incibe_
INSTITUTO NACIONAL DE
CIBERSEGURIDAD

Strategies to raise the level of awareness in the health sector

Marco Antonio Lozano Merino
@marcoalome

What is INCIBE (Spanish National Cybersecurity Institute)?

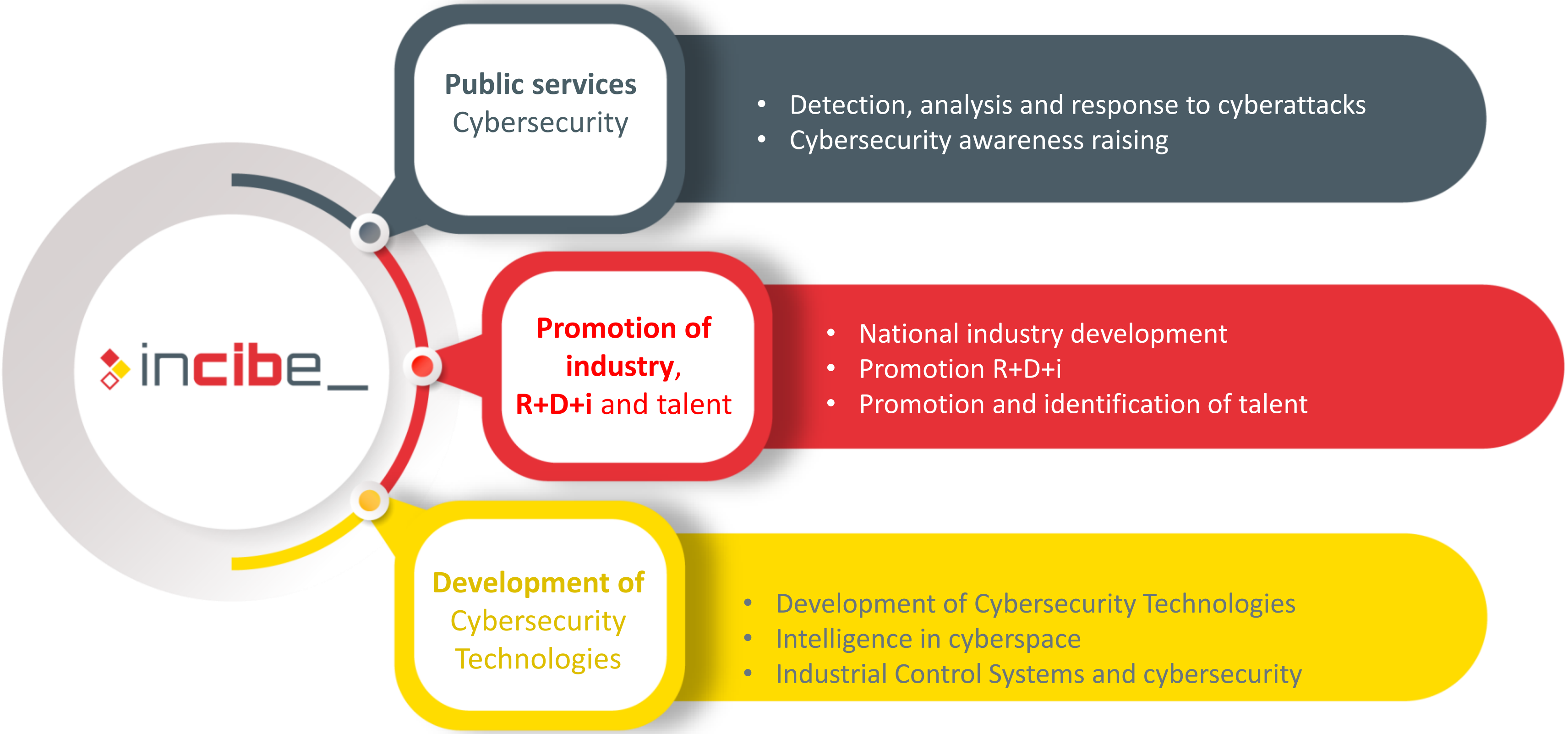
Reference entity for the **development of cybersecurity** and the **didital confidence** of:

Citizens

Companies**, especially strategic sectors**

Commercial State Company attached to the Ministry of Economy and Business throught the Secretary of State for Digital Advancement, which leads different actions for cybersecurity at national and international level.

What do we do?



incibe_

Public services
Cybersecurity

- Detection, analysis and response to cyberattacks
- Cybersecurity awareness raising

Promotion of industry, R+D+i and talent

- National industry development
- Promotion R+D+i
- Promotion and identification of talent

Development of
Cybersecurity Technologies

- Development of Cybersecurity Technologies
- Intelligence in cyberspace
- Industrial Control Systems and cybersecurity

incibe_
SPANISH NATIONAL CYBERSECURITY INSTITUTE

2018 cybersecurity balance

INCIBE-CERT

A public service for the **protection of citizens and companies**

111.519
Managed Incidents
Of which:

102.414 ...from companies & citizens

722 ...from strategic operators

8.383 ...from RedIRIS

77 Teams from **35** countries at the International CyberEx 2018

861 Ransomware incidents resolved

18.104 New vulnerabilities documented

540 Security alerts

incibe-cert_

85.596
Notifications sent from INCIBE-CERT to third parties to get them involved in the research and resolution of incidents

Internet User Security Office

OSI Oficina de Seguridad del Internauta

Raise awareness on the citizens
INCIBE cybersecurity helpline:
900 116 117

4.811 Calls from citizens answered

123.594 Notifications sent to citizens by our Antibotnet service

Safe Internet for Kids

is4k INTERNET SEGURA FORKIDS

Children, young people, families and educators awareness
INCIBE cybersecurity helpline:
900 116 117

