Laboratorio 4

Deivis J. Castro

LABORATORIO: Ciberseguridad en el sector comercio

Paso1: Identificación de Activos Críticos

Objetivo: Determinar los activos esenciales de la empresa que requieren protección prioritaria.

Actividades:

- Definición de activos críticos: Explicar qué son y por qué son fundamentales en la seguridad informática. Son elementos clave cuya vulnerabilidad puede afectar gravemente la organización.
- Ejercicio grupal: Solicitar a los participantes que identifiquen los activos más relevantes, como:
    - Bases de datos de clientes.
    - Servidores web.
    - Información financiera (tarjetas de crédito).
- Clasificación de activos: Evaluar su nivel de criticidad (*alto, medio, bajo*) y priorizar la protección de aquellos con mayor impacto en la operación, como bases de datos y sistemas de pago.

Tipos de Activos Críticos:

1. Información Sensible

- Datos financieros (*números de tarjetas, fechas de vencimiento, CVV*).
- Información personal (*nombre, dirección, teléfono, correo electrónico*).
- Historial de compras y preferencias.
- Credenciales de acceso (*usuarios, contraseñas cifradas*). Valor: Altamente sensible. Su exposición compromete la privacidad, seguridad financiera y reputación de la empresa.

2. Infraestructura Tecnológica

- Servidor web (*plataforma de comercio electrónico*).
- Servidor de aplicaciones (*gestiona la lógica del negocio*).
- Base de datos (*almacena información crítica*).

- Pasarela de pagos (*payment gateway*).
- Sistemas de respaldo y recuperación. Valor: Esenciales para la operación. Un ataque puede interrumpir ventas, causar filtraciones o pérdida de datos.

3. Plataforma de Comercio Electrónico

- Sitio web o CMS (*Shopify, WooCommerce, Magento*).
- Plugins y extensiones instaladas.
- Plantillas de correos automáticos y confirmaciones de pedido. Valor: Medio-alto. Su vulnerabilidad puede facilitar fraudes, redirección maliciosa o estafas.

4. Cuentas Administrativas

- Accesos de administrador a servidores, bases de datos y sitios web.
- Credenciales de pago, hosting, DNS y correo electrónico. Valor: Críticas. Su compromiso otorga control total sobre el entorno.

5. Seguridad de Red y Conexiones

- Cortafuegos (*firewall*).
- Certificados SSL/TLS.
- Configuración de red (*VPNs, routers, switches*).
- Seguridad en la nube (*si aplica*). Valor: Alta. Protege el tráfico de datos y previene accesos no autorizados.

6. Recursos Humanos

- Personal de TI, atención al cliente y marketing digital.
- Accesos, formación y prácticas seguras. Valor: Alto. Un error humano o una cuenta comprometida puede generar incidentes de seguridad.

7. Políticas y Procedimientos

- Normativas de seguridad de la información.
- Protocolos de gestión de incidentes.
- Manual de recuperación de desastres (*DRP*).
- Documentación de cumplimiento normativo (*PCI-DSS*).

