**🧑‍🏫 Taller de Ciberseguridad – Caso E-Shop Online**

**Guía para el Mentor – Lenguaje claro y práctico**

**✅ 1. Identificación de Activos Críticos**

**Objetivo:** Identificar los activos más críticos de la empresa que deben ser protegidos.

🔹 **Explicación sencilla:**  
Un *activo crítico* es todo lo que si se daña, se borra o lo roban, afecta gravemente al negocio. Son cosas que no pueden fallar.

🔹 **Activos clave de E-Shop Online:**

* **Base de datos de clientes:** nombres, direcciones, historial de compras y tarjetas.
* **Servidor de aplicaciones web:** donde funciona la tienda en línea.
* **API de pago:** conecta con el banco o el sistema que cobra al cliente.
* **Backups:** copias de seguridad de toda la información importante.
* **Sistema de autenticación:** lo que permite a los clientes iniciar sesión en sus cuentas.

🔹 **Clasificación por nivel de criticidad:**

* **Nivel 1 (Muy Crítico):** Base de datos de clientes, API de pago.
* **Nivel 2 (Crítico):** Servidor de aplicaciones web, Backups.
* **Nivel 3 (Moderado):** Sistema de autenticación de usuarios.

**✅ 2. Análisis de Amenazas y Riesgos**

**Objetivo:** Identificar qué amenazas puede enfrentar cada activo y qué tan grave sería el impacto.

🔹 **Amenazas frecuentes en tiendas online:**

* **Phishing:** suplantación de identidad (por ejemplo, correos falsos).
* **Ransomware:** virus que secuestra los datos y pide un rescate.
* **DDoS:** ataque que satura el servidor y lo deja fuera de servicio.
* **Inyección SQL:** forma de robar datos modificando las consultas.
* **Pérdida o corrupción de Backups:** por error humano o ataques.

🔹 **Análisis de riesgos de la empresa (ejemplo):**

| **Activo** | **Amenaza** | **Riesgo** | **Impacto** | **Probabilidad** | **Mitigación** |
| --- | --- | --- | --- | --- | --- |
| Base de datos de clientes | Ransomware | Secuestro de datos sensibles | Alto | Medio | Backups diarios cifrados, mantener software actualizado |
| API de pago | Inyección SQL | Robo de datos financieros durante pagos | Muy alto | Alto | Pruebas de seguridad, autenticación robusta |
| Servidor web | Ataque DDoS | Sitio fuera de línea y pérdida de ventas | Alto | Alto | Servicios anti-DDoS, uso de CDN |
| Sistema de autenticación | Phishing | Robo de contraseñas de clientes | Medio | Medio | MFA (doble autenticación), capacitación en seguridad |
| Backups | Corrupción / pérdida | Imposibilidad de recuperar los datos en caso de fallo | Muy alto | Bajo | Automatizar verificación de backups, almacenamiento cifrado y redundante |

**✅ 3. Formación del Equipo de Respuesta a Incidentes**

**Objetivo:** Tener un equipo preparado para actuar rápidamente en caso de ataque.

🔹 **Roles sugeridos:**

* **Coordinador de Incidentes:** organiza y dirige la respuesta.
* **Técnico de Seguridad:** analiza y corrige los problemas.
* **Responsable de Comunicaciones:** informa a clientes y empleados.
* **Asesor Legal:** verifica que todo se maneje según la ley.

🔹 **Ejemplo de equipo:**

| **Rol** | **Nombre** | **Contacto** |
| --- | --- | --- |
| Coordinador de Incidentes | Laura Martínez | laura@eshoponline.com |
| Técnico de Seguridad | Juan Pérez | juan.seguridad@eshop.com |
| Comunicaciones | Ana Gómez | ana@eshoponline.com |

**✅ 4. Desarrollo de Procedimientos de Detección**

**Objetivo:** Detectar a tiempo si algo sospechoso está ocurriendo.

🔹 **Herramientas recomendadas:**

* Splunk u otro visor de registros (logs).
* Sistemas de alertas automáticas.

🔹 **Monitoreo clave:**

* Fallos repetidos de inicio de sesión (más de 5 veces).
* Transacciones sospechosas (montos altos o desde otros países).

🔹 **Ejercicio sugerido:**  
Pedir a los estudiantes que diseñen un procedimiento básico de monitoreo con alertas diarias.

**✅ 5. Elaboración del Plan de Contención**

**Objetivo:** Actuar rápido para evitar que el daño se propague.

🔹 **Escenario simulado:** Ataque DDoS al servidor web.

🔹 **Acciones inmediatas:**

* Aislar el servidor.
* Activar respaldo o redirigir a un servidor alternativo (CDN).
* Notificar al proveedor de protección anti-DDoS.
* Comunicar a los clientes que el sitio está en mantenimiento.

**✅ 6. Plan de Recuperación y Continuidad del Negocio**

**Objetivo:** Volver a operar lo más pronto posible tras un incidente.

🔹 **Escenario simulado:** Ransomware cifra la base de datos de clientes.

🔹 **Plan de recuperación:**

* Restaurar la última copia de seguridad.
* Verificar que los datos estén completos y sin errores.
* Informar a los clientes sobre lo sucedido con claridad.