ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles para estudiantes

Ciberresiliencia en Sanidad

ESCAPE: Preparando a los Profesionales Sanitarios para los Ciberataques	
Ciberresiliencia en Sanidad	
Idioma	*Español*

Índice

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: Preparando a los Profesionales Sanitarios para los Ciberataques	
Ciberresiliencia en Sanidad	
Idioma	*Español*

1. Ciberresiliencia en Sanidad

Este documento incluye 6 preguntas diseñadas para concienciar sobre la resiliencia digital y los desafíos de la ciberseguridad en ambientes clínicos. Las preguntas han sido adaptadas a partir de la revista BSI “Cyberresilienz stärken – Vom Schutz zum Widerstand” (recuperada el 01/2025), publicada por la Oficina Federal Alemana para la Seguridad de la Información (BSI).

2. Clasificación

Categoría	**Marcar lo que corresponda**
Sector	☐ Sanidad
	☑ **General**
Temas Tratados	☑ **Ciberseguridad**
	☐ Protección de datos
Tipo de Situación	☐ Prevención
	☐ Impacto (cuando ocurre o ha ocurrido) en la atención del paciente.
	☑ **Impacto en todas las demás actividades sin incluir la atención directa del paciente.**
Idioma de los materiales originales	☐ Holandés
	☐ Inglés
	☑ **Alemán**
	☐ Italiano
	☐ Español

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: Preparando a los Profesionales Sanitarios para los Ciberataques	
Ciberresiliencia en Sanidad	
Idioma	*Español*

Tipo de material	☑ **Cuestionario de preguntas**
	☐ Juegos
	☐ Aplicaciones y vídeos interactivos
	☐ Listas de verificación

3. Preguntas del Cuestionario

1) Estás trabajando en emergencias cuando un apagón afecta a la monitorización de los pacientes. ¿Por qué es la ciberresiliencia especialmente crítica en entornos sanitarios?

   a. Porque el personal médico normalmente no está formado en nuevas tecnologías.
   b. Porque los hospitales no pueden permitirse largos periodos de inactividad debido a la seguridad de los pacientes.
   c. Porque las aplicaciones de salud se están volviendo cada vez más populares.
   d. Porque el programa antivirus raramente se utiliza en las clínicas.

Respuesta correcta: b. Porque los hospitales no pueden permitirse largos periodos de inactividad debido a la seguridad de los pacientes.

Retroalimentación: La seguridad de los pacientes depende de la disponibilidad del sistema. La ciberresiliencia garantiza la continuación del cuidado incluso durante un ataque.

2) Estás configurando una nueva cuenta de usuario en una estación de trabajo compartida. ¿Cuál es el objetivo principal del enfoque 'Confianza Cero' en los sistemas informáticos hospitalarios?

   a. Aislar completamente las estaciones clínicas de trabajo. To fully isolate clinical workstations.
   b. Verificar todos los intentos de acceso, independientemente de su origen.
   c. Eliminar la necesidad de contraseñas.
   d. Confiar en los dispositivos una vez hayan sido registrados.

Respuesta Correcta: b. Verificar todos los intentos de acceso, independientemente de su origen.

Retroalimentación: 'Confianza Cero' significa 'nunca confiar, siempre verificar'. Incluso el acceso interno debe ser comprobado contínuamente.

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.

3) El hospital experimenta un cibersecuestro de datos (ataque de ransomware). ¿Cuál es un elemento clave de la ciberresiliencia en este caso? Tu red hospitalaria sufre un ataque de encriptación repentino.

   a. Apagar la conexión a internet permanentemente. Shutting down the internet connection permanently.
   b. Tener copias de seguridad offline de los datos revisadas regularmente.
   c. Culpar al departamento de informática.
   d. Pagar el rescate rápidamente.

Respuesta Correcta: b. Tener copias de seguridad offline de los datos revisadas regularmente.

Retroalimentación: La resiliencia incluye la capacidad para restaurar sistemas. Las copias de seguridad son esenciales para evitar la pérdida de datos.

4) Durante una sesión de formación, tu equipo se encuentra con una simulación de una situación de ransomware. ¿Cómo pueden los simulacros regulares de emergencia mejorar la resiliencia digital en los equipos de atención sanitaria?

   a. Aumentan el miedo contra las ciberamenazas.
   b. Mejoran las rutinas físicas de evacuación.
   c. Entrenan al personal para una respuesta rápida y coordinada durante incidentes informáticos.
   d. Reducen la necesidad de actualizaciones informáticas.

Respuesta Correcta: c. Entrenan al personal para una respuesta rápida y coordinada durante incidentes informáticos.

Retroalimentación: Practicar emergencias informáticas ayuda a los equipos a actuar rápido y a estar calmados durante incidentes reales.

5) Un compañero/a olvida cerrar la sesión en una terminal de documentación. ¿Qué papel juega el comportamiento humano en el mantenimiento de la ciberresiliencia en clínicas?

   a. Un papel central. La concienciación del usuario es fundamental para prevenir fisuras.
   b. Ninguno, ya que los sistemas técnicos manejan la seguridad
   c. Sólo el personal informático necesita ser cauteloso.
   d. El personal médico debería evitar usar ordenadores.

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.

Respuesta Correcta: a. Un papel central. La concienciación del usuario es fundamental para prevenir fisuras.

Feedback: La concienciación y un comportamiento responsable por parte de todo el personal es vital para prevenir incidentes.

6) Te percatas de un correo electrónico sospechoso pero lo borras sin comunicarlo. ¿Por qué es importante avisar de incidentes informáticos cercanos a suceder en hospitales?

   a. Para castigar a la persona responsable.
   b. Para mejorar las estadísticas.
   c. Para alertar a los medios de comunicación rápidamente.
   d. Para identificar las vulnerabilidades del sistema antes de que haya daño real.

Respuesta Correcta: d. To identify system weaknesses before real damage occurs.

Retroalimentación: Informar de incidentes cercanos a suceder ayuda a las organizaciones a aprender y mejorar sus defensas antes de que ocurra un daño real.

4. Más información

Este cuestionario de preguntas está inspirado por temas centrales tratados en la revista BSI “Cyberresilienz stärken – Vom Schutz zum Widerstand” (recuperada el 01/2025), publicada por publicada por la Oficina Federal Alemana para la Seguridad de la Información (BSI). Las preguntas no son citas directas, sino que han sido adaptadas y contextualizadas para su uso en formaciones relacionadas con la atención sanitaria y la educación en seguridad digital. Puede acceder a la publicación completa aquí: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2025_01.pdf

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.