53.387 People reached through **1.610** awaraness - raising actions in the child environment

681 Volunteers registered in the **CyberCooperation** programe

Protect your business

Companies awareness

INCIBE cybersecurity helpline: **900 116 117**

protege tu empresa

8.368 Students in the cybersecurity course for companies

11.667 Self-diagnoses at our *"Do you know your risks?"* service

6.391 Users of our *"Cybersecurity itineraries by business sectors"* service

Industry development, R+D+i and talent promotion

enise_

2.380 Participants

96 Speakers

170 Bilateral meetings

Summer BootCamp

330 Participants from **44** countries

cyber camp

29.000 followers & **64 speakers**

4th edition **CyberOlympics.** **232** registered educational centers & **1.631** participants

CTF
45 invidual CTF finalists and **404** participants

Hackathon
21 teams & **65** participants

Communication

Social Media

101.154 followers

52.314 likes

13.847 followers

17.254 subscribers

3.225.349 Unique users at INCIBE websites

Awards

- **2018 AUTELSI Award**
- **2018 College of Engineering Computing of Galicia Award**
- **2018 ICT Security Trophy**
- **2018 ICT Security Trophy extraordinary jury**

Apps

Hackend

CONAN Mobile

246.595 INCIBE Apps total users

Hackers vs Cybercrooks

CyberScouts

INCIBE-CERT: services for ICT and cybersecurity professionals

incibe-cert_

https://www.incibe-cert.es

Information

Blogs, guides, studies and cybersecurity highlights

Alerts

Security advisories, ICS advisories, vulnerabilities and alert level

Specialized training

Courses of ICS cybersecurity, mobile devices, basic/advanced for spanish law enforcement…

Incidents

Competent institution in incident resolution for citizens and companies in Spain

Protege tu Empresa: cybersecurity for SMEs

900 116 117

Línea de ayuda
EN CIBERSEGURIDAD

protege tuempresa

https://www.incibe.es/protege-tu-empresa

Information	Training	Tools	Attention to the entrepreneur
Blogs, newsletters, what are you interested in?, security advisories	Cybersecurity for SMEs, sectorial training videos, rol game, awareness raising kit, Hackend serious game, guides, workshops, and online MOOC for microenterprises and freelancers	Antibotnet service, GDPR, antiransomware service, catalogue of solutions, risk self-diagnosis tool, company policies, and trust seals	Cybersecurity helpline: 900 116 117, contact form to solve questions about services and cybersecurity issues, fraud report

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

INCIBE-CERT: competent CERT for private companies and citizens

- Royal Decree-Law 12/2018, 7 September 2018, Network and Information systems Security, published on 8 September 2018 in the Official State Gazette, establishes INCIBE-CERT as the CSIRT of reference for citizens, private law entities and communities that do not belong to the scope of action of CCN-CERT.
- In case of incident management involving critical private sector operators, INCIBE-CERT is jointly operated by INCIBE and CNPIC.

Collaboration with other entities and CERTs

- INCIBE is a member of the main national and international cybersecurity forums and working groups, actively collaborating with strategic actors that deal with different aspects of cybersecurity, such as incident response, information exchange, awareness raising, policy development or the promotion of standardization, among others.

APWG RESEARCH PARTNER

APWG ACCREDITED REPORTER

CERT

FIRST Improving Security Together

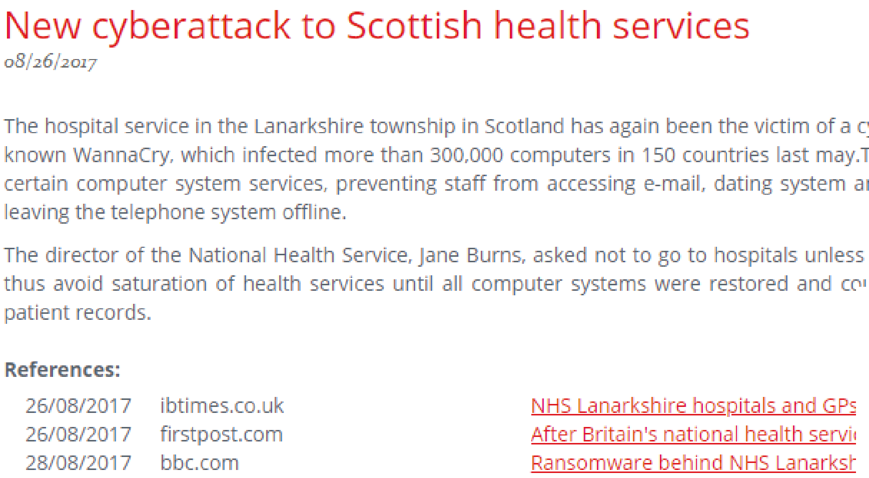
ECS EUROPEAN CYBER SECURITY ORGANISATION

enisa European Network and Information Security Agency

ACCREDITED BY TI TRUSTED INTRODUCER

What is essential about cybersecurity in the health sector?

Do you know any cases? (I)



New cyberattack to Scottish health services

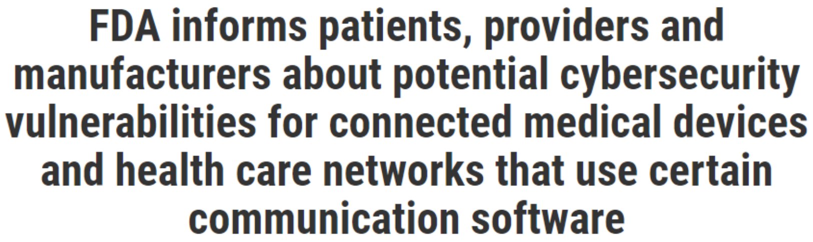
08/26/2017

The hospital service in the Lanarkshire township in Scotland has again been the victim of a cyber attack similar to the well-known WannaCry, which infected more than 300,000 computers in 150 countries last may.This attack caused incidents in certain computer system services, preventing staff from accessing e-mail, dating system and patient records, as well as leaving the telephone system offline.