Nº	Activo	Tipo de Activo	Descripción	Nivel de Criticidad
1	**Datos de tarjetas de crédito**	Información	Números, vencimiento, CVV de tarjetas	**Alta**
2	**Datos personales de clientes**	Información	Nombre, dirección, email, teléfono, historial de compras	**Alta**
3	**Base de datos de clientes y transacciones**	Tecnológico	Motor y estructura de datos que contiene información sensible	**Alta**
4	**Servidor web y de aplicaciones**	Tecnológico	Hospeda el sitio y ejecuta la lógica de negocio	**Alta**
5	**Plataforma de pagos (pasarela)**	Tecnológico / Tercero	Proveedor externo que gestiona los pagos electrónicos	**Alta**
6	**Sistema de backups**	Tecnológico	Copias de seguridad para restaurar datos ante incidentes	**Media-Alta**
7	**Certificado SSL/TLS**	Tecnológico	Garantiza la seguridad de las comunicaciones web	**Media**
8	**Cuentas de administrador**	Acceso / Credenciales	Accesos privilegiados a sistemas críticos y plataformas	**Alta**
9	**Plataforma de comercio electrónico**	Tecnológico	CMS o framework (Shopify, WooCommerce, etc.)	**Media-Alta**
10	**Red local / conectividad segura**	Tecnológico	VPN, firewall, routers, configuración de red	**Media**
11	**Empleados con acceso privilegiado**	Humano	Personal técnico y administrativo con acceso a sistemas sensibles	**Alta**
12	**Documentación de políticas y planes (DRP, PCI-DSS, etc.)**	Organizacional	Procedimientos para responder a incidentes y asegurar cumplimiento	**Media**
13	**Proveedor de hosting y DNS**	Tercero / Infraestructura	Infraestructura externa que permite el funcionamiento del sitio web	**Media-Alta**
14	**Emails corporativos**	Comunicación	Cuentas usadas para comunicaciones internas y con clientes	**Media-Baja**
15	**Redes sociales de la empresa**	Comunicación / Imagen	Canales públicos de contacto y reputación	**Media-Baja**
16	**Reputación de la empresa**	Intangible		**Crítica**

Alta: Pérdida o exposición compromete seriamente la seguridad, privacidad o continuidad del negocio.

Media: Afecta operaciones y reputación, pero se puede contener sin impacto crítico.

Baja: Impacto limitado o indirecto.

Paso 2: Evaluación de Amenazas y Riesgos.

Objetivo: Identificar las amenazas más relevantes y analizar los riesgos asociados a cada activo crítico.

Actividades:

- **Introducción a las amenazas cibernéticas:** Explicar los principales riesgos que enfrenta una empresa de comercio electrónico, incluyendo:
    - **Phishing:** Correos fraudulentos diseñados para engañar a los empleados y obtener credenciales.
    - **Malware:** Software malicioso que compromete la seguridad de los sistemas.
    - **Ransomware:** Ataques que bloquean datos esenciales y exigen un pago para su recuperación.
    - **DDoS (Denegación de Servicio):** Saturación de servidores que provoca la caída del sitio web.
- **Análisis de riesgos en grupo:** Identificar amenazas específicas para cada activo crítico previamente definido.
- **Discusión y priorización:** Evaluar la probabilidad e impacto de cada amenaza, determinando cuáles representan mayor riesgo para la empresa en términos de pérdida de datos, interrupción de servicios y afectación a la reputación.

Nº	Activo Crítico	Amenazas Probables	Probabilidad	Impacto	Nivel de Riesgo	Cómo puede afectar al negocio	Cómo mitigar el riesgo
1	Datos de tarjetas de crédito	Robo de datos, acceso no autorizado, malware, phishing	Alta	Alto	Crítico	Multas regulatorias (PCI-DSS), pérdida de confianza del cliente, demandas legales	Cifrado de datos, cumplimiento PCI-DSS, autenticación multifactor (MFA), segmentación de red
2	Datos personales de clientes	Filtración de datos, errores humanos, vulnerabilidad web	Media-Alta	Alto	Alto	Daño reputacional, quejas de clientes, sanciones por protección de datos	Cifrado, DLP (prevención de pérdida de datos), formación al personal, revisión de código
3	Base de datos de clientes	Inyección SQL, ransomware, acceso indebido	Alta	Alto	Crítico	Interrupción de operaciones, pérdida masiva de datos	Validación de entradas, copias de seguridad cifradas, actualización de sistemas, control de accesos
4	Servidor web y de aplicaciones	Ataques DDoS, explotación de vulnerabilidades, defacement	Media	Alto	Alto	Sitio web caído, pérdida de ventas	WAF (Firewall de aplicaciones web), parcheo frecuente, monitoreo continuo, balanceo de carga
5	Plataforma de pagos (pasarela)	Intercepción de datos, spoofing, uso indebido de API	Media	Alto	Alto	Transacciones comprometidas, pérdida de ingresos	TLS fuerte, autenticación API, validación de origen, pruebas de seguridad periódicas
6	Sistema de backups	Fallos de respaldo, pérdida o corrupción de datos	Media	Alto	Alto	Imposibilidad de recuperación	Estrategia 3-2-1 de backups, verificación periódica, respaldo offline, cifrado de copias
7	Certificado SSL/TLS	Expiración, configuración incorrecta, MITM	Media-Baja	Medio	Medio	Sitio "no seguro", pérdida de confianza	Renovación automática, escaneo de certificados, configuración segura (TLS 1.2/1.3), pruebas SSL
8	Cuentas de administrador	Robo de credenciales, acceso interno malintencionado	Alta	Alto	Crítico	Acceso total a los sistemas, sabotaje	MFA obligatorio, principio de mínimo privilegio, monitoreo de actividad, rotación de credenciales
9	Plataforma de comercio electrónico	Plugins maliciosos, falta de actualización	Media	Medio	Medio	Fallos en el sitio, pérdida de funcionalidad	Actualizaciones frecuentes, análisis de vulnerabilidades, control de cambios, plugins de confianza

