Ciberseguridad en el sector comercio electrónico

**Duración:**

2 horas

**Objetivos del Laboratorio:**

1. Fortalecer la seguridad de la información y protección de datos sensibles.
2. Preparar a la empresa para responder eficazmente ante incidentes de seguridad.
3. Diseñar pautas para un plan de recuperación y continuidad del negocio.

**Materiales Necesarios:**

* Repositorio en GitHub
* Acceso a la plataforma Academia Cisco
* Computador
* Acceso a Internet

**Estructura del Laboratorio:**

**Perfil de la Empresa:**

**Tipo:** Pequeña empresa de comercio electrónico  
**Actividad:** Venta de productos en línea y almacenamiento de datos de tarjetas de crédito.  
**Objetivo general del taller:** Presentar la importancia de la ciberseguridad en el comercio electrónico.

**1. Identificación de Activos Críticos**

**Objetivo:** Identificar los activos más críticos de la empresa.

**Actividades:**

* Introducción al concepto de activos críticos.
* Ejercicio grupal: Listado de activos importantes (bases de datos, servidores, sitio web).
* Clasificación por nivel de criticidad y priorización.

**2. Análisis de Amenazas y Riesgos**

**Objetivo:** Evaluar amenazas cibernéticas y riesgos por activo.

**Actividades:**

* Explicación de amenazas (phishing, malware, ransomware, DDoS).
* Ejercicio grupal: Relación amenazas vs. activos.
* Discusión sobre impactos y priorización.

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

**Objetivo:** Definir roles y responsabilidades para enfrentar incidentes.

**Actividades:**

* Presentación del equipo de respuesta a incidentes (CSIRT).
* Simulación: Asignación de roles (comunicaciones, técnico, legal, etc.).
* Elaboración de un listado de contactos y responsabilidades.

**4. Desarrollo de Procedimientos de Detección**

**Objetivo:** Establecer procedimientos de detección temprana.

**Actividades:**

* Explicación de herramientas (logs, sistemas de detección de anomalías).
* Demostración: Revisión de logs de seguridad.
* Ejercicio grupal: Procedimiento básico de monitoreo.

**5. Elaboración del Plan de Contención**

**Objetivo:** Minimizar el impacto de un incidente.

**Actividades:**

* Explicación de estrategias de contención.
* Ejercicio grupal: Plan que incluya aislamiento, desconexión y notificación.
* Revisión y retroalimentación de los planes.

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

**Objetivo:** Establecer medidas para recuperación tras un incidente.

**Actividades:**

* Presentación de buenas prácticas en recuperación y continuidad.
* Ejercicio grupal: Crear plan de recuperación (copias de seguridad, comunicación).
* Simulación de recuperación ante un escenario hipotético.

**7. Conclusiones y Preguntas**

**Objetivo:** Recapitular los aprendizajes y resolver dudas.

**Actividades:**

* Repaso general del taller.
* Espacio de preguntas y respuestas.
* Cierre y entrega de material complementario.

**8. Evaluación del Taller**

**Objetivo:** Recoger retroalimentación del grupo.

**Actividades:**

* Discusión final con comentarios y sugerencias.

**Lista de Verificación:**

* Revisar los conceptos en Academia Cisco.
* Subir un documento PDF al repositorio GitHub con las actividades realizadas.