Laboratorio 4 Cursos CiberSeguridad

Jesús Rodrigo Toro Navarro

Jerry Rivera Sanchez

Seguridad informática

Universidad Popular del Cesar

Valledupar, Cesar

PASO 1

1)Identificar los activos más críticos de la empresa que deben ser protegidos

Base de datos de clientes

Historial de ventas y transacciones

Contratos con proveedores y clientes

Documentación financiera y contable

Planes estratégicos y de negocio

Propiedad intelectual (patentes, software, diseños, etc.)

2) Clasificar estos activos por nivel de criticidad y priorizar su protección:

Activo	**Nivel de Criticidad**	**Justificación**
Base de datos de clientes	**Alto**	Contiene datos personales y financieros. Su pérdida o filtración puede causar sanciones legales y dañar la reputación.
Historial de ventas y transacciones	**Alto**	Esencial para análisis financieros, auditorías, y control de ingresos. Su alteración puede impactar gravemente las decisiones.
Contratos con proveedores y clientes	**Alto**	Información legal y comercial crítica. Su pérdida puede romper relaciones comerciales y generar litigios.
Documentación financiera y contable	**Alto**	Información sensible para cumplimiento fiscal, auditorías y toma de decisiones estratégicas.
Planes estratégicos y de negocio	**Medio**	Información confidencial y competitiva. Importante para el futuro de la empresa, pero no afecta operaciones diarias.
Propiedad intelectual (patentes, software, etc.)	**Alto**	Clave para la ventaja competitiva. Su filtración o robo puede suponer una pérdida económica significativa.

Prioridad de Protección (Orden de Acción Recomendado)

1. **Base de datos de clientes**

   Protección inmediata con cifrado, control de acceso y monitoreo.

2. **Propiedad intelectual (patentes, software, diseños, etc.)**

   Requiere medidas legales y tecnológicas (cifrado, almacenamiento seguro, control de acceso).

3. **Documentación financiera y contable**

   Protección con respaldo frecuente, cifrado, y sistemas de acceso solo a personal autorizado.

4. **Contratos con proveedores y clientes**

   Asegurar mediante sistemas de gestión documental seguros y respaldo fuera del sitio.

5. **Historial de ventas y transacciones**

   Protección con sistemas de respaldo, cifrado y control de cambios.

6. **Planes estratégicos y de negocio**

   Aunque sensibles, se pueden proteger con sistemas internos de clasificación y acceso limitado.

PASO 2

Identificar las amenazas más probables y evaluar los riesgos para cada activo

Activo	Amenazas Probables	Probabilidad	Impacto	Nivel de Riesgo
Base de datos de clientes	Robo de datos (hackeo), acceso no autorizado, fuga de información interna	Alta	Alto	**Alto**
Historial de ventas y transacciones	Manipulación de datos, pérdida por error humano o técnico	Media	Alto	**Alto**
Contratos con proveedores y clientes	Alteración maliciosa, robo de información, eliminación accidental	Media	Alto	**Alto**
Documentación financiera y contable	Acceso no autorizado, ransomware, eliminación o modificación involuntaria	Media	Alto	**Alto**
Planes estratégicos y de negocio	Filtración externa, espionaje industrial, acceso no autorizado	Baja	Alto	**Medio-Alto**
Propiedad intelectual (software, diseños)	Robo por competencia, copia no autorizada, hackeo de sistemas de desarrollo	Media	Alto	**Alto**

Priorizar las amenazas y discutir posibles impactos en el negocio.

Amenaza	Activo afectado	Nivel de Riesgo	Posibles impactos en el negocio
Robo o filtración de datos de clientes	Base de datos de clientes	**Alto**	- Sanciones legales (Ley de protección de datos) - Daño a la reputación - Pérdida de confianza de clientes
Ransomware o pérdida de documentación contable	Documentación financiera y contable	**Alto**	- Imposibilidad de operar o reportar - Multas fiscales - Pérdida financiera
Robo de propiedad intelectual (PI)	Propiedad intelectual (software, diseños)	**Alto**	- Pérdida de ventaja competitiva - Daños económicos por uso indebido de PI
Manipulación o pérdida del historial de ventas	Historial de ventas y transacciones	**Alto**	- Análisis financiero incorrecto - Malas decisiones estratégicas
Alteración o robo de contratos clave	Contratos con proveedores y clientes	**Alto**	- Conflictos legales - Pérdida de relaciones comerciales
Filtración de planes estratégicos	Planes estratégicos y de negocio	**Medio-Alto**	- Ventaja competitiva comprometida - Daños en fusiones, negociaciones o alianzas

