Transformación Digital y Ciberseguridad

Dirección de la Innovación y Gestión del Cambio. UHU

CIBERSEGURIDAD
LA PRÓXIMA PANDEMIA

GUERRAS EN LA SOCIEDAD MUNDIAL INFORMACIONAL

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Prof. Dr. Manu Martínez López - Dpto. Dirección de
va

Protección de la innovación

- Una vez la innovación se ha convertido en producto, hay que tratar de impedir que los competidores imiten la tecnología, lo cual no resulta fácil en la época actual.

- La apropiabilidad describe hasta qué punto un innovador puede capturar el valor que se deriva de la innovación en forma de beneficios.

- Como residente o como nuevo participante, hay ciertas cosas que un innovador puede hacer para prolongar el tiempo durante el cual continúe obteniendo beneficios de la ventaja.

- Mostramos algunos instrumentos y actuaciones que puede utilizar la empresa para proteger sus innovaciones:

  - Patente (título de propiedad que se hace público)
  - Secreto industrial (conocimiento no patentado, no se hace público)
  - Efecto experiencia (economías de escala)
  - Tiempo de liderazgo (economías de escala)
  - Disuasión económica (barreras de entrada)

Protección de la innovación

La ley que protege los secretos empresariales

La Ley 1/2019, de 20 de febrero de 2019, de Secretos Empresariales transpone al derecho español la Directiva (UE) 2016/943, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas.

Esta es la primera ley concreta en España que viene a regular los secretos empresariales.

Y, ¿Qué se entiende cómo el secreto empresarial? La ley en su artículo 1 lo define como: cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero, pero reuniendo los siguientes requisitos:

a) Ser secreto, esto es, no es generalmente conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas;

b) tener un valor empresarial,

c) haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto

Así conforme a lo anterior podría ser un secreto empresarial:

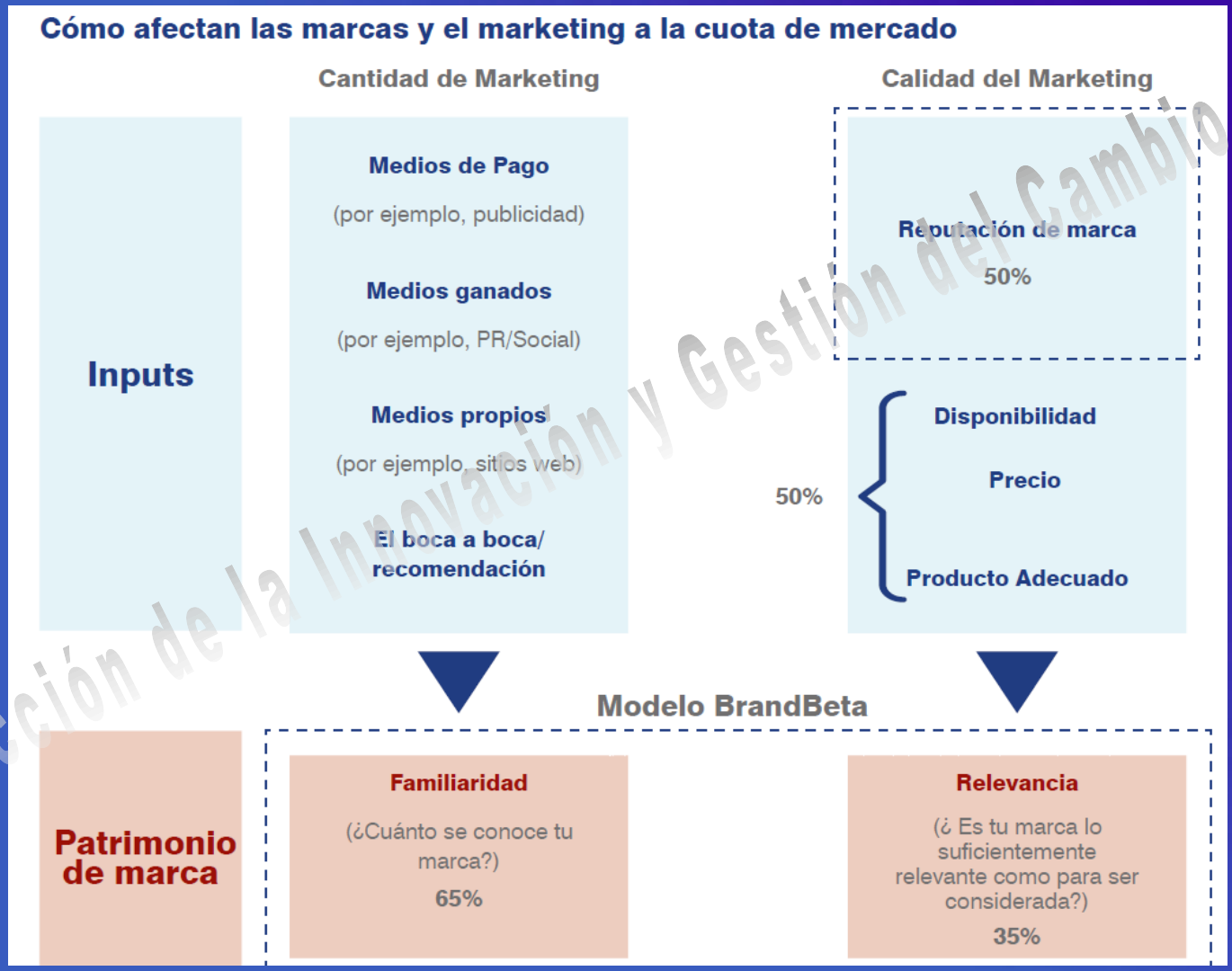
Listas de clientes, planes de negocio, un invento (obviamente no patentado), procedimiento de fabricación, entre muchos otros.

Las empresas, entre su REPUTACIÓN Y EL MIEDO A DENUNCIAR

La Unidad de Investigación Tecnológica de la Policía cree que muchas veces se minimiza el impacto de los ataques

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Transformación Digital y Ciberseguridad



Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Transformación Digital y Ciberseguridad

CIBERSEGURIDAD
LA PRÓXIMA PANDEMIA

GUERRAS EN LA SOCIEDAD MUNDIAL INFORMACIONAL

Lo primero útil que podemos hacer es conocer las **5 Leyes básicas de la Ciberseguridad** de **Nick Espinosa**:

1. Si existe una **vulnerabilidad** en un sistema se acabará explotando.
2. Todo sistema es **vulnerable** en algún momento.
3. Las personas confían en cosas en las que **NO** deberían **confiar**.
4. Nuevas tecnologías traen nuevas **vulnerabilidades**.
5. En caso de duda, **volver a la 1ª Ley**

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Nueva ISO 27002:2022. La navaja suiza de la seguridad

La **ISO 27001**:2013 es la norma internacional que proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (**SGSI**) con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como cumplimiento legal.

¿Qué propone la ISO 27001?

Brinda una norma internacional para sistemas de gestión de seguridad de la información. Con la certificación del uso de la norma **ISO 27001**:2013, la empresa puede demostrar a sus clientes actuales y potenciales, así como a sus proveedores y accionistas, la integridad en el manejo de la seguridad de la información.

Transformación Digital y Ciberseguridad

ISO 27002:2022: principales cambios en la nueva guía de controles de seguridad de la información

Principales novedades de la norma ISO 27002:2022

A continuación, un resumen de los principales cambios de la norma ISO27001:2022 frente a la versión anterior:

1. **Cambio en el nombre de la norma**: Se ha eliminado el término "*Código de prácticas*" del nombre de la nueva norma ISO 27002. Su nombre actual es "***Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información***", lo cual refleja un contexto más amplio y que incluye ahora la prevención, detección y respuesta a ciberataques, así como la protección de los datos.
2. **Cambios en controles de seguridad**: La norma ISO 27002:2013 contenía 114 controles (divididos en 14 Anexos). La versión 2022 contiene 93 controles, divididos en 4 cláusulas que se enfocan hacia el contexto de aplicación del control así:

- Controles Organizativos: 37 controles
- Controles de Personas: 8 controles
- Controles Físicos: 14 controles
- Controles Tecnológicos: 34 controles

De los 93 controles actuales:

- 58 se han actualizado
- 24 representan la fusión de controles anteriores
- 11 se han introducido como nuevos controles

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

ISO 27002:2022: principales cambios en la nueva guía de controles de seguridad de la información

Los nuevos controles

La actualización a ISO 27002:2022 incorpora **11 nuevos controles**:

- Inteligencia de amenazas.
- **Seguridad de la información en la nube.**
- Continuidad del negocio.
- Seguridad física y su supervisión.
- Configuración.
- Eliminación de la información.
- **Encriptación de datos.**
- Prevención de fugas de datos.
- Seguimiento y monitoreo.
- Filtrado web.
- Codificación segura.

Transformación Digital y Ciberseguridad

Digitalización:

Hacer lo mismo que se hacía antes, pero mediante sistemas informáticos. No aporta mucho valor ya que no optimiza los procesos.

Transformación Digital:

Cambio profundo en los procesos de la organización, buscando eficiencia y eficacia. Normalmente se busca sistematizar lo que aporta valor a la organización y automatizar lo que no aporta valor, con el objeto de poder dedicar recursos a lo que aporta valor. Puede requerir la "reinvención" de la organización e implica ser valiente y disruptivo.

Fuente: Fernando Acero Martín
Coronel (Reserva) y CISO
Global en Grupo Oesía

Ventajas de la transformación

a) Contar con datos fiables y métricas.
b) Optimización de la estructura de la organización.
c) Mayor rapidez de reacción ante cambios.
d) Reducción de costes.
e) Mayor agilidad en los procesos de negocio.
f) Mayor productividad del personal.
g) Mayor capacidad de teletrabajo.
h) Mejora de las comunicaciones.
i) Mejoras en el marketing.
j) Mejora en la imagen de marca.
k) Mejora en la experiencia de los clientes.
l) Incremento en los beneficios.

Costes de la transformación

a) La inversión necesaria para el hardware, software, implantación y formación.
b) Las inversiones para el mantenimiento del hardware, el software y formación del personal.
c) Las inversiones necesarias para la renovación del software y del hardware.
d) Las inversiones en ciberseguridad.
e) Los ajustes de plantilla, por ejemplo, contratando personal de ciberseguridad y para la gestión TIC.
f) La curva de aprendizaje para adaptarse a la nueva realidad digital de la empresa.

