Ciberseguridad y Compliance en la Empresa

Una Aproximación práctica

@Curro_Rico

Abogado y Consultor
Especialista en **Empresas de Base Tecnológica**
MERCURE·HUB

@JavierTallon
jtallon@jtsec.es
Ingeniero en Informática
Especialista en Seguridad Tecnológica
jtsec Beyond IT Security

Financiado por:

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

Beneficios de implantar protocolos de cumplimiento normativo en relación a la seguridad tecnológica

Aproximación terminológica: definición y ámbito del compliance (cumplimiento normativo)

Aspectos y riesgos legales **Aspectos y riesgos tecnológicos**

1.- Ciberseguridad y Cumplimiento Normativo: aproximaciones y certificaciones.
2.- Protección de sistemas de información. Medios tecnológicos de la empresa. BYOD
3.- Equipos de trabajo. Estrategias (permisos, jerarquías, software indicado, autenticación biométrica)
4.- Cumplimiento de normas: LOPD, conservación de datos, etc
5.- Aseguramiento de daños propios y de terceros
6.- IoT: vulnerabilidades de la industria 4.0, privacidad, seguridad, IA, etc
7.- Detección y respuesta ante amenazas
8.- Sectores regulados: salud, finanzas, energía...

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

¿QUÉ ES EL CUMPLIMIENTO NORMATIVO?

La conciencia por parte de los ciudadanos y los empresarios de que existen normas que hay que acatar por el bien común, cuyo incumplimiento tiene consecuencias.

El establecimiento de hábitos de conducta y protocolos que consigan de manera efectiva que la ley se cumpla.

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

¿En qué consiste?

1. Cultura de *cumplimiento PREVENTIVO*:
   Nuestro proyecto está bajo un marco legal obligatorio

2. Medidas de *cumplimiento PREVENTIVO*:
   Establecer procedimientos para garantizar el cumplimiento de las normas. Propietarios, gerentes, trabajadores, externos.

3. Consecuencias del cumplimiento:
   - Evitación de sanciones
   - Crecimiento sólido
   - Mejor reputación de cara al cliente
   - Continuidad de negocio

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

¿Qué espectro abarca?

- Normas generales
  - Empresa: Mercantiles, tributarias y fiscales
  - Trabajadores: PRL, Seguridad Social, RRHH
  - Proveedores: Due diligence
  - Clientes: Consumidores y usuarios
  - Propiedad Intelectual e Industrial
  - Penales
- Normas específicas (sectoriales)
  - Actividades que requieren Tratamiento de residuos
  - Actividades financieras
  - Actividades para las que se requiere colegiación oficial
  - Actividades sanitarias y farmacéuticas
  - Cualquier otra actividad que se encuentre especialmente regulada

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

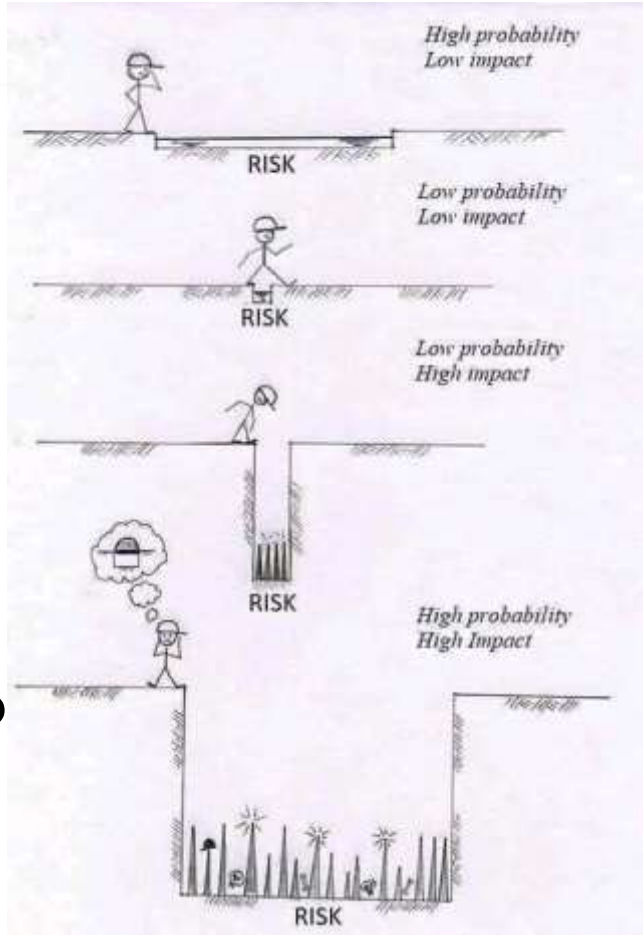
1.- Ciberseguridad y Cumplimiento Normativo: aproximaciones y certificaciones.

