

# Ciberseguridad, un desafío mundial



• Las infraestructuras críticas de países que no estén preparadas para defenderse de ciberataques no deberían conectar sus infraestructuras a la red.

**P. 26**

• Como la electricidad, que es un servicio básico, el Gobierno debería garantizar un internet seguro al ciudadano.

**P. 33**

• Las técnicas de autenticación tienen que garantizar la protección de los datos, es decir, la privacidad del usuario mediante sistemas de cifrado fuerte.

**P. 38**

• Se insta a que los datos puedan ser monitorizados por el país que los posee o sus empresas más allá de los límites territoriales nacionales.

**P. 65**



Nuevas capacidades informáticas y una "inteligencia artificial" cada día más poderosa están permitiendo automatizar los ataques y dotarlos de dimensiones masivas.

# Agradecimientos

---

Nuestro agradecimiento a **D<sup>a</sup>. Amaya Quincoces**, periodista y autora de este informe. Su trabajo ha sido decisivo para poder plasmar las conclusiones de la esta tendencia del Future Trends Forum.

Nuestro agradecimiento a todos los miembros del Future Trends Forum (FTF) que han hecho posible el éxito de nuestra última reunión, especialmente a aquellos que han participado activamente en la realización de esta producción:

Por su inestimable colaboración en la elaboración de esta publicación:

**Eden Shochat**  
**Fabio Assolini**  
**John Lyons**  
**Caroline Baylon**  
**Inbar Raz**  
**Steve Wilson**  
**Evan Wolff**  
**Kevin Sale**  
**Richard Parry**

En la organización y metodología de la reunión del Future Trends Forum:

**Chris Meyer**



**Garrick Jones**  
**Clemens Hackl**  
**Jake Holmes**



**Fernando de Pablo**

Y por último, agradecer a las personas del equipo, por su compromiso y buen hacer en el desarrollo del contenido de esta publicación:

**Fundación Innovación Bankinter**  
**Sergio Martínez-Cava**  
**Marce Cancho**  
**María Teresa Jiménez**  
**Lara García de Vinuesa**  
**Pablo Lancry**

Las opiniones expresadas en este informe son del autor y no reflejan la opinión de los expertos que participaron en la reunión del Future Trends Forum.



# Ponentes y asistentes

**Abdou Naby Diaw**

Jefe de Oficina de Seguridad (CSO) Vodafone.

**Carlos Jiménez**

Presidente y fundador de Secuware.

**Caroline Baylon**

Directora, Programa de Investigación sobre Seguridad Cibernética, Centro de Investigación de Decisiones Estratégicas.

**Drew Dean**

Director de Programas en SRI International.

**Eden Shochat**

Fundador de Aleph y Patrono de Fundación Innovación Bankinter.

**Emilio Méndez**

Director del Centro de Nanomateriales Funcionales del Departamento de Energía del Laboratorio Nacional de Brookhaven y patrono de Fundación Innovación Bankinter.

**Evan Wolff**

Socio en Crowell & Moring.

**Fabio Assolini**

Analista de la empresa Kaspersky.

**Fernando Vega**

Director de Seguridad de la Información en el grupo Bankinter.

**Ilya Ponomarev**

Miembro del Parlamento Ruso, presidente del Subcomité de Innovación y Capital de Riesgo de la Duma.

**Inbar Raz**

Vicepresidente de Investigación del Perimeter X.

**Isaac Gutiérrez**

Jefe Internacional de Ciberseguridad en Prosegur.

**Jens Schulte - Bockum**

Ex CEO de Vodafone Alemania y patrono de la Fundación Innovación Bankinter.

**John Lyons**

Presidente ejecutivo y fundador de Alianza Internacional de Protección de Seguridad Cibernética (ICSPA).

**Julia Li**

Presidenta y fundadora de Global HCD.

**Kevin Sale**

Especialista en Seguridad IT en la Universidad Abdullah de Ciencia y Tecnología.

**Khoo Boon Hui**

Ex presidente de INTERPOL.

**Michael Osborne**

Manager de Privacidad y Seguridad de Informática Cognitiva y Departamento de Soluciones Industriales del IBM Research Division.

**Michael Schrage**

Investigador del MIT Digital Lab.

**Miguel Rego**

Director general del Instituto Nacional de Seguridad de España (Incibe).

**Philip Lader**

Ex presidente no-ejecutivo de WPP y patrono de Fundación Innovación Bankinter.

**Ram Levi**

Experto de Seguridad Cibernética, CEO de Konfidias, co-fundador de Seguridad Cibernética de Londres (LCS).

**Richard Kivel**

Senior manager en Bridgewater y presidente de Rhapsody Biológicos. Patrono de Fundación Innovación Bankinter.

**Richard Parry**

Fundador en Parry Advisory.

**Rolf Reinema**

Director de Tecnología en Siemens.

**Steve Wilson**

Vicepresidente de Constellation Research.

**Tan Chin Nam**

Asesor corporativo y ex secretario permanente de MAD y patrono de Fundación Innovación Bankinter.

**Wilfred Vanhonacker**

Profesor de Marketing en Coca-Cola, Escuela de Negocios Olayan AUB y patrono de Fundación Innovación Bankinter.

Muchas gracias,

**Fundación Innovación Bankinter**

# Índice

## 08

**Prólogo**

Eden Shochat

8/9

## 10

**Cap. 1 Amenazas de la ciberseguridad**

10/27

**Introducción**

12

**1.1** Los cibercriminales se lucran en internet

13/15

**1.2** El *software* se come el mundo

16/19

Prólogo de **Fabio Assolini****1.3** Ciberguerra, ciberespionaje y ciberterrorismo

20/23

Prólogo de **John Lyons****1.4** Los riesgos de conectar las infraestructuras críticas a internet

24/26

Prólogo de **Caroline Baylon****Conclusiones**

27

## 28

**Cap. 2 La seguridad del internauta**

28/49

**Introducción**

30

**2.1** El "Internet de las Cosas", un paraíso para el cibercriminador

31/35

Prólogo de **Inbar Raz****2.2** Las debilidades de la identidad digital

36/39

Prólogo de **Steve Wilson****2.3** Intimidad y privacidad versus seguridad

40/45

Prólogo de **Evan Wolff****2.4** Cómo mejorar la ciberseguridad

46/48

Prólogo de **Kevin Sale****Conclusiones**

49

## 50

**Cap. 3 La ciberseguridad del futuro**

50/69

**Introducción**

52/53

**3.1** Una "hoja de ruta con diez propuestas"

55/68

Prólogo de **Richard Parry****Conclusiones**

69

## 70

**Predicciones de los expertos**

70



## Prólogo de **Eden Shochat**

Fundador de Aleph y Patrono de Fundación Innovación Bankinter.

---

- El ciberataque sufrido por JPMorgan Chase en 2014 puso en peligro 83 millones de cuentas de particulares y pequeñas empresas.

Los investigadores descubrieron un rastro de 75 empresas ficticias creadas por los cuatro sospechosos, cuya actividad se remontaba a 2007, y que habían cosechado "cientos de millones de dólares en ganancias ilícitas". En otro incidente,

un grupo asociado con el Ejército Popular de Liberación llevó a cabo la "Operación Aurora", una serie de ataques cibernéticos dirigidos a docenas de empresas, entre ellas Google, Adobe y Northrop Grumman (uno de los fabricantes del caza furtivo

F-35). Según McAfee, el principal objetivo de estos ataques era acceder a, y posiblemente modificar, repositorios de código fuente pertenecientes a estas empresas de alta tecnología y seguridad y a la empresa contratista de defensa.

Es de vital importancia entender que la guerra cibernética también puede utilizarse como arma militar. En Ucrania, más de 80.000 ciudadanos sufrieron un apagón causado por un (no confirmado) programa malicioso ruso que afectó a los centros de control de múltiples plantas de energía. El Departamento de Seguridad Nacional de Estados Unidos demostró, ya en 2007, cómo 21 líneas de código podían destruir un generador de energía. El ataque de Stuxnet (un gusano informático dañino) en las instalaciones nucleares iraníes supuso la demostración de un ataque real contra la vida en estado puro. Esto provocó que EE.UU. y muchos otros países crearan "cibercomandos", tanto para fines defensivos como ofensivos.

Ya pagamos por fraude en las tasas que se aplican por cada transacción que realizamos con nuestra tarjeta de crédito. El impacto de estos riesgos y amenazas es extremadamente amplio. Los particulares temen una posible suplantación de identidad y el generalizado "chantaje mediante datos bloqueados", los gobiernos intentan protegerse contra el espionaje cibernético y contra posibles ataques a los activos críticos de su infraestructura por parte de otros estados o naciones, y las empresas deben hacer frente a ataques cibernéticos que conllevan una pérdida financiera y la destrucción de su imagen de marca, como el que sufrió Sony en 2015. Uno de los mayores desafíos a los que se enfrentan los organismos de defensa es que los ataques raramente se cometen en el marco de una única frontera nacional. Los atacantes de JPMorgan estaban ubicados en Israel, Rusia y posiblemente en más países. Estas cuestiones transfronterizas hacen que la reducción y el castigo de estos delitos cibernéticos resulte compleja (entre los estados occidentales) e incluso imposible (si el ataque se realiza desde otros países o bien desde uno con menos tratados de extradición, como China).

## Esta es nuestra realidad hoy en día

El mañana es mucho más preocupante. Hemos podido beneficiarnos de sistemas de reconocimiento de voz y de reconocimiento facial, de vehículos autónomos y de oponentes de juego superinteligentes mediante profundos avances en el aprendizaje. Estos mismos avances en inteligencia artificial (IA) pueden permitir a los atacantes cibernéticos dirigir un ataque a un número significativo de objetivos de gran valor, creando así una nueva forma de amenaza persistente avanzada. Básicamente, ya no tendrán que elegir entre los ataques puntuales contra objetivos muy específicos de gran valor y ataques a gran escala contra un número indefinido de objetivos vulnerables. Esta nueva generación de malware basado en IA podría ser capaz de evolucionar continuamente mediante nuevos métodos de ataque y de buscar incansablemente nuevos vectores para obtener un beneficio económico, militar o de otro tipo establecido por su operador.