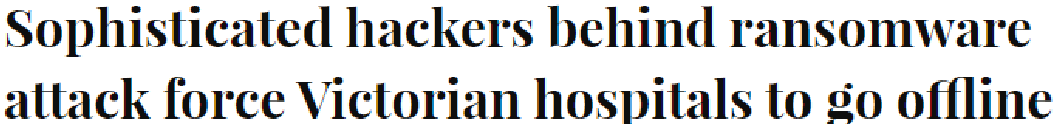
The director of the National Health Service, Jane Burns, asked not to go to hospitals unless it was for an urgent case and thus avoid saturation of health services until all computer systems were restored and could be returned the access to patient records.

References:

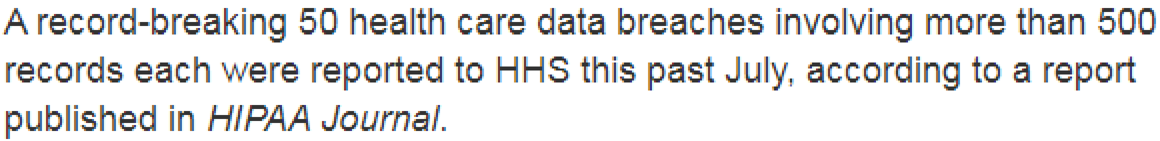
26/08/2017	ibtimes.co.uk	NHS Lanarkshire hospitals and GPs
26/08/2017	firstpost.com	After Britain's national health servi
28/08/2017	bbc.com	Ransomware behind NHS Lanarksh



FDA informs patients, providers and manufacturers about potential cybersecurity vulnerabilities for connected medical devices and health care networks that use certain communication software

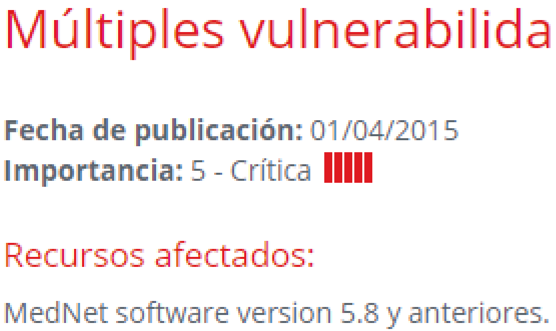


Sophisticated hackers behind ransomware attack force Victorian hospitals to go offline



A record-breaking 50 health care data breaches involving more than 500 records each were reported to HHS this past July, according to a report published in *HIPAA Journal*.

Do you know any cases? (II)

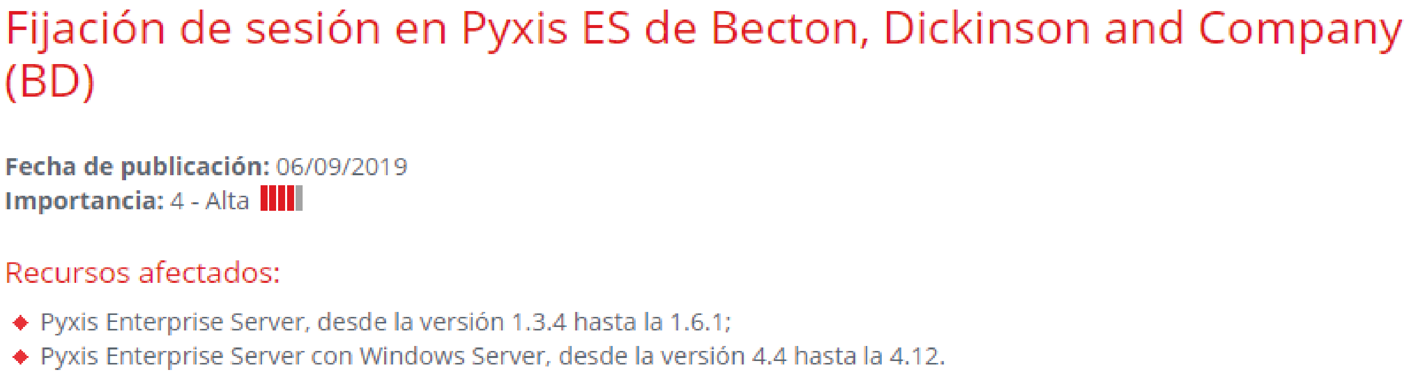


Múltiples vulnerabilidades en Hospira MedNet

Fecha de publicación: 01/04/2015
Importancia: 5 - Crítica ▮▮▮▮▮

Recursos afectados:

MedNet software version 5.8 y anteriores.



Fijación de sesión en Pyxis ES de Becton, Dickinson and Company (BD)

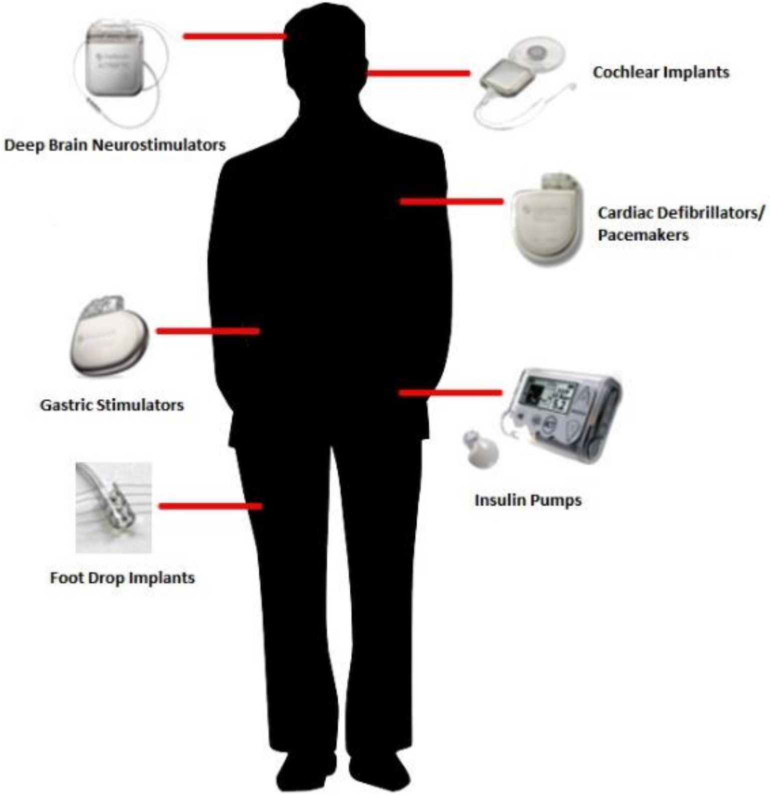
Fecha de publicación: 06/09/2019
Importancia: 4 - Alta ▮▮▮▮▯