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

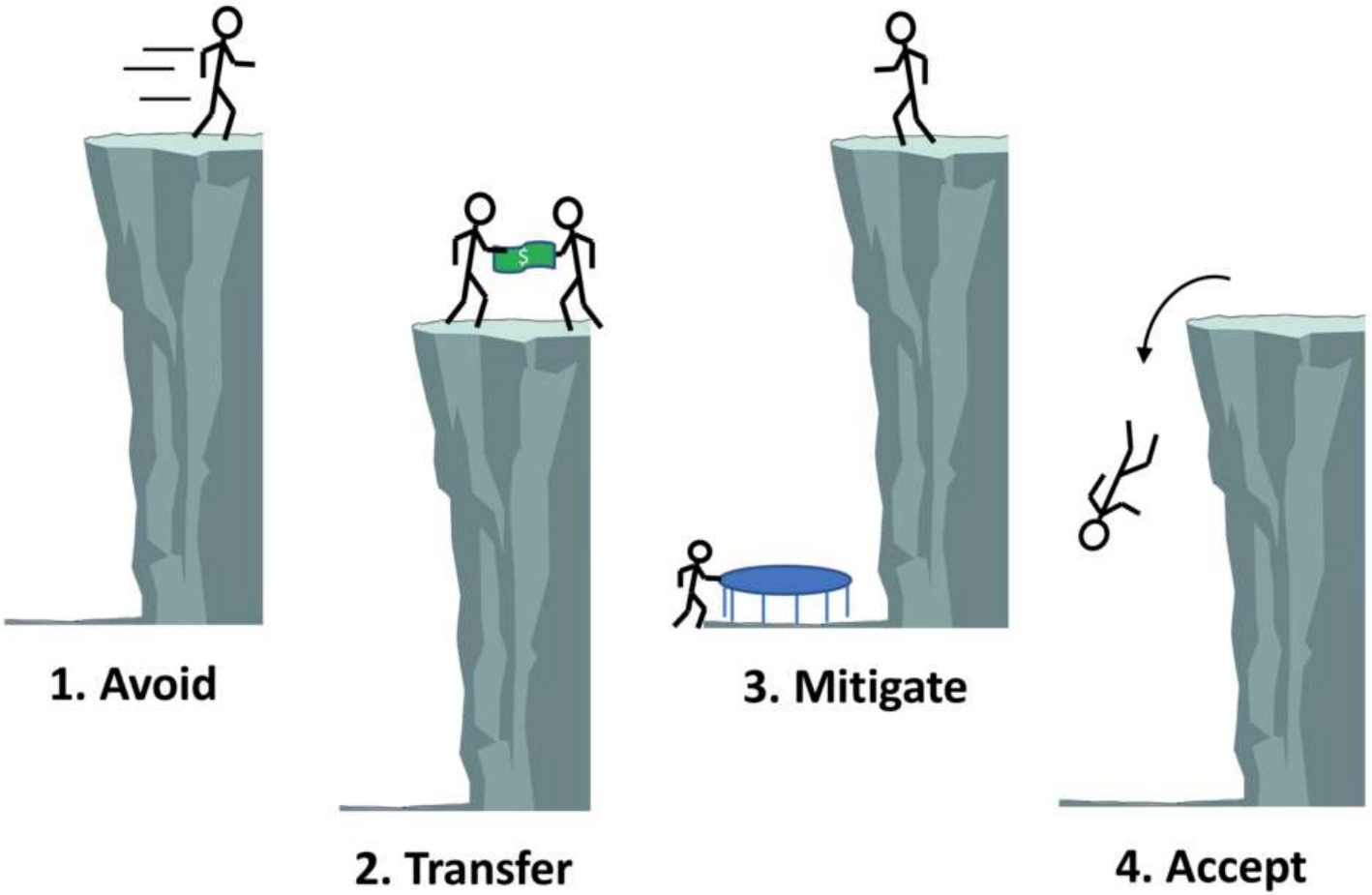
- ¿Cuánta ciberseguridad es suficiente?

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

- Análisis de riesgos
  - MTD
  - RTO
  - RPO
- ¿Cuánto valen mis activos?
  - SLE = AV * EF
  - ALE = SLE * ARO



CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA



CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

- ¿Cómo cumplir?
  - A) Aprovechando lo que dicen los expertos

  - B) Siguiendo las mejores prácticas / exigencias de la industria

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

2.- Protección de sistemas de información. Medios tecnológicos de la empresa. BYOD

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

- ¿Cómo se mitigan los riesgos?

- Controles
  - ISO 27002
  - NIST Cybersecurity Framework
  - …

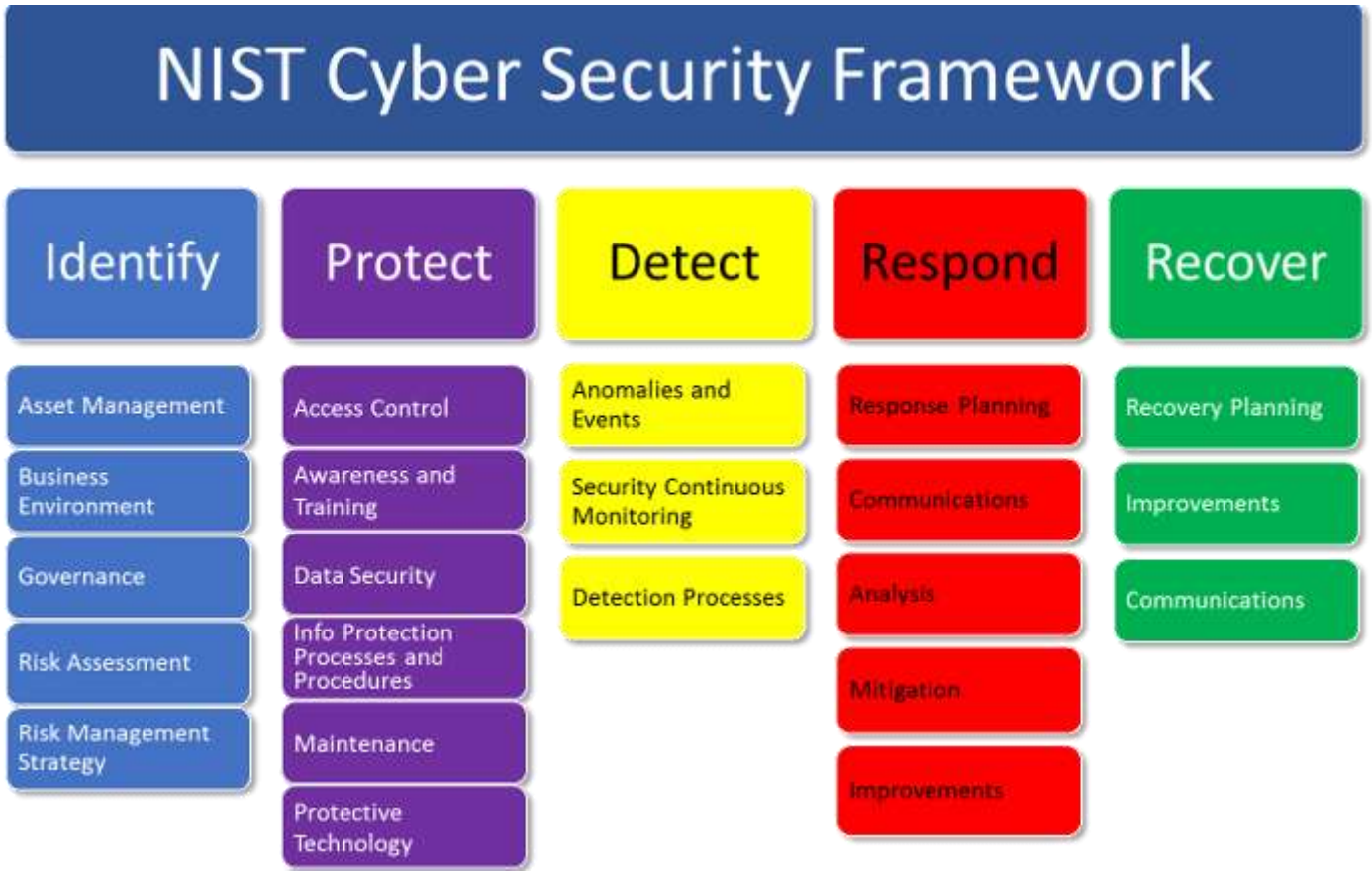
CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

