LABORATORIO 4

JERRY RIVERA SANCHEZ

JESÚS TORO NAVARRO

CIBERSEGURIDAD

VALLEDUPAR - CESAR

2025

1. Paso 1: Identificación de Activos Críticos

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

Actividades:

Explicación: Introducir el concepto de activos críticos y su importancia.

Ejercicio: Pedir a los participantes que enumeren los activos más importantes de su empresa, como bases de datos de clientes, servidores, sitio web, etc.

Activo	**Nivel de Criticidad**	**Justificación**
Base de datos de clientes	Alta	Contiene información personal y de contacto de todos los clientes.
Sitio web	Media	Canal de comunicación e interacción con los usuarios.
Servidores de correo	Alta	Medio principal de comunicación corporativa.
ERP (sistema de gestión empresarial)	Alta	Maneja operaciones financieras, logística y recursos humanos.
Computadoras de empleados	Media	Herramientas de trabajo directo, con acceso a información crítica.

2. Análisis de Amenazas y Riesgos

Objetivo: Identificar las amenazas más probables y evaluar los riesgos para cada activo crítico.

Actividades:

Explicación: Describir diferentes tipos de amenazas cibernéticas (phishing, malware, ransomware, DDoS).

Ejercicio: Pedir a los participantes que enumeren los activos más importantes de su empresa, como bases de datos de clientes, servidores, sitio web, etc

Activo	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Base de datos de clientes	Ransomware	Alta	Alto	Alto
Sitio web	DDoS	Media	Media	Media
Servidor de correo	Phishing	Alta	Alta	Alto
ERP	Malware	Media	Alto	Alto
Computadoras	Acceso no autorizado	Alta	Media	Media

3. Formación del Equipo de Respuesta a Incidentes

Objetivo: Definir roles y responsabilidades para la respuesta a incidentes.

Actividades:

Explicación: Presentar la estructura y funciones de un equipo de respuesta a

incidentes.

Ejercicio: Asignar roles dentro de un equipo simulado (responsable de comunicaciones, técnico de sistemas, legal, etc.).

Discusión: Crear un listado de contactos de emergencia y responsabilidades.

Rol	**Persona asignada**	**Función**
Coordinador general	Jerry Rivera Sánchez	Dirige la respuesta al incidente.
Técnico de sistemas	Jesús Toro Navarro	Investiga causas técnicas y soluciones.

LISTADO DE CONTACTO DE EMERGENCIA

- **María González: +57 300 111 2222**
- **Soporte técnico 24/7: soporte@empresa.com**
- **Policía cibernética: 123**

4. Desarrollo de Procedimientos de Detección

Objetivo: Establecer procedimientos para detectar incidentes de seguridad de manera

temprana.

Actividades:

Explicación: Describir las herramientas y técnicas para monitoreo de logs, detección de anomalías, y sistemas de alertas.

Demostración: Mostrar un ejemplo de cómo configurar y revisar logs de seguridad.

Ejercicio: Diseñar un procedimiento básico de monitoreo para su empresa.

Procedimiento Básico:

1. Monitoreo diario de logs del firewall y antivirus.
2. Configuración de alertas automáticas ante accesos sospechosos o cambios en archivos críticos.
3. Revisión semanal de intentos de inicio de sesión fallidos.
4. Uso de herramientas como Wazuh, SIEM o Splunk.

5. Elaboración del Plan de Contención

impacto.

Objetivo Desarrollar un plan para contener un incidente de seguridad y minimizar su

Actividades:

Explicación: Explicar la importancia de la contención en la respuesta a

incidentes.

Ejercicio: Crear un plan de contención que incluya el aislamiento de sistemas afectados, desconexión de redes, y notificación al equipo de respuesta.

Plan de Contención:

1. Identificar sistemas afectados.
2. Aislar inmediatamente del resto de la red.
3. Cambiar contraseñas de los accesos comprometidos.
4. Informar al equipo de respuesta.
5. Activar medidas de respaldo (uso de sistemas de respaldo si es necesario).

6. Plan de Recuperación y Continuidad del Negocio

Objetivo: Desarrollar un proceso para la recuperación de datos y la continuidad del negocio tras un incidente.

Actividades:

Explicación: Presentar las mejores prácticas para la recuperación de datos y la continuidad del negocio.

Ejercicio: Elaborar un plan de recuperación, incluyendo

restauración desde copias de seguridad y notificación a clientes.

Plan de Recuperación:

1. Verificar estado de las copias de seguridad.
2. Restaurar sistemas afectados desde el backup más reciente.
3. Validar integridad de los datos recuperados.
4. Comunicar a los clientes el restablecimiento de los servicios.
5. Registrar lecciones aprendidas para futuras mejoras.

Simulación de Escenario:
Supongamos un ataque de ransomware en la base de datos.

- El sistema se aísla.
- Se restaura un backup de hace 6 horas.
- Se emite un comunicado a los clientes sobre lo sucedido y el tiempo de recuperación.

7. Conclusiones y Preguntas

Objetivo: Recapitular los aprendizajes y aclarar dudas.

Actividades:

Recapitulación: Repasar los principales puntos tratados durante el taller.

Preguntas y Respuestas: Abrir el espacio para preguntas finales y discusiones.

Cierre: Agradecimiento a los participantes y entrega de material complementario, si corresponde.

- **Punto Clave:** La ciberseguridad no es solo tecnología, es también personas y procesos.
- **Recomendación:** Hacer simulacros cada 6 meses y actualizar el plan de respuesta.
- **Preguntas frecuentes:** ¿Cómo saber si un correo es phishing? ¿Cada cuánto hacer backups?