Estos escenarios presentes y futuros ponen de manifiesto la importancia de estar preparados. Sin duda, la ciberdefensa resulta sumamente difícil ya que, mientras que los defensores necesitan tener éxito el 100% de las veces y cubrir la totalidad del terreno de juego, el atacante solo necesita tener éxito una vez, por lo general, en el punto de menor resistencia. Este informe del Future Trends Forum incluye recomendaciones sobre educación, el establecimiento de regulaciones (tratando de minimizar, al mismo tiempo, el riesgo de un exceso regulatorio) y la gestión de los retos por parte de las fuerzas del orden mediante la colaboración transfronteriza.

Compartimos este informe como uno de los muchos pasos necesarios para la educación y como instigador para un debate más amplio. Espero que la información presentada sea beneficiosa, incluso si en ocasiones resulta desalentadora.





# Amenazas de la ciberseguridad

---

1

---

## Fabio Assolini

Analista de la empresa Kaspersky.

## John Lyons

Presidente ejecutivo y fundador de Alianza Internacional de Protección de Seguridad Cibernética (ICSPA).

## Caroline Baylon

Directora, Programa de Investigación sobre Seguridad Cibernética, Centro de Investigación de Decisiones Estratégicas.

Una nueva era digital se abre camino con amenazas crecientes para la seguridad mundial. Los cibercriminales se han vuelto mucho más sofisticados, organizados y peligrosos en sus ataques con los que obtienen enormes beneficios económicos.

**E**l fenómeno de conexión de todo a internet o "Internet de las Cosas" (IoT, por sus siglas en inglés) es imparable con sensores cada vez más abundantes y baratos que hacen más accesibles los objetivos a los cibercriminales, amparados en sus tropelías, en ocasiones, por sus propios gobiernos que no los castigan ni persiguen. A todo esto se añaden nuevas capacidades informáticas y una "inteligencia artificial" cada día más poderosa, que están permitiendo automatizar los ataques y dotarlos de dimensiones masivas mediante redes de ordenadores autocontrolables

y capaces de tomar decisiones propias. Ciberguerra, ciberespionaje y vigilancia masiva son amenazas ya actuales a las que se sumarán otras muchas en camino. Más allá del infinito mundo de ventajas económicas y sociales vinculadas a la revolución que ha supuesto internet, nuevos peligros acechan en el ciberespacio: posibles guerras lidiadas por armas autónomas o entre máquinas y hombres, asesinatos que podrían ser perpetrados desde el mismo internet, grandes sabotajes contra infraestructuras críticas de los países. Al parecer, sólo será cuestión de tiempo.



# Los cibercriminales se lucran en internet

## 1.1

► **La industria de la ciberseguridad mueve** presupuestos millonarios que crecen progresivamente. Anualmente este área moviliza entre 70.000 y 80.000 millones de dólares al año. Para el horizonte de 2020 las previsiones apuntan a que la cifra podría ser 2,5 veces mayor, según **Khoo Boon Hui**, ex presidente de INTERPOL ([ver vídeo](#)).

En paralelo prospera otro mundo muy peligroso, el del cibercrimen, responsable de ataques contra empresas y gobiernos cada vez mayores, más sofisticados y organizados, con beneficios millonarios para sus autores. Son enormes las pérdidas que causa a las economías. Sólo el año pasado, la cifra fue de entorno a 400.000 millones de dólares estadounidenses, según estimaciones de los expertos, aunque podría ser mucho mayor, dado que las víctimas no suelen revelar datos.

El auge de teléfonos móviles, tabletas y todo tipo de sensores conectados a internet, junto con la expansión de robots y sistemas de inteligencia artificial cada vez más potentes y máquinas de aprendizaje automático más y más sofisticadas con conexión a la red "complican las cosas". El ciberespacio está bajo la lupa mundial ante un previsible despunte del cibercrimen global, mucho más agresivo y lucrativo aún para los atacantes.

## Nadie está libre de peligros en el ciberespacio

Cualquiera puede convertirse en objetivo de los cibercriminales. Al pagar con una tarjeta de crédito, al conectarse a la *wifi* de un hotel, etc. Los cibercriminales están siempre

al acecho y se aprovechan de cualquier vulnerabilidad de los sistemas para acceder a datos privados de las personas dispersos en cantidades ingentes en internet y mejorar así la planificación de sus fechorías.

El uso inapropiado del "Internet de las Cosas" dispara las amenazas no sólo contra el mundo digital sino también el físico. Terroristas y ciberatacantes pueden manipular los sistemas informáticos de las infraestructuras nacionales que ofrecen servicios básicos a los países: redes eléctricas, telecomunicaciones, banca, agua, etc.

**Khoo Boon Hui** ▼  
Ex presidente de INTERPOL.

[ver vídeo](#) 



Varias personas han muerto ya como consecuencia del cibercrimen. Algunas se han suicidado al ver desvelados en internet datos que han puesto en entredicho su reputación. Otras a causa de ciberextorsión bajo la amenaza de los criminales de desvelar imágenes comprometidas de las víctimas en internet, como detalles sexuales íntimos.

Por otra parte, los cibercriminales parecen tener barra libre para traficar sin apenas dejar rastro (armas, drogas, niños) actuando desde entornos tan "oscuros" como la llamada "Deep Web", ese enorme espacio virtual supuestamente inescrutable, conocido como internet profundo, que escapa al control de los motores de búsqueda tradicionales, tipo Google.

En internet, "estamos consumidos por el terrorismo", según el ex presidente de INTERPOL. Se está incrementando la actividad de los ciberdelincuentes convencionales y también la de los cibercriminales profesionales. Sus acciones son más fácilmente enmascarables en internet que en el mundo real por la ausencia de fronteras físicas y porque no existe jurisprudencia internacional para penalizar a los ciberculpables.

Muchos estados carecen de leyes para castigar estas conductas y los criminales, desde sus casas con un simple ordenador, pueden atacar objetivos en cualquier parte del mundo. Se necesita cooperación internacional contra el cibercrimen más allá de la labor que realizan entidades como INTERPOL Global Complex for Innovation (IGCI) <http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation> y Europol <https://www.europol.europa.eu/>, e iniciativas como el Convenio sobre ciberdelincuencia, también conocido como Convenio de Budapest, que incluye actualmente a unos cuarenta países.

Se requiere que las empresas y los gobiernos que luchan contra el cibercrimen compartan información para adelantarse a las amenazas o luchar contra ellas de forma más eficaz cuando se producen. "Cada crimen internacional es un crimen local en algún lugar", asegura el ex presidente de INTERPOL **Khoo Boon Hui**. Cada país debería aplicar legislación

contra los cibercriminales en sus fronteras y cooperar a nivel internacional cuando los delitos vayan más allá. La colaboración entre gobiernos y empresas es fundamental y se necesitan asimismo alianzas público-privadas para compartir conocimiento y experiencia en temas de ciberseguridad.

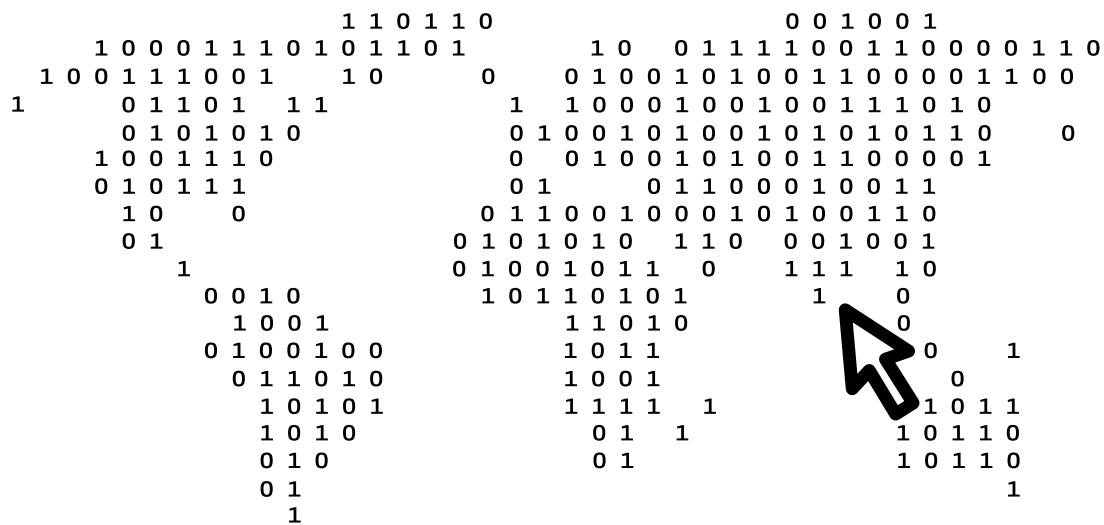
## Un foro de expertos mundiales en ciberseguridad

El ex presidente de INTERPOL forma parte de la treintena de expertos internacionales que han debatido conjuntamente sobre los desafíos de la ciberseguridad mundial en el marco del foro sobre tendencias futuras (*Future Trends Forum - FTF*) de Fundación Innovación Bankinter <https://www.fundacionbankinter.org/es>, durante su vigesimoquinta edición, celebrada en diciembre de 2015 en Madrid.

Coordinados por **Chris Meyer**, consejero delegado de Nerve LLC, los participantes han dialogado durante dos días a puerta cerrada sobre cómo avanzar hacia un mundo más seguro, y han logrado pergeñar un ambicioso y detallado decálogo de propuestas a modo de "hoja de ruta", dirigida a los distintos agentes en el mundo vinculados con temas de ciberseguridad para su posible implementación.

Durante la reunión del Future Trends Forum, los expertos han planteado distintas hipótesis de cómo sería la vida en diferentes modelos de sociedad en función del peso de unos factores o otros:

- En uno de esos mundos la privacidad estaría por encima de todo.
- El segundo sería anárquico o libertario en cuanto a leyes.
- En el tercero se antepondría el comercio a todo lo demás.
- El cuarto sería un sistema cerrado con vigilancia absoluta.