- **1. Políticas de Seguridad** (GRC Gobernanza / Riesgo / Cumplimiento) ¿Quién está al mando?
- **2. Organización de la Seguridad de la Información** (responsabilidades, dispositivos móviles y teletrabajo)
- **3. Seguridad de los Recursos Humanos** (el eslabón más débil, educación, phishing, insiders)
- **4. Gestión de los Activos** (inventario, uso aceptable, clasificación de la información, ¿USBs?)
- **5. Control de Accesos**
- **6. Cifrado**
- **7. Seguridad Física** (controles de entrada, inundaciones, incendios, ¿bloqueo de pantalla?)

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

- **8. Seguridad de las Operaciones** (logs, AV, actualizaciones, auditorías...)
- **9. Seguridad de las Comunicaciones** (cortafuegos, puede cualquiera conectarse a una roseta en mi oficina?)
- **10. Adquisición de sistemas, desarrollo y mantenimiento** (¿Qué criterios sigo al desarrollar? ¿Y al adquirir sistemas o productos?)
- **11. Relaciones con los Proveedores** (¿qué confianza deposito en ellos?)
- **12. Gestión de Incidencias que afectan a la Seguridad de la Información**
- **13. Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio**
- **14. Conformidad**: conformidad con requisitos legales y contractuales; revisiones de la seguridad de la información.

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA



CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

3.- Equipos de trabajo.
Estrategias (permisos, jerarquías, software indicado, autenticación biométrica)

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

Company Says Hilton's a Hacker...Lohan a Victim ?

149 8/23/2006 2:07 PM PDT

Paris Hilton was recently terminated from her SpoofCard account for allegedly breaking into unauthorized voice mail boxes. SpoofCard calling cards offer the ability to change what someone sees on their caller ID display when they receive a phone call.

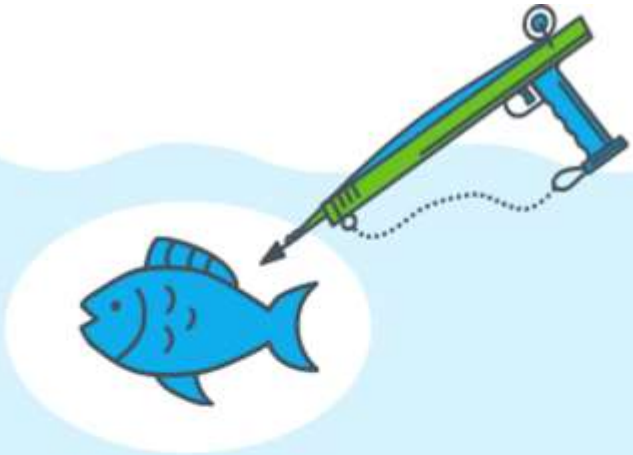
SpoofCard announced today that it had terminated the accounts of more than 50 customers, including **Paris Hilton**, who they claim used the SpoofCard service to obtain unauthorized access to voice mail accounts on a national mobile telephone network. Many of the terminated customers and the victims whose mailboxes were accessed are well-known celebrities, including **Lindsay Lohan.**

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

PHISHING

IS A BROAD, AUTOMATED ATTACK
THAT IS LESS SOPHISTICATED.



SPEAR-PHISHING

IS A CUSTOMIZED ATTACK ON A SPECIFIC
EMPLOYEE & COMPANY

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

2 de 292

Nueva politica Grupo El Corte Inglés

Departamento Informatico 12:20 (hace 1 minuto)
para mí

GRUPO El Corte Inglés

Buenos días,

Desde el departamento informático se ha establecido una nueva política de seguridad que requiere que todas las cuentas de correo electrónico de [redacted] superen un mínimo nivel de seguridad. Se ha detectado que su cuenta no cumple con dicha política.

- Longitud mínima de 12 caracteres.
- No utilizar palabras precibles como atarfil o datos personales
- No es necesario que contenga caracteres especiales, aunque pueden ser utilizados para generar una clave más segura.