Transformación Digital y Ciberseguridad

Realidad de la transformación

a) En teoría, aumento de ingresos en un 11% y reducción de costes en un 20% (necesidad ante la pandemia).
b) Éxito solamente en el 30% de los casos (hay que hacerlo bien).
c) No hay garantías de que las ventajas se mantengan en el tiempo (hay cambios disruptivos que hay que detectar y gestionar).

CUANTO MAYOR ES LA TRANSFORMACIÓN, MÁS CIBERDEPENDIENTE ES LA ORGANIZACIÓN (DATA-CENTRIC), POR LO QUE ES MÁS SENSIBLE A LOS CIBERATAQUES.

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Transformación Digital y Ciberseguridad

Problemas estructurales

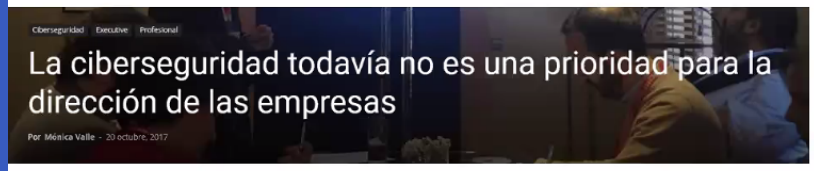
(ElevenPathts 2020 p. 8) ya en 2019 se constataba que "la industria de la ciberseguridad se enfrentaba a dos realidades opuestas: por un lado, era necesario que todas las **organizaciones incrementasen el nivel de sofisticación de sus defensas para poder protegerse** ante amenazas cada vez más avanzadas; por otro, había (y sigue habiendo) **una gran escasez de profesionales expertos y los presupuestos, aunque crecientes, seguían siendo (y siguen siendo) limitados. Por ello, construir una ciberdefensa avanzada está lejos de las capacidades de la mayoría de las empresas**."

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Transformación Digital y Ciberseguridad

Insuficientes inversiones

Transformación sin ciberseguridad = desastre



Actualidad, Mercados, Seguridad, Tecnología

La inversión en ciberseguridad crece un 10,7% en 2019

21 de octubre de 2019, 09:18

Más del 90% de los ciberataques a empresas logran su objetivo

Es una realidad. En esta época de crecimiento de la digitalización **los ciberataques también van en aumento**. El informe 2019 Cyberthreat Defense Report de CyberEdge Group recoge que el **93,7%** de los ataques producidos a través de la red a empresas e instituciones española **se han saldado con éxito**.

La cantidad de ataques cibernéticos registrados el pasado año **aumentó de forma exponencial hasta superar los 10.500 millones de incidentes en todo el mundo**, según un reciente estudio. Solo en **2018** se han descubierto casi **75.000 nuevos tipos de ataques cibernéticos**

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Transformación Digital y Ciberseguridad

Insuficientes inversiones

Transformación sin ciberseguridad = desastre

Así lo demuestran los datos aportados al informe de la nueva Directiva NIS2, que reflejan que el ciberdelito se duplicó en 2019 y el ransomware se triplicó en 2020 y que, sin embargo, las empresas e instituciones europeas siguen **invirtiendo en ciberseguridad un 41% menos** que Estados Unidos.

El pronóstico más reciente también muestra datos preocupantes: los daños causados por el ransomware podrían **alcanzar los 17 mil millones de euros** al acabar el año 2021, lo que multiplica por 57 los costes correspondientes a 2015. Y se prevé que, en 2021, las empresas sufran un ataque de ransomware cada 11 segundos, frente a los 40 segundos de 2016.

Sistemas de ciberseguridad

Inversión, nunca un gasto

Cuanto mayor es la transformación digital, más ciberdependiente es una organización y mayor es el impacto de un ciberataque. En estas organizaciones, "data-centric" la información es su principal activo y como tal, se ha de proteger adecuadamente y dicha protección es una inversión que debe estar en el plan de negocio como una parte integral del mismo.

Type of attack	Average total cost of an attack	Percent of total cost spent on preventing an attack[1]	Average cost savings resulting from the ability to prevent an attack*
Phishing	$ 832,500	18%	$ 682,650
Zero-day	$ 1,238,000	12%	$ 1,089,440
Spyware	$ 691,500	26%	$ 511,710
Nation-state	$ 1,501,500	9%	$ 1,366,365
Ransomware	$ 440,750	10%	$ 396,675
Total/Average	$ 4,704,250	15%	$ 4,046,840

Fuente: Ponemon Institute 2020

Varias tendencias y tecnologías están acelerando la transformación de la industria de la ciberseguridad, que superará los 170.000 millones de dólares en 2022, según Gartner.

Transformación Digital y Ciberseguridad

Ciberseguridad inversión

1) Nos permite evitar un ciberataque con graves consecuencias económicas y reputacionales, que además también puede implicar indemnizaciones y sanciones.
2) El gasto en ciberseguridad es entre un 10% y un 20% del gasto necesario para recuperarse.
3) Lo demandan los clientes para poder hacer negocio con ellos, por lo que es una necesidad intrínseca al negocio. Lo que implica alinear nuestra madurez en ciberseguridad con la de los clientes más exigentes.
4) La ciberseguridad tiene impacto en la valoración de la empresa y cada vez más.

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Europa impone más obligaciones de ciberseguridad a las empresas

* *La UE exigirá el refuerzo de la seguridad de la cadena de suministro*
* *Bruselas incluye a un mayor número de sectores obligados*

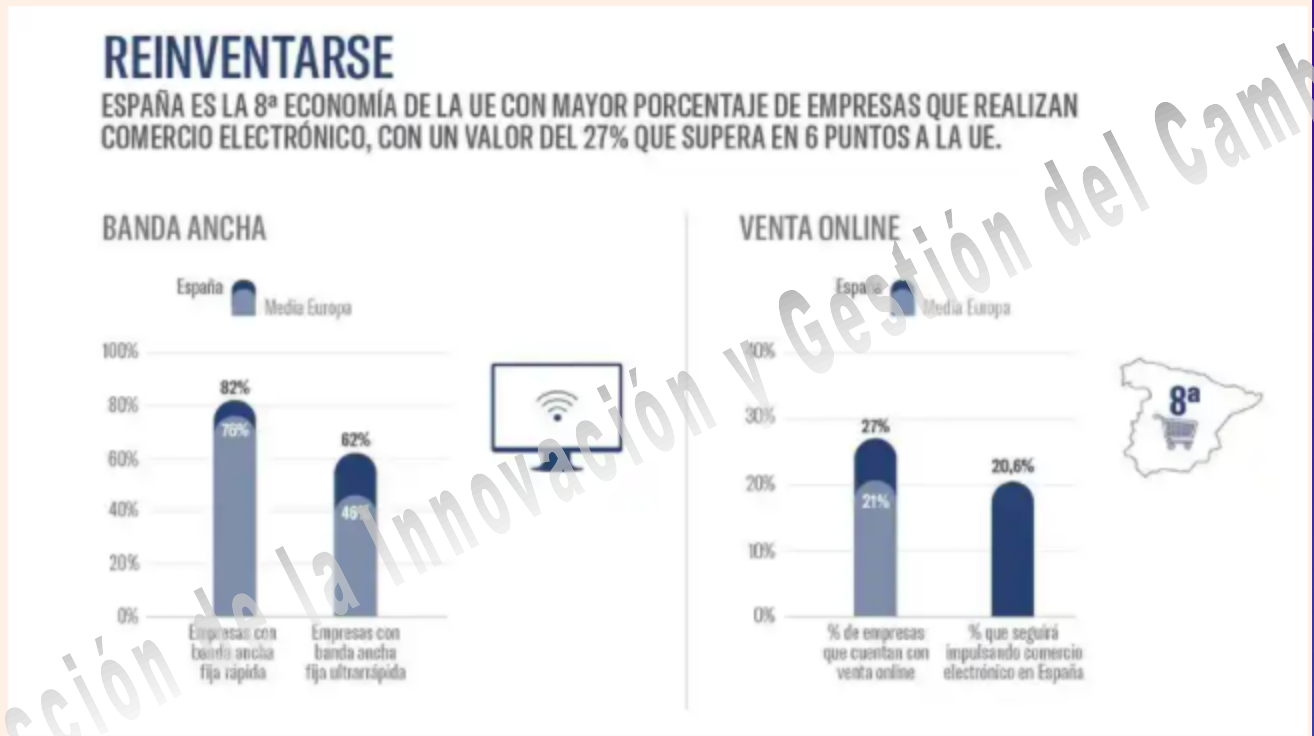
La futura Directiva europea de ciberseguridad (NIS2) incluirá aspectos relacionados con la respuesta a incidentes de seguridad, el refuerzo de la seguridad de la cadena de suministro, **el cifrado de la información**, o la divulgación de vulnerabilidades. Asimismo, se prevé que la ciberseguridad se reconozca expresamente como una responsabilidad empresarial al más alto nivel gerencial, lo que puede suponer una revisión de la responsabilidad legal de los administradores y directivos de estas compañías.

Transformación Digital y Ciberseguridad

España supera a Europa: el 60% de empresas va a invertir en digitalización en 2021

Rendimiento digital y teletrabajo en España. Fuente: #EActiVate e Ivie.

España supera a Europa: el 60% de empresas va a invertir en digitalización en 2021



Implantación de banda ancha y ecommerce. Fuente: #EActiVate e Ivie.

Destaca el elevado porcentaje de empresas españolas con **conexión de banda ancha fija rápida** (82%) y ultrarrápida (62%), también por encima -muy por encima- de la media europea (76% y 46%, respectivamente).

