Actividades evaluativas y Trabajo Práctico: Seguridad Informática

Actividad 1: Juego de roles

Nombre: ¿Qué harías si...?
Objetivo: Analizar situaciones reales y decidir respuestas adecuadas ante incidentes de seguridad.
Modalidad: Grupal.

Instrucciones:
1. recibirán 3 escenarios distintos (ej. ataque de ransomware, phishing, fuga de datos).
2. Representarán una empresa y deberán decidir:
   - ¿Cómo reaccionarían ante el incidente?
   - ¿Qué herramientas usarían?
   - ¿Qué harían para evitar que vuelva a suceder?
3. Presenten su análisis en una puesta en común

Escenarios propuestos:

Escenario 1: Ataque de Ransomware

- La empresa recibe un ataque de ransomware: todos los archivos críticos han sido cifrados. Los atacantes exigen un rescate en criptomonedas.
- ¿Qué hacen? ¿Pagan o no pagan? ¿Cómo restauran los sistemas? ¿Cómo comunican el incidente a los usuarios/clientes?
- ¿Qué políticas de respaldo implementarían para el futuro?

Escenario 2: Ataque de Phishing Interno

- Varios empleados reciben un correo falso que parece de Recursos Humanos solicitándoles ingresar sus contraseñas. Algunos cayeron en la trampa y dieron sus credenciales.
- ¿Cómo detectan y contienen el daño? ¿Cómo alertan al resto de los empleados?
- ¿Qué controles y capacitaciones implementarían para minimizar el phishing en adelante?

Escenario 3: Fuga de Datos Sensibles

INTEGRANTES DE CIBER DATA:
Eric Roth-Mia Ferreyra-Timoteo Sayago-Braian Junco-Mayra Chocou

- Se descubre que un empleado descargó sin permiso una base de datos con información personal de clientes y la compartió fuera de la empresa.
- ¿Qué acciones toman respecto al incidente y al empleado? ¿Cómo comunican la situación a las autoridades o clientes?
- ¿Qué nuevas políticas de control de acceso o monitoreo implementarían?

Actividad 2: Campaña de concienciación

Nombre: Que no te engañen
Objetivo: Diseñar mensajes claros para alertar a los usuarios sobre peligros comunes.
Modalidad: Grupal.

Instrucciones:
1. Elijan una amenaza (phishing, ransomware, etc.).
2. Diseñen una campaña simple (puede ser un folleto digital, una imagen, un video corto o una presentación).
3. Debe incluir:
   - Qué es el ataque
   - Cómo detectarlo
   - Cómo evitarlo
   - Consejos finales.
4. Exposición en clase o subida al aula virtual.

Actividad 3: Trivia de seguridad

Nombre: Cibertrivia
Objetivo: Repasar los conceptos clave en un formato lúdico.
Modalidad: Grupal.

Instrucciones:
1. Participarán en una trivia con preguntas sobre:
   - Tipos de malware
   - Medidas de protección
   - Casos reales
   - Herramientas como firewalls o antivirus
2. Las preguntas serán múltiples choice, verdadero/falso y preguntas abiertas simples.
3. Puntos por respuestas correctas. El grupo ganador tendrá una mención especial.

Esta actividad puede realizarse digital (Kahoot, Wordwall, Genially)

INTEGRANTES DE CIBER DATA:
Eric Roth-Mia Ferreyra-Timoteo Sayago-Braian Junco-Mayra Chocou

RESPUESTAS

Actividad 1: Juego de roles

Escenario 1: Ataque de Ransomware

- La empresa recibe un ataque de ransomware: todos los archivos críticos han sido cifrados. Los atacantes exigen un rescate en criptomonedas.
- ¿Qué hacen? ¿Pagan o no pagan? ¿Cómo restauran los sistemas? ¿Cómo comunican el incidente a los usuarios/clientes?
- ¿Qué políticas de respaldo implementarían para el futuro?

GUIA ORIENTADA A NOVATOS:

Pasos básicos para reaccionar

Aislar las computadoras afectadas

- ✓ Desconecta inmediatamente las máquinas infectadas de internet y de la red interna.
- ✓ Ejemplo: Como cuando un niño enfermo se queda en casa para no contagiar a otros.