Para configurar su cuenta acceda al siguiente formulario:

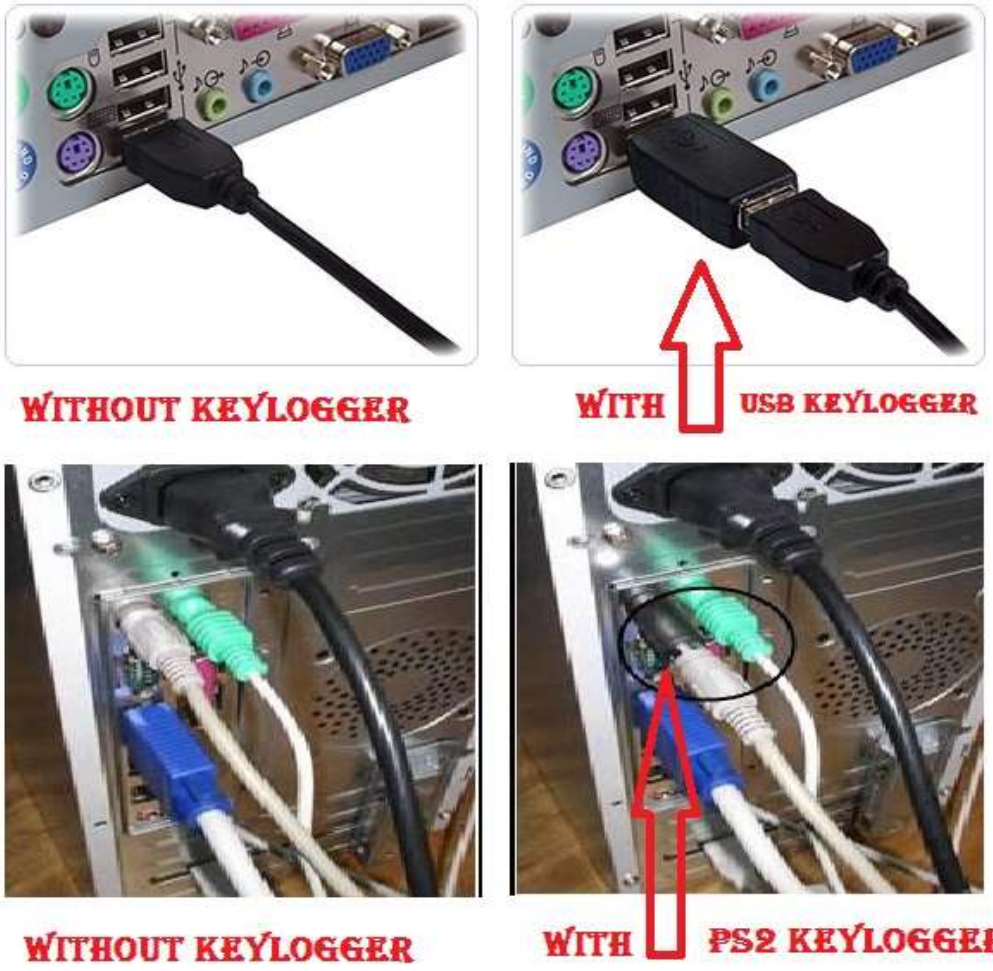
Formulario de acceso

AVISO: Este procedimiento deberá completarse a lo largo del día de hoy o su cuenta será bloqueada. Perdone las molestias, por la celeridad del proceso.

El Corte Inglés IT Department
Departamento de Tecnologías de la Información

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA



CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

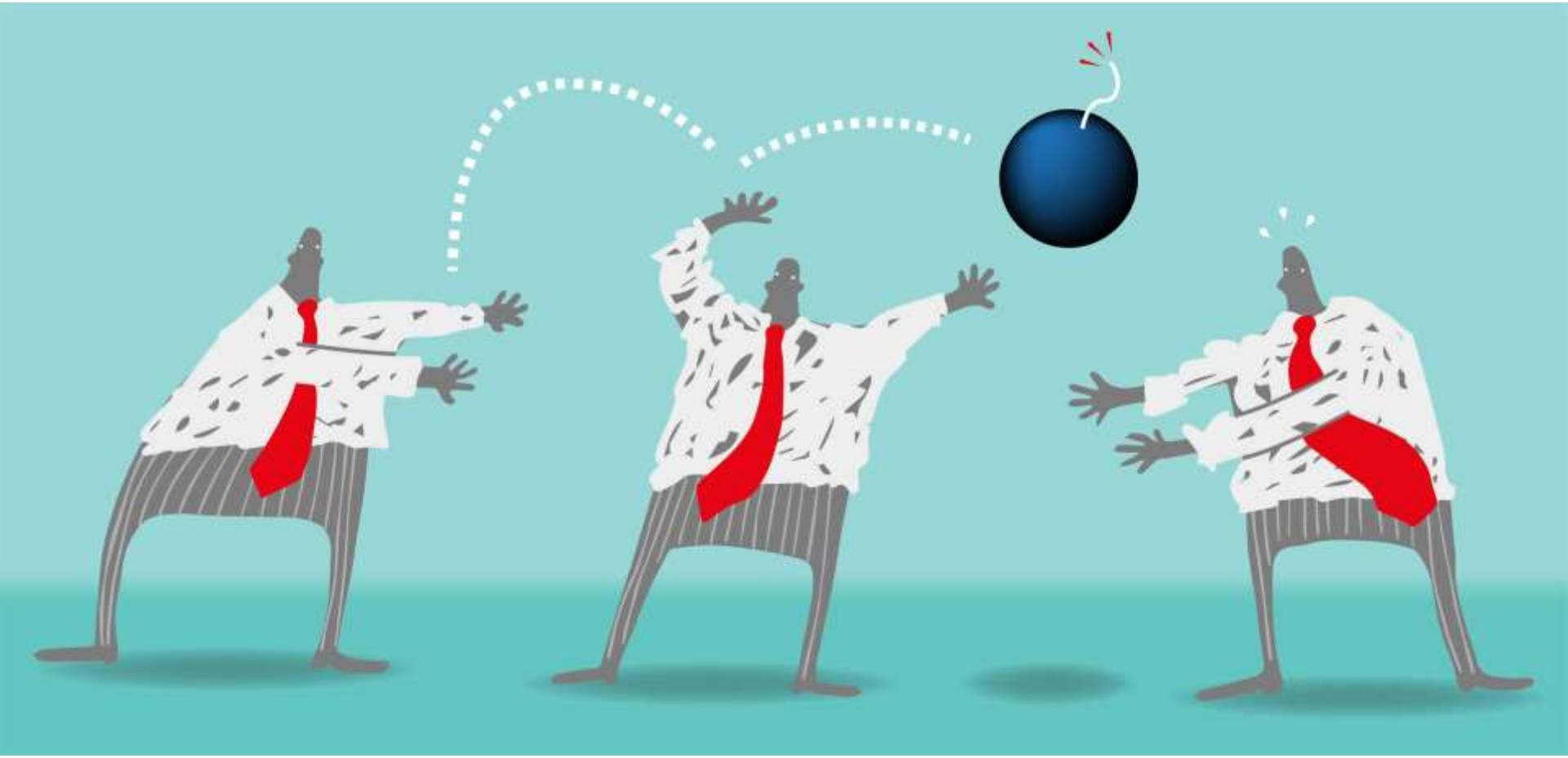
CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