El año de los grandes ciberataques en España

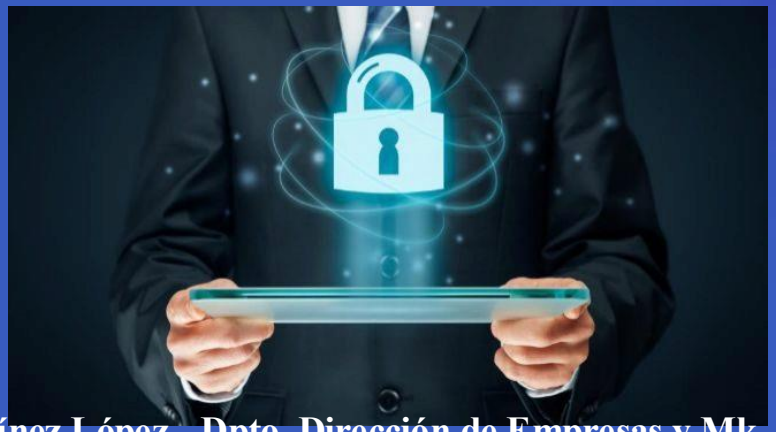
Solo en España se han dado de media 40.000 ciberataques cada día durante 2021, lo que supone un incremento del 125 por ciento

Más de medio millón de ataques en España desde 2017

En los últimos meses, diferentes empresas y administraciones como el Ayuntamiento de Sevilla, Telemadrid o el Clínic de Barcelona, han sido víctimas de ciberataques. En total, desde 2017 nuestro país ha recibido 695.101 ataques según la empresa de seguridad Pandora FMS.

Félix Barrio, director del Incibe: «Las mafias ofrecen dinero a trabajadores descontentos para que faciliten ciberataques»

La IA, la conectividad 5G y el cibercrimen organizado van a dar muchos problemas en 2024, según el jefe del Instituto Nacional de Ciberseguridad



TIPOS DE CIBERATAQUES

Tu internet

RANSOMWARE
Es un programa que restringe el acceso a determinados archivo y pide un rescate para liberar esta información.

MALWARE
Son programas que dañan los equipos informáticos y/o extraen información de los usuarios sin que ellos consientan su autorización.

TROYANOS
Son programas que al ejecutarlos permiten un acceso remoto al equipo infectado.

SPYWARE
Es un software espía que recopila información de un ordenador sin conocimiento de su propietario y la transfiere a otros dispositivos.

PHISHING
El Phishing es el robo de información personal y/o financiera del usuario, a través de la falsificación de un ente de confianza.

DDoS
Son ataques a webs que provocan su colapso y la denegación de servicio a los clientes.

TIPOS DE CIBERATAQUES

1. Spyware

El fin de este malware es infectar un ordenador ajeno para recopilar información contenida en él. Una vez que está en poder de esos datos, los transmite a una entidad externa sin conocimiento y/o consentimiento del propietario. Numerosos hackers lo emplean para lucrarse de la venta de información sensible. Teniendo en cuenta que vivimos en la era del big data y la gran cantidad de datos que generan y manejan las empresas diariamente, se trata de un tipo de virus muy dañino.

2. Phising

Otro de los peligros a los que se enfrentan con frecuencia las empresas es el phising. Este tipo de ciberataque es especialmente peligroso porque se expande vía e-mail, lo que hace que su transmisión sea muy rápida. De nuevo, el robo de información es el fin principal de los cibercriminales. ¿Y cómo acceden a esos datos requeridos de personas o empresas concretas? Mediante los correos electrónicos infectados.

3. Adware

Realmente, este software **utilizado para mostrar publicidad** está muy enfocado en robar datos a usuarios, pero también puede afectar a las empresas. En este caso, el soporte no son correos electrónicos, sino anuncios mediante los que se obtiene información de los internautas.

4. Ransomware

La frecuencia de este tipo de ataques cada vez es mayor. Lo que se consigue con ellos es **bloquear el sistema de una empresa o institución**, solicitando un rescate a cambio de liberarlo. Los efectos pueden ser catastróficos, pues la empresa en cuestión queda totalmente paralizada. Grandes compañías han sufrido ataques de este tipo recientemente, generando un considerable revuelo mediático. El lado positivo es que los virus ransomware, cada vez más perfeccionados y enfocados a dispositivos móviles, se han visibilizado mucho más en la sociedad.

5. Gusanos

Junto con los troyanos, los gusanos constituyen uno de los ataques más comunes de Internet. Su método de actuación es sencillo: se transmiten replicándose, enviando así **copias a otros equipos** y propiciando una rápida y peligrosa extensión. El primer gusano informático de la historia, el gusano Morris, data de 1988, y desde entonces la fórmula ha continuado perfeccionándose para atacar a todo tipo de equipos.

Transformación Digital y Ciberseguridad

Ransomware

La amenaza más probable y peligrosa

Ransomware

Robo y secuestro de la información, si no se paga en el tiempo establecido por los ciberdelincuentes, la información es **publicada o subastada en internet**, con todo lo que ello supone. Por lo que es mejor prevenir que curar

Supone grandes pérdidas económicas y reputacionales, al margen de sanciones o indemnizaciones por daños a terceros.

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Transformación Digital y Ciberseguridad

Ransomware

La amenaza más probable y peligrosa

Sophos **News**

El 53% de las empresas españolas fueron víctimas de un ataque de ransomware el año pasado

Actualidad · nota de prensa · Ransomware · Sophos

20 MAY 2020

El 60% de las pymes afectadas por un ciberataque cierra en 6 meses

Por **INESE** - 22 noviembre, 2019 1402 0

- **Almost three quarters of ransomware attacks result in the data being encrypted.**

51% of organizations were hit by ransomware in the last year. The criminals succeeded in encrypting the data in 73% of these attacks.

Lo que implica que un 23,85% de las empresas españolas podrían estar cerrando anualmente por este tipo de ciberataques.

Según un reciente informe de la firma de ciberseguridad Sophos, en el que han participado 5.000 responsables de TI de empresas de 26 países del mundo, durante 2019 el 51 por ciento de las compañías sufrieron un ataque de este tipo. Cifra que crece en el caso concreto de España hasta alcanzar el 53 por ciento

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Transformación Digital y Ciberseguridad

Ransomware

Daño reputacional y repetición de ataques

Casi un 60% de los usuarios cambiaría de compañía si es atacada

SEGURIDAD

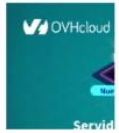
Un informe de la firma Arcserve muestra la escasa tolerancia de los clientes con las organizaciones que han sido objetivo de campañas de malware.

Por qué las organizaciones caen víctimas de repetidos ataques de ransomware

Algunas organizaciones son golpeadas con ransomware varias veces. Los investigadores de amenazas explican por qué ocurren los ataques repetidos y cómo las víctimas pueden evitar que vuelva a ocurrir.

por Alexander Culafi, TechTarget

Publicado 17 jun 2020



Los repetidos ataques de ransomware se han convertido en una ocurrencia común en los últimos años. Según un informe de 2017 del proveedor de protección de datos Druva, el 50 % de los 832 profesionales de TI encuestados dijeron que su organización había sido golpeada con ransomware varias veces. En su encuesta mundial de 2018 de 2.700 gerentes de TI, el proveedor de seguridad de punto final Sophos descubrió que la mayoría de las organizaciones sufrían múltiples ataques con un número promedio de dos por año.

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Las empresas, entre su

REPUTACIÓN Y EL MIEDO A DENUNCIAR

La Unidad de Investigación Tecnológica de la Policía cree que muchas veces se minimiza el impacto de los ataques

Muchos casos no se denuncian y se mantienen en la más estricta confidencialidad para no alarmar a los clientes

No proteger los datos deja expuesta información comercial que un exempleado puede llevarse a la competencia

Un ciberataque tarda en detectarse 170 días y se necesitan 45 para solucionarlo

Ninguna empresa es menos vulnerable ni menos atractiva para un cibercriminal, que puede apuntar tanto a pymes como a grandes compañías

Además del robo de datos, también hay ataques dirigidos a sabotear torres de refrigeración, generadores eléctricos, etc.

Transformación Digital y Ciberseguridad

Ransomware

La pandemia

Aumentan un 160% los ataques de ransomware en España en el tercer trimestre

Actualidad 08 OCT 2020

Ciberataque /

El ciberataque a un hospital alemán provoca la primera muerte en el mundo por ransomware

Medios locales de la ciudad alemana de Düsseldorf informan de la muerte una paciente en un hospital tras sufrir el centro hospitalario un ataque de hackers contra los sistemas informáticos que complicaron el tratamiento de la enferma.

Antena 3 Noticias

Publicado: 18.09.2020 12:12
Actualizado: 18.09.2020 12:46

Hay dudas sobre la puesta en marcha de los planes de emergencia

Adeslas continúa sin restablecer al 100% sus sistemas seis semanas después del ataque por ransomware

Por Redacción - 25 octubre 2020

Tanto afecta a la valoración de la empresa, sus datos financieros, como sus capacidades reales de ciberseguridad. De nada sirven tener datos financieros saneados, si se recibe un ciberataque mayor y se producen daños reputacionales y económicos graves.

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Air Europa pide a sus clientes que cancelen sus tarjetas de crédito tras sufrir un ciberataque

que siga los siguientes pasos:", dice el email.

1. Identifique la tarjeta usada para efectuar pago/s en la página web de AIR EUROPA.
2. Contacte con su entidad bancaria.
3. Solicite la anulación/cancelación/sustitución de esa tarjeta para poder evitar el posible uso fraudulento de su información.
4. No facilite información personal, su pin, nombre o cualquier otro dato personal a través de teléfono, mensaje o email, incluso cuando se identifiquen como su entidad bancaria.
5. No pinche enlaces que le avisen de operaciones fraudulentas. Póngase en contacto directo con su entidad bancaria por medios constatables.
6. Recopile cualquier prueba de posible uso no autorizado de su tarjeta y denúncielo ante las Fuerzas y Cuerpos de Seguridad del Estado.

El CNI confirma un ciberataque masivo a empresas españolas

Telefónica lo ha confirmado pero otras compañías lo niegan

BBVA, Santander, Iberdrola, Gas Natural o Vodafone

Telefónica

El *ransomware* 'WannaCry' causó pérdidas de 3.500 millones de euros infectando 300.000 ordenadores de 150 países en 2017, entre ellos los de la multinacional española. Encriptaba todos los datos del equipo de forma que el usuario no pudiera acceder a ellos salvo con una clave que solo podrían obtener previo **pago de un rescate, que era de 300 dólares en bitcoin por PC 'hackeado'.**

El SEPE sufre un ataque informático que paraliza sus servicios

El ciberataque al SEPE provocó que sus técnicos trabajaran 19.000 horas extras en jornadas maratonianas y festivos: así levantaron una barricada contra el 'ransomware'

El personal estuvo movilizado **20 horas al día durante 3 semanas, los 7 días de cada una de ellas.** De hecho, los técnicos continuaron movilizados en Semana Santa, que se celebró apenas unas semanas después de que se detectase el incidente. Un incidente que los protocolos de ciberseguridad del SEPE llegó a detectar, pero no logró frenar a tiempo.