Prioridad de acción (orden de atención recomendado):

1. **Proteger la base de datos de clientes**
   (por el alto valor legal, comercial y reputacional)
2. **Fortalecer la seguridad financiera y contable**
   (impacto directo en operaciones y cumplimiento legal)
3. **Blindar la propiedad intelectual**
   (clave para la innovación y diferenciación en el mercado)
4. **Controlar y asegurar los contratos**
   (prevención de conflictos legales y pérdida de confianza)

5. **Respaldar y asegurar el historial transaccional**
   (decisiones de negocio dependen de estos datos)
6. **Confidencialidad en planes estratégicos**
   (importante, aunque con menor frecuencia de ataque)

PASO 3 : Definir roles y responsabilidades para la respuesta a incidentes.

Función	**Descripción**
Detección y análisis del incidente	Identificar y entender el tipo, alcance y origen del incidente.
Contención del incidente	Evitar que el daño se propague (aislar sistemas, revocar accesos, etc.).
Erradicación y recuperación	Eliminar la amenaza y restaurar los sistemas afectados.
Comunicación	Informar a partes interesadas internas y externas, incluyendo clientes y autoridades.
Legal y cumplimiento	Asegurar que se cumplan normativas y preparar reportes legales, en caso de ser necesario.
Lecciones aprendidas	Evaluar lo ocurrido y mejorar las políticas de seguridad.

Contacto	**Rol / Departamento**	**Teléfono / Correo**	**Responsabilidad en Incidentes**
Coordinador del ERI	Seguridad TI	coord_eri@empresa.com	Liderar la respuesta, convocar al equipo
Responsable de Comunicaciones	Comunicación Interna/Externa	prensa@empresa.com	Gestionar mensajes oficiales
Encargado de Sistemas	Infraestructura TI	soporte@empresa.com	Aislamiento de sistemas, respaldo, recuperación

Legal / Cumplimiento	Departamento Jurídico	legal@empresa.com	Evaluar y notificar posibles implicaciones legales
Proveedor de Ciberseguridad	Empresa externa (si aplica)	contacto@ciberseguridad.com	Apoyo técnico externo, análisis forense
Agencia reguladora (ej. autoridad de datos)	Externo	contacto@autoridad.gob	Notificación obligatoria en caso de fuga de datos personales
Policía Cibernética	Externo	ciberpolicia@seguridad.gob	Investigación si se detecta delito o ataque externo

PASO 4: Establecer procedimientos para detectar incidentes de seguridad de manera temprana

Monitoreo Continuo de Sistemas y Redes

Implementar Alertas y Umbrales de Actividad Sospechosa

Registro y Análisis de Logs

Sensibilización y Canal de Reportes Internos

Pruebas de Penetración y Escaneos de Vulnerabilidades

Checklists de Revisión Proactiva

Inteligencia de Amenazas (Threat Intelligence)

Simulacros de Incidentes y Ataques Simulados

Ejemplo básico en Windows:

Visualizar logs desde el Visor de Eventos (Event Viewer):

1. Abrir el **Visor de eventos** (eventvwr.msc)
2. Ir a: **Registros de Windows > Seguridad**

3. Filtrar por ID de evento:
    - **4624**: Inicio de sesión exitoso
    - **4625**: Intento fallido de inicio de sesión

Puedes crear una tarea programada o alerta basada en estos eventos usando el programador de tareas o herramientas SIEM.

Ejemplo Básico Linux

Ver logs de autenticación

sudo tail -f /var/log/auth.log

Buscar intentos fallidos de inicio de sesión

grep "Failed password" /var/log/auth.log

PASO 5: Desarrollar un plan para contener un incidente de seguridad y minimizar su impacto.

Plan de Contención de Incidentes de Seguridad (Versión Operativa)

1. Detección inicial del incidente

- Fuente: Sistema SIEM, antivirus, usuario interno, escaneo de red, etc.
- Acción:
    - Registrar el evento con hora, origen y sistema implicado.
    - Notificar al responsable de ciberseguridad.