10	Red local / conectividad segura	Accesos remotos no seguros, red mal segmentada	Media	Alto	Alto	Accesos no autorizados	VPN segura, segmentación de red, control de acceso basado en roles (RBAC), monitoreo de tráfico
11	Empleados con acceso privilegiado	Ingeniería social, errores humanos, amenazas internas	Media-Alta	Alto	Alto	Brechas internas de datos	Concienciación, registros de auditoría, separación de funciones, controles de comportamiento
12	Políticas y planes de seguridad	Desactualización, desconocimiento del personal	Media	Medio	Medio	Mala respuesta a incidentes	Actualización anual, formación periódica, distribución clara de políticas
13	Proveedor de hosting / DNS	Caídas del servicio, ataque a terceros	Media	Medio	Medio	Inaccesibilidad al sitio	Contrato con SLA, DNS redundante, monitoreo externo, copias espejo
14	Emails corporativos	Phishing, spoofing, malware	Alta	Medio	Medio-Alto	Suplantación de identidad, entrada de malware	Filtros anti-phishing, autenticación SPF/DKIM/DMARC, capacitación de usuarios
15	Redes sociales de la empresa	Suplantación, ataques de reputación	Media	Bajo	Bajo-Medio	Daño a la marca	Autenticación 2FA, monitoreo de cuentas, respuesta rápida, uso de cuentas verificadas

Paso 3: Creación del Equipo de Respuesta a Incidentes

Objetivo: Establecer roles y responsabilidades clave para gestionar incidentes de seguridad de manera eficiente.

Actividades:

- Presentación de la estructura del equipo: Explicar las funciones de cada integrante en la respuesta a incidentes. Roles esenciales incluyen:
    - **Coordinador de Comunicaciones:** Supervisa la comunicación interna y externa durante el incidente.
    - **Especialista Técnico:** Responsable de la contención y mitigación del problema.
    - **Encargado Legal:** Evalúa las implicaciones normativas y jurídicas del incidente.

- **Ejercicio grupal:** Asignar roles dentro de un equipo simulado para que los participantes comprendan sus responsabilidades.
- **Discusión:** Elaborar un listado de contactos de emergencia y definir sus funciones (técnicos, proveedores de servicios, soporte legal).

Estructura del Equipo de Respuesta a Incidentes

1. **Coordinador del CSIRT:** Supervisa la planificación y ejecución de la respuesta a incidentes, además de ser el enlace con la alta dirección.
2. **Analistas de Seguridad**: Detectan, investigan y eliminan amenazas, proporcionando asesoramiento técnico.
3. **Especialistas en Comunicación**: Gestionan la difusión de información dentro y fuera de la empresa, asegurando claridad y transparencia.
4. **Responsable Legal y de Cumplimiento:** Garantiza que las acciones del equipo cumplan con regulaciones y normativas internas.
5. **Representante de IT/Infraestructura:** Implementa medidas técnicas como el aislamiento de sistemas y la recuperación de datos.
6. **Enlace con Gestión de Riesgo**: Evalúa el impacto del incidente y coordina estrategias para mantener la continuidad del negocio**.**