Recursos afectados:

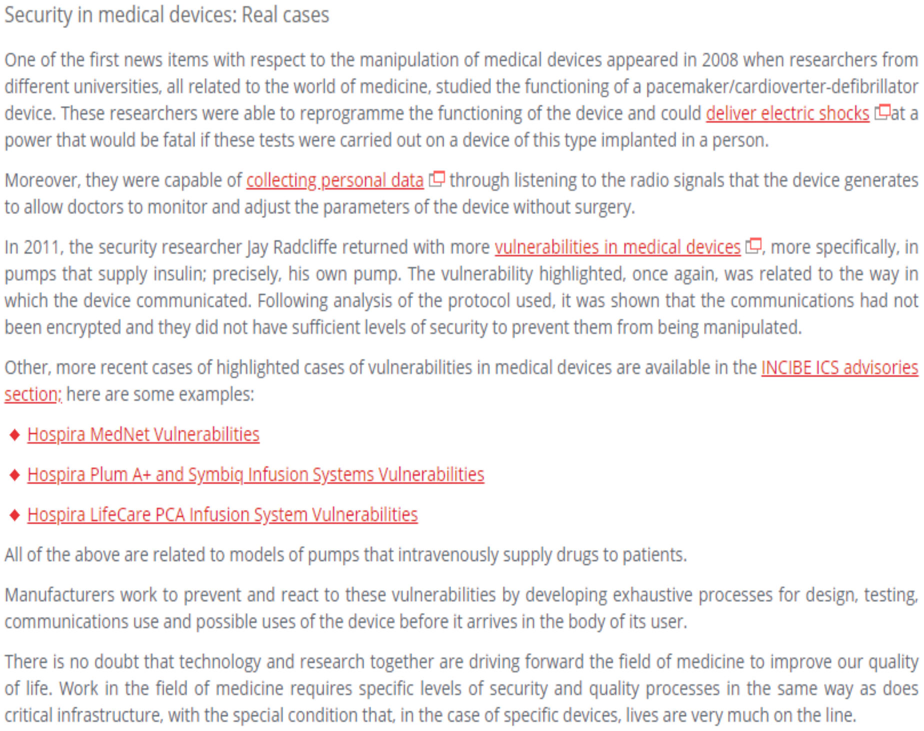
- Pyxis Enterprise Server, desde la versión 1.3.4 hasta la 1.6.1;
- Pyxis Enterprise Server con Windows Server, desde la versión 4.4 hasta la 4.12.

SECURITY BY DEFAULT

Vulnerabilities in medical devices?



- Sample of medical devices -



Security in medical devices: Real cases

One of the first news items with respect to the manipulation of medical devices appeared in 2008 when researchers from different universities, all related to the world of medicine, studied the functioning of a pacemaker/cardioverter-defibrillator device. These researchers were able to reprogramme the functioning of the device and could deliver electric shocks at a power that would be fatal if these tests were carried out on a device of this type implanted in a person.

Moreover, they were capable of collecting personal data through listening to the radio signals that the device generates to allow doctors to monitor and adjust the parameters of the device without surgery.

In 2011, the security researcher Jay Radcliffe returned with more vulnerabilities in medical devices, more specifically, in pumps that supply insulin; precisely, his own pump. The vulnerability highlighted, once again, was related to the way in which the device communicated. Following analysis of the protocol used, it was shown that the communications had not been encrypted and they did not have sufficient levels of security to prevent them from being manipulated.

Other, more recent cases of highlighted cases of vulnerabilities in medical devices are available in the INCIBE ICS advisories section; here are some examples:

- Hospira MedNet Vulnerabilities
- Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities
- Hospira LifeCare PCA Infusion System Vulnerabilities

All of the above are related to models of pumps that intravenously supply drugs to patients.

Manufacturers work to prevent and react to these vulnerabilities by developing exhaustive processes for design, testing, communications use and possible uses of the device before it arrives in the body of its user.

There is no doubt that technology and research together are driving forward the field of medicine to improve our quality of life. Work in the field of medicine requires specific levels of security and quality processes in the same way as does critical infrastructure, with the special condition that, in the case of specific devices, lives are very much on the line.

EMPLOYEES, THE MOST IMPORTANT PIECES IN CYBERSECURITY

- Cybersecurity is a key factor for **building trust** and for the success of any organization.

- People are the most important pieces and the **weakest link**.

- Cybersecurity will require a high degree of **commitment** from people.