2. Aislamiento del sistema afectado

Acción	**Responsable**
Desconectar el equipo de la red (no apagar si es malware)	Técnico de sistemas
Bloquear el acceso remoto al sistema	Administrador de red
Identificar procesos o conexiones sospechosas	Analista de seguridad
Cambiar credenciales del usuario o servicio comprometido	Soporte TI

3. Desconexión de red (si aplica)

Acción	Responsable
Cortar tráfico de red entrante/saliente al sistema comprometido	Infraestructura / TI
Cerrar puertos sospechosos en firewall	Administrador de red
Detener VPN si se detecta uso indebido	Encargado de redes

4. Notificación al equipo de respuesta a incidentes (ERI)

A quién se notifica	Medio sugerido	Tiempo estimado
Líder del equipo ERI	Teléfono / Mensajería segura	Inmediato
Responsable de ciberseguridad	Correo con bitácora inicial	< 15 minutos
Área legal (si hay fuga de datos)	Correo y llamada directa	< 30 minutos
Comunicaciones corporativas	Slack / Teams / Correo	Si el incidente se hace público

5. Validación del aislamiento y análisis preliminar

Acción	Responsable
Verificar que el sistema ya no tiene acceso a red	Técnico de TI
Analizar logs para entender alcance inicial	Analista de ciberseguridad
Registrar evidencia inicial (memoria, tráfico, disco)	Soporte técnico/seguridad

PASO 6: Desarrollar un proceso para la recuperación de datos y la continuidad del negocio tras un incidente.

Proceso de Recuperación de Datos y Continuidad del Negocio

1. Evaluación del daño

Paso	**Acción**	**Responsable**
Identificación de sistemas afectados	Verificar qué servidores, apps o dispositivos fueron comprometidos	TI / Seguridad
Evaluación de pérdida de datos	Comparar estado actual con el último respaldo válido	Ciberseguridad / Backup
Clasificación del impacto	¿Se afectaron funciones críticas del negocio?	Gestión de continuidad

2. Activación del plan de recuperación

- Activar el **Plan de Continuidad del Negocio (BCP)** y el **Plan de Recuperación ante Desastres (DRP)**.
- Declarar nivel de incidente:
    - **Alto impacto:** requiere recuperación inmediata y uso de backups.
    - **Medio / Bajo impacto:** recuperación parcial o paulatina.

3. Recuperación de datos desde respaldos

Acción	**Detalle**
Verificar integridad del respaldo	Validar que esté limpio y actualizado (libre de malware)
Restaurar sistemas críticos	En orden de prioridad: ERP, correo, base de datos, etc.
Realizar pruebas de restauración	Comprobar que el sistema restaurado funciona correctamente
Documentar tiempos y fallos en recuperación	Para futuras mejoras del proceso

4. Restablecimiento de operaciones

Área	Acción
Sistemas	Verificar funcionalidad total y monitoreo post-incidente
Seguridad TI	Confirmar eliminación de amenazas, aplicar parches de seguridad
RRHH / Operaciones	Notificar a empleados sobre el retorno al sistema normal
Clientes / Usuarios externos	Comunicar normalización de servicios si aplica

5. Revisión post-incidente

Actividad	Descripción
Análisis forense	Determinar causa raíz del incidente
Evaluación de tiempos de recuperación	Comparar con objetivos definidos (RTO, RPO)
Mejora de planes	Actualizar protocolos de backup, respuesta y continuidad
Informe final	Detallar hallazgos, acciones tomadas y recomendaciones futuras

CONCLUSION

En un entorno cada vez más digitalizado y expuesto a riesgos, **proteger los activos de información y garantizar la continuidad operativa** no es opcional, sino una necesidad estratégica para cualquier organización. A través de este ejercicio, hemos establecido una serie de buenas prácticas y procesos fundamentales para enfrentar incidentes de seguridad de forma **proactiva, coordinada y efectiva**.

Los principales aprendizajes y pilares del proceso son:

1. Identificación de Activos Críticos

Reconocer qué información y sistemas son más valiosos permite priorizar su protección, desde bases de datos de clientes hasta propiedad intelectual o documentación financiera.

2. Monitoreo y Detección Temprana

Implementar herramientas de monitoreo de logs y alertas automatizadas ayuda a **identificar amenazas en etapas tempranas**, reduciendo su impacto. La detección oportuna es el primer paso hacia una respuesta efectiva.

3. Contención Inmediata

Actuar rápidamente para **aislar sistemas comprometidos, desconectar redes y activar protocolos** es esencial para evitar que un incidente se propague o cause más daño. La coordinación del equipo de respuesta es clave en esta fase.

4. Recuperación y Continuidad del Negocio

Contar con respaldos seguros y planes claros de recuperación (RTO y RPO definidos) permite **restaurar operaciones en el menor tiempo posible**, garantizando que la empresa siga funcionando incluso ante una crisis.

5. Documentación y Mejora Continua

Cada incidente debe ser una oportunidad de aprendizaje. Documentar el evento, analizar su causa raíz y actualizar los procedimientos fortalece la postura de seguridad a largo plazo.