Funciones Principales del Equipo

- **Preparación:** Desarrollo de protocolos, formación del personal y simulacros de respuesta.
- **Identificación:** Detección de anomalías y clasificación de incidentes según su gravedad.
- **Contención:** Implementación de medidas para evitar la propagación del ataque.
- **Erradicación:** Eliminación de amenazas y refuerzo de seguridad.
- **Recuperación:** Restauración de sistemas y verificación de su integridad antes de reactivarlos.
- **Lecciones aprendidas:** Evaluación del incidente, mejoras en protocolos y documentación de hallazgos.

Normativas y Buenas Prácticas

- **NIST SP 800-61r2:** Guía para la gestión de incidentes de seguridad informática.
- **ISO/IEC 27035:** Estándares para la administración de incidentes de seguridad.
- **CERT/CC:** Recomendaciones para la respuesta efectiva ante incidentes.

Paso 4: Desarrollo de Protocolos de Detección

Objetivo: Establecer métodos y procesos que permitan identificar de forma temprana incidentes de seguridad.

Actividades:

- **Explicación**: Presentar las herramientas y técnicas utilizadas para el monitoreo de seguridad, por ejemplo:
    - **Sistemas de detección de intrusiones (IDS):** Dispositivos o software que detectan accesos o comportamientos anómalos.
    - **Análisis de logs:** Examinar los registros generados por los sistemas en busca de actividades irregulares.
    - **Alertas de seguridad:** Configurar notificaciones automáticas que informen sobre eventos sospechosos.
- **Demostración**: Realizar una presentación práctica sobre la configuración y revisión en tiempo real de los registros de seguridad.
- **Ejercicio Grupal:** Diseñar, en conjunto, un protocolo básico de monitoreo personalizado para la empresa.

Ejemplos de Sistemas de Detección de Intrusiones (IDS)

1. NIDS (Network-based IDS)

- Monitorean el tráfico de red para detectar patrones sospechosos.

Nombre	Características clave	Tipo	Licencia
Snort	Muy popular, basado en reglas, desarrollado por Cisco	NIDS	Open Source
Suricata	Multihilo, soporte de protocolos modernos, DPI	NIDS	Open Source
Zeek (Bro)	Análisis profundo de protocolos, scripting flexible	NIDS	Open Source
Cisco Secure IPS (anteriormente Sourcefire)	Integrado en soluciones de red Cisco, prevención activa	NIDS/IPS	Comercial
Security Onion	Distribución completa con Snort, Suricata, Zeek y ELK	NIDS	Open Source

2. HIDS (Host-based IDS)

- Monitorean actividad en equipos específicos (procesos, archivos, registros).

Nombre	Características clave	Tipo	Licencia
OSSEC	Detección de rootkits, monitoreo de integridad, alertas	HIDS	Open Source
Wazuh	Fork de OSSEC con mejoras, integración con ELK	HIDS	Open Source
AIDE	Detección de cambios en archivos (FIM)	HIDS	Open Source
Tripwire	Control de integridad de archivos, versiones comercial y libre	HIDS	Comercial/Open Source
Samhain	Auditoría de integridad y detección de rootkits	HIDS	Open Source

Otros IDS híbridos o embebidos

Nombre	Descripción
Prelude SIEM	Framework modular que permite integrar sensores NIDS/HIDS
AlienVault OSSIM	SIEM con detección de intrusos integrada
CrowdStrike Falcon *(más EDR que IDS)*	Detecta y responde a intrusiones en endpoints

Paso 5: Elaboración del Plan de Contención

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

Actividades:

Explicación: Explicar la importancia de actuar rápidamente para contener el ataque, con ejemplos como:

Aislamiento de sistemas afectados.

Desconexión de redes comprometidas.

