Laboratorio 4

Héctor Díaz

1. Un activo es todo aquello que representa un valor tangible y/o intangible para la organización, bajo este concepto un activo critico es cualquier recurso, infraestructura o sistema que si se ven comprometidos, pueden afectar la operación, estabilidad y competitividad de la organización.

Activos Criticos:

a. Red y conexiones seguras:
   - Cortafuegos (Firewall)
   - Certificados SSL/TLS
   - Configuración de red (VPNs, routers, switches, hubs)

   Valor alto, Protege el trafico de datos y evita el acceso no autorizado

b. Información:
   - Datos de tarjetas de crédito (número, fecha de vencimiento, CVV si se almacena)
   - Datos personales: nombre, dirección, teléfono, correo electrónico
   - Historial de compras y preferencias
   - Credenciales de acceso: usuarios y contraseñas

   valor crítico, altamente sensible, su filtración compromete la privacidad, seguridad del cliente y la organización

c. Infraestructura de servidores:
   - Servidor web (donde opera la tienda online)
   - Servidores de aplicaciones (gestiona la lógica de negocio)
   - Base de datos donde se almacenan datos sensibles

- Plataformas de pagos y pasarela (payment Gateway)
- Sistemas de backup y recuperación

Valor critico, altamente esencial para la organización, un ataque o fallo puede interrumpir ventas, filtraciones o perdida total de datos

d. Plataformas de correo electrónico:
    - Sitio web o CMS por ejemplo Shopify, WooCommerce, Magneto.
    - Plugins o extensiones instaladas.
    - Plantillas de correo automáticos y confirmaciones de pedidos.

    Valor medio-alto, Su compromiso puede llevar a vulnerabilidades, redirección maliciosa o estafas.

e. Empleados y contratistas:
    - Personal de IT, atención al cliente, marketing digital, etc.
    - Accesos, formación, comportamiento seguro

    Valor alto, Un error humano o una cuenta comprometida puede causar un incidente de ciberseguridad

f. Políticas y procedimientos:
    - Política de seguridad de información
    - Procedimientos de gestión de incidentes
    - Manual de recuperación de desastres DRP
    - Documento de cumplimiento normativo PCI-DDS

Valor medio-alto, ayudan a prevenir, detectar y responder correctamente a incidentes.

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**

2.

Phishing: es el uso comunicación digital por medio de correo electrónico en las que se suplanta la identidad de una persona o empresa con el objetivo de engañar a otras personas para que revelen datos confidenciales o implementen un software malicioso.

Malware: es un software diseñado para dañar dispositivos o redes.

Ransonware: un ataque malicioso en el que los agentes de amenaza cifran los datos de una organización y exigen un pago (rescate) para restablecer el acceso a ellos

DDoS: Sobrecarga los servidores y provoca la caída del sitio.

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	Ataques DDoS, explotació	Media	Alto	Alto	Sitio web caído,	WAF (Firewall de aplicaciones

	aplicaciones	n de vulnerabilidades, defacement				pérdida de ventas	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

3.

Responsable de Comunicaciones: Encargado de coordinar la comunicación interna y externa durante el incidente.
Técnico de Sistemas: Responsable de la contención técnica y mitigación.
Legal: Evalúa las implicaciones legales del incidente.
o **Ejercicio Grupal**: Asignar roles dentro de un equipo simulado para cada participante.
o **Discusión**: Crear un listado de contactos de emergencia y sus responsabilidades (técnicos, proveedores de servicios, soporte legal).
Resultado Esperado: Definir un equipo de respuesta a incidentes con roles claros y establecidos para una acción rápida en caso de emergencia.

Estructura un Equipo de Respuesta ante Incidentes

1. El Coordinador o Jefe del CSIRT

Es quien está al frente de planificar, coordinar y supervisar cómo se responde a los incidentes. También es el contacto con los directivos y otras personas importantes para la empresa.

2. Analistas de Seguridad / Técnicos de Respuesta

Son expertos en encontrar, investigar, contener y eliminar incidentes por completo. Están atentos a las alertas, analizan qué pasa y dan consejos técnicos para solucionar problemas.

3. Especialistas en Comunicación

Se encargan de informar a todos, tanto dentro como fuera de la empresa, cuando hay un incidente. Preparan informes, dan actualizaciones y se aseguran de que todos sepan lo que está pasando.

4. Responsable de Asuntos Legales y Cumplimiento

Se asegura de que todo lo que haga el equipo cumpla con las leyes y las normas internas.

Se encarga de temas como avisar si ha habido fallos de seguridad, guardar pruebas y dar apoyo legal.

5. Representante de IT/Infraestructura

Ayuda a poner en marcha medidas técnicas, como aislar sistemas o recuperar copias de seguridad.

Trabaja junto a los que administran los sistemas y las redes.

6. Enlace con Gestión del Riesgo o Continuidad del Negocio

Calcula cómo afecta el incidente a las cosas más importantes que hace la empresa. Pone en marcha planes para seguir funcionando si es necesario.

Qué hace Principalmente el Equipo de Respuesta ante Incidentes

a. Preparación

Crear normas, formas de actuar y planes para responder a los incidentes.

Formar al personal y hacer simulacros para practicar (ejercicios de simulación).

Poner en marcha herramientas para estar atentos y dar la voz de alarma.

b. Identificación

Detectar si pasa algo raro o si hay programas maliciosos.