Strategies of INCIBE to help us raise our awareness level

Awareness kit

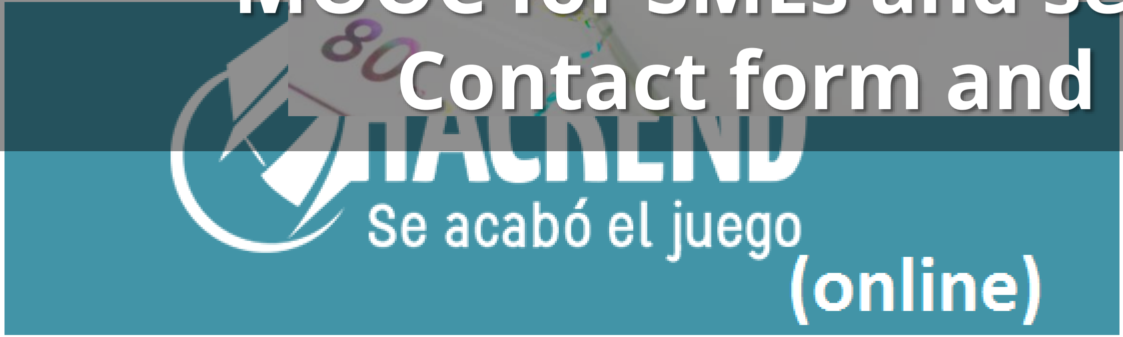
Self-diagnostic tool (ADL)

Interactive itineraries

Hackend, game over

MOOC for SMEs and self-employed

Contact form and helpline

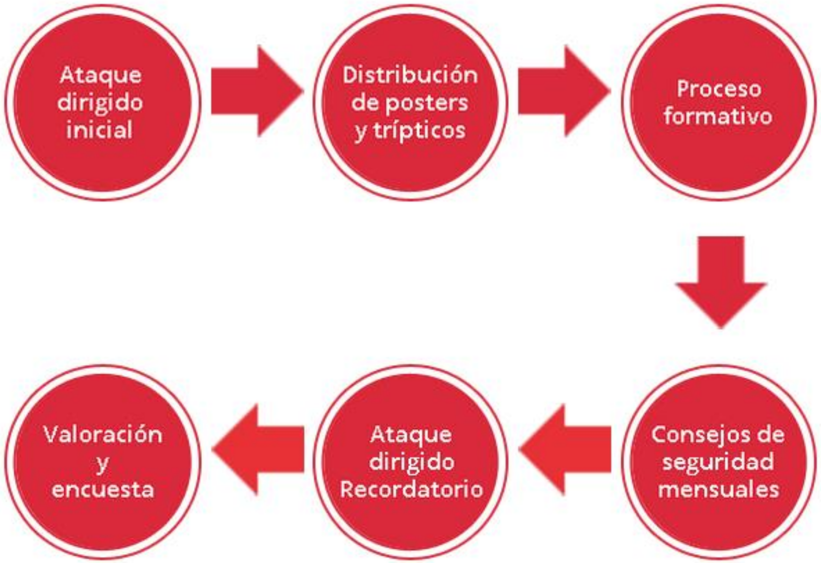


(online)

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Awareness kit

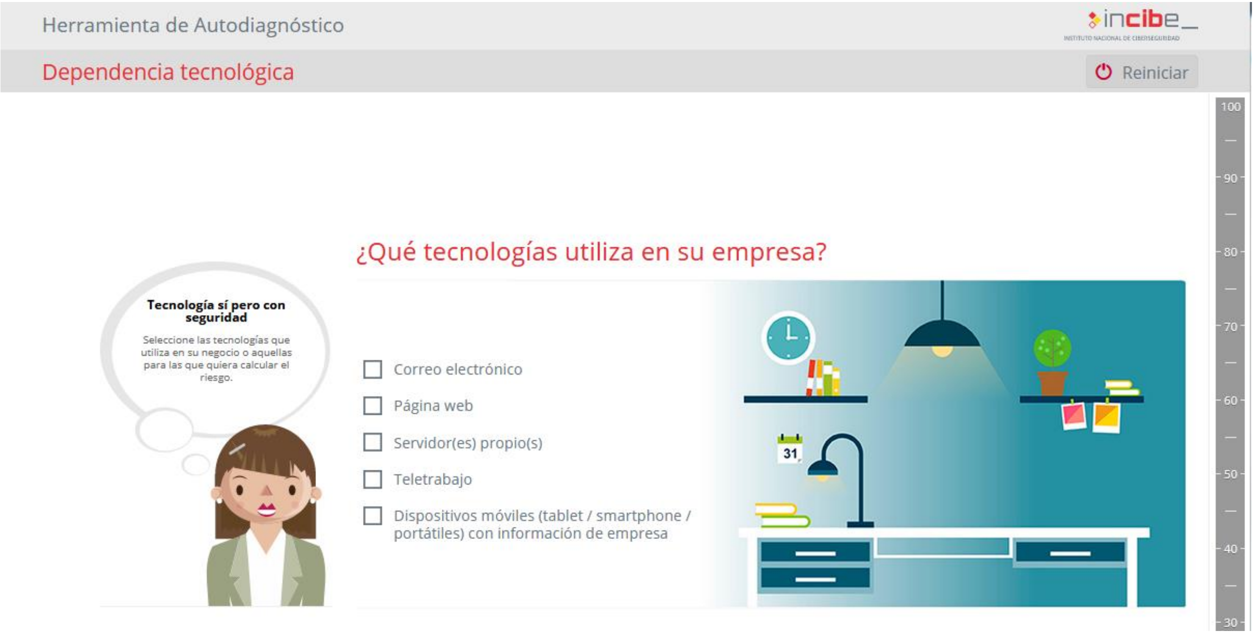
- LA INFORMACIÓN
- LOS SOPORTES
- EL PUESTO DE TRABAJO
- DISPOSITIVOS MÓVILES



Ataque dirigido inicial → Distribución de posters y trípticos → Proceso formativo → Consejos de seguridad mensuales → Ataque dirigido Recordatorio → Valoración y encuesta

Self-diagnostic tool (ADL)