Media Markt sufre un ciberataque que bloquea sus servidores días antes del Black Friday

A principios del mes de noviembre, en plena preparación de la campaña de Black Friday, de nuevo un **ataque de 'ransomware' bloqueó los servidores de MediaMarkt**, por culpa del cual se vieron afectadas sus tiendas en España, Alemania, Bélgica y Holanda.

La empresa digital española de compra y reparto a domicilio **Glovo** es la víctima del tercer ciberataque recogido por IEBS Business School. La compañía hizo público que el 29 de abril había sufrido un acceso no autorizado a sus sistemas a través de una antigua interfaz del panel de administración.

Ciberataque a Europa: La Ser, Everis y otras empresas bloqueadas por ransomware

Phone House también experimentó uno de los ataques más destacados en España en 2021. La empresa sufrió un ataque cibernético el **11 de abril** que dejó al descubierto datos sensibles de millones de clientes de la cadena de servicios de telecomunicaciones.

Otro de los grandes incidentes lo sufrió el **fabricante tecnológico taiwanés Acer** también en marzo, cuando experimentó un ataque de 'ransomware'. Los delincuentes, que infectaron sus sistemas pidieron uno de los mayores rescates solicitados hasta la fecha: 50 millones de dólares, a cambio de descifrar los archivos que habían sido encriptados.

El ciberataque a la UAB afectará hasta finales de año: la difícil gestión de una universidad sin acceso a su sistema informático durante meses

El pasado 11 de octubre, la Universidad Autónoma de Barcelona (UAB) sufrió un ciberataque cuyas consecuencias todavía duran y se prevé que duren al menos hasta mediados de diciembre. El ataque afectó al sistema de virtualización que aloja gran parte de los servicios corporativos de la universidad, lo que a la práctica dejó sin funcionar la página web oficial, los correos oficiales, el Campus Virtual y la red de internet. **Alumnos, profesores e investigadores se quedaron sin acceso al sistema informático de la universidad**, obstaculizando gran parte de sus tareas diarias.

La gravedad del ciberataque a la Universidad Autónoma de Barcelona: hay más de 650.000 archivos comprometidos

Desde el equipo TIC UAB, que ha estado informando a los usuarios a través de Twitter o Telegram, se explica que una vez finalizada la inspección se procederá a **reinstalar Windows 10 en todos los ordenadores**, recomendando que si se tienen documentos guardados en el disco duro se guarden en la nube o en USB externos.

En el caso de las aulas de informática están dando servicio, pero sin conexión a ninguna red. **Para los profesores sí se permite utilizar portátiles en clase, pero sin conexión**, según describe un FAQ creado por el equipo TIC.

El próximo 2 de noviembre está previsto que se pueda volver a trabajar con el entorno de Microsoft (One Drive, Outlook, Teams), con quien se está colaborando. **Como alternativa al Campus Virtual, se utilizará Teams** como herramienta corporativa.

Garmin pagó millones de dólares por obtener la clave de descifrado del ransomware WastedLocker

Todo apunta a que se trata del «ransomware» llamado **WastedLocker**, diseñado por Evil Corp, un grupo ciberdelincuentes rusos cuyo líder está buscado por el FBI. Su funcionamiento consiste en la instalación de un código malicioso en pantallas falsas de actualizaciones de software para hacerse con el control de los equipos informáticos. Tiene, además, **la capacidad para personalizarse en función de las víctimas.**

Filtran un fichero con 1.400 millones de contraseñas robadas ¿Es la tuya una de ellas?

La compañía de ciberinteligencia española-estadounidense **4iQ**, dedicada exclusivamente a detectar bases de datos de usuarios y contraseñas en la **Deep Web** (la zona de Internet donde el contenido no es indexado por los motores de búsqueda convencionales), reconoce, **a través de su blog**, **haber descubierto un fichero que contiene 1.400 millones de contraseñas**, lo que lo convierte en **la mayor base de contraseñas robadas conocida hasta la fecha.**

El equipo de 4iQ hallaba el pasado 5 de diciembre **un fichero con un peso de 41 gigabites** formado por 1.400 millones de contraseñas en texto no encriptado. Por lo tanto, las contraseñas han estado visibles para todo el mundo que haya accedido al foro en el que se ha encontrado el fichero. Según explica el fundador y director de tecnología Julio Casal, la compañía ha probado algunas de estas contraseñas y "la mayoría" se ha mostrado como válida. Por lo tanto, cualquier persona puede acceder a estas contraseñas a través de este foro clandestino.

Filtran un fichero con 1.400 millones de contraseñas robadas ¿Es la tuya una de ellas?

	Count	Password		Count	Password
1	9218720	123456	21	370652	666666
2	3103503	123456789	22	354784	123
3	1651385	qwerty	23	347187	monkey
4	1313464	password	24	343864	dragon
5	1273179	111111	25	311371	1qaz2wsx
6	1126222	12345678	26	300279	123qwe
7	1085144	abc123	27	299984	121212
8	969909	1234567	28	298938	myspac
9	952446	password1	29	291132	a123456
10	879924	1234567890	30	276473	qwe123
11	866640	123123	31	270488	1q2w3e4r
12	834468	12345	32	268121	zxcvbnm
13	621078	homelesspa	33	263605	7777777
14	564344	iloveyou	34	255079	123abc
15	527158	1q2w3e4r5t	35	250732	qwerty123
16	470562	qwertyuiop	36	241721	qwerty1
17	468554	1234	37	241495	987654321
18	417878	123456a	38	227701	222222
19	398114	123321	39	226785	555555
20	371637	651321	40	220363	1' 2233

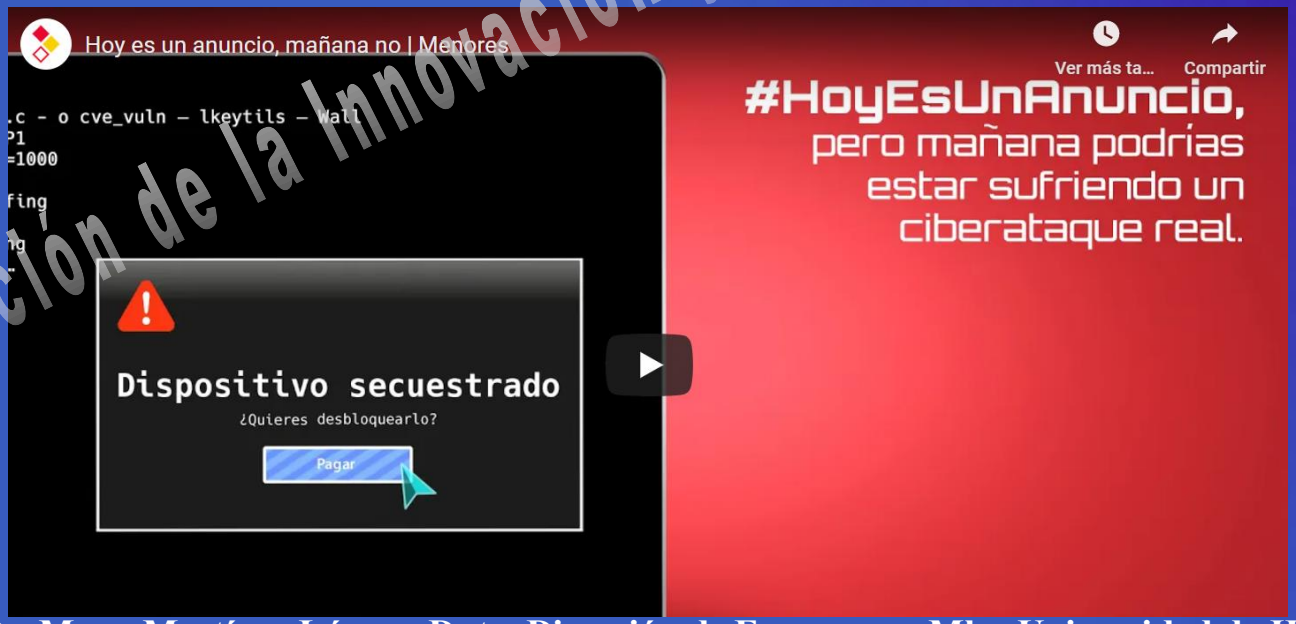
GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

¿Necesitas ayuda en ciberseguridad?

INCIBE pone a disposición de empresas, ciudadanos, padres, menores y educadores una línea telefónica gratuita de ayuda en ciberseguridad: **017**. Horario de 9:00 a 21:00 horas.



Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Transformación Digital y Ciberseguridad

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Transformación Digital y Ciberseguridad

Cómo identificar un correo electrónico malicioso

Cientos de emails fraudulentos llegan a nuestras bandejas de correo y, aunque muchos son eliminados, otros consiguen su objetivo, ser leídos. Depende de nosotros saber cómo identificar un correo electrónico malicioso:

1 REMITENTE
¿Esperabas un email de esta persona/entidad?
Comprueba que el email coincida con la persona o entidad remitente que dice ser o si está suplantando a alguien.

2 ASUNTO
¿Capta tu atención el asunto del correo?
La mayoría de correos fraudulentos utilizan asuntos llamativos e impactantes para captar tu atención. Ten en cuenta esta consideración.

3 OBJETIVO DEL MENSAJE
¿Cuál es el objetivo del correo?
Una entidad de servicios como el banco, suministros del hogar (agua, gas) u otros nunca te pedirá tus datos personales por correo. Además, si es de carácter urgente, amenazante o con ofertas y promociones muy atractivas, es muy posible que sea un fraude.

4 REDACCIÓN
¿Tiene errores ortográficos o parece una mala traducción de otro idioma?
Revisa la redacción en busca de errores de ortografía o gramaticales. Además, si no está personalizado o parece una traducción automática, sospecha.

5 ENLACES
¿Los enlaces llevan a una página legítima?
Sitúa el cursor encima del enlace, o mantén presionado el enlace en dispositivos móviles, podrás ver la URL real a la que redirige. Si no coincide o es una web sin certificado de seguridad (https://), no hagas clic.

6 ADJUNTOS
¿Contiene un archivo adjunto que no estabas esperando o es sospechoso?
Analiza los adjuntos antes de abrirlos, puede tratarse de un *malware*.
Los antivirus y analizadores de ficheros te ayudarán a identificar si están infectados.