Notificación inmediata al equipo de respuesta**.**

1. Clasificación del Incidente

Antes de contener, se debe identificar y clasificar el tipo de incidente:

Tipo de incidente	**Ejemplos**
Malware/Ransomware	Cifrado de archivos, comportamiento anómalo
Phishing	Correos fraudulentos, robo de credenciales
Acceso no autorizado	Usuarios desconocidos o sin permisos accediendo
DDoS	Saturación de servicios, caídas
Exfiltración de datos	Descarga masiva no autorizada

2. Acciones inmediatas (contención rápida)

Acción	**Detalle**
Aislar sistemas comprometidos	Desconectar dispositivos de la red para evitar propagación
Cambiar credenciales comprometidas	Forzar cambio de contraseñas y revocar sesiones
Deshabilitar cuentas	Suspender cuentas sospechosas o vulneradas
Bloquear tráfico sospechoso	En firewalls, proxies o IDS/IPS (por IP, puerto, protocolo)
Detener servicios comprometidos	Detener temporalmente servicios afectados para evitar daños

3. Contención a mediano plazo (estabilización)

Acción	**Detalle**
Aplicar parches urgentes	Corregir vulnerabilidades conocidas explotadas
Reforzar reglas en firewalls y IDS/IPS	Basadas en indicadores de compromiso (IOC)
Implementar segmentación temporal	Separar redes críticas de entornos afectados
Registrar toda la actividad	Captura de logs, hashes de archivos, IPs involucradas para análisis posterior

4. Comunicación del incidente

Acción	**Responsable**	**Público**
Notificar al CSIRT / equipo de TI	Usuario afectado o SOC	Interno
Informar a directivos / legal / cumplimiento	CSIRT	Interno
Notificación externa (si aplica)	Legal o comunicaciones	Autoridades, clientes, reguladores

5. Criterios para contener sin destruir evidencia

No formatear ni reiniciar los equipos comprometidos sin autorización del equipo forense.

Capturar la memoria RAM y estado del sistema si se sospecha de malware avanzado.

Preservar los discos en estado original si hay intención de emprender acciones legales.

6. Verificación y transición a recuperación

Confirmar que el ataque está contenido (sin nuevas alertas).

Validar integridad de los sistemas y datos.

Preparar la fase de recuperación segura con sistemas limpios y parchados.

7. Documentación durante la contención

Elemento	Ejemplo
Línea de tiempo del incidente	Hora de detección, contención, escalamiento
Recursos comprometidos	IPs, usuarios, sistemas
Acciones tomadas	Quién, qué, cuándo
Logs y evidencia	Capturas, archivos, tráfico

8. Herramientas útiles para la contención

EDR (CrowdStrike, SentinelOne, Defender): para aislamiento rápido.

SIEM (Splunk, Wazuh, QRadar): para correlación y alertas.

Firewalls / IDS/IPS (pfSense, Suricata, Cisco ASA): para bloqueo de tráfico.

Sysinternals / Volatility: para análisis de sistemas afectados.

Paso 6: Desarrollo del Plan de Recuperación y Continuidad del Negocio

Objetivo: Diseñar un procedimiento que permita restaurar la información y asegurar el funcionamiento continuo del negocio tras un incidente**.**

Actividades

Presentación Teórica: Explicar las prácticas recomendadas para recuperar datos y garantizar la continuidad operativa, abarcando aspectos como**:**

- **Restauración a partir de respaldos:** Verificar que la información crítica se respalde periódicamente.
- **Comunicación con los clientes:** Informar de forma clara y transparente a los clientes en caso de que sus datos se vean afectados.
- **Ejercicio en Grupo:** Cada grupo debe elaborar un plan de recuperación que haga especial énfasis en la reconstitución de los datos esenciales y en la estrategia de comunicación dirigida a los clientes.
- **Debate y Simulación:** Realizar una simulación de un escenario de recuperación y evaluar la respuesta de cada grupo para identificar aciertos y áreas de mejora.