Investigar el tipo de ransomware

- ✓ Identifica el "nombre" del virus (ejemplo: WannaCry, Locky).
- ✓ Usa herramientas como ID Ransomware (gratis) para saber de qué se trata.

¿Pagar o no pagar?

- ✓ No se recomienda pagar: 3 de cada 10 empresas que pagan no recuperan sus datos.
- ✓ El pago financia a los delincuentes y no garantiza solución.

Cómo recuperar los archivos

Si tienes copias de seguridad (backups):

- ✓ Usa backups limpios almacenados en discos externos o servicios en la nube.
- ✓ Verifica que no estén infectados antes de restaurar (como revisar comida caducada antes de comerla).

INTEGRANTES DE CIBER DATA:
Eric Roth-Mia Ferreyra-Timoteo Sayago-Braian Junco-Mayra Chocou

Si NO tienes backups:

- ✓ Software de recuperación como Recuva:
- ✓ Intenta recuperar archivos recién eliminados (como buscar fotos borradas por error en el celular).

- Éxito limitado: Funciona mejor si actúas rápido (primeras 24-48 horas).

Cómo avisar a clientes y empleados

- **Comunica con claridad**:

  - ✓ Di que hubo un problema técnico (sin detalles alarmantes).
  - ✓ Ejemplo: "Estamos resolviendo una falla en nuestros sistemas. Volveremos a la normalidad pronto".

  - ✓ **Ofrece ayuda**: Proporciona un correo o teléfono para consultas.

Cómo evitar futuros ataques

1. **Haz copias de seguridad (backups) inteligentes**:

   - ✓ **Guárdalas fuera de internet**: Usa discos duros externos que solo conectes al hacer la copia.
   - ✓ **Cifrado AES-256**: Protege las copias con un "candado digital" imposible de romper (como una caja fuerte).

2. **Prepara a tu equipo**:

   - ✓ **Capacitación básica**: Enseña a reconocer correos sospechosos (ejemplo: "Haz clic aquí para recibir un premio").
   - ✓ **Simulacros mensuales**: Envía correos falsos de prueba para entrenar a los empleados.

3. **Usa protecciones automáticas**:

   - ✓ **Antivirus actualizado**: Como un guardia que revisa todo lo que entra a la computadora.
   - ✓ **Firewall**: Funciona como un "portero" que bloquea accesos no autorizados.

INTEGRANTES DE CIBER DATA:
Eric Roth-Mia Ferreyra-Timoteo Sayago-Braian Junco-Mayra Chocou

GUIA PARA AVANZADOS

Primeramente se aislarían los sistemas afectados para que no se propague el ataque, seguidamente se identificaría la familia del ransomware y la empresa recopilaría evidencia del ataque.

Dependiendo la información sustraída, el precio del rescate y la gravedad del caso, se pagaría el rescate o no, sin embargo el 35% de los rescates pagados no se cumplen.

Restauración de sistemas

- Eliminar el ransomware mediante herramientas actualizadas de antivirus (como por ejemplo: **Bitdefender** que utiliza mecanismos de escaneo de comportamiento) y EPP (Endpoint Protection).
- Restaurar datos desde backups limpios, asegurando su integridad antes de la implementación.
- Verificar sistemas para detectar restos de malware o herramientas de acceso remoto instaladas por atacantes.
- Si no hay backups, usar software de recuperación de archivos como **RECUVA** que se caracteriza por enfocarse en recuperar archivos como "espacio libre" en el sistemas, siendo útil para recuperar los archivos cuando el ataque es reciente (éxito limitado).

COMUNICACION

Se comunicaría del incidente a los usuarios sin dar información muy técnica para no asustar a los posibles clientes.

POLITICAS DE RESPALDO

- Tener backups de la información para que en caso de un ataque se tengan copias de respaldo
- Almacenamiento offline: Protege contra infecciones en redes conectadas
- Cifrado AES-256: (El cifrado es un algoritmo de cifrado simétrico ampliamente utilizado para proteger datos sensibles en todo tipo de sistemas y comunicaciones digitales) Evita fugas de datos si el backup es interceptado
- Pruebas de restauración: Garantiza funcionalidad mediante simulacros trimestrales

---

Escenario 2: Ataque de Phishing Interno

INTEGRANTES DE CIBER DATA:
Eric Roth-Mia Ferreyra-Timoteo Sayago-Braian Junco-Mayra Chocou

- Varios empleados reciben un correo falso que parece de Recursos Humanos solicitándoles ingresar sus contraseñas. Algunos cayeron en la trampa y dieron sus credenciales.
- ¿Cómo detectan y contienen el daño? ¿Cómo alertan al resto de los empleados?
- ¿Qué controles y capacitaciones implementarían para minimizar el phishing en adelante?

GUIA PARA NOVATOS

1. **Identificar quién fue afectado**
    - Usar herramientas de seguridad (como alarmas digitales) que detectan accesos sospechosos a las cuentas.
    - Ejemplo: Como cuando un sistema de cámaras identifica a un intruso en una tienda.
2. **Proteger las cuentas**
    - Cambiar todas las contraseñas de los empleados afectados inmediatamente.
    - Bloquear el acceso a información sensible: DNI, direcciones, datos bancarios (como poner un candado a un archivero importante).
3. **Avisar a todo el equipo**
    - Enviar una alerta urgente por correo, SMS o reuniones explicando:
        - "¡Cuidado! Están enviando correos falsos que parecen de RRHH".
        - "Nunca compartas tu contraseña por correo o mensajes".
    - Hacer un simulacro 48 horas después: Enviar un correo falso de prueba para ver quién sigue cayendo en la trampa.

Cómo evitar futuros ataques

Herramientas automáticas:

Nombre	¿Qué hace?	Ejemplo
Filtro antispam	Bloquea correos falsos antes de que lleguen a la bandeja de entrada	Como un portero que no deja pasar a estafadores
Bloqueo DNS seguro	Impide acceder a enlaces peligrosos en correos o mensajes	Como un GPS que evita calles con baches
Autenticación en dos pasos	Pide un código extra (además de la contraseña) para entrar a las cuentas	Como un segundo candado en la puerta de tu casa

INTEGRANTES DE CIBER DATA:
Eric Roth-Mia Ferreyra-Timoteo Sayago-Braian Junco-Mayra Chocou

Capacitaciones esenciales:

- Enseñar a reconocer correos sospechosos:
    - Errores de ortografía (ej. "Urjente" en vez de "Urgente").
    - Enlaces raros (ej. *www.recursos-humanos-falso.com*).
- Prácticas mensuales: Simular correos falsos para entrenar a los empleados (como un simulacro de incendio, pero digital).

GUIA PARA AVANZADOS

En primer lugar se identificarían a los usuarios afectados mediante sistemas de detección de intrusiones. Luego se forzaría un reset de las contraseñas de las cuentas afectadas, también se restringiría el acceso a la base de datos sensible (DNI, dirección, información de la empresa en la que trabaja, etc).

Luego de lo descripto, se emitiría una alerta inmediata a cada empleado mediante distintos medios como correo electrónico, SMS, reuniones virtuales o presenciales, cartas.

Para probar esta alerta se haría un simulacro de phishing 48 horas después.

CONTROLES Y CAPACITACIONES

- Las medidas que se toman serian:
    - Recursos antispam: Se utilizarían para asi evitar que sean enviados a la bandeja principal de correos de cada trabajador
    - Bloqueo DNS: prohíbe el acceso a sitios malisiosos mediante links.
    - Autentificaciones: Mediante su implementación no se concurriría en la suplantación de identidad.

Escenario 3: Fuga de Datos Sensibles

- Se descubre que un empleado descargó sin permiso una base de datos con información personal de clientes y la compartió fuera de la empresa.
- ¿Qué acciones toman respecto al incidente y al empleado? ¿Cómo comunican la situación a las autoridades o clientes?
- ¿Qué nuevas políticas de control de acceso o monitoreo implementarían?

INTEGRANTES DE CIBER DATA:
Eric Roth-Mia Ferreyra-Timoteo Sayago-Braian Junco-Mayra Chocou

GUIA PARA NOVATOS

Pasos básicos para reaccionar

1. **Suspender al empleado sospechoso**
    - Ejemplo: Como cuando un profesor separa a un alumno que hizo trampa en un examen, mientras investiga.
    - Investigación forense: Expertos revisan computadoras y correos para encontrar pruebas (como detectives digitales).
2. **Si se confirma el robo de datos:**
    - Despedirlo con causa: Pierde su trabajo inmediatamente por romper las reglas.
    - Denunciar a la justicia: Abrir un caso legal por poner en riesgo la privacidad de las personas (como denunciar un robo en una casa).

Cómo informar a clientes y autoridades

- Avisar a la Agencia de Protección de Datos:
    - Ejemplo: Reportar un accidente a las autoridades para que te ayuden.
    - Plazo: Debe hacerse en menos de 72 horas después de descubrir el problema.
- Hablar con los clientes afectados:
    - Mensaje claro: "Tuvimos un problema de seguridad. Estos son los datos que pudieron verse. Esto es lo que estamos haciendo para protegerte".
    - Ofrecer ayuda gratis: Un equipo especial atenderá consultas por teléfono, correo o WhatsApp.

Cómo evitar que vuelva a pasar

Herramientas clave:

Nombre	¿Qué hace?	Ejemplo
Control de accesos	Solo los empleados que necesitan ver datos sensibles pueden acceder	Como dar llaves de una caja fuerte solo al gerente

INTEGRANTES DE CIBER DATA:
Eric Roth-Mia Ferreyra-Timoteo Sayago-Braian Junco-Mayra Chocou

Nombre	¿Qué hace?	Ejemplo
Sistemas anti-fugas	Bloquean intentos de copiar/mandar datos sin permiso	Como una alarma que suena si alguien abre una ventana
Prohibición de USB	No se pueden usar pendrives en las computadoras (salvo casos autorizados)	Como prohibir bolsos grandes en un concierto para evitar robos
Monitoreo 24/7	Alertas automáticas si alguien accede a datos raros	Como cámaras de seguridad que graban movimientos sospechosos

Ejemplo de mensaje a clientes

Asunto: Importante: Medidas de seguridad por incidente en sus datos
Mensaje:
"Estimado cliente,
Lamentamos informarle que detectamos acceso no autorizado a algunos datos personales. No se han reportado fraudes, pero le recomendamos:

1. Cambiar sus contraseñas si usó las mismas en otros sitios.
2. Revisar sus cuentas bancarias por movimientos extraños.
3. Contactarnos al 0800-XXX-XXXX para ayuda gratuita.
   Gracias por confiar en nosotros. Seguimos trabajando para protegerlo."

GUIA PARA AVANZADOS

Suspendemos al empleado implicado y lanzamos una investigación forense No hay duda de que: quien viola la confianza de la empresa y expone datos de clientes debe afrontar temas legales y laborales severas cuando se confirma la responsabilidad tomamos la medida de despedirlo con una causa y llevamos el caso a la Justicia ,porque no solo traicionó a la empresa, sino que puso en riesgo la privacidad de miles de personas

Informamos a la Agencia de Acceso a la Información Pública ni bien tenemos el reporte cerrado
Y a los clientes les contamos la verdad : les explicamos qué pasó, qué datos pudieron verse afectados y qué acciones estamos tomando para protegerlos.
También ponemos a disposición un equipo especial para atender cualquier duda o problema que puedan tener.

INTEGRANTES DE CIBER DATA:
Eric Roth-Mia Ferreyra-Timoteo Sayago-Braian Junco-Mayra Chocou

Rediseñamos todos los permisos de acceso: el que no necesita ver datos sensibles para trabajar, no los ve Implementamos sistemas de prevención de fuga de datos : si alguien intenta copiar, mandar o descargar datos sin autorización, lo frenamos .
Prohibimos usar pendrives y dispositivos externos en las computadoras de la empresa, salvo casos excepcionales y bien controlados.
Monitoreamos los accesos de manera constante y armamos alertas automáticas para detectar cualquier movimiento sospechoso.

INTEGRANTES DE CIBER DATA:
Eric Roth-Mia Ferreyra-Timoteo Sayago-Braian Junco-Mayra Chocou