Finalmente, **no olvides utilizar el sentido común y aplicar todos los contenidos que se encuentran en la OSI** para convertirte en un usuario ciberseguro.

¡Sigue estas pautas y disfruta de un correo electrónico libre de riesgos!

GOBIERNO DE ESPAÑA · VICEPRESIDENCIA TERCERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · @INCIBE · INCIBE · @INCIBE · 017

Mantente al día con nuestras campañas de concienciación para estar informado.
¡Es nuestra mejor defensa!
www.incibe.es | www.osi.es

OSI Oficina de Seguridad del Internauta · @osiseguridad · osiseguridad

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

10 CONSEJOS PARA LA CIBERSEGURIDAD EN LA EMPRESA

MES EUROPEO DE LA SEGURIDAD CIBERNÉTICA

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Comisión Europea

PRIORIDAD

Una Europa adaptada a la era digital

Capacitar a las personas con una nueva generación de tecnologías

Acciones


Inteligencia artificial


Estrategia europea de datos


Estrategia industrial europea


Informática de alto rendimiento


Ley de Mercados Digitales


Ley de Servicios Digitales


Ciberseguridad


Capacidades digitales


Conectividad

Transformación Digital y Ciberseguridad

Las principales amenazas 2021

Ransomware

Robo y secuestro de la información, si no se paga en el tiempo establecido por los ciberdelincuentes, la información es **publicada o subastada en internet**, con todo lo que ello supone. Por lo que es mejor prevenir que curar

Supone grandes pérdidas económicas y reputacionales, al margen de sanciones o indemnizaciones por daños a terceros.

Ciberespionaje

Ciberespionaje, una amenaza al desarrollo económico y la defensa. El resultado es **el incremento de las Campañas de ciberespionaje**, tanto de motivación económica, como política. **Importantes datos de investigaciones avanzadas en materia de tecnologías de la información, marítima, energética o de Defensa se han exfiltrado** junto con datos personales, en ciertos casos.

Javier Candau
Jefe de Ciberseguridad del CCN

CIBERSEGURIDAD
LA PRÓXIMA PANDEMIA

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Transformación Digital y Ciberseguridad

CIBERSEGURIDAD
LA PRÓXIMA PANDEMIA

GUERRAS EN LA SOCIEDAD MUNDIAL INFORMACIONAL

Lo primero útil que podemos hacer es conocer las **5 Leyes básicas de la Ciberseguridad** de **Nick Espinosa**:

1. Si existe una **vulnerabilidad** en un sistema se acabará explotando.
2. Todo sistema es **vulnerable** en algún momento.
3. Las personas confían en cosas en las que **NO** deberían **confiar**.
4. Nuevas tecnologías traen nuevas **vulnerabilidades**.
5. En caso de duda, **volver a la 1ª Ley**

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Transformación Digital y Ciberseguridad

Ciberespionaje

La pandemia

europapress / españa

Publicado 17/09/2020 13:12 CET

El CNI avisa de más ciberataques en la pandemia: ciberespionaje por la vacuna, desinformación y ataques al teletrabajo

Ciberespionaje — España

China, Corea del Norte, Irán y Rusia están detrás de los 36 ciberataques que han sacudido a España en 2019

REPUBLICA | 13/12/2019

La 'guerra silenciosa' se ha cebado principalmente con organizaciones y corporaciones estatales de importancia estratégica en nuestro país

europapress / portaltic / ciberseguridad

Publicado 03/09/2020 18:44 CET

Una campaña de ciberespionaje de origen chino ataca a Europa con la Covid-19 como cebo para distribuir 'malware'

Malware es un término general para referirse a cualquier tipo de "malicious software" (software malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento.

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Transformación Digital y Ciberseguridad

Metodología ABCDE

A. ACTUALIZACIÓN
B. BASTIONADO (CONFIGURACIÓN DE SEGURIDAD)
C. CONCIENCIACIÓN / CIBERINTELIGENCIA
D. DEFENSA ACTIVA
E. EXTENDER LA CIBERSEGURIDAD A TODO EL PERÍMETRO

ADEMÁS:
Formar parte activa de la comunidad de ciberinteligencia generando y compartiendo muestra ciberinteligencia.
(Línea de Acción 1 Estrategia Nacional de Ciberseguridad de 2019.)

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Transformación Digital y Ciberseguridad

Áreas de la ciberseguridad

A. IDENTIFICACIÓN
B. DETECCIÓN
C. DEFENSA
D. RESPUESTA
E. RECUPERACIÓN

ADEMÁS:
Formar parte activa de la comunidad de ciberinteligencia generando y compartiendo muestra propia ciberinteligencia.
(Línea de Acción 1 Estrategia Nacional de Ciberseguridad de 2019.)

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Transformación Digital y Ciberseguridad

Recomendaciones

a) Transformación con enfoque holístico y con la ciberseguridad por diseño y por defecto.
b) Seguir la metodología ABCDE con precisión.
c) Realizar un análisis de riesgos formal y basar las decisiones de ciberseguridad en el resultado del mismo.
d) Disponer de un seguro de ciberriesgos, pero nunca como sustituto de la ciberseguridad.
e) Considerar la ciberseguridad como una inversión necesaria para mantener el negocio y para poder hacer negocios con terceros.
f) Tener un buen plan de continuidad de negocio.

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Transformación Digital y Ciberseguridad

Las principales amenazas 2021

Ransomware

Robo y secuestro de la información, si no se paga en el tiempo establecido por los ciberdelincuentes, la información es **publicada o subastada en internet**, con todo lo que ello supone. Por lo que es mejor prevenir que curar

Supone grandes pérdidas económicas y reputacionales, al margen de sanciones o indemnizaciones por daños a terceros.

Ciberespionaje

Ciberespionaje, una amenaza al desarrollo económico y la defensa. El resultado es **el incremento de las Campañas de ciberespionaje**, tanto de motivación económica, como política. **Importantes datos de investigaciones avanzadas en materia de tecnologías de la información, marítima, energética o de Defensa se han exfiltrado** junto con datos personales, en ciertos casos.

Javier Candau
Jefe de Ciberseguridad del CCN

CIBERSEGURIDAD
LA PRÓXIMA PANDEMIA

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

Protección de la innovación

Un ciberataque masivo golpea a varias grandes empresas de EEUU

Amazon y Netflix. La compañía Amazon, que además de su popular portal de comercio electrónico proporciona a través de su servidor AWS servicios de internet a otras compañías como la cadena de televisión on line Netflix, ha informado de interrupciones esporádicas.

PayPal. "El ciberataque ha impedido que algunos de nuestros clientes puedan pagar con PayPal en ciertas regiones", ha afirmado la portavoz de la compañía, Amanda Miller. "PayPal no ha sido atacado directamente", ha remachado.

***The New York Times* y *Financial Times*.** Las webs de numerosos medios de comunicación también han sufrido los efectos: entre otros, CNN, *The New York Times*, *Boston Globe*, *Financial Times* y *The Guardian*.

Spotify, Reddit, Airbnb y The Verge. Con millones de usuarios en todo el mundo, estas plataformas han confirmado también una interrupción del servicio.

Adobe | Apple | Sony Playstation | Sony Pictures | Citigroup | Bancos de 30 países | Instituciones Financieras

JP Morgan | Ashley Madison | G20 | Pentágono | eBay | Home Depot | Target

¿Qué falla en la seguridad informática estadounidense?

Los ataques informáticos a entidades financieras han subido un 60% en un año. El último, una acción coordinada contra siete bancos estadounidenses presuntamente organizada por hackers rusos. ¿Qué está fallando? Y lo más importante: ¿Cuál es la solución?

¿Qué esta pasando en la seguridad informática estadounidense? El FBI y el Servicio Secreto están investigando estos días un incidente presuntamente con origen en hackers rusos que habrían realizado este mes una ofensiva masiva y coordinada contra siete grandes entidades, entre las que está JPMorgan Chase, según informó recientemente Bloomberg.

Se sospecha que pudieron acceder a datos personales de los clientes, aprovechando una vulnerabilidad en las aplicaciones para móviles, pero no consta que hayan tocado sus cuentas bancarias. El FBI investiga si se trató de una represalia por las sanciones impuestas por Washington a Rusia por su vinculación en la actual crisis en Ucrania.

La portavoz de JPMorgan, Patricia Wexler, ya ha saltado a la palestra para señalar que grandes empresas son blanco frecuente de este tipo de ataques, por lo que cuentan con múltiples formas de defensa.

La mejor defensa, un buen ataque

Un grupo de bancos de Wall Street tiene previsto reunirse con el Departamento del Tesoro estadounidense y otros altos cargos del Gobierno de Estados Unidos el próximo mes de septiembre para abordar cómo cooperar en la lucha contra los ciberataques.

El programa del encuentro no se ha elaborado aún, pero sí se ha identificado a todos los asistentes, según han informado a Reuters fuentes cercanas a estos planes. Banqueros y altos cargos del Gobierno trabajarán en fórmulas de alertar a las empresas financieras sobre los ciberataques, sin violar la privacidad de las empresas atacadas.

BANCA

S&P bajará el ráting a los bancos mal protegidos frente a los ciberataques

La amenaza de los ciberataques contra los bancos crece en paralelo al uso de las nuevas tecnologías y a la oferta digital.

Los bancos fortalecen sus defensas para proteger su negocio así como los datos y la confianza de sus clientes. Pero no solo deben hacerlo por eso. La agencia de ráting Standard & Poor's (S&P) les acaba de dar otra razón.

Si los bancos no están lo suficientemente blindados frente a los piratas informáticos la firma estadounidense les puede bajar la nota. «Vemos la débil seguridad frente a los ciberataques como una amenaza emergente que puede suponer un riesgo más alto para las entidades financieras en el futuro, y posiblemente dar lugar a rebajas de calificación», anticipa.

El analista de S&P Stuart Plesser subraya en un reciente informe que los bancos son la diana permanente de los delincuentes cibernéticos debido al gran valor de los datos que atesoran, a la elevada interconexión del sistema financiero y a su papel como conductos de divisas.

1,5 millones de dólares al que encuentre una vulnerabilidad en iOS 10

Una compañía de seguridad aumenta su programa de recompensas dado el alto nivel de seguridad anunciado por Apple para su sistema operativo móvil

Una compañía de seguridad *Black Hat*, llamada Zerodium, ha puesto una **suculenta recompensa para quien consiga encontrar una vulnerabilidad** en el nuevo sistema operativo móvil de Apple, iOS 10. En concreto, quien consiga encontrar vulnerabilidades para realizar un ataque de día cero, recibirá nada más y nada menos que **un millón y medio de dólares por revelar cómo lo ha hecho**.

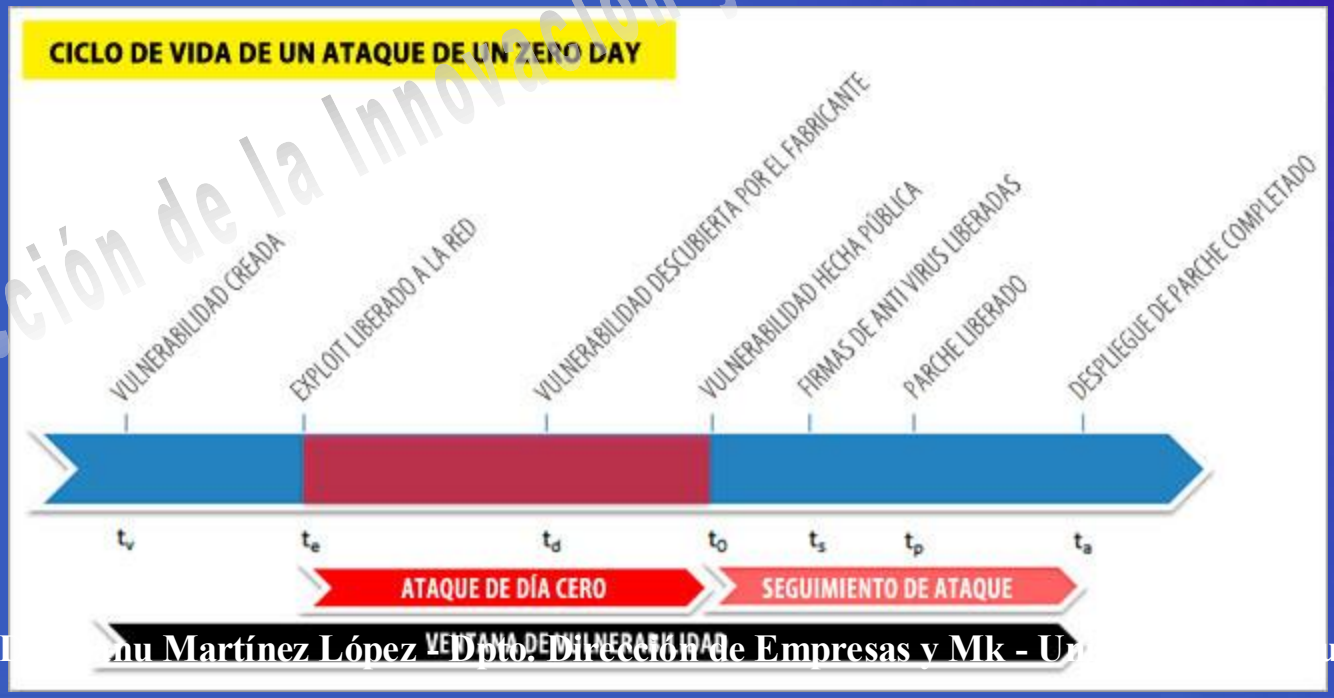
"Un ataque de día-cero (en inglés zero-day attack o 0-day attack) es un ataque contra un sistema que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que, por lo general, son desconocidas para el fabricante del producto"

El motivo por el que se ofrecen este tipo de recompensas es que, después, **las vulnerabilidades encontradas se venden a los fabricantes, en este caso Apple, o incluso a los gobiernos**. En comparación, hackear iOS 9 estaba premiado "solo" con un millón de dólares. Entonces, ¿a qué se debe el incremento en la cifra de la recompensa?

¿Qué es una vulnerabilidad 0-day?

Cuando un proveedor de software saca al mercado un nuevo producto con alguna brecha de seguridad de la que no son conscientes ni el proveedor ni la empresa antivirus, se denomina vulnerabilidad de día cero o exploit de día cero.

Día cero hace referencia al tiempo que hace que "los buenos" son conscientes de un problema de seguridad del software. Existen dos tipos de día cero. Una vulnerabilidad de día cero es una brecha en la seguridad del software y puede estar en un navegador o en una aplicación. Por otra parte, un exploit de día cero es un ataque digital que se aprovecha de una vulnerabilidad de día cero para instalar software malicioso en un dispositivo.



Estados Unidos es el mayor comprador de malware del mundo asegura Reuters

ZERODIUM, el fabricante de exploits que compra vulnerabilidades a precio de oro

Los zero-days son un arma

"*Mi trabajo era tener 25 ataques de día-cero en un pendrive USB*", afirmó un ex ejecutivo de una contratista de defensa que compraba vulnerabilidades de hackers independientes para entregárselos al gobierno norteamericano.

Los ataques de día-cero son un tipo de exploit que consiste en utilizar vulnerabilidades que se desconocen tanto públicamente como por parte del fabricante del producto, por lo que es considerado 'uno de los más peligrosos instrumentos de una ciberguerra'.

Exploit (del inglés **exploit**, "explotar" o 'aprovechar') es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

La brecha de Log4j muta a ciberpandemia: millones de ataques por gobiernos y ciberdelincuentes

En solo una semana, una pequeña brecha de seguridad se ha convertido en la mayor amenaza informática de los últimos años, un problema que "permanecerá años con nosotros".

El agujero está en Log4j, un registro de logs que distribuye gratis la Apache Foundation y que está presente en servicios como Twitter, Cloudflare, Amazon, Minecraft...

Así es el fallo de seguridad más grande de la década, que abre la puerta de tu móvil a cualquier ciberdelincuente

La vulnerabilidad ha sido bautizada como Log4jShell y ha recibido el código de vulnerabilidad CVE-2021-44228. Se trata de una vulnerabilidad de día cero, es decir: cuando se ha detectado **no contaba con parches para segurizar el agujero**, con lo que muchos ciberdelincuentes ya la podrían haber empleado.

Además de las pruebas de concepto que han trascendido por parte de los propios expertos de la industria, los ciberdelincuentes habrían llegado a ejecutar códigos de ejecución en remoto contra servidores de Minecraft. Investigadores de Check Point han desvelado hace unas horas que **se han hecho más de 100.000 intentos de aprovechar este agujero.**

Y de esos 100.000, no todos los intentos han sido gestionados por los especialistas en ciberseguridad.

China toma represalias contra Alibaba por descubrir la vulnerabilidad de Log4J... y no compartirla primero con el gobierno

El Ministerio de Industria y Tecnología de la Información de la República Popular China ha anunciado **la suspensión durante medio año de un acuerdo de colaboración público-privada que mantenía con Alibaba Cloud**, la subsidiaria de cloud computing de Alibaba, para trabajar en el campo de la ciberseguridad y el intercambio de información.

El régimen chino quiere dejar claro a sus tecnológicas cuál debe ser su orden de prioridades

...unos meses antes, en su país, el gobierno había aprobado nuevas regulaciones de divulgación de vulnerabilidades que **obligan a los proveedores de software y de telecomunicaciones afectados por vulnerabilidades críticas a revelarlas en primer lugar a las autoridades** gubernamentales.

SI ESTAMOS EN CIBERGUERRA, ¿DÓNDE ESTÁN LAS CIBERARMAS?

CIBERARMAS DE DESTRUCCIÓN MASIVA Y ESPIONAJE: STUXNET, DUQU, FLAME Y GAUSS

El Virus informático **Stuxnet**(mejor dicho un gusano informático o un worm) ataco 5 veces la Central de Enriquecimiento de Uranio en Natanz, Irán, desde Junio de 2009 a Mayo de 2010. Stuxnet ocupo zero-days(o brechas de seguridad que no habían sido detectadas) y 2 Certificados digitales, de la mas prestigiosa y reconocida firma en este ámbito, **VeriSign**.

- 25 de Enero de 2010: Stuxnet obtiene un certificado digital válido, originalmente emitido a Realtec Semiconductor Corps por el proveedor líder de servicios de autentificación, Verisign.
- En Marzo de 2010 Stuxnet se actualiza e incluye el exploit(vulnerabilidad) MS 10-046. El MS 10-046 permitía a Stuxnet ejecutar tarea administrativas en el computador infectado, cuando se desplegaba un especial icono que fuera llamado por aplicación de windows.
- En ese momento el número total de vulnerabilidades en Windows, en los cuales Stuxnet podía usar, incrementaron a 4.
- **Ningún virus de computador o malware antes de Stuxnet había incluso usado más que una vulnerabilidad.** Y esta fue la razón central en porque Stuxnet no pudo ser detectado por sobre 1 año.
- El 17 de Junio de 2010 , la empresa de Anti Virus VirusBlockAda en Belarusia, anunció que habían identificado desconocido worm en un computador de un cliente iraní.
- El Troyano es activado si encuentra el programa **PCS7** (Step 7 Software) de Siemens están instalados. **El Software Step 7 viene pre-instalado en los notebooks industriales de Siemens(Simatic Field PG)**
- Stuxnet fue específicamente diseñado para sabotear dispositivos manufacturados por 2 compañías: Vacon en Finlandia , Fararo Paya en Irán. Estos dispositivos eran usados para controlar los motores de las centrífugas de enriquecimiento de Uranio en Irán.
- Debido a las sanciones impuestas por la ONU , la única forma que tenía Irán de conseguir software y materiales , era a través del mercado negro.
- Octubre de 2011: Duqu colecta datos de Inteligencia desde sistemas de control industrial en orden a preparar a Stuxnet para un exitoso ataque a las centrífugas de Uranio de Irán.

SI ESTAMOS EN CIBERGUERRA, ¿DÓNDE ESTÁN LAS CIBERARMAS?

CIBERARMAS DE DESTRUCCIÓN MASIVA Y ESPIONAJE: STUXNET, DUQU, FLAME Y GAUSS

¿Como Stuxnet pudo estropear las centrífugas de enriquecimiento de Uranio en Irán?

Primero que todo, el Virus tenía que conseguir llegar a un notebook específico(**Simatic Field PG**, notebook industrial de Siemens) de un técnico que entrara a la central de Natanz, por eso, el medio de diseminación fue principalmente a través de un Pendrive USB, la gracia es que **Stuxnet** fue programado inteligentemente, pues a la tercera copia desde el USB, el Stuxnet en el USB cometía un Harakiri, o sea, se suicidaba en el USB y no dejaba rastros de él, pero si quedaba en el último computador.