Proceso Resumido para la Recuperación de Datos y Continuidad del Negocio

1. **Evaluación del Impacto y Establecimiento de Prioridades**
    - **Meta:** Determinar detalladamente qué sistemas y procesos han sido comprometidos, priorizando aquellos de mayor impacto en la operativa del negocio.
    - Se deben identificar y clasificar los activos afectados según criterios de RTO y RPO, definidos conforme a las necesidades empresariales**.**
2. **Recuperación de Información Desde Copias de Seguridad**
    - **Meta**: Restaurar la información perdida o comprometida utilizando respaldos confiables.
    - Confirmar la integridad de los backups para asegurarse de que no contienen malware ni están corruptos, y proceder a la restauración en entornos seguros.
    - Verificar que la información recuperada cumpla con el margen definido en el RPO y documentar todo el proceso.
3. **Reinstalación y Fortalecimiento de la Seguridad en los Sistemas**
    - **Meta:** Garantizar que los sistemas y plataformas sean confiables para su operación.
    - En caso de sospecha de infecciones persistentes, reinstalar los sistemas desde medios limpios, aplicar parches y configuraciones seguras, y fortalecer los controles de acceso.
    - Revocar credenciales comprometidas y emitir nuevas contraseñas tras documentar el impacto en los usuarios.
4. **Verificación de la Funcionalidad de los Sistemas**
    - **Meta:** Comprobar que las aplicaciones y servicios restaurados operen según lo esperado.
    - Ejecutar pruebas end-to-end y de aceptación de usuario (UAT) para confirmar que los datos y procesos estén íntegros y completos.
5. **Reanudación de las Operaciones Críticas**
    - **Meta:** Reactivar las funciones esenciales del negocio, asegurando que los servicios clave se recuperen y operen de forma estable.

Buenas Prácticas para la Recuperación y Continuidad del Negocio

- **Gestión Eficiente de Backups:**
    - Implementar la estrategia 3-2-1 (tres copias de datos en dos medios distintos y una almacenada fuera del sitio, ya sea offline o en la nube).
    - Programar respaldos automáticos y realizar pruebas periódicas de restauración, asegurando que se ubiquen bajo cifrado y controles de acceso.
- **Definición de Parámetros de Recuperación:**
    - RTO (Tiempo Objetivo de Recuperación): Tiempo máximo tolerable sin acceso a un servicio sin repercusiones significativas.
    - RPO (Punto Objetivo de Recuperación): Cantidad de datos que se pueden perder entre respaldos sin causar daños críticos.
- **Plan Documentado y Probado:**
    - Desarrollar y ensayar un Business Continuity Plan (BCP) y un Disaster Recovery Plan (DRP) que integren roles, recursos, y procedimientos claros, además de criterios para su activación.
    - Realizar simulacros regulares involucrando a todos los participantes.
- **Aseguramiento en la Recuperación:**
    - Confirmar que los sistemas recuperados estén libres de infecciones y aplicar parches y configuraciones de seguridad necesarias antes de volver a producción.
    - Actualizar contraseñas y revisar accesos en entornos comprometidos.
- **Verificación Post Recuperación:**
    - Validar la integridad de los datos recuperados y ejecutar pruebas funcionales para asegurar que todo opere de forma correcta.
    - Documentar cualquier discrepancia o pérdida de información para futuros análisis.
- **Comunicación Estructurada:**
    - Mantener informados a todos los equipos, la dirección y las partes interesadas sobre el estado de la recuperación y la continuidad del negocio de manera constante.

Norma / Estándar	Enfoque principal
ISO/IEC 27001	Gestión de seguridad de la información. Incluye control A.17 para continuidad del negocio en seguridad
ISO/IEC 27031	Directrices específicas para la continuidad de las TIC y recuperación tras incidentes
ISO 22301	Sistema de gestión de la **continuidad del negocio** (BCMS) – enfoque integral
NIST SP 800-34 Rev.1	Guía para la planificación de contingencia para sistemas de TI
NIST SP 800-61 Rev.2	Manejo de incidentes de seguridad informática – incluye fases de recuperación
COBIT 2019	Gobierno y gestión de TI – incluye controles sobre continuidad y recuperación
ITIL v4	Mejores prácticas para la gestión de servicios TI – incluye gestión de incidentes y continuidad del servicio