

# **ESCAPE:**

## **Preparing healthcare professionals for cyberattacks**



**Material for learners**

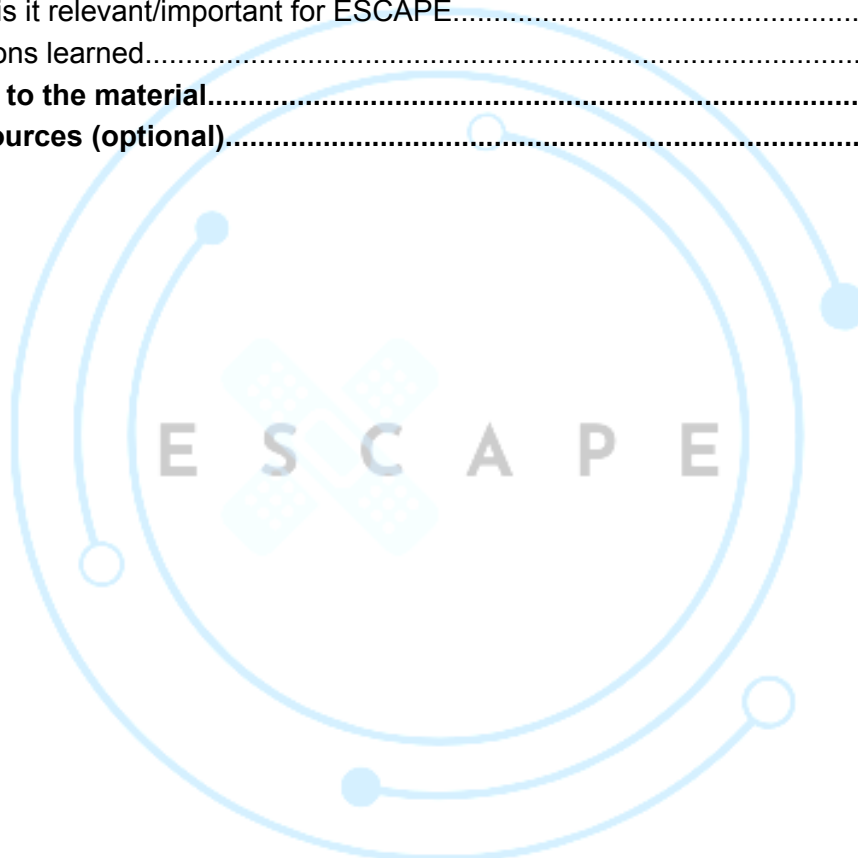
---

*Sequential videos for general topics about  
cybersecurity*

ESCAPE: Preparing healthcare professionals for cyberattacks	
Videos secuenciales sobre temas generales de ciberseguridad	
Language	Spanish

## Table of contents

<b>1. Name of the material and description.....</b>	<b>3</b>
<b>2. Classification.....</b>	<b>3</b>
<b>3. Description.....</b>	<b>4</b>
3.1. Origin.....	4
3.2. Why is it relevant/important for ESCAPE.....	4
3.3. Lessons learned.....	4
<b>4. Direct link to the material.....</b>	<b>5</b>
<b>5. Other resources (optional).....</b>	<b>5</b>



Co-funded by  
the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Videos secuenciales sobre temas generales de ciberseguridad	
Language	Spanish

**Vídeos secuenciales sobre temas generales de ciberseguridad**  
 “Vídeos secuenciales sobre temas generales de ciberseguridad”. A series of short videos about everyday situations that can affect cybersecurity and the decisions that can be made to resolve them.

## 1. Classification

Category	Mark if applies
Sector	<input type="checkbox"/> Healthcare
	<input type="checkbox"/> General public
	<input type="checkbox"/> Other
Topics covered	<input checked="" type="checkbox"/> Cybersecurity
	<input checked="" type="checkbox"/> Data protection
Situation type	<input checked="" type="checkbox"/> Prevention
	<input type="checkbox"/> Impact
	<input type="checkbox"/> Impact on all other activities not involving direct patient care.
Language of the original materials	<input type="checkbox"/> Dutch
	<input type="checkbox"/> English
	<input type="checkbox"/> German
	<input type="checkbox"/> Italian
	<input checked="" type="checkbox"/> Spanish
Type of the material	<input type="checkbox"/> Guidelines or manuals



Co-funded by  
the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Videos secuenciales sobre temas generales de ciberseguridad	
Language	Spanish

	<input checked="" type="checkbox"/> Case or examples
	<input type="checkbox"/> Training courses
	<input type="checkbox"/> Others

## 2. Description

This material offers a series of short videos featuring everyday situations that can affect cybersecurity, how to create a Security Master Plan, and provides direct links to additional videos and information for a deeper dive into this type of content.

### 2.1. Origin

The material was created by INCIBE, the Spanish “National Cybersecurity institution”. It is a national organisation dependent on the Ministry of digital transformation and economic issues. It is considered as the reference entity for cybersecurity development, improvement of citizen digital trust, and academic research in that matter in Spain.

### 2.2. Why is it relevant/important for ESCAPE

This material is highly relevant because it emphasizes the importance of cybersecurity for the protection of patient data and company information. It also shows that common measures, such as the use of antivirus software and backups, are not enough to ensure the integrity of confidential information. It highlights the importance of the Security Master Plan and provides guidelines to significantly enhance cybersecurity.

### 2.3. Lessons learned

- **Introduction:** The material aims to highlight everyday situations that can create a breach in cybersecurity and how to act to avoid those risks.
- **Target group:** Healthcare professionals and healthcare enterprise managers.
- **Risks summary:**
  - Sharing passwords.
  - Unprotected workstation.
  - Sensitive documentation in plain sight.
  - Data leaks.
  - Non-updated software or less protected software.
  - Phishing.
  - Ransomware.
  -



Co-funded by  
the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Videos secuenciales sobre temas generales de ciberseguridad	
Language	Spanish

- **Solutions or contingency measures:**
  - Subscription to newsletter of INCIBE.
  - Keep all systems updated on all devices.
  - User awareness in cybersecurity.
  - Use encryption tools.
  - Use secure networks.
- **Tips and tricks:**
  - Security copies policy.
  - Invest in staff training.
  - Software update policy.
  - Do not share passwords or sensitive information.
  - Limit methods of data extraction, copying, and deletion.
  - Block access to external webmails.
  - Control of emails to third parties.
  - Restrictions on the use of USB ports.
  - Block access and emails of employees who are no longer part of the workforce.
  - Encrypt information.

### 3. Direct link to the material

[https://itinerarios.incibe.es/?contador\\_pagina=2&IT\\_actual=3](https://itinerarios.incibe.es/?contador_pagina=2&IT_actual=3)

### 4. Other resources (optional)

The material includes several links to get deeper into specific topics or to additional material.



Co-funded by  
the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.