- En el último lo que se plantea es una parábola sobre la ciberseguridad que plantea cuáles serían las consecuencias de un posible sistema económico y social controlado en el futuro por cinco grandes tecnológicas: Microsoft, Apple, Google, Facebook y Alibaba, y al que se bautiza con el nombre de *Magfa*, por las letras iniciales de los nombres de esas empresas.

Los debates han contribuido a perfilar una imagen del panorama actual de la seguridad en internet, identificar debilidades y amenazas así como las fortalezas de los países para hacerles frente, con el objetivo de plantear posibles soluciones para mejorar la ciberseguridad, y que irían dirigidas a todos los estamentos sociales: gobiernos, legisladores, consumidores, empresas, industria, educadores, etc.

## Cómo avanzar hacia un mundo más seguro

Los expertos confían en que las medidas que se pudieran adoptar a partir de ahora contribuirían a mejorar la seguridad del mundo en el futuro. Para 2020, esperan que se hayan logrado ciertos hitos: estándares de calidad que garanticen la generalización de *software* seguro en la industria;

mejores estrategias de seguridad en el trabajo; un mundo interconectado con mayor protección para el consumidor; mayor concienciación sobre ciberseguridad. Asimismo, un comercio digital seguro en todo tipo de transacciones; mejores técnicas de autenticación digital para garantizar la privacidad, por ejemplo, de los registros médicos, que será un ámbito clave; mayor cooperación global y leyes internacionales que garanticen el cumplimiento de penas por parte de los ciberdelincuentes.

Mirando más allá, hasta 2025, los ponentes confían en que las empresas se responsabilizarán más en temas de seguridad, se apoyará más a los consumidores en temas de seguridad *online* y asimismo dispondrán de información suficiente y de calidad a su alcance sobre cómo realizar transacciones virtuales de forma segura. Se espera además que los gobiernos interactuarán virtualmente con el ciudadano con mayor normalidad, y ciertos grupos que para entonces podrían estar ya digitalizados, como refugiados o monjes ahora aislados, también tendrán acceso a campañas educativas para manejarse con seguridad en internet. Para 2030, uno de los objetivos claves sería garantizar un consumo financiero seguro en la red, con ciudadanos menos vulnerables a posibles sabotajes para realizar tranquilamente transacciones en internet.



## Prólogo de **Fabio Assolini**

Analista de la empresa Kaspersky.

[ver video](#)

# ● El software se está comiendo el mundo.

**E**l título corresponde a una cita de Marc Andreessen de hace cinco años. Andreessen describió cómo las tecnologías disruptivas podrían cambiar nuestra economía y nuestra forma de hacer negocios. En la actualidad, la predicción de Marc ha resultado ser muy real.

Cada vez son más y de mayor relevancia las empresas basadas en software y que se comercializan como servicios online. Las tecnologías disruptivas están modificando nuestro modo de vida. ¿Habría imaginado alguna vez que el mayor distribuidor de películas del mundo no sería propietario de ningún cine? Netflix está revolucionando la forma de ver películas y series. ¿Y el hecho de que la compañía de taxis más grande del mundo no posea ningún taxi? La llegada de Uber ha sido mal acogida en muchos países. También se da el caso de que el mayor proveedor de alojamiento no posee propiedades inmobiliarias. Airbnb permite a cualquier persona alquilar una habitación. No hay duda acerca de la importancia económica del software. Sabemos que las empresas modernas se basan, cada vez más, en software. Sin embargo, a pesar de esta importancia, el software tiene un problema universal: **fallos y vulnerabilidades**.

Los encargados de desarrollar el software son seres humanos, por lo que es natural que surjan errores y fallos. El impacto de un fallo depende de la rapidez con la que una empresa reaccione al tener conocimiento de él. Todavía encontramos grandes empresas de software que no están preparadas para

responder rápidamente ante un informe de error. Pocas empresas han adoptado estándares como el ciclo de vida de desarrollo de seguridad (Security Development Lifecycle o SDL). En cualquier caso, no importa qué metodología de desarrollo de software se adopte, **siempre existirán errores en el software**.

Los cibercriminales lo saben y lo utilizan para su beneficio: sería posible infectar millones de ordenadores explotando una sola vulnerabilidad en un programa como Flash Player. Sin embargo, los delincuentes cibernéticos no son los únicos; los gobiernos tienen un gran interés en aquellos fallos de software (los llamados ataques de día cero) que han permitido digitalizar el espionaje gubernamental y corporativo en todo el mundo. Este interés se ha traducido en la creación de un mercado lucrativo (los gobiernos son compradores voraces de fallos de día cero e influyen en la adopción de una criptografía y de una estructura y estándares de software débiles) **en detrimento de la seguridad en todo el mundo**.

En conclusión, y con vistas a 2020, creo que, en un futuro próximo, nos enfrentaremos a estrictas regulaciones de la investigación de la seguridad, a mercados de fallos de día cero y a la divulgación de vulnerabilidades de software. También creo en una **gran fragmentación de los sistemas operativos** debido a la adopción generalizada de dispositivos móviles. Windows ya no será el líder. Los cibercriminales tendrán que adaptar sus ataques a estas nuevas plataformas.

# El *software* se come el mundo

1.2

► **Hace unos pocos años** el emprendedor estadounidense **Marc Andreessen**, cofundador de la empresa Netscape Communications Corporation y cocreador de Mosaic, uno de los primeros navegadores web con interfaz gráfica, aseguró: "El *software* se está comiendo el mundo". De hecho, actualmente la mayor empresa cinematográfica, Netflix, no tiene ningún cine, sino *software*; la compañía líder mundial de taxis, Uber, no posee vehículos, y el mayor proveedor de alojamiento, Airbnb, carece de inmuebles físicos. Y no sólo se come el mundo el *software*, que está transformando la economía y la forma en que se hacen negocios, sino que cada vez es más "inteligente", acompañado de ordenadores capaces de aprender por sí mismos, de sus propias experiencias, y tomar decisiones mediante el llamado "aprendizaje profundo", con "inteligencia artificial".

"El *software* está creando toda una nueva revolución en nuestro mundo", asegura **Fabio Assolini**, analista de la empresa Kaspersky. "Estamos viviendo momentos muy interesantes con tecnologías innovadoras que ganan mucha popularidad y están cambiando nuestra forma de vivir", añade. [\(ver vídeo\)](#).

"El problema es que el *software* siempre tendrá vulnerabilidades. Así será no importa la metodología de desarrollo que se adopte", lo cual, por otra parte es comprensible, teniendo en cuenta que lo realiza el ser humano. Y el peligro es que los cibercriminales saben que el *software* siempre tendrá fallos y se aprovechan de eso. Frente a ello, lo recomendable es que las empresas garanticen la seguridad durante todo el proceso de desarrollo del producto, desde sus orígenes, con lo que se denomina *Security Development Lifecycle (SDL)*.

## Los países, también a la caza de vulnerabilidades

El interés por estos fallos del *software* no es sólo de los cibercriminales. Algunos gobiernos se están sumando a este "juego" de explotar vulnerabilidades. En concreto a ciertos países les interesan mucho las vulnerabilidades *0-day* (Día Cero), un tipo de fallos que ni el fabricante ni el desarrollador del producto saben que existen y que son muy cotizados porque dan acceso al *software* y pueden ser aprovechados para infectar sistemas o para campañas de espionaje de ordenadores en todo el mundo.





Estas vulnerabilidades "Día Cero" están alimentando un enorme "mercado clandestino" en internet. "Algunos gobiernos pagan mucho dinero por una sola de ellas, por ejemplo, de un iPhone. Les permite hacer ciberespionaje o comprometer compañías infectando sus ordenadores", según Assolini.

Una de sus predicciones para 2020 es que los gobiernos regularán con determinación la investigación para la seguridad en estos mercados de vulnerabilidades "Día Cero". Buscarán su control absoluto para su propio beneficio.

## Existe un enorme potencial del *software* gracias al auge de "la inteligencia artificial".

**Eden Shochat** ▼

Fundador de Aleph y Patrono de Fundación Innovación Bankinter.



Además las autoridades de los países intentarán regular a las compañías que venden esas vulnerabilidades y para esa fecha además muchas naciones aplicarán regulaciones severas a las empresas de *software* y también a las compañías que operan y venden esas vulnerabilidades y las exportan a otros países.

## Sistemas informáticos cada vez más "inteligentes"

Por su parte, **Eden Shochat**, fundador del Fondo de Capital Riesgo Aleph, advierte del enorme potencial del *software* gracias al auge de "la inteligencia artificial", y que más allá de sus incuestionables aportaciones a la sociedad, desata nuevos peligros en temas de ciberseguridad. En una próxima fase de evolución, los ordenadores podrían ser capaces de mejorar la planificación de los ataques a partir del uso de datos personales a los que tienen muy fácil acceso en internet, como la denominada Información Personal Identificable de los Internautas (PII). Esa capacidad de la que se están dotando los ordenadores para rastrear contenidos y analizar de forma "inteligente" la información de la que disponen permitirá a los cibercriminales definir mejor el alcance de sus objetivos y dirigir más eficientemente sus ataques.

Los sistemas informáticos continúan siendo altamente inseguros, pese a los muchos avances implementados en los últimos años en temas de seguridad. Seguimos produciendo *software* de lo más variado y no parece que eso vaya a cambiar. Sin embargo, se tiene que mejorar su calidad, asegura **Drew Dean**, director de Programas en SRI International ([ver video](#)).

Ha insistido en la gran evolución del *software* en los últimos quince años con mejoras muy significativas a la hora de poder resolver fallos informáticos. "Si siguiéramos usando las tecnologías de defensa del 2000 teniendo en cuenta cómo está interconectado ahora el mundo estaríamos en una situación más complicada aún", señala.

# El coste de añadir la seguridad desde el propio diseño en el producto ronda el 30 por ciento del importe total del mismo.