ANÁLISIS DE RIESGOS EN 5 MINUTOS



Herramienta de Autodiagnóstico

Dependencia tecnológica

Reiniciar

Tecnología sí pero con seguridad

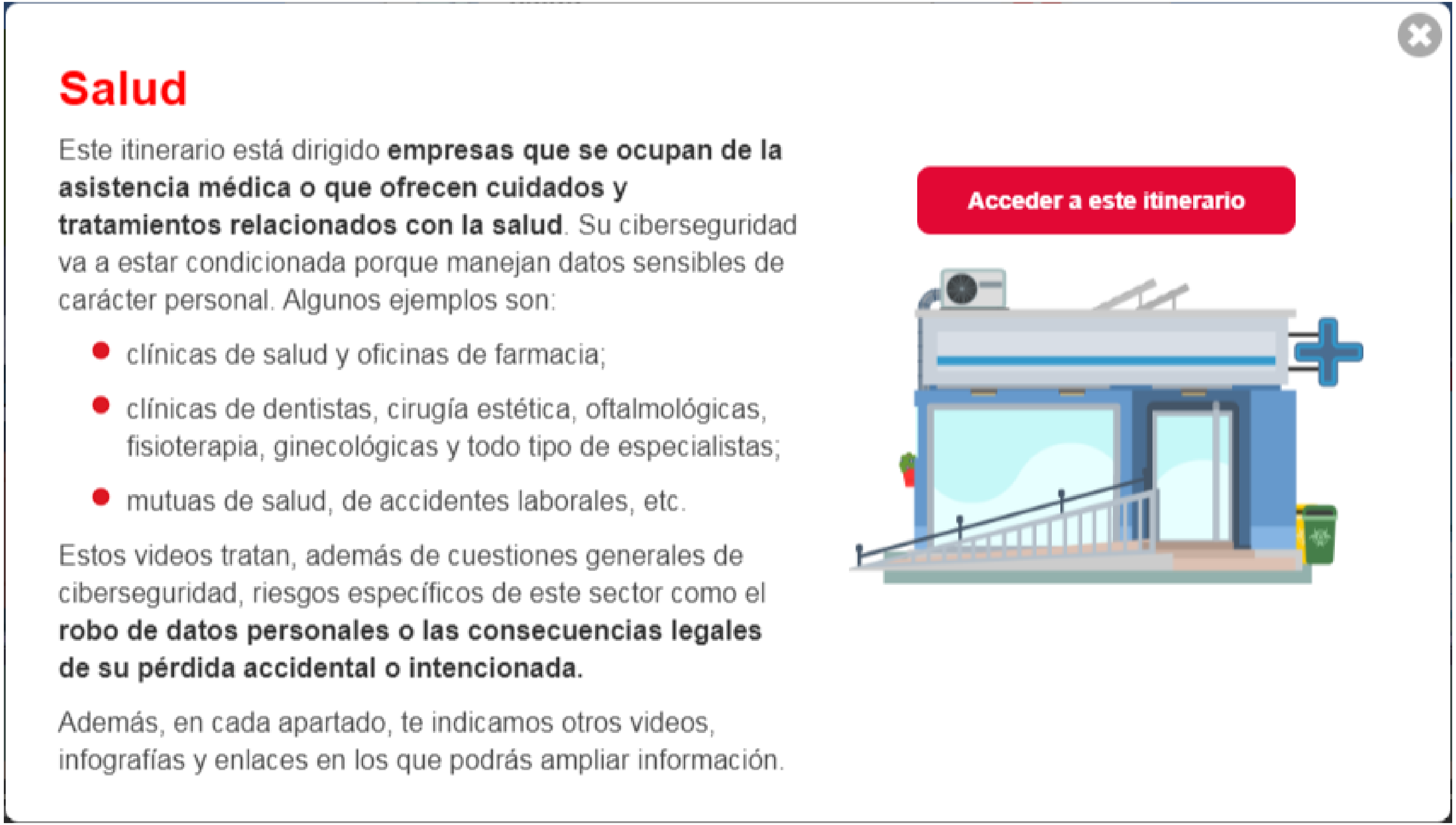
Seleccione las tecnologías que utiliza en su negocio o aquellas para las que quiera calcular el riesgo.

¿Qué tecnologías utiliza en su empresa?

- ☐ Correo electrónico
- ☐ Página web
- ☐ Servidor(es) propio(s)
- ☐ Teletrabajo
- ☐ Dispositivos móviles (tablet / smartphone / portátiles) con información de empresa