4.- Cumplimiento de normas:
LOPD, conservación de datos, etc

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

5.- Aseguramiento de daños propios y de terceros

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA



CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

Información de la gestión del riesgo

a. ¿Confima que la actividad de su negocio no incluye ninguna de las siguientes? Sí ☐ No ☐
   - Servicios de procesamiento de pagos;
   - Instituciones financieras, compañías de seguros, corredurías de seguros;
   - Juegos de azar y apuestas;
   - Entidades de la administración pública (nacionales o locales);
   - Producción, distribución, publicidad o transmisión de contenidos pornográficos;
   - Agencias de calificación de créditos, agencias de rating;
   - Redes sociales personales o profesionales, incluyendo páginas web o servicios de citas.
   - Hospitales, clínicas y centros de planificación familiar;
   - Servicios públicos, tales como el suministro de gas, electricidad, agua o internet.

b. ¿Procesa, almacena o transfiere menos de 100.000 registros personales (información relativa a una persona física) anualmente? Sí ☐ No ☐

c. ¿Dispone de un antivirus actualizado e instalado en todos los sistemas y equipos, y dispone de Firewalls en todas las conexiones de red a redes externas? Sí ☐ No ☐

d. ¿Dispone de un sistema de autenticación e identificación previo para el acceso a los sistemas informáticos (usuario y contraseña), con obligación de cambiar la contraseña periódicamente? Sí ☐ No ☐

e. ¿Realiza usted copias de seguridad realizadas con una periodicidad de al menos cada 7 días y guardadas en sistemas o soportes de datos separados? Sí ☐ No ☐

f. ¿Dispone de un proceso formal de implantación de parches (actualizaciones críticas de software)? Sí ☐ No ☐

g. Si usted (o un proveedor externo en su nombre) procesa, almacena o transmite datos de tarjetas de pago, conteste a la siguiente pregunta:
   - ¿Usted (o su proveedor externo) cumple con el Estándar de Seguridad de la Industria de tarjetas de pago (PCI DSS)? Sí ☐ No ☐

Si ha contestado 'no' a alguna de la preguntas anteriores, por favor póngase en contacto con su corredor de seguros para un estudio individualizado.

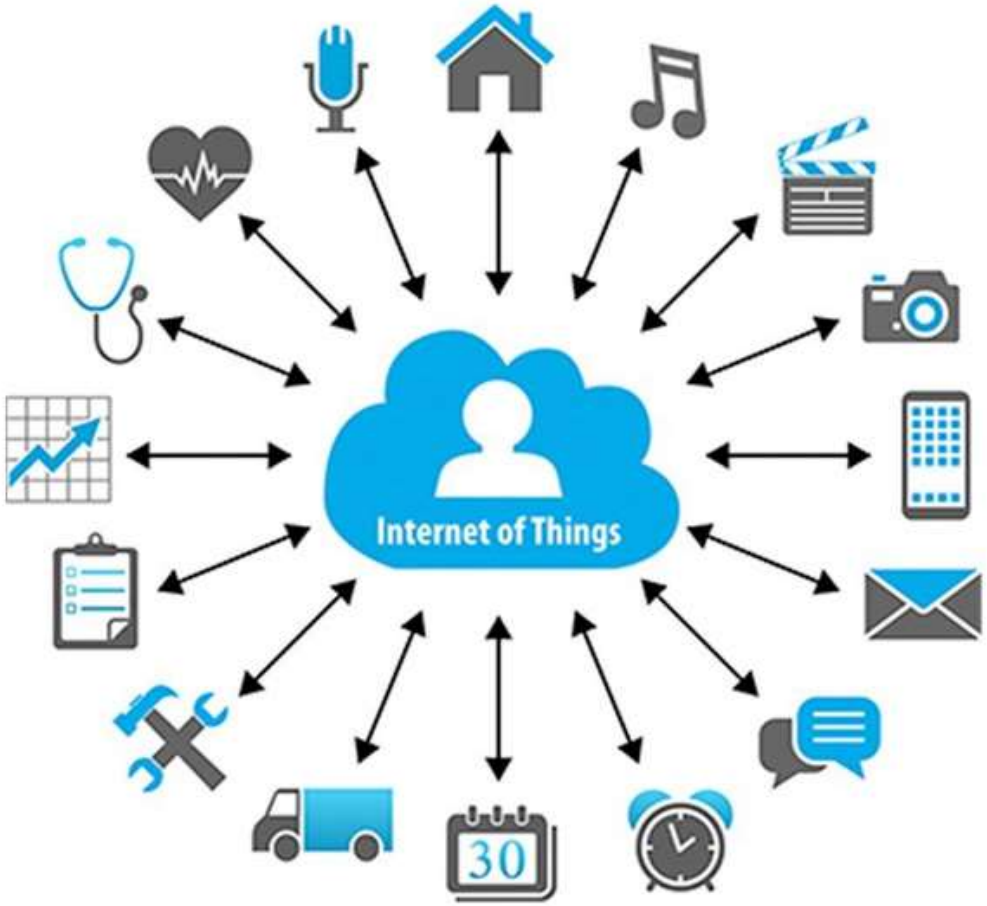
CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

- Periodos de carencia > 12 horas
- Gastos de recuperación de datos excesivos para la mayoría de escenarios
- Si aplican mejor para temas de sanciones (siempre y cuando no seamos de sectores concretos, ej, finanzas).

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

6.- IoT: vulnerabilidades de la industria 4.0, privacidad, seguridad, IA, etc

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA



CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

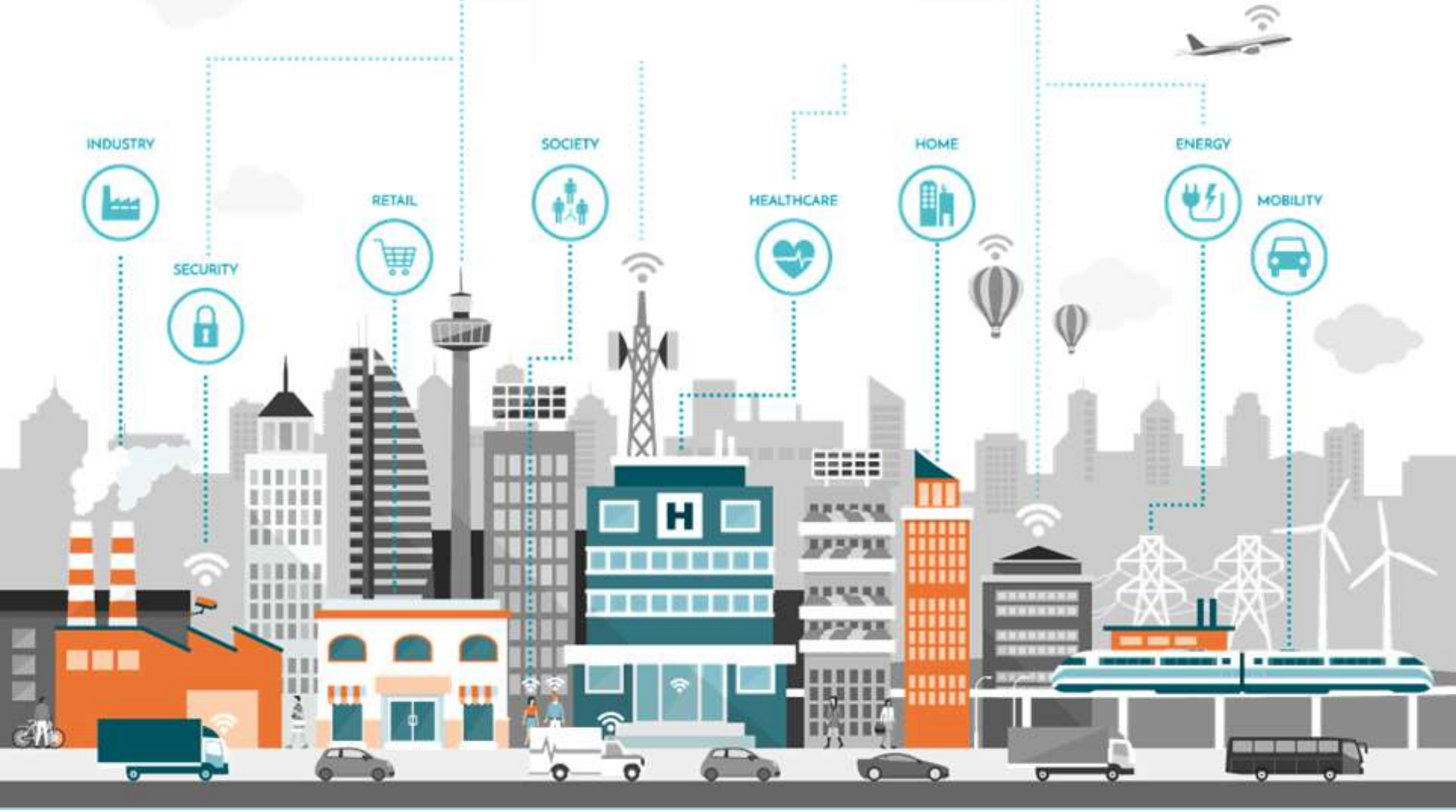
CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

Hackers Illustrate Trick That Turns Amazon Echo And All Smart Speakers Into Spy Bugs

Amazon was swift to respond to the Defcon hacking conference demonstration, updating all devices with the necessary corresponding security fixes.

By Loukia Papadopoulos
August, 13th 2018

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA



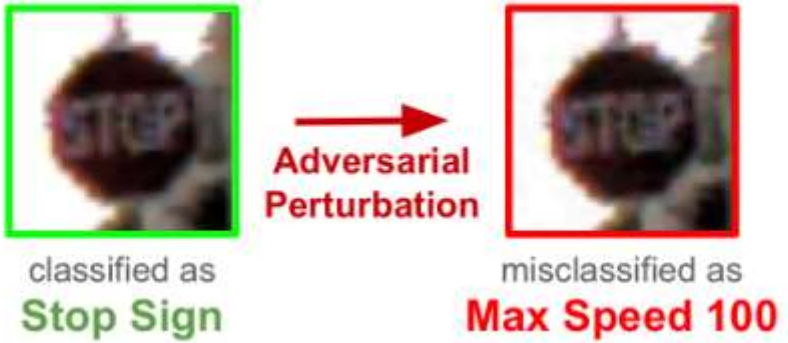
CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