Cuando Stuxnet encontraba el programa PCS7(Step 7 Software) que viene pre-instalado en los notebooks industriales de Siemens(Simatic Field PG) y estableciera conexión, Stuxnet penetra dentro del controlador(PLC/Programmable logic controller) y modifica el código de programación del controlador y oculta los cambios. Así Stuxnet tiene el control sobre 186 frecuencia de drivers de convertidor, operando a alta velocidad.

Sobre un periodo de meses Stuxnet cambia las **frecuencia de salida**, lo cual cambia la rapidez de un rotor centrífugo,. Las frecuencias de operación normales son entre **807 Hz y 1210 Hz**, con una *frecuencia estándar* de **1064 Hz**. Por cortos periodos de tiempo, no mas de **15 minutos**, Stuxnet *sube la frecuencia* a **1410 Hz**, lo cual esta sobre el limite de *1210 Hz* y entonces cambia de vuelta a 1064 Hz. Después de 27 días Stuxnet hace caer la frecuencia de salida a**2Hz** por *5 minutos*. Cada 27 días repite la misma rutina , de acelerar y desacelerar la centrifuga. Esto ocurrió desde el 2009 hasta el 2010, lo que llevó a que más de 1000 centrifugas se estropearan, y los operadores de estas no sabían por que, pues en la pantalla les aparecían siempre valores normales.

CIBERSEGURIDAD
LA PRÓXIMA PANDEMIA

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

SI ESTAMOS EN CIBERGUERRA, ¿DÓNDE ESTÁN LAS CIBERARMAS?

CIBERARMAS DE DESTRUCCIÓN MASIVA Y ESPIONAJE: STUXNET, DUQU, FLAME Y GAUSS

¿Por que Irán?

Por su programa de enriquecimiento de Uranio, si bien las centrífugas principalmente (A) que hacen es enriquecer uranio en una bajo nivel(**LUE**), hay otras centrífugas que podrían eventualmente enriquecer el uranio en un alto nivel(**HUE**), para que se pueda hacer una bomba nuclear de este, se necesita alto enriquecimiento, 85%. Se estima que la planta donde está esas centrifugas es chica, bien podría hacer 1 bomba nuclear por año. El proceso es que el **uranio–238** pasa a la centrifugadora y al girar el **uranio–235** se queda en el centro y el 238 se va a los bordes, el uranio 235 en el centro es pasado en cascada hacia la próxima centrifugadora para que siga el proceso. La casaca puede enriquecer el uranio en 5%.

¿Como un empresa en Bielorrusia más bien pequeña pudo encontrar el Stuxnet y las otras empresas más grandes no?

Tal vez la explicación más lógica viene de los mismos de**VirusBlockAda**, ellos dijeron que encontraron el virus en un computador de un cliente iraní, el hint fue que el equipo se reiniciaba constantemente. Entonces cae la duda plausible, que no descubrieron Stuxnet, Stuxnet se mostró a público, ¿Y con qué fin? , para esa fecha ya había completado sus mayores funciones, así que ahora tenía que pasar de ser un ciber arma de destrucción masiva, a un arma de propaganda, lo cual dejaría a los de Irán confundidos y temerosos por las nuevas capacidades del virus, cuál sería su próxima variación?, hacer explotar la planta?, que mas?....La ciber arma había cumplido su función ahora se necesitaba hacerla pública y sembrar el miedo, con la propaganda adecuada.

¿Quién estuvo detrás de la creación de la denominada Familia Stuxnet?

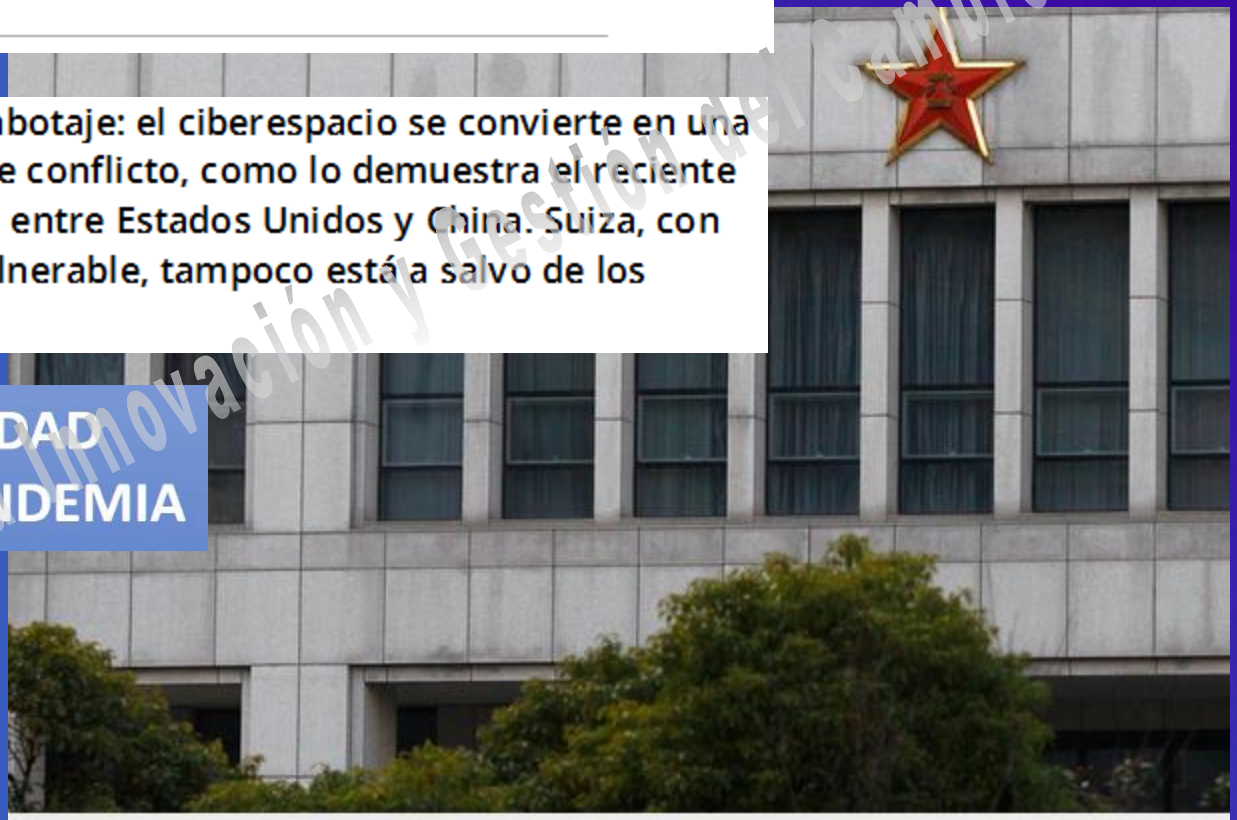
Se sospecha de Estados Unidos e Israel, Israel fue fácil, pues en el propio código salían palabras que referenciaban reinas y acontecimientos que pasaron(Refinar esta parte)

CIBERGUERRA

Virus informáticos, más peligrosos que la bomba

Espionaje, robo de datos, sabotaje: el ciberespacio se convierte en una nueva zona de amenaza y de conflicto, como lo demuestra el reciente intercambio de acusaciones entre Estados Unidos y China. Suiza, con una infraestructura muy vulnerable, tampoco está a salvo de los ataques cibernéticos.

CIBERSEGURIDAD
LA PRÓXIMA PANDEMIA



Según fuentes estadounideses, los ataques contra la administración y empresas estadounidenses han salido de este edificio de Shanghai, sede de la Unidad 61398 de piratería del ejército chino.

¿Le preocupa un ciber apocalipsis? AIG puede venderle un seguro

¿Puede un solo ataque derrumbar toda la Internet?

El escenario apocalíptico de la aseguradora se asemeja a la escena vivida en la Bolsa de Nueva York el pasado 8 de julio.

La suspensión por tres horas de la bolsa de Nueva York el mismo día en que una falla de redes obligó a mantener en tierra a todos los vuelos de United Airlines en Estados Unidos hizo que las personas de todo el país pensaran en una sola cosa: un ciberataque.

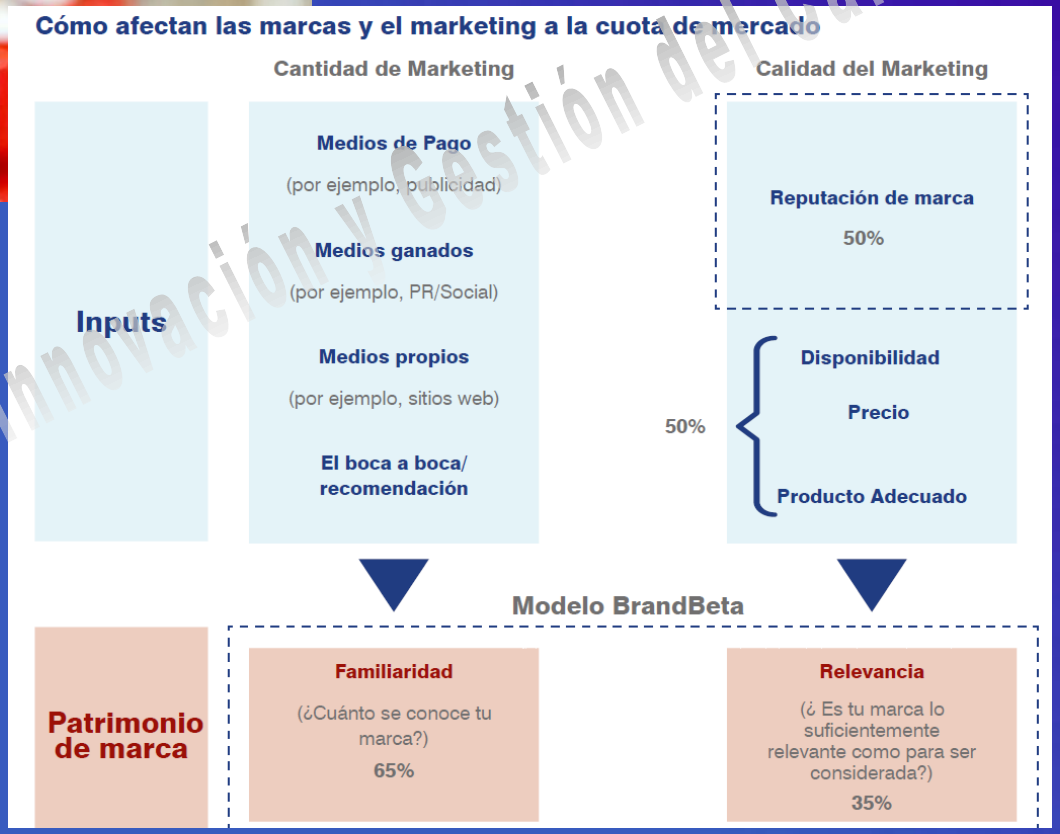
No lo fue, pero los incidentes del 8 de julio se acercaron al escenario de Armagedon que Austin Berglas, un ex agente del FBI, describió en una entrevista unas semanas antes, en el cual el Nasdaq, el sistema de metro de Nueva York y el proveedor de energía Con Edison se caen al mismo tiempo.

