los canales oficiales.
- Contactar a clientes frecuentes explicando el cambio y medidas adoptadas.

Carlos Alberto Rasgo Solano

Paso 6: Plan de Recuperación y Continuidad del Negocio

Plan definido:

- **Respaldo:** Hacemos respaldos automáticos diarios en un servidor externo (encriptado).
- **Pruebas de restauración:** Se realizan cada semana simulaciones de restauración parcial.
- **Continuidad:** Tenemos una landing page con información y contacto que se activa si el sitio principal falla.
- **Comunicación externa:** Hay un comunicado prediseñado para informar a los clientes si ocurre una filtración o caída importante.

Simulación reciente:
Probamos recuperar una copia de la base de datos en otro servidor y logramos restablecer el sistema completo en 1.2 horas.