https://adl.incibe.es

Interactive itineraries



Salud

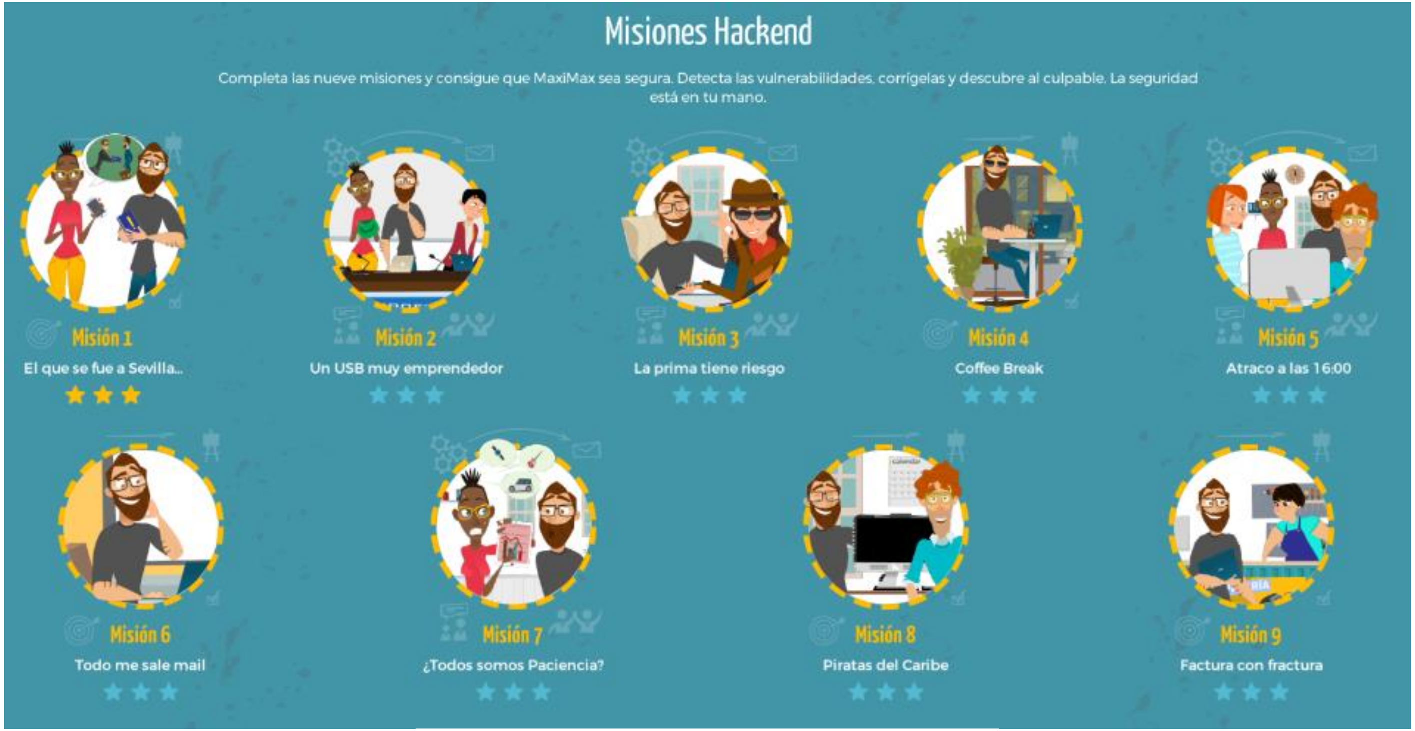
Este itinerario está dirigido **empresas que se ocupan de la asistencia médica o que ofrecen cuidados y tratamientos relacionados con la salud**. Su ciberseguridad va a estar condicionada porque manejan datos sensibles de carácter personal. Algunos ejemplos son:

- clínicas de salud y oficinas de farmacia;
- clínicas de dentistas, cirugía estética, oftalmológicas, fisioterapia, ginecológicas y todo tipo de especialistas;
- mutuas de salud, de accidentes laborales, etc.

Estos videos tratan, además de cuestiones generales de ciberseguridad, riesgos específicos de este sector como el **robo de datos personales o las consecuencias legales de su pérdida accidental o intencionada.**

Además, en cada apartado, te indicamos otros videos, infografías y enlaces en los que podrás ampliar información.

Hackend, game over



Misiones Hackend

Completa las nueve misiones y consigue que MaxiMax sea segura. Detecta las vulnerabilidades, corrígelas y descubre al culpable. La seguridad está en tu mano.