EM ‹ España | Madrid | Noticias Madrid Central

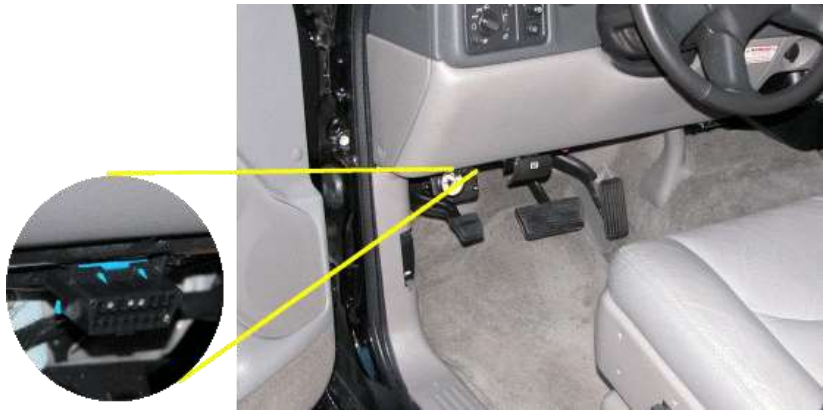
Hackean con un vídeo porno una pantalla publicitaria de la calle Preciados

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA



CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

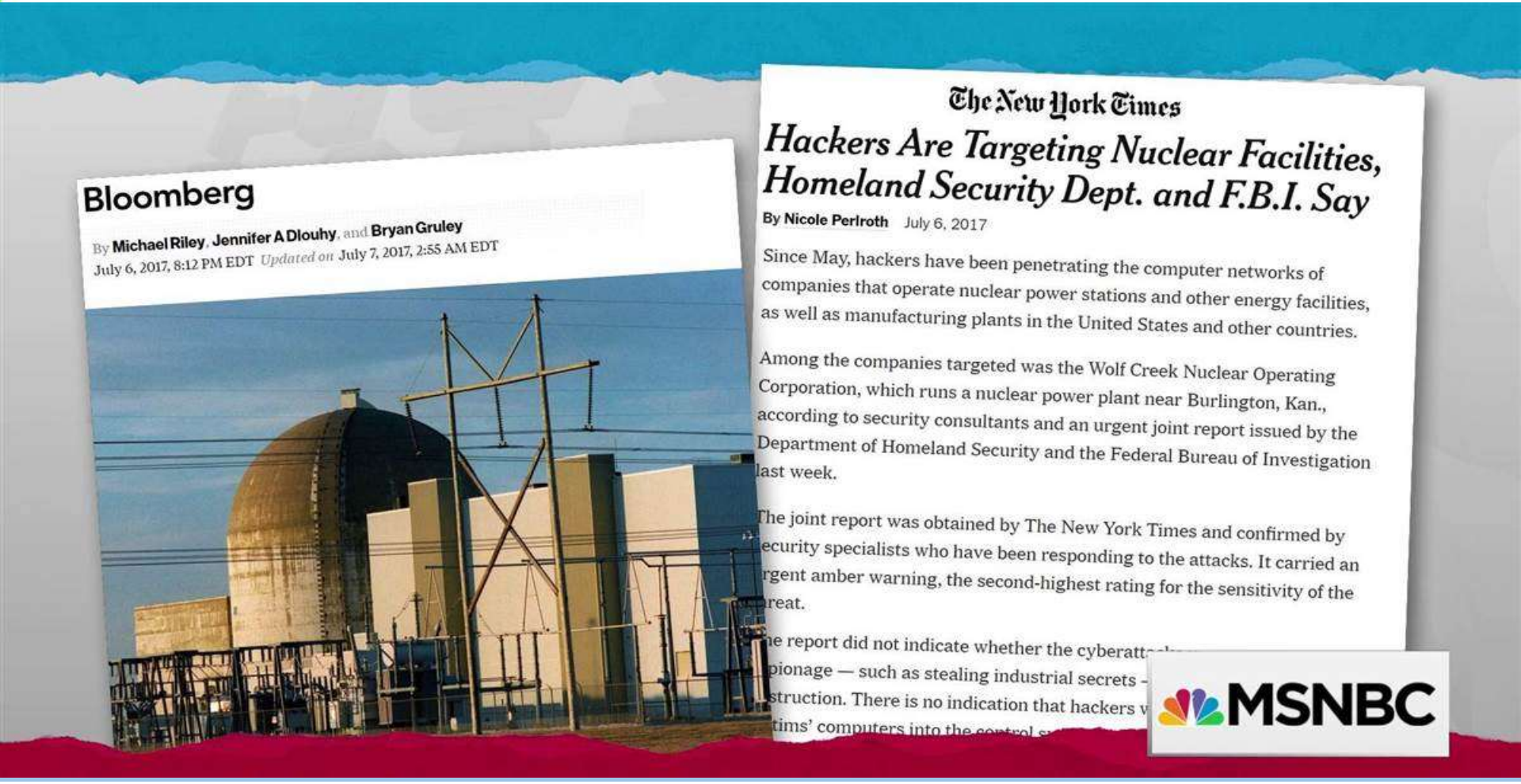
CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA



CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA



CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

La Policía investiga si una gasolinera de 'low cost' pudo ser manipulada para que se pudiera repostar gratis

Ocurrió durante todo el fin de semana. Hasta que dicho surtidor fue precintado, numerosas personas acudieron a llenar el depósito de su coche al correrse la voz

FRANCISCO GIL / DOS HERMANAS / 12 MAR 2018 / 13:23 H - ACTUALIZADO: 12 MAR 2018 / 14:04 H.

SHODAN

ZoomEye

censys
Security driven by data

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

7.- Detección y respuesta ante amenazas

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

8.- Sectores regulados: salud, finanzas, energía...

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

El Gobierno británico confirma un ataque informático a gran escala en sus hospitales públicos

- La primera ministra Theresa May se muestra convencida de que todo forma parte de un «ataque internacional»en el que se han visto implicados otros países y organizaciones.