Berglas, quien estableció la unidad de cibercrimen del FBI en Nueva York en 2009, se unió a la empresa de investigaciones corporativas K2 Intelligence en abril. Uno de los propietarios de la firma es American International Group (AIG), que está buscando vender pólizas de seguro para el daño a la propiedad y la infraestructura causado por hackers y ciberterroristas.

LA ERA DE LA DESINFORMACIÓN

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

LA ERA DE LA DESINFORMACIÓN



Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

LA ERA DE LA DESINFORMACIÓN

Fake News: un arma de destrucción masiva que amenaza nuestra democracia

"Estamos en una nueva Guerra Fría"

¿Estamos viviendo una guerra mundial encubierta en Internet? No lo cree **David Alandete**, pese a que ha escrito un libro de plena actualidad: '**Fake News, la nueva arma de destrucción masiva', editorial Deusto** (de la que tomamos el título para este artículo, porque es certero), que podría indicar lo contrario. En él se habla de la **guerra híbrida librada en Ucrania**, con soldados que no estaban vestidos de soldados ni llevaban bandera, del **Brexit**, **del auge de los populismos, del triunfo de Trump**...

> “El bulo se ha convertido en un arma destructiva sin precedentes al alcance de grandes empresas, gobiernos e incluso ciudadanos

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

LA ERA DE LA DESINFORMACIÓN

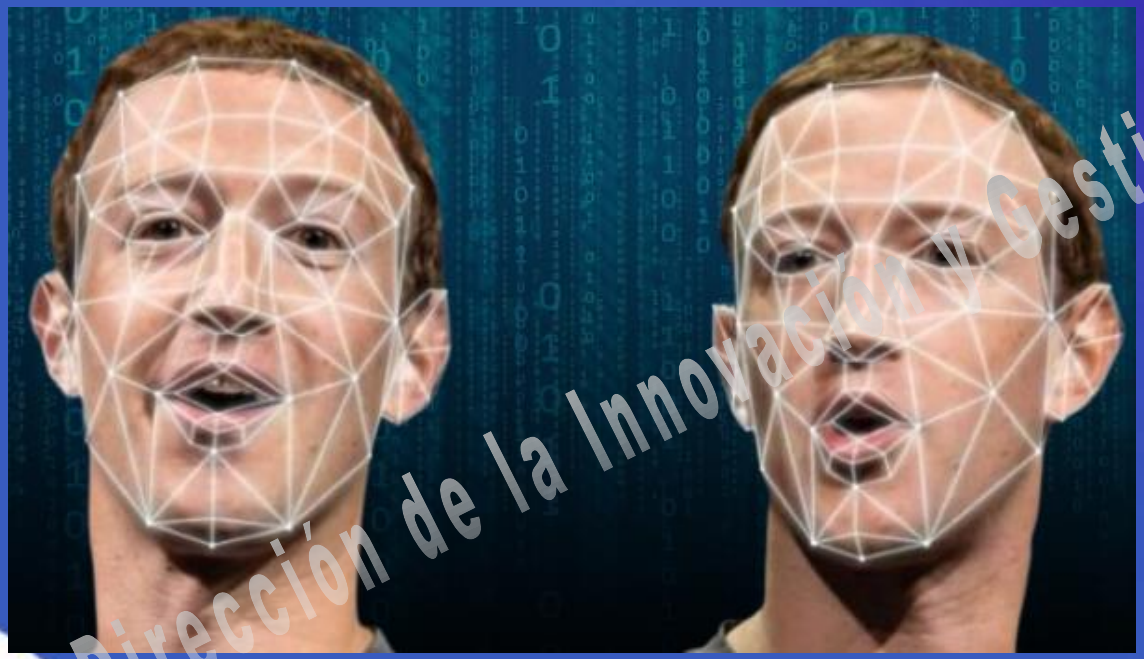
"El meme quizá es la estrategia más peligrosa", dijo Duke. "Con siete o 20 palabras, alguien puede decir algo que no es cierto y la gente lo creerá y lo compartirá. Toma dos minutos crearlo".

La línea divisoria entre propaganda e información es cada vez más borrosa, también en las democracias occidentales

"Una mentira puede viajar por medio mundo mientras la verdad está poniéndose los zapatos."

LA ERA DE LA DESINFORMACIÓN

Deepfakes: la realidad hackeada



La Inteligencia Artificial también está al servicio de la desinformación. Es el *deepfake*: algoritmos al servicio de la creación de audios y vídeos falsos, desvirtuando todavía más la ya diluida frontera entre realidad y ficción.

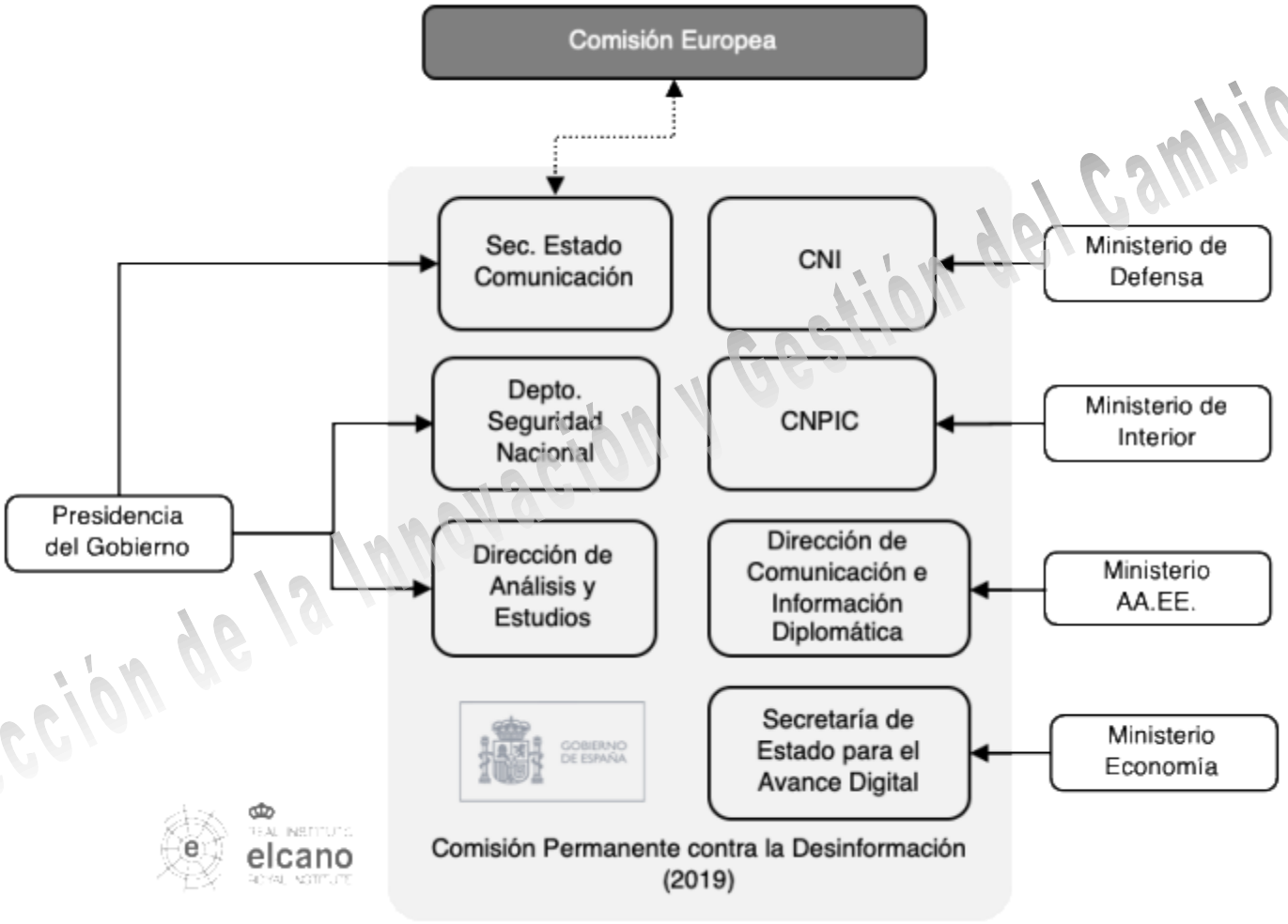
Hace dos años, la Universidad de Washington presentó un proyecto piloto conocido como *Synthesizing Obama*, un algoritmo capaz de manipular vídeos sincronizados con movimientos faciales que usaba la imagen del expresidente de Estados Unidos, Barack Obama, para reproducirla en contextos distintos repitiendo la misma declaración. ¿Cuál de ellas era la auténtica?

En octubre, Facebook creó un fondo de 10 millones de dólares para desarrollar herramientas que detecten rápidamente las imágenes falsas.

Prof. Dr. Manu Martínez López - Dpto. Dirección de Empresas y Mk - Universidad de Huelva

LA ERA DE LA DESINFORMACIÓN

Ilustración 9. Estructura de la Comisión Permanente contra la Desinformación (2019)



Elaboración propia sobre datos del Gobierno de España (2019).

Transformación Digital y Ciberseguridad

Dirección de la Innovación y Gestión del Cambio. UHU

CIBERSEGURIDAD
LA PRÓXIMA PANDEMIA

GUERRAS EN LA SOCIEDAD MUNDIAL INFORMACIONAL

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Prof. Dr. Manu Martínez López - Dpto. Dirección de
va