Misión 1
El que se fue a Sevilla...
★ ★ ★

Misión 2
Un USB muy emprendedor
★ ★ ★

Misión 3
La prima tiene riesgo
★ ★ ★

Misión 4
Coffee Break
★ ★ ★

Misión 5
Atraco a las 16:00
★ ★ ★

Misión 6
Todo me sale mail
★ ★ ★

Misión 7
¿Todos somos Paciencia?
★ ★ ★

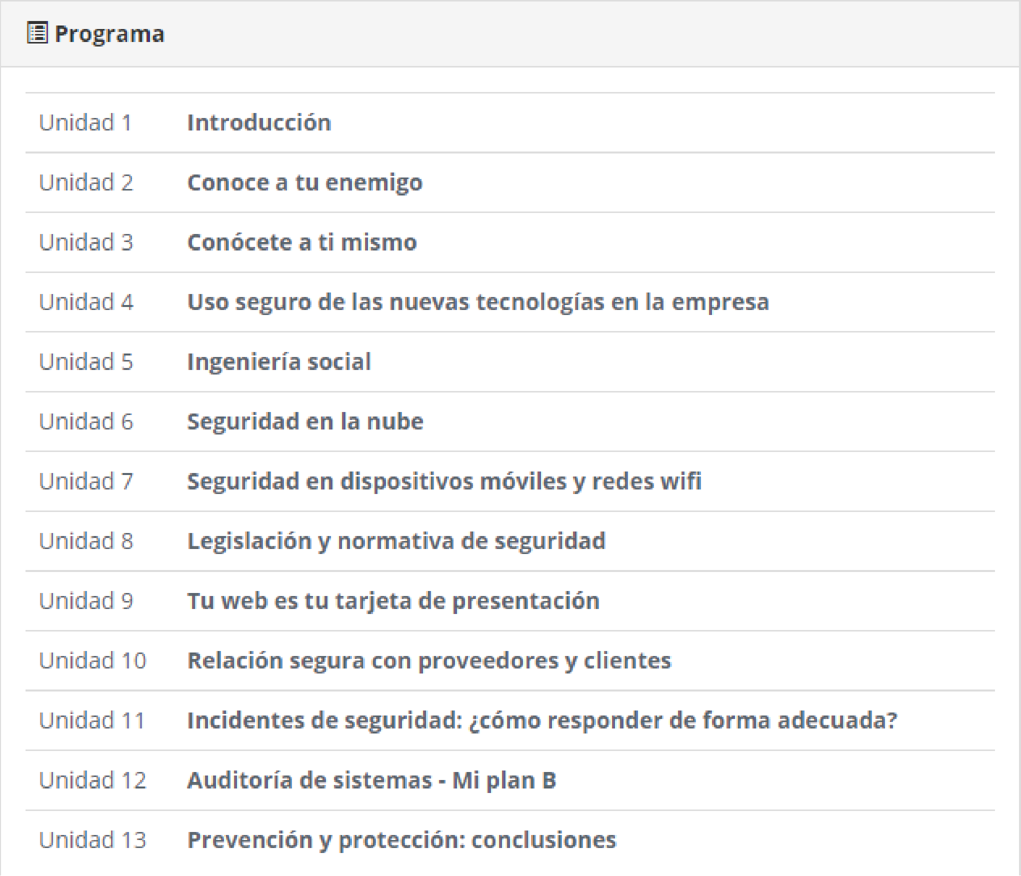
Misión 8
Piratas del Caribe
★ ★ ★

Misión 9
Factura con fractura
★ ★ ★

Fun&Serious
GAME FESTIVAL

PREMIOS TITANIUM 2016
HACKEND
MEJOR SERIOUS GAME

MOOC for SMEs and self-employed



Programa

Unidad 1	**Introducción**
Unidad 2	**Conoce a tu enemigo**
Unidad 3	**Conócete a ti mismo**
Unidad 4	**Uso seguro de las nuevas tecnologías en la empresa**
Unidad 5	**Ingeniería social**
Unidad 6	**Seguridad en la nube**
Unidad 7	**Seguridad en dispositivos móviles y redes wifi**
Unidad 8	**Legislación y normativa de seguridad**
Unidad 9	**Tu web es tu tarjeta de presentación**
Unidad 10	**Relación segura con proveedores y clientes**
Unidad 11	**Incidentes de seguridad: ¿cómo responder de forma adecuada?**
Unidad 12	**Auditoría de sistemas - Mi plan B**
Unidad 13	**Prevención y protección: conclusiones**

Cybersecurity helpline

Línea de ayuda

EN CIBERSEGURIDAD

incibe_

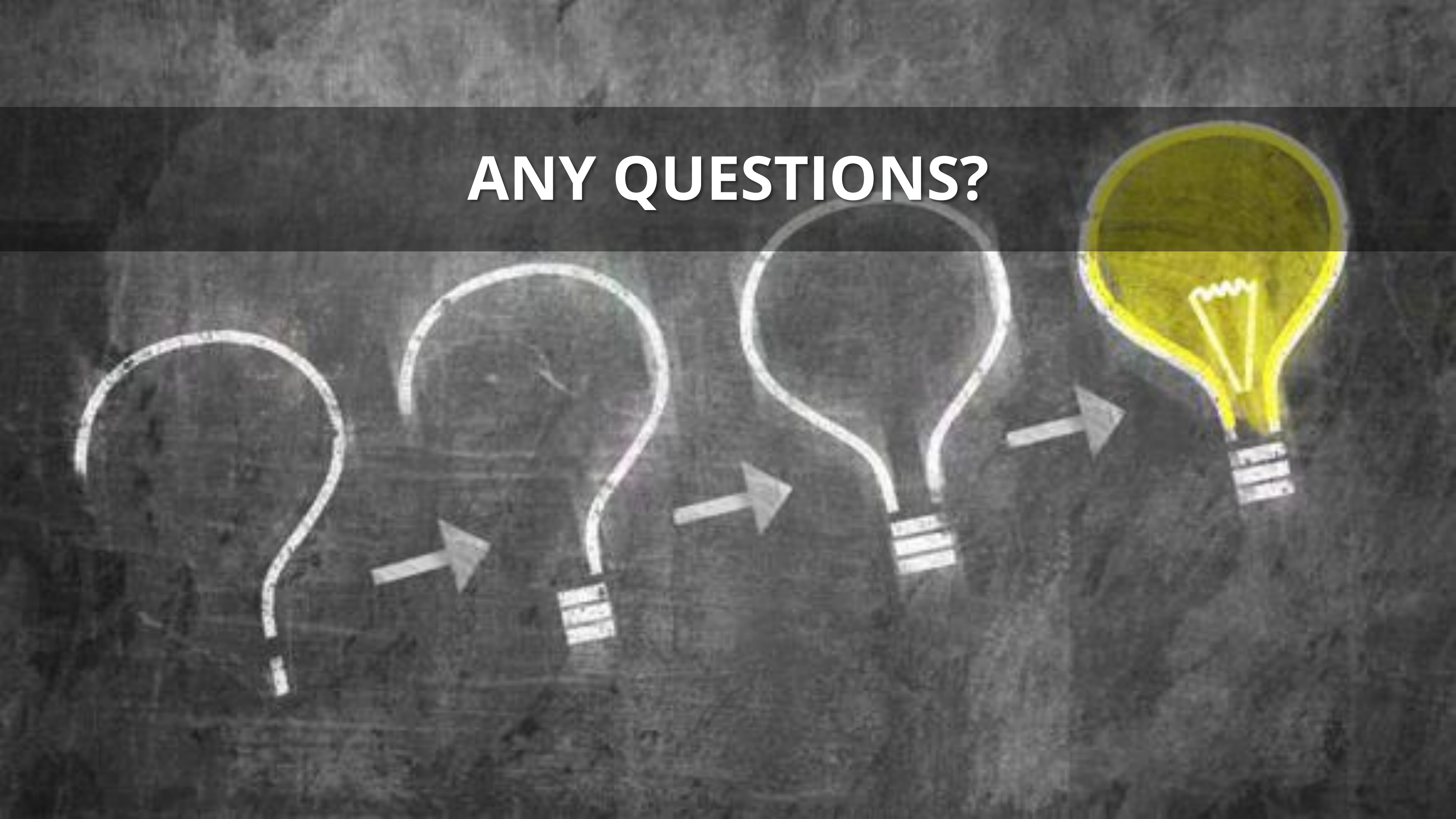
INSTITUTO NACIONAL DE CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

protege tuempresa

is4k INTERNET SEGURA FORKIDS

ANY QUESTIONS?



Follow us…

https://www.incibe.es/

Social networks