Decidir qué incidentes son más importantes y urgentes.

c. Contención

Hacer cosas para que el incidente no se extienda ni cause más daño. Aislar los sistemas afectados para que el problema no llegue a otros sitios.

d. Erradicación

Eliminar lo que causó el incidente (virus, cuentas robadas, fallos de seguridad). Asegurarse de que no quede ni rastro del que atacó.

e. Recuperación

Devolver los servicios y sistemas a un estado seguro y en funcionamiento. Comprobar que todo está bien antes de volver a ponerlo en marcha.

Lecciones Aprendidas / Después del Incidente

- Analizar por qué pasó, qué daño causó y cómo actuó el equipo.
- Mejorar las formas de actuar y las medidas de prevención.
- Hacer un informe sobre el incidente (análisis post-mortem).

Normas y buenas prácticas que se suelen seguir

- NIST SP 800-61r2: Guía para saber cómo actuar ante incidentes de seguridad informática.
- ISO/IEC 27035-1/2/3: Normas para gestionar los incidentes de seguridad de la información.
- CERT/CC: Consejos y formas recomendadas de manejar los incidentes.

4.

Sistemas de detección de intrusiones (IDS).

Análisis de logs: Revisar los registros en busca de actividad anómala.

Alertas de seguridad: Configurar sistemas de alerta para recibir notificaciones ante eventos sospechosos.

o **Demostración**: Mostrar cómo configurar y revisar logs de seguridad en tiempo real.

o **Ejercicio Grupal**: Diseñar un procedimiento básico de monitoreo adaptado a 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

5.

Aislamiento de sistemas afectados.
Desconexión de redes comprometidas.
Notificación inmediata al equipo de respuesta.
o **Ejercicio Grupal**: Crear un plan de contención que incluya las medidas a tomar en las primeras 24 horas.
o **Discusión**: Revisar los planes

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.

6.

Proceso resumido de la recuperación de los datos y la continuidad de negocio

1. Evaluación del daño y priorización

Objetivo: Valorar que información o qué procesos se han visto afectados (en este caso, priorizando los más críticos).
Identificar de forma detallada aquellos sistemas y datos que han de considerarse comprometidos o perdidos.
Clasificar los procesos según el camino de retorno que produzca un impacto mayor en el negocio.
Habilitar los planes de recuperación de la continuidad de negocio siguiendo aquellas prioridades de RTO/RPO definidas entre la organización y la RM (requerimientos del negocio).

2. Restauración de los datos a partir de backups

Objetivo: Recuperar la información perdida o afectada desde copias de seguridad seguras.
Comprobar que los backups (en cuanto a su integridad) no se encuentren infectados de malware ni corruptos.
Restaurar en ambientes seguros y controlados, para actuar en el proceso del negocio antes de volver a la producción.
Comprobar que los datos estén actualizados (dentro del RPO definido).
Documentar la restauración de los backups.

3. Reinstalación y aseguramiento de sistemas

Objetivo: Asegurar que sistemas operativos y plataformas sean confiables para ser usados.
Reinstalar sistemas a partir de los medios de instalación "limpios" si existe sospecha de persistencia de malware.
Aplicar parches, configuraciones seguras y refuerzo de controles de acceso.
Revocar credenciales comprometidas, documentar usuarios a partir de listas de uso y crear nuevas credenciales para quienes lo necesiten.

4. Verificación de la funcionalidad

Objetivo: Comprobar si sistemas y aplicaciones devuelven los resultados esperados.
Ejecutar pruebas funcionales de los servicios restaurados (pruebas de extremo a extremo, end-to-end).
Involucrar a los usuarios clave mediante pruebas de usuario (pruebas UAT).
Comprobar que los datos restaurados son coherentes y que están completos.

5. Reanudación de operaciones críticas
Objetivo: Llevar a cabo la recuperación de tales operaciones críticas.

Mejores Prácticas de Recuperación de Datos y Continuidad del Negocio

1. **Backups eficaces**

Implementar la estrategia 3-2-1: tres copias de los datos, en dos medios distintos, y una fuera del site (offline o en la nube).
Realizar copias automatizadas y programadas.
Probar periódicamente la restauración de backups.
Proteger copias cifrando y definiendo un control de acceso adecuado.

2. Definir RTO y RPO

RTO (Recovery Time Objective): cuánto tiempo se puede estar sin acceder a un servicio antes de que esto afecte gravemente al negocio.
RPO (Recovery Point Objective): cuánto tiempo de datos se pueden perder (máximos tolerados entre respaldos).

3. Tener un plan documentado y ensayado

Diseñar un Business Continuity Plan (BCP) y un Disaster Recovery Plan (DRP).
Incluir responsables, recursos, procedimientos y criterios de activación.
Ejecutar simulacros periódicos con todos los involucrados.

4. Seguridad de la recuperación

Verificar que los sistemas restaurados no están infectados.
Poder aplicar parches y configuraciones seguras antes de volver a poner sistemas en producción.
Modificar contraseñas y validar accesos en ambientes comprometidos.

5. Verificación post recuperación

Validar la integridad de los datos restaurados e inspeccionar que estén en estado consistente.
Ejecutar pruebas funcionales de los sistemas relevantes.
Documentar y analizar cualquier discrepancia o pérdida de datos.

6. Comunicación estructurada

Mantener informado al equipo, dirección y partes implicadas de cuál es el estado de la recuperación.

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