Francisco Javier De Las Heras

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

ABC TECNOLOGÍA Móviles Electrónica Redes Videojuegos

Publicidad

Fallece Barnaby Jack, el «hacker» que podía atacar dispositivos cardiacos

- Barnaby Jack, de 35 años, muere sin causas aparentes una semana antes del inicio de la gran cita anual de los «hackers» en Nevada

Barnaby Jack - REUTERS

Publicidad

LO MÁS LEÍDO EN ABC

Tecnología | ABC

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

hipertextual

TECNOLOGÍA

Más de 400 mil pacientes actualizaron su marcapasos para evitar un hackeo

TWITTEAR COMPARTIR Paloma Beamonte - Ago 31, 2017 - 3:08 (CET)

Unos 465 mil personas con un marcapasos tuvieron que actualizar su dispositivo por una vulnerabilidad que permitía a hackers tomar control vía remota.

Las personas confían más en la IA que en los políticos

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

First ATM Jackpotter Sentenced in US Gets a Year in Prison
Gizmodo - Sep 28, 2018
The DOJ revealed in February it had charged Rodriguez and Alex Alberto Fajin-Diaz for their alleged involvement in a **jackpotting** scheme.
ATM 'jackpotter' sentenced to year in US prison
International - Engadget - Sep 28, 2018

'Jackpotting' hackers stole $267000 from Western Washington banks
Q13 FOX - Oct 1, 2018
The new scam is called "**jackpotting**", and it has been hitting banks and credit unions across the U.S. over the past year. According to a U.S. ...
FOX 12 Investigation: **'Jackpotting'** hackers stole more than $267K ...
Highly Cited - KPTV.com - Oct 1, 2018

2 Venezuelans sentenced for **'jackpotting'** ATMs
Fox17 - Nov 14, 2018
GRAND RAPIDS, Mich. – Two members of a crime syndicate from Venezuela have been sentenced for "**jackpotting**" an ATM machine in St.
2 men involved in crime syndicate sentenced for ATM thefts
International - WNDU-TV - Nov 14, 2018

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

HOME NEWS SPORTS OPINION ENTERTAINMENT LIFE MORE SUBSCRIPTION

Code-cracking teens hack into Grant Avenue ATM

Doug Lunney

Published:
June 8, 2014

Updated:
June 8, 2014 1:15 PM CDT

Filed Under:
Winnipeg SUN › News

A couple of 14-year-old computer whizzes have the Bank of Montreal upgrading their security measures after they hacked an ATM machine.

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

A password for the Hawaii emergency agency was hiding in a public photo, written on a Post-it note

Kif Leswing Jan. 16, 2018, 3:07 PM

AP/Composite/Rob Price

- **A false alert warning of an inbound missile was broadcast in Hawaii on Saturday.**
- **Since then, people have discovered that a photo taken in Hawaii's Emergency Management Agency for a news article in July includes a sticky note with a password.**
- **Hawaii says the alert was sent was because "an employee pushed the wrong button," not because of a hack, but the photo has sparked criticism about the agency's level of security.**

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

diariodeburgos.es

10°

Suscríbete

BURGOS PROVINCIA REGIÓN ESPAÑA MUNDO DEPORTES OPINIÓN GALERÍAS

MIRANDA

Un ataque cibernético detiene la fábrica de Hydro en Miranda

RAÚL CANALES - miércoles, 20 de marzo de 2019

CIBERSEGURIDAD Y COMPLIANCE EN LA EMPRESA

Código fuente del vehículo autónomo de Tesla fue robado

24 mar. 2019, 10:51:00 Comenta primero!

gigantes, robo

La compañía automotriz Tesla Motors ha presentado una demanda en contra de un antiguo empleado quien, presuntamente, habría robado el código fuente de Autopilot, el sistema de conducción semiautónomo de Tesla, para entregarlo a la empresa china Xpeng, dedicada al diseño y fabricación de vehículos eléctricos, reportan profesionales de la escuela de hackers éticos del Instituto Internacional de Seguridad Cibernética.

No obstante, esto se trata de un asunto más allá del uso de patentes de código abierto, pues los ingenieros de Xpeng copiaron la interfaz de usuario del sistema Autopilot para implementarla en uno de sus vehículos eléctricos. La polémica creció después de que Tesla afirmara que Guangzhi Cao, ex empleado del proyecto Autopilot, fue quien robó el código fuente de Autopilot, mencionan los expertos de la escuela de hackers éticos.

Información y Consultas en
masempresas.cea.es

/CEA.es @CEA.es_ /CEA.es

CEA +empresas

Gracias

MERCUREHUB legal financial tech advisors

jtsec BEYOND IT SECURITY

Financiado por:

CEA 40 Aniversario Confederación de Empresarios de Andalucía

JUNTA DE ANDALUCIA Consejería de Economía, Conocimiento, Empresas y Universidad

Información y Consultas en
masempresas.cea.es

CEA +empresas

CREACIÓN DE EMPRESAS • MEJORA DE LA COMPETITIVIDAD
REEMPRENDE • GESTIÓN FINANCIERA • MARKETING
INNOVACIÓN EMPRESARIAL • TICS
CONOCIMIENTO • INTERNACIONALIZACIÓN

CEA 40 ANIVERSARIO
Confederación de Empresarios de Andalucía

Financiado por:
JUNTA DE ANDALUCIA
Consejería de Economía, Conocimiento, Empresas y Universidad

Colaboran:
Asempal
cec CONFEDERACIÓN EMPRESARIOS PROVINCIA DE CÁDIZ
ceco
CGE CONFEDERACION GRANADINA DE EMPRESARIOS
FOE Federación Onubense de Empresarios
CEJ CONFEDERACION DE EMPRESARIOS DE JAEN
cem CONFEDERACIÓN DE EMPRESARIOS DE MÁLAGA
ces

Fomento de la Cultura Emprendedora y del Autoempleo

Participa en **#masempresas**