Sería interesante construir un protocolo seguro para el direccionamiento de internet. Han destacado los progresos en los últimos años en lo relativo a las Extensiones de Seguridad para el Sistema de Nombres de Dominio (*Domain Name System Security Extensions, o DNSSEC*). Los cibercriminales lo tienen ahora más difícil aunque es cierto que persisten muchos peligros. Dean plantea soluciones como las redes en internet semiprivadas, que identifiquen a las partes contrarias que son de fiar y que se comuniquen de forma selectiva sólo con esas que generan confianza. La clave en este asunto podría ser la confianza. No es un problema técnico, porque establecer redes privadas es sencillo, sino saber confiar en quien realmente lo merece, según los expertos.

## Seguridad versus rentabilidad

Para los fabricantes, desde el punto de vista económico, una de las dificultades en temas de seguridad está en determinar cuándo debería incorporarse ese parámetro en el producto antes de que sea demasiado tarde. El hecho de desconocer si un nuevo producto tendrá éxito o no en el mercado complica las cosas. De hecho, las inversiones en seguridad antes de haber conseguido cuota de mercado son realmente "una pérdida de dinero", especialmente en el caso de las pequeñas empresas cuyo futuro es más incierto, según **Drew Dean**.

El coste de añadir la seguridad desde el propio diseño en el producto ronda el 30 por ciento del importe total del mismo, según datos orientativos facilitados por **Rolf Reinema**, director de Tecnología en Siemens. Añade que más del 80 por ciento de los problemas de seguridad en el ciberespacio se asocian a la calidad del *software*.

---

**Drew Dean** ▼  
Director de Programas en SRI International.

[ver video](#) 





## Prólogo de **John Lyons**

Presidente ejecutivo y fundador de Alianza Internacional de Protección de Seguridad Cibernética (ICSPA).

[ver video](#)



- La guerra cibernética se define como "las acciones de un estado nación para penetrar en los ordenadores o redes de otra nación con el fin de causar daños o trastornos".

**M**uchas personas sugerirían que el ciberterrorismo se refiere a la voluntad de un grupo terrorista de causar muerte o lesiones graves utilizando herramientas de ataque basadas en Internet. Si bien, por desgracia, estos ataques son posibles, afortunadamente hasta la fecha no tenemos ninguna constancia de que grupos terroristas empleen estas tácticas. Eso no quiere decir que no estén dispuestos a hacerlo y, en consecuencia, existen estrategias de ciberseguridad nacional que intentan hacer frente a estas vulnerabilidades.

Sin embargo, es más común que los grupos terroristas utilicen herramientas basadas en Internet y software, tales como aplicaciones de voz y de texto encriptados y redes de anonimato, para planificar y respaldar sus operaciones. Teniendo en cuenta que vivimos en un mundo donde las tensiones van en aumento, tanto a nivel estatal como en lo que respecta al incremento de la actividad terrorista, cuyo objetivo es infligir daños significativos y generar división en la sociedad, ¿cuáles son los puntos clave que deben abordarse?

**Atribución:** No siempre es fácil, incluso para los países más avanzados y maduros, con gran capacidad cibernética, identificar el origen de los ciberataques.

**Defensa primero:** La mayoría de los países eligen construir y aumentar primero su capacidad cibernética defensiva. Pero no es posible llevar a cabo esta labor de forma correcta si no se dispone de conocimientos y comprensión de las armas cibernéticas ofensivas que existen y de las técnicas y metodologías que pueden utilizarse contra ellos.

**Ciberestrategia MAD:** Una estrategia basada en la destrucción mutua asegurada (Mutually Assured Destruction o MAD) del adversario.

**Consecuencias no deseadas de un ataque:** No siempre es posible aislar a las víctimas de un ataque cibernético.

En conclusión, es muy probable que cada vez con más frecuencia presenciemos el despliegue de armas ofensivas cibernéticas nacionales como precursor de un conflicto armado.

Los gobiernos tienen mucho trabajo que hacer si queremos ver este tipo de amenazas mitigadas con suficiente efectividad, para que podamos sentirnos cómodos respecto a la seguridad futura de nuestros sistemas conectados a Internet.



# Ciberguerra, ciberespionaje y ciberterrorismo

1.3

► **Antes del año 2020** habrá algún suceso significativo con pérdida de vidas vinculado directamente a cierto ciberataque perpetrado por alguna nación o Estado o por algún grupo terrorista. Este es uno de los pronósticos para esa fecha de **John Lyons**, jefe ejecutivo del International Cybersecurity Protection Alliance (ICSPA) en el Reino Unido. [\(ver video\)](#).

Otra de sus predicciones es que algunos gobiernos dispondrán de medios técnicos para bloquear comunicaciones en internet para reducir el flujo de contenidos radicales por parte de grupos terroristas en distintas partes del mundo y también adoptarán medidas para combatir los mecanismos de cifrado y vigilar con éxito en internet a grupos hostiles para interceptar sus comunicaciones.

## El poder de la persuasión militar

Al hablar de ciberseguridad, Lyons centra gran parte de su intervención a tomar en consideración viejas lecciones aprendidas de la época de la Guerra Fría, aquella larga rivalidad que enfrentó a EEUU y la Unión Soviética tras la Segunda Guerra Mundial. Destaca como idea central "la disuasión", y la denominada Distracción Mutua Asegurada, MAD, por sus siglas en inglés, como una de las claves para mantener un equilibrio de fuerzas en el mundo que evite ataques entre las partes.

También ahora, en la nueva era de internet, explica, habría que convencer a los adversarios de que "estamos muy preparados" desde el punto de vista tecnológico para emprender posibles actuaciones

ciberoofensivas, y además "tenemos capacidades y habilidades" para implementarlas y asimismo "reconocemos que el opuesto tiene potencial tecnológico similar" y está preparado para proteger con éxito sus redes.

"Creo que las operaciones ciberoofensivas podrían ser la clave para una sociedad futura más estable", aunque habría que "escapar de esa esquizofrenia política en la que nuestros líderes caen de vez en cuando, y ser más maduros", es decir, mantener planteamientos coherentes los países, en lugar de modificarlos continuamente al albur de las circunstancias, añade.

Explica que la mencionada estrategia de Distracción Mutua Asegurada requiere equilibrio entre capacidades ofensivas y defensivas. "Se tiene que ser bueno en ambas". Si un país está preparado tecnológicamente para atacar, pero no tiene aseguradas sus infraestructuras, en ese caso, la estrategia MAD fracasará. "Creo que no se puede tener una cosa sin la otra en términos militares", insiste.

La estrategia de Distracción Mutua Asegurada requiere equilibrio entre capacidades ofensivas y defensivas.

Por su parte, **Miguel Rego**, director general del Instituto Nacional de Ciberseguridad Español (Incibe), advierte de ciertas técnicas que están usando los países y que podrían considerarse del entorno de la ciberguerra. "Muchas veces se está viendo *malware* o código malicioso sofisticado que permite acceder a información sensible de administraciones públicas y empresas en otros países". ¿Cómo debería evolucionar la legislación internacional de cara al 2020 para prevenir y regular este tipo de prácticas?

"Creo que habrá que esperar a resolver cuestiones previas como quién posee internet y donde reside su soberanía antes de poder entrar a discutir sobre leyes internacionales", le responde **John Lyons**. "Las diferencias entre los países respecto a la soberanía de la red complican otros temas legales. No veo demasiados desarrollos en esto posiblemente en los próximos cinco, diez años", añade.

**Carlos Jiménez** ▲  
Presidente y fundador de Secuware.



## Conflictos ciber-ciber y de máquinas contra personas

**Drew Dean** advierte de la presencia de nuevos actores en las guerras, como las armas autónomas, que podrían cambiar los equilibrios políticos de poder en el mundo. La próxima vez que se produzca un conflicto armado de fuerza mayor por naciones avanzadas se verá combinado con "cibernética", es decir, con armamento dotado de inteligencia artificial que tomará decisiones por sí mismo.

Eso ya está ocurriendo, añade categórico **Eden Shochat**. Agrega que teniendo en cuenta el desarrollo actual de robots, drones y vehículos autónomos, para el futuro podría pensarse en la posibilidad de conflictos ciber-ciber, es decir de armas "inteligentes" contra armas "inteligentes". Recuerda que, al fin y al cabo, los robots básicamente lo que hacen es implementar *software* y también podrían ser atacados por *software*.

**Drew Dean** responde que, previsiblemente, se verán batallas entre máquinas y humanos. No obstante, es escéptico respecto a la posibilidad de que se vayan a producir, al menos por ahora, guerras ciber-ciber con consecuencias relevantes. No se imagina que un conflicto entre máquinas llegue a ser decisivo hasta el punto de que pueda desencadenar la rendición de una de las partes enfrentadas. Los efectos del disparo de un dron contra otro dron enemigo no serán determinantes en el desenlace final de una guerra.

## ¿Inteligencias artificiales perversas?

En el libro *Daemon*, de Daniel Suárez, un éxito de ventas en EEUU, un *software* autónomo crea una especie de realidad aumentada para cada uno y amenaza con acabar con el mundo interconectado. En la saga de las películas *Terminator* para matar a los seres humanos *Skynet* es el sistema de inteligencia artificial que lidera el ejército de las



**Miguel Rego** ▲

Director general del Instituto Nacional de Seguridad de España (Incibe).



**Inbar Raz** ▲

Vicepresidente de Investigación del Perimeter X.

máquinas. "¡Esto no parece muy probable hoy por hoy!". No quiero decir que no vaya a ocurrir, simplemente no estamos en esa fase todavía, asegura **Inbar Raz**, de PerimeterX.

Advierte de la amenaza de explotar vulnerabilidades a escala masiva de forma automatizada con el uso de cientos de máquinas al mismo tiempo en el marco del "Internet de las Cosas". Alerta además del peligro de una inteligencia artificial peligrosa.

¿Qué pasaría si se fuera más allá y se cruzara la actual línea de defensa a la que se circunscribe la inteligencia artificial, para dar el salto al lado perverso de los ataques?, se pregunta Raz consternado. Explica que la inteligencia artificial permite que las armas se conviertan en semiautónomas, que no sean controladas realmente por el hombre. Es posible que cierta gente pueda plantearse la creación de una "inteligencia artificial peligrosa". De hecho los incentivos para ello serían muy importantes teniendo en cuenta que "el mercado del ciberdelito es muy lucrativo".

**Carlos Jiménez**, presidente de Secuware, recuerda que en 2001 "nadie nos había enseñado a usar un avión como arma", en referencia al brutal atentado terrorista contra las Torres Gemelas en EEUU. Pues bien, explica, "deberíamos trasladar eso mismo a los ordenadores". Estos y los dispositivos móviles también son armas potenciales, que además pueden ser fácilmente ubicadas en los lugares que se quiere atacar. Para su funcionamiento, sólo se

necesita que alguien las use desde su interior o por control remoto. Cuando se habla de prácticas como vigilancia masiva de los gobiernos para controlar a los ciudadanos en internet y de cómo colocar troyanos en los sistemas para prevenir ataques, como argumentan los gobernantes para dichas acciones de control, el problema es que esas mismas redes de ordenadores pueden ser utilizadas por gente con intenciones criminales.

Las llamadas "*botnets*" o redes de ordenadores que se ejecutan de forma automática y autónoma controlados generalmente desde un nodo central, habitualmente para fines criminales, no son armas en sí pero pueden convertirse en dispositivos atacantes en el sentido de que son capaces de ser activados y sus efectos se multiplican y expanden de inmediato a millones de aparatos. La solución no sería facilitar el acceso a los sistemas a los gobiernos sino garantizar que el manejo de los mismos cuenta con garantías de seguridad. Cuando se conduce un coche, se requiere permiso de conducir. Pues bien, para manejar ciertos ordenadores, también se habría de exigir algo similar, explica Jiménez a modo de ejemplo.





## Prólogo de **Caroline Baylon**

Directora, Programa de Investigación sobre Seguridad Cibernética,  
Centro de Investigación de Decisiones Estratégicas.

[ver video](#)

- En el caso de gran parte de nuestras infraestructuras críticas, contar con un "espacio de aire", es decir, estar completamente aislada de la red pública de Internet, ha constituido tradicionalmente la principal defensa contra ataques cibernéticos.

**S**in embargo, dichas infraestructuras críticas están cada vez más conectadas a Internet. Incluso en sectores como el nuclear, que cuentan con regulaciones muy estrictas, algunas instalaciones permiten el acceso remoto a través de redes privadas virtuales (VPN) o disponen de conexiones a Internet no documentadas u olvidadas, algunas de ellas instaladas por contratistas externos. Por otra parte, los espacios de aire no son una garantía de protección; Stuxnet ha demostrado que solamente hace falta una unidad flash para vulnerar la seguridad de un espacio de aire.

Muchos sistemas de control industrial utilizados en infraestructuras críticas se diseñaron en la década de los 60, cuando era inconcebible que un individuo con malas intenciones tratara de atacarlos. Como resultado de ello, carecen de medidas básicas de seguridad tales como la autenticación y el cifrado, lo que los hace "inseguros por diseño". Por otra parte, la flexibilidad del código implica que cualquier atacante que pueda atravesar las defensas perimetrales puede realizar cambios lógicos muy difíciles de detectar. Además, las soluciones de seguridad informática estándar que se utilizan en entornos de TI domésticos o de oficina, tales como parches, son difíciles de implementar en entornos industriales.

# Los riesgos de conectar las infraestructuras críticas a internet

1.4

► **El riesgo de un ciberataque serio** en alguna planta nuclear está aumentando dada la vinculación cada vez mayor de dichas infraestructuras a sistemas digitales. Esa tendencia a la digitalización junto con la falta de concienciación en los niveles directivos sobre los riesgos que ello implica hace que el personal de las instalaciones pudiera no estar siendo realmente consciente de las cibervulnerabilidades a las que se exponen y por ello no se estén preparando adecuadamente a nivel de ciberseguridad para hacer frente a potenciales ataques.

Así se desprende de un informe publicado en octubre de 2015 del Instituto de Relaciones Internacionales británico, conocido como Chatham House <https://www.chathamhouse.org/>. **Caroline Baylon**, coautora de la publicación, ha advertido de que antes de 2020 podría producirse algún cibermacroataque contra alguna red eléctrica que dejaría sin servicio a áreas importantes del país afectado durante al menos un día. Dada su magnitud, se informaría de ello en los medios de comunicación. Para ese mismo horizonte, alerta de que algún grupo terrorista podría juntarse con algún equipo de ciberatacantes profesionales a los que pagarían por sus servicios para atacar alguna infraestructura crítica. ([ver vídeo](#)).

Se ha referido no sólo a los riesgos de ciberseguridad de las propias infraestructuras nacionales sino también a los vinculados con los materiales y piezas que suministran los proveedores. "Es realmente complicado garantizar una absoluta integridad en la cadena de suministro. Todo el mundo está muy preocupado por esto" y advierte del problema que

supone que los productos no dispongan de seguridad desde el diseño. También se ha referido a la situación particularmente de riesgo de las infraestructuras críticas en países en vías de desarrollo, pues sólo ahora algunos de ellos están empezando a aprender sobre ciberseguridad.

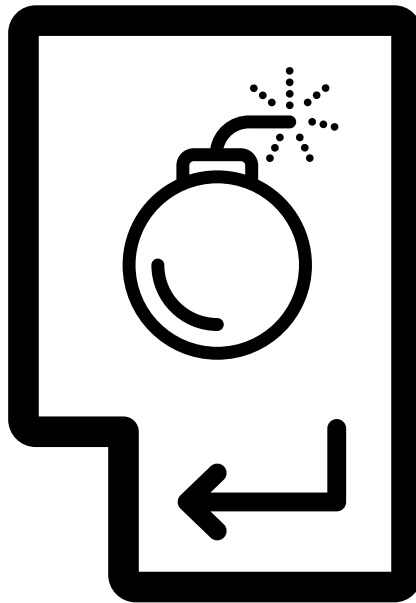
## El caso del código malicioso *Stuxnet* contra una central nuclear iraní

En este contexto, los participantes han recordado el ciberataque contra una central iraní que salió a la luz en 2010, mediante el código malicioso *Stuxnet* que supuso un verdadero varapalo para el programa nuclear de ese país. El ciberataque habría sido perpetrado supuestamente por la Agencia de Seguridad Nacional de Estados Unidos (NSA), y por el Mosad, el servicio secreto israelí, según la mayoría de indicios.

Este sofisticado virus, operativo desde al menos 2007, fue introducido en los sistemas informáticos de una central iraní y produjo un sobrecalentamiento de alrededor de un millar de las 5.000 centrifugadoras, convirtiéndose en el primer caso de un ciberataque capaz de dañar una infraestructura del mundo físico.

"Creo que no deberíamos considerar ese ataque como el Santo Grial de las intervenciones ciberofensivas", dado que el adversario no era particularmente sofisticado, ha dicho Lyons, de ICSPA.

# Las infraestructuras críticas de países que no estén preparadas para defenderse de ciberataques no deberían conectar sus infraestructuras a la red.



En la actualidad, "existen objetivos mucho más complicados que podrían ser vapuleados". Por ello, "no deberíamos relajarnos por aquel éxito", añade.

Las infraestructuras críticas de países que no estén preparadas para defenderse de ciberataques no deberían conectar sus infraestructuras a la red, responde Lyons a Caroline Baylon, quien le pregunta además si habría de invertirse más dinero en "kill switches" o mecanismos de parada instantánea en esas instalaciones para garantizar la seguridad en situaciones de emergencia.

"Sí", responde rotundo Lyons. "Pienso que es peligroso que no seamos capaces de desconectar esas infraestructuras en caso de cualquier tipo

de ataque". Los gobiernos en países con mayor riesgo de vulnerabilidades de esas instalaciones podrían colaborar con la ciberseguridad negando la licencia para operar a los responsables de esas infraestructuras si no están lo suficientemente preparadas para defenderse frente a ataques. "Se deberían exigir esos altos estándares, pero no se está haciendo", lamenta.

De cara a 2020, por su parte, **Steve Wilson**, vicepresidente de Constellation Research, dice que confía en que finalmente "se entrará en razón". Una de sus predicciones para entonces es que se habrán prohibido los termostatos "inteligentes" en los reactores nucleares. "No confío en que el software vaya a portarse bien".

# Conclusiones

## Cap. 1 — Amenazas de la ciberseguridad

► **Los ciberataques son un problema** que ya está aquí, aunque se incrementan anualmente de forma exponencial y cada vez son más sofisticados y perversos, lo que está agravando seriamente el problema. Los cibercriminales aspiran a retos mayores con tecnologías a su alcance cada vez más potentes y accesibles fácilmente en internet, según los expertos.

Al mismo tiempo, ciertos gobiernos están usando técnicas de ciberguerra y acuden frecuentemente a los mercados de venta de vulnerabilidades 0-day para poder acceder desde esas "puertas traseras" a los sistemas informáticos y realizar vigilancia masiva de ciudadanos y de empresas bajo el argumento de la seguridad. Según los participantes, el problema de dar vía abierta a esos accesos es que también pueden utilizarlos los cibercriminales.

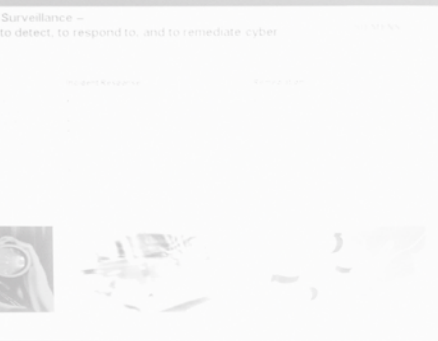
La "inteligencia artificial", con todas sus bondades económicas y sociales, podría llegar a hacerse muy perversa y provocar en el futuro que las máquinas adoptaran por su cuenta decisiones malvadas contra

las personas. De momento no se vislumbran guerras ciber-ciber, es decir, de armas autónomas entre sí, aunque podrían producirse en un horizonte más lejano.

Por otra parte, las redes de ordenadores controladas de forma remota por cibercriminales permiten masificar los efectos de los ataques como de hecho ya está ocurriendo, aunque el problema irá a más con el "Internet de las Cosas", según los expertos.

En cuanto a las infraestructuras singulares, éstas representan una seria amenaza en términos de seguridad conectadas a internet dado que un ciberataque puede poner en jaque servicios esenciales de las ciudades como la electricidad, el agua, el gas. Por todo esto, el *software* debería ser seguro, pese a las dificultades que ello implica, mientras que los dispositivos habrían de garantizar la seguridad desde el diseño pese al desembolso económico que supone a las empresas cuando ni siquiera tienen garantías de que venderán sus productos.





# La seguridad del internauta

---

2

---

## **Inbar Raz**

Vicepresidente de Investigación del Perimeter X.

## **Steve Wilson**

Vicepresidente de Constellation Research.

## **Evan Wolff**

Socio en Crowell & Moring.

## **Kevin Sale**

Especialista en Seguridad IT en la Universidad  
Abdullah de Ciencia y Tecnología.

- El "Internet de las Cosas", ese fenómeno de conexión de todo con todo que avanza de forma vertiginosa, traerá inevitablemente sorpresas en temas de seguridad no siempre gratas, como ya está ocurriendo.

**L**as revolucionarias innovaciones informáticas en esta era de ordenadores cada vez más potentes e "inteligentes", junto con la proliferación de sensores progresivamente más diminutos y baratos, están siendo factores determinantes para la interconectividad global. Cualquier dispositivo electrónico conectado a la red, por pequeño que sea, puede convertirse automáticamente en potencial objetivo de ciberataques y eso entraña muy serios riesgos para la seguridad de las personas.

Ningún sector parece librarse de la seducción de internet, coinciden los expertos. Determinados ámbitos serán sin embargo más sensibles. Por ejemplo el sanitario: con pulseras y brazaletes en pleno auge ya en distintos lugares del mundo, que miden todo tipo de parámetros

biomédicos y que mandan indiscriminadamente los datos que recopilan a internet, bajo el riesgo de ser accesibles por cualquiera y de poder poner en jaque la intimidad de sus dueños.

El tema de la privacidad en el "Internet de las Cosas" está haciendo saltar las alarmas. Los millones de datos puestos en circulación en la red por este fenómeno pueden delatar detalles privados de las personas cuando son procesados y analizados de forma masiva por los superpotentes ordenadores que existen hoy en día. Por otra parte, los sistemas actuales de verificación de identidades digitales no garantizan siempre la privacidad de la persona y tampoco los sistemas de comunicación son cien por cien fiables a la hora de asegurar que el receptor del mensaje sea el único indiscutiblemente que pueda leerlo.



## Prólogo de **Inbar Raz**

Vicepresidente de Investigación del Perimeter X.

[ver video](#)

- En la actualidad, nuestra vida está controlada por los ordenadores, que sin excepción ejecutan *software*. Si este contiene errores, estos se convierten en vulnerabilidades que pueden utilizarse para provocar daños. Los hackers y los gobiernos suelen utilizar estos errores para alcanzar sus objetivos.

Estos errores existen básicamente debido a la falta de seguridad en la fase de diseño, ya sea porque los proveedores se apresuran a sacar el producto o simplemente porque no tienen a nadie que sea lo suficientemente experto. Los proveedores no tienen ningún incentivo para cambiar o mejorar, ya que normalmente no reciben ningún castigo por la creación de código vulnerable, ni tan siquiera si este ya se ha aprovechado para provocar daños.

Nos gustaría cambiar esta situación mediante la creación de una nueva norma para el desarrollo seguro, de manera que, por un lado, no se impidan la innovación ni la creatividad y, por el otro, se impongan unas regulaciones más estrictas sobre el *software* que tiene una gran

incidencia sobre el público, los gobiernos o las infraestructuras críticas.

La "Norma diferencial para el control de la seguridad" dice de manera muy clara que, cuanto más popular o influyente sea su producto, más estrictas serán las normas de seguridad que tendrá que cumplir. Las empresas de nueva creación podrán continuar realizando sus proyectos de manera muy rápida para lanzar su producto, pero a medida que la popularidad del producto vaya creciendo o si el producto termina instalado en lugares críticos, los requisitos de cumplimiento aumentarán en consonancia.

De esta manera, esperamos reducir de manera importante los incidentes de seguridad del *software* que tiene un gran efecto sobre el público.



# El "internet de las cosas", un paraíso para el ciberdelito

2.1

► **Frigoríficos inteligentes que informan** al dueño cuando le falta algo, automóviles autónomos y semiautónomos, que alertan al conductor por ejemplo si se duerme, y todo un sinfín de dispositivos, como televisores, pulseras, relojes, que proliferan por todas partes, están ya conectados a internet para facilitar la vida a la gente. "Estamos rodeados de estos aparatos. El Internet de las cosas ya está aquí", asegura **Inbar Raz**, de PerimeterX.

El problema de una conectividad omnipresente es que "todos nos convertimos en posibles atacantes y asimismo todos nos convertimos en posibles víctimas de ciberamenazas". Actualmente, cualquiera

puede crearse su propio dispositivo y conectarlo a internet, asegura Raz. De hecho, los ordenadores cada vez son más baratos, pequeños, accesibles y fáciles de manejar. Por ejemplo, *Raspberry Pi Zero* es un diminuto PC por muy pocos euros con grandes funcionalidades, o *Arduino* es una plataforma de *hardware* libre, desarrollada por españoles, que permite construir y programar en casa dispositivos electrónicos muy baratos.

Cualquier dispositivo con conexión a internet permite no sólo atacar sino acceder a plataformas utilizadas para ello. Raz se ha referido a una red de ordenadores controlada por cibercriminales, descubierta hace unos meses, que se aprovechaba de frigoríficos "inteligentes" infectados desde donde se enviaban oleadas de correos no deseados por el receptor. ¿Quién imaginaria que esto iba a ocurrir?, se pregunta.

Se necesita algún tipo de regulación en temas de ciberseguridad, además de exigencias como el *Security Development Lifecycle (SDL)* y la seguridad "by design" o desde el diseño mismo del dispositivo, ha dicho. La seguridad tiene que ser "una característica" del producto, un requisito inherente al mismo y no algo que se incorpora arbitrariamente dependiendo del fabricante. Bajo esa premisa, al usuario no se le debe cargar con la responsabilidad de gestionarla cuando utiliza un dispositivo, sino que tiene que ser seguro por sí de antemano, señala el experto.

"Cuando mi automóvil se estropea, lo llevo al taller. No necesito saber cómo funciona el motor, ni quiero saberlo. Cuando el decodificador se rompe llamo al técnico, no necesito saber cómo funciona. Lo mismo ocurre con el médico, él es

**Rolf Reinema** ▾  
Director de Tecnología en Siemens.

[ver video](#) 



quien estudia durante muchos años para saber cómo curarme, yo no tengo por qué saberlo", añade.

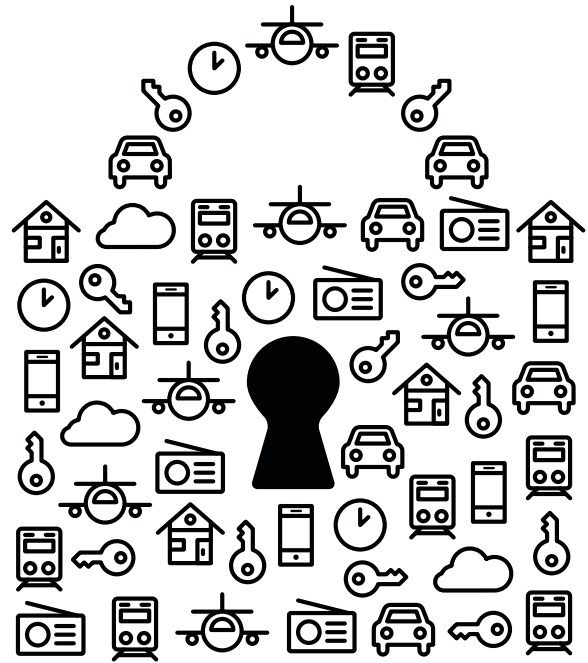
## La seguridad de Internet debería regularse como servicio básico

Como la electricidad, que es un servicio básico, el Gobierno debería garantizar un internet seguro al ciudadano. Se trata de un recurso del que también se abastecen los países, y debería ser regulada su seguridad por el Gobierno. A nivel individual, el ciudadano por su cuenta no puede hacer gran cosa para garantizar que sea seguro, explica Raz.

Sus dos predicciones para 2020 son las siguientes: una es que cualquiera podrá tener acceso a los datos privados de otra persona y éstos estarán todavía más esparcidos que hoy en día por internet. Además los ciber sobornos serán mucho más fáciles de realizar: el ciberdelincuente sólo habrá de presionar un botón para exigir a la víctima que pague si quiere ver liberado su ordenador de los virus con los que le ha infectado.

Su segunda previsión es que se producirá algún asesinato desde internet. Hasta el momento esto no ha ocurrido. Lo que sin embargo sí ha habido ya son muertes indirectamente vinculadas con delitos en la red, como suicidios de personas, víctimas de ciberextorsión y chantajes bajo la amenaza de ver publicados sus datos íntimos por parte de ciberdelinquentes si no les pagan cuantiosas sumas de dinero.

En el ámbito de la ciberseguridad de las empresas, **Rolf Reinema**, director de Tecnología de Siemens, una compañía con un ambicioso programa de seguridad, ha advertido de que el gran desafío actual en ciberseguridad es saber cómo tratar lo desconocido en el mundo de las amenazas. "Sólo se puede buscar aquello que se conoce", ha dicho. "Estamos bajo el riesgo constante de ataques. No se puede prevenir todo lo que va a ocurrir.



Como la electricidad, que es un servicio básico, el Gobierno debería garantizar un internet seguro al ciudadano.

La pregunta es ¿cómo tratamos el problema?", se pregunta. La respuesta inmediata sería monitorizar datos y ver dónde están escondidos "los malos". En general no sabemos su ubicación y de ahí el interés por monitorizarlos. [\(ver vídeo\)](#).

Se ha referido a dos desafíos. Uno, diferenciar qué es realmente un ataque frente a un comportamiento anormal de un usuario convencional, porque no están tan claros los límites. El segundo, avanzar en el desarrollo de tecnologías que permitan la detección del ataque desde el momento mismo en que se produce.

## El cifrado seguro de sistemas como disciplina en la Universidad

En ese contexto de amenazas, el papel de la Universidad parece que puede resultar determinante a la hora de promover la formación de expertos en cifrado seguro aunque no está ocurriendo así. "Hablamos de diseño con seguridad pero tenemos un problema de raíz. No se estudia en ciencias de la computación, al menos en España", lamenta **Fernando Vega**, director de Seguridad de la Información en el grupo Bankinter. ¿Ocurre lo mismo en otros países? ¿cómo se vislumbra el futuro en este asunto?, se pregunta el experto.

A las universidades, en general, no parece preocuparles el tema de la formación en cifrado seguro, explica Fabio Assolini, de Kaspersky. Al final esto es algo que se aprende una vez que los alumnos están ya en el mundo laboral, cuando trabajan en la industria de la ciberseguridad. De hecho, muchas empresas se están especializando en control de código fuente y en la resolución de vulnerabilidades. Reitera que "las universidades no están enseñando a sus alumnos a codificar de forma segura y eso es algo que tienen que cambiar".

## Ojo con los niños en internet y "las chucherías" virtuales

La educación de los pequeños desde edades tempranas para aprender a protegerse en internet es fundamental, según los expertos. "En esta nueva era de internet los niños tienen que comprender que no deben aceptar chucherías virtuales de webs extrañas, del mismo modo que los pequeños de otras épocas aprendían a no aceptar caramelos de gente que no conocían", asegura en tono distendido **Michael Osborne**, de IBM.

A nivel global, la mayoría de los expertos coinciden en la necesidad de concienciación del consumidor de protegerse y especialmente los menores en su



**Fernando Vega** ▲  
Director de Seguridad de la Información en el grupo Bankinter.



**Michael Osborne** ▲  
Manager de Privacidad y Seguridad de Informática Cognitiva y Departamento de Soluciones Industriales del IBM Research Division.

A nivel global, la mayoría de los expertos coinciden en la necesidad de concienciación del consumidor de protegerse.

navegación por internet o al realizar transacciones. En los debates se ha discrepado sin embargo sobre el nivel de responsabilidad que debería atribuirse a la persona o individuo en esa tarea de ver garantizada su seguridad. Mientras que algunos defienden especialmente un comportamiento precavido del consumidor como clave para su seguridad, otros son más favorables a trasladar el peso de la responsabilidad preferentemente a la industria, que tiene que garantizar productos seguros de por sí. No obstante, la opinión generalizada es que las soluciones tienen que pasar por la colaboración conjunta entre consumidores, legisladores, gobiernos, industria, empresas, etc.





**"Todos nos  
convertimos en  
posibles atacantes  
y asimismo todos  
nos convertimos en  
posibles víctimas de  
ciberamenazas"**

---

**Inbar Raz**

Vicepresidente de Investigación  
del Perimeter X.



## Prólogo de **Steve Wilson**

Vicepresidente de Constellation Research.

[ver video](#)

- Es bien sabido que la mayoría de los fraudes de Internet están relacionados con deficiencias en la autenticación digital. Saber realmente con quién estamos tratando por Internet puede resultar una tarea difícil.

La falta de certeza sobre el origen de mensajes de correo electrónico y sitios web puede conducir a fraudes cibernéticos; verificaciones de identidad poco estrictas permiten la suplantación de identidad y la creación de identidades falsas. La respuesta a los problemas de identidad tiende a ser intensificar las acciones de identificación. Con el tiempo, hemos tratado de reforzar las débiles identidades digitales mediante códigos de verificación de tarjeta (CVC), mecanismos de identificación basados en conocimientos, y datos biométricos, pero estas credenciales adicionales también son susceptibles de ser robadas y utilizadas fraudulentamente.

Por fin, parece que la tendencia está cambiando, y los ingenieros del ámbito de la identificación están dejando de prestar atención a "quién" somos para centrarse en "qué" somos. Es decir, ¿qué es lo que necesitamos saber acerca de una persona para hacer negocios con ella? ¿Qué atributos específicos de

una persona son relevantes en el contexto de cada transacción? La identidad es abstracta y fluida, y, a la hora de la verdad, resulta muy difícil de procesar para un ordenador. Estamos haciendo un mejor progreso ahora, retrocediendo un nivel para fijarnos en atributos concretos: credenciales, calificaciones, afiliaciones, números de cuenta, identificadores de salud, datos demográficos, etc.

La gestión de la identidad actual debe prestar atención **al contexto** de las transacciones y los atributos relevantes concretos, **la relación** entre las partes y la preservación de esta en la red y **la procedencia** de los atributos (de dónde vienen, quién da fe de ellos).

De este modo, avanzaremos en pos de la facilidad de uso, la reducción de contraseñas, la protección ante la suplantación de identidad y el fraude, mayor facilidad para demostrar la identidad, mayor privacidad y menor divulgación de datos personales.

# Las debilidades de la identidad digital

## 2.2

► **La identidad de un individuo** es justamente lo opuesto a su privacidad. La identidad es lo que se necesita saber de alguien y la privacidad precisamente lo contrario, lo que no se tiene que conocer de esa persona, explican los expertos.

Identificar exactamente con quién se está interactuando es fundamental en la vida real pero también en la digital. En el ciberespacio, las cosas se complican porque no se ve físicamente a la persona con la que uno se comunica. A pesar de que existen atributos asociados a la identidad digital del individuo, estos pueden ser modificados, enmascarados e incluso sustituidos por otros de forma fraudulenta. Hay distintos sistemas de autenticación e identificación digitales pero todavía no existe uno unificado en el mercado. "Se necesitan protocolos de autenticación seguros para un futuro en confianza", asegura **Drew Dean**, de SRI International.

En el mundo físico se tienen muchas personalidades: culturales, lúdicas, laborales. Algunas se mezclan fácilmente aunque otras no. En cambio en la vida *online* la convergencia de personalidades brilla por su ausencia. La identidad digital es matemática, precisa, asegura **Steve Wilson**, de Constellation Research. [\(ver video\)](#).

## La clave está en saber qué es la persona y no quién es

La autenticación busca proporcionar seguridad. Consiste en la confirmación de la identificación digital mediante alguna característica u objeto único del sujeto. Pero ¿qué es lo que realmente se necesita conocer de alguien en la vida digital?, preguntan los expertos. No se trata de saber quién

es la persona, sino qué es. "Da igual que el individuo se llame de un modo o de otro. Eso es irrelevante". Lo importante es saber que la persona realmente es quien dice ser y no ha cometido previamente nada ilícito que le impida continuar con una transacción, explica **Richard Parry**, jefe de Parry Advisory.

El modo en el que una madre conoce a un hijo es totalmente irrelevante para un banco. Lo fundamental es que las claves que utilice para operar se correspondan con las utilizadas por la persona a quien le fueron otorgadas. "Lo importante es que a quien se dio unas llaves tenga control de ellas" y que, por el contrario, no estén siendo usadas por otra persona sin autorización para ello, añade por su parte **Steve Wilson**.

La verificación de la identidad es clave para identificar a la gente y poder gestionar el riesgo que implica tratar con las personas para hacer negocios, por ejemplo. Hay sectores más sensibles al uso fraudulento de la identidad digital como el financiero

La autenticación busca proporcionar seguridad. Consiste en la confirmación de la identificación digital mediante alguna característica u objeto único del sujeto.

y bancario, la sanidad o el comercio *online*. El fraude en internet tiene mucho que ver con las debilidades en torno a la autenticación de una persona, que es fácil de replicar y manipular, insisten los expertos.

## El mundo digital no implica confiar en todo el mundo

Es una utopía pensar que en el mundo digital se pueden hacer negocios con cualquier extraño y que se puede confiar en toda identidad tras unos y ceros, advierte el **Steve Wilson**, vicepresidente de Constellation Research. En la vida *online* se tendrían que rechazar las experiencias supuestamente inseguras del mismo modo que se hace en la física, añade el experto.

En temas de autenticación digital se necesita "una llave física", un número que conecte un punto con otro y nada más. "Se da a la gente los candados para esa identificación, pero como nación no hay forma de saber a quién se han dado las llaves. No tenemos esquema nacional", advierte Parry.

En lugar de tratarse a la gente como fichas o "*tokens*", que incorporan datos para identificar a la persona, los individuos podrían pasar a ser fichas en sí, cuya información confirmaría automáticamente si quien uno dice ser lo es

Las técnicas de autenticación tienen que garantizar la protección de los datos, es decir, la privacidad del usuario mediante sistemas de cifrado fuerte.

realmente y si se trata de una persona apta para ciertas transacciones de acuerdo a sus antecedentes.

Los expertos han debatido también sobre biometría, una tecnología de identificación que reconoce características morfológicas y de comportamiento únicas de las personas, e intransferibles, como el rostro, fondo del ojo, etc. Wilson opina que no hay ni habrá jamás biometría en el mundo con las características ingenieriles que permitan una fiabilidad suficiente. Parecido piensa el director de programas en SRI International, **Drew Dean**, quien asegura que esa tecnología tiene índices de fallos en el reconocimiento que "no son triviales".

## La necesidad de sistemas de cifrado fuerte

Las técnicas de autenticación tienen que garantizar la protección de los datos, es decir, la privacidad del usuario mediante sistemas de cifrado fuerte, y no tan frágiles como hasta ahora, señalan los expertos. El contenido de las comunicaciones debe ser ilegible para quienes no posean la clave para descifrarlo, incluidos los gobiernos, precisan. Se necesita una autenticación fuerte para propósitos legítimos, que dote de seguridad y transparencia las relaciones digitales de los individuos con las empresas y los gobiernos.

Por su parte, el parlamentario ruso **Ilya Ponomarev**, presidente del Subcomité de Innovación y Capital Riesgo de la Duma, advierte de lo paradójico que resulta que muchos exijan para sí mismos que se anteponga la privacidad por encima de todo y por otra parte reclamen máxima transparencia al Gobierno. "Sí para los demás la transparencia, pero no para ellos", advierte. Este tipo de planteamientos terminará provocando previsiblemente perturbaciones en zonas como Europa, añade. En su opinión, debería alcanzarse un gran acuerdo social respecto a estos temas teniendo en cuenta sobre todo a aquellos negocios relacionados con las nuevas tecnologías a los que les afectarán especialmente.





"Se necesitan  
protocolos de  
autenticación  
seguros para un  
futuro en confianza"

---

**Drew Dean**

Director de Programas en SRI International.



## Prólogo de **Evan Wolff**

Socio en Crowell & Moring.

[ver video](#)

# ● Seguridad cibernética vs privacidad: cómo fomentar la confianza

Los actuales debates sobre políticas globales ponen de relieve el tira y afloja existente entre la seguridad cibernética, que aboga por una mayor vigilancia y más intercambio de información, y la privacidad, con su expectativa de que la información personal esté protegida por encima de todo. La confianza, desde tres perspectivas diferentes, es la clave para reducir esta tensión y armonizar las necesidades de seguridad cibernética con las expectativas de privacidad.

En primer lugar, las personas deben confiar en la tecnología y en los custodios de la información personal, no solo para proteger sus datos, sino también para proporcionar soluciones cuando alguna cosa falla. Esa confianza surge de la transparencia de dichos custodios acerca de cómo se recoge, se protege, se utiliza, se comparte y se elimina la información electrónica.

En segundo lugar, las empresas deben confiar en que los sistemas de seguridad de la información y los controles correspondientes proporcionen una protección razonable y acorde con el riesgo para sus datos empresariales y de propiedad intelectual, así como para los datos de sus clientes y socios. Las empresas también necesitan confiar en que la tecnología sea suficientemente sólida y flexible

como para cumplir con una serie de regulaciones gubernamentales, iniciativas para la puesta en común de la información y requisitos de privacidad en constante evolución.

En tercer lugar, los países deben confiar en que la tecnología, las políticas y las prácticas de seguridad cibernética de las que dependen resulten suficientes para defender sus fronteras electrónicas contra las amenazas informáticas, y deben proteger al mismo tiempo los datos de sus ciudadanos y empresas de una forma que logre un equilibrio razonable entre las necesidades de seguridad y de cumplimiento de la legislación nacional y las expectativas de privacidad de los ciudadanos.

La tecnología, las herramientas y las políticas de seguridad cibernética son fundamentales para la protección de la información y para la seguridad física, al igual que las leyes y políticas de privacidad son necesarias para proteger la información personal. La confianza en que la seguridad cibernética y la privacidad no solo pueden coexistir sino también complementarse entre sí solamente se puede generar mediante el debate acerca de la intersección entre ambas, los desafíos que suponen la una para la otra, y la importancia que tienen para cada una de ellas la transparencia y la responsabilidad.



# Intimidad y privacidad versus seguridad

2.3

► **Desde las polémicas revelaciones** de Edward Snowden, a partir de 2013, los ciudadanos saben que los gobiernos en el mundo tienen un interés serio en el acceso a todos los datos que circulan por internet. El ex informático de la *National Security Agency* (NSA) <https://www.nsa.gov/> destapó las prácticas poco éticas del Gobierno estadounidense y su programa "Prism" que utilizaba vulnerabilidades *0-day* o "Día Cero" para controlar a ciertos sectores de la población.

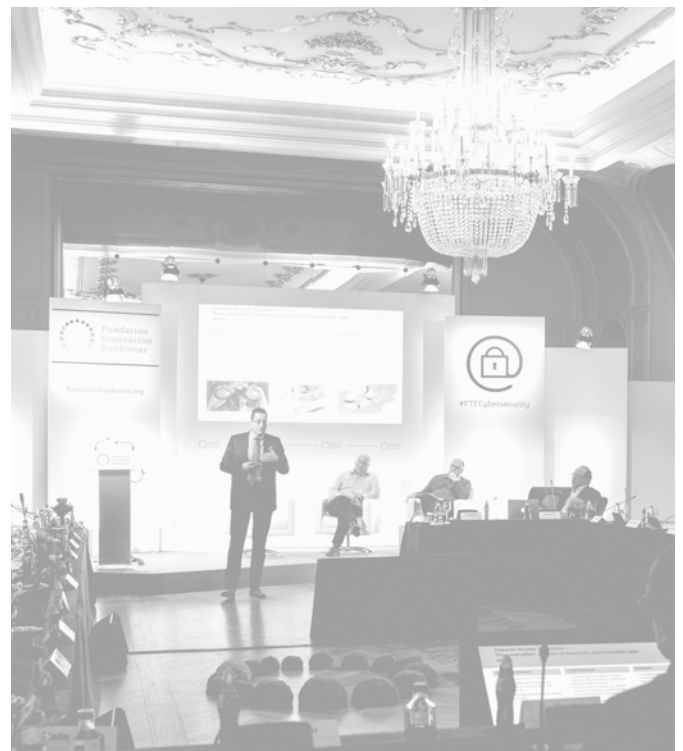
## ¿Estaría justificada en las sociedades modernas la pérdida de la privacidad para obtener supuestamente seguridad ciudadana?

Uno de los cinco escenarios de sociedad con el que han trabajado los expertos es precisamente el de un sistema que llegara a estar completamente vigilado por el Gobierno, y que no sería descartable desde el punto de vista tecnológico en la nueva era de internet gracias a la expansión de sistemas y sensores a bajo precio, y que lo harían posible en algunos países. Especialmente después de algún macroatentado terrorista que hubiera sumido en el pánico más absoluto a la población. La conclusión de un modelo así es que no habría privacidad y la gente acabaría con muchos desórdenes mentales.

Por el contrario, según los expertos, en un mundo en el que la privacidad estuviera por encima de todo sería complicado garantizar la seguridad, porque los datos estarían siempre cifrados para no ser desvelados, incluidos los de las comunicaciones entre terroristas. No obstante, los individuos

tendrían control de sus datos y su privacidad estaría salvaguardada. Los cibercriminales tenderían a abusar del fácil acceso en internet a todo tipo de información, advierten los expertos.

"Realmente no creo en la privacidad en internet. Creo que necesitamos autenticación más estricta para la privacidad y la seguridad en internet cuando sea necesario que así sea, pero cuando no, habría de prevalecer el anonimato", explica **Evan Wolff**, socio en Crowell & Moring ([ver video](#)). En el ciberespacio en estos momentos los ciudadanos están en desventaja y los criminales en ventaja, insiste. ¿Por qué? se pregunta. La gestión de la identificación digital es realmente complicada y la de la autenticación, mayor aún. Autenticar quién es uno en el



Para 2020 predicen que se habrán reducido los ciclos de detección de amenazas en las empresas con el uso de más cantidad de sistemas predictivos y analítica "inteligente" de seguridad.



ciberespacio y comprobar que las identidades digital y real de la persona coinciden se ha convertido en algo muy difícil mientras que lograr que el usuario se mantenga anónimo es "muy muy fácil", añade. Por ejemplo el popular servicio de comunicaciones "WhatsApp" apenas pide datos para darse de alta.

El experto confía en que los próximos grandes avances en programación e innovación en tecnología serán determinantes para mejorar los sistemas de autenticación y determinar conceptos sobre la privacidad que benefician a los ciudadanos digitales, y puedan verse más protegidos frente a

los cibercriminales. También espera que los países y las grandes empresas empiecen a organizarse para trabajar juntas en estos objetivos.

Una de sus predicciones para 2020 es que las empresas serán más transparentes respecto a lo que están haciendo con los datos de sus clientes, y eso contribuirá a garantizar su privacidad. Las regulaciones serán parte del proceso pero no serán determinantes, porque este tipo de cosas no funciona con imposiciones legales, señala.

Desde el ámbito empresarial, **Rolf Reinema**, de Siemens, asegura que "tenemos que encontrar un equilibrio apropiado entre el necesario control de la seguridad, por un lado, pero también preservar la privacidad, por el otro. Normalmente la tendencia es recopilar todo y luego analizarlo. Eso tiene algunas implicaciones negativas para la privacidad, porque estos datos que recogen las empresas para prevenir ciberataques podrían ser asimismo utilizados para otros propósitos.

## El uso de datos personales por parte de las empresas

Algunas empresas trabajan con herramientas de detección de amenazas y de monitorización que son muy potentes pero pueden introducirse vulnerabilidades en sus infraestructuras. El procesamiento de millones de datos en tiempo real o

"Big Data" es ahora posible gracias a los actuales ordenadores cada vez más inteligentes que además permiten determinar pautas, tendencias y patrones de comportamiento de cibercriminales y vaticinar posibles amenazas a partir del análisis de los datos.

Como los gobiernos cuando monitorizan a los ciudadanos bajo el argumento de la seguridad, las empresas tienden a recolectar todos los datos posibles para luego mirar los que les pueden ser útiles, insiste. "Debemos estar seguros de que

El ciudadano no hace nada, es la tecnología la que se encarga de garantizarle la seguridad.

estos datos no son indebidamente utilizados. Nos centramos en la recogida de los datos, pero muchas veces no nos centramos en cómo protegerlos también. Y estos datos podrían ser interesantes para otros", según Reinema.

Para 2020 predice que se habrán reducido los ciclos de detección de amenazas en las empresas con el uso de más cantidad de sistemas predictivos y analítica "inteligente" de seguridad que dispararán las alarmas mucho antes que ahora en caso de ciberamenazas. Ello dotará a las empresas de indicadores de ciberseguridad en tiempo real y agilizará la mitigación de ataques.

En torