ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles para estudiantes

Restaurar el laboratorio - El incidente de *ransomware*

ESCAPE: Preparing healthcare professionals for cyberattacks	
Restaurar el laboratorio - El incidente de ransomware	
Idioma	Español

Índice

1) Restore the lab - Ransomware incident.....3
2) Classification.....3
3) Game.....4
4) More information.....6

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Restaurar el laboratorio - El incidente de ransomware	
Idioma	Español

1) Restaurar el laboratorio - El incidente de ransomware

Este rompecabezas consta de cinco preguntas relacionadas con distintos tipos de ataques que pueden producirse en una entidad sanitaria. Elige con prudencia para proteger adecuadamente tus datos valiosos frente a los ciberdelincuentes.

2) Clasificación

Categoría	**Marcar si aplica:**
Sector	☑ Sanitario
	☐ Público general
	☐ Otro
Temas cubiertos	☑ Ciberseguridad
	☑ Protección de datos
Tipo de situación	☑ Prevención
	☐ Impacto (ej. Cuando está ocurriendo o ha ocurrido) en el cuidado del paciente
	☑ Impacto en otras actividades que no implican el cuidado del paciente
Idioma del material original	☐ Neerlandés
	☐ Inglés
	☐ Alemán

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Restaurar el laboratorio - El incidente de ransomware	
Idioma	Español

	☐ Italiano
	☑ Español
Tipo del material	☐ Preguntas de cuestionario.
	☑ Juegos
	☐ Aplicaciones y vídeos interactivos
	☐ Listas de verificación

3) Juego

Resolver cinco desafíos de ciberseguridad. Cada respuesta correcta entrega un fragmento de la clave final de descifrado. Una vez ensamblados los cinco fragmentos en orden, se obtiene la **clave completa** para "desbloquear" el ransomware que está bloqueando los datos clínicos de un laboratorio.

Este juego se puede realizar fácilmente en el aula con **grupos pequeños**.

1. Dividir a los participantes en equipos de 2 a 4 personas..
2. Dar a cada equipo el **Desafío 1**. Cuando respondan correctamente, entregarles el **Fragmento 1** (en papel o tarjeta). Luego pasar al Desafío 2, y así sucesivamente.
3. Cuando un equipo tenga los cinco fragmentos, deben ensamblarlos en el orden **1** → **5** para formar la **clave final**. Usar esta clave para abrir el recurso bloqueado (ZIP protegido con contraseña, página web de "descifrado" controlada por el profesor o un sobre con "datos restaurados")
4. Cada reto incluye la respuesta correcta para el profesor y una breve explicación.

Clave final:

Los cinco fragmentos combinados, en orden, forman la frase de contraseña:

PH + AR + MA + SA + FE → PHARMA-SAFE

(Profesor: esta es la contraseña que se establece en el recurso bloqueado).

1) **Desafío 1: ¿Qué es ransomware?** (Fragmento = Ph). Un usuario del laboratorio abre un archivo y de repente no puede acceder a los registros de pacientes. Aparece un mensaje que exige un pago para recuperar los archivos. ¿Cuál de las siguientes opciones define mejor el ransomware?

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

a) Software que copia en secreto los registros de pacientes para enviarlos a un atacante.
b) Un programa que cifra archivos o sistemas y exige un pago para restaurar el acceso.
c) Un ataque web que roba contraseñas registrando las pulsaciones de teclado.
d) Un escaneo de red que busca servidores abiertos.

Respuesta correcta: Un programa que cifra archivos o sistemas y exige un pago para restaurar el acceso.

Feedback: El ransomware cifra o bloquea datos y luego exige un rescate para obtener la clave de descifrado o restaurar el acceso. Las otras opciones describen otras amenazas (exfiltración de datos, *keyloggers*, escaneos) pero no el comportamiento de pago por acceso.

2) Desafío 2: **Correo de phishing** (Fragmento = AR). El laboratorio recibe un correo que parece provenir del proveedor de software: “Actualización urgente: haga clic aquí para instalar un parche crítico.” El enlace lleva a una URL extraña y solicita credenciales de administrador.. Como auxiliar de farmacia, ¿cuál es la mejor acción inmediata?
   a) Hacer clic en el enlace e introducir las credenciales rápidamente, es urgente.
   b) Responder solicitando más detalles e incluir las credenciales.
   c) No hacer clic en el enlace; reportar el correo a IT/seguridad y eliminarlo.
   d) Reenviar el correo a colegas con “FYI” para que actualicen también.

Respuesta correcta: No hacer clic en el enlace; reportar el correo a IT/seguridad y eliminarlo.

Feedback: El *phishing* imita remitentes confiables. Nunca se deben introducir credenciales en un enlace recibido de un correo inesperado. La acción segura es reportarlo a IT/seguridad para que puedan verificar y bloquear dominios maliciosos. Responder o reenviar el correo puede propagar la amenaza.

3) Desafió 3: **Contraseña fuerte** (Fragmento = MA). El sistema del laboratorio utiliza contraseñas como *Lab123* o *password*. La dirección quiere mostrar un ejemplo más seguro al personal. ¿Cuál de las siguientes opciones representa la contraseña más segura para una cuenta de personal (sin usar generadores de frases de contraseña)?
   a) Lab2025!
   b) P@55w0rd
   c) M5r!c7bQ#4t
   d) MyLab

Respuesta correcta: M5r!c7bQ#4t

Feedback: La opción C es larga, combina letras mayúsculas y minúsculas, números y símbolos de forma impredecible, ofreciendo la mayor entropía. Las opciones A y B usan patrones predecibles o sustituciones comunes; D es muy débil. (*Mejor práctica:* usar contraseñas únicas y largas o un gestor de contraseñas).

4) Desafío 4: **Mala configuración de red** (Fragmento = SA). El servidor DNS del laboratorio es accesible públicamente aunque debería ser interno, y no hay firewall perimetral que bloquee tráfico saliente. Un atacante aprovechó estas debilidades para instalar malware y controlar máquinas de forma remota. ¿Qué cambio reduciría inmediatamente la posibilidad de que un atacante externo reclute máquinas internas en una botnet?
   a) Publicar la IP del DNS en la web de la empresa para que los administradores la encuentren.
   b) Cerrar o restringir el servicio DNS a la red interna y aplicar un firewall perimetral para bloquear conexiones entrantes/salientes innecesarias.

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

c) Desactivar antivirus en todas las máquinas para reducir falsos positivos.
d) Cambiar la contraseña del Wi-Fi del laboratorio, dejando el DNS accesible públicamente.

Respuesta correcta: Cerrar o restringir el servicio DNS a la red interna y aplicar un firewall perimetral para bloquear conexiones entrantes/salientes innecesarias.

Feedback: Restringir servicios internos (DNS) y desplegar un firewall para controlar el tráfico son mitigaciones inmediatas y efectivas. Publicar el DNS o desactivar antivirus empeora la situación; cambiar solo la contraseña Wi-Fi no protege los servicios expuestos.

5) Desafío 5: **Pasos de respuesta ante incidentes** (Fragmento = FE). Se sospecha ransomware y algunas máquinas muestran mensajes de cifrado. La dirección pide al equipo cuál es la secuencia inmediata correcta de acciones para limitar daños. ¿Cuál es el orden correcto de acciones de respuesta ante incidentes de ransomware?
   a) Notificar clientes → Restaurar desde copias de seguridad → Aislar sistemas infectados → Documentar el incidente.
   b) Aislar sistemas infectados → Preservar evidencia (imagen forense/logs) → Notificar a IT/seguridad y dirección → Erradicar y recuperar desde copias de seguridad.
   c) Pagar rescate → Reiniciar sistemas → Ignorar registros → Continuar trabajando.
   d) Reinstalar todo el software → Eliminar copias de seguridad → Informar a prensa.

Respuesta correcta: Aislar sistemas infectados → Preservar evidencia (imagen forense/logs) → Notificar a IT/seguridad y dirección → Erradicar y recuperar desde copias de seguridad.

Feedback: Primero, aislar máquinas infectadas para detener la propagación; luego, preservar evidencia para investigación; notificar a los equipos correspondientes; y finalmente erradicar el malware y recuperar desde copias de seguridad limpias. Las otras opciones incluyen acciones inseguras o incorrectas.

Notas de implementación para el profesor

- Hojas impresas con los desafíos (una por estación) o diapositivas proyectadas.
- Cinco tarjetas por equipo con los fragmentos (el profesor las entrega cuando se responde correctamente). Alternativamente, un papel por fragmento.
- Un recurso “bloqueado”: ZIP protegido con contraseña, PDF con contraseña o sobre etiquetado “Clave de descifrado dentro”. (Contraseña = **PHARMA-SAFE**).
- Opcional: nota de rescate falsa como elemento de inmersión.
- **Tiempo sugerido:** 40–60 minutos en total. Tiempo medio: 6–10 minutes por desafío + 10 minutes para cerrar el desafío y obtener conclusiones.

4) Más información

Estas preguntas han sido inspiradas y adaptadas al sector sanitario a partir de los escenarios presentados por el CCN en la siguiente página web: https://angeles.ccn-cert.cni.es/Escape-Room/. Este material se encuentra publicado en español, dado que el CCN (Centro Criptológico Nacional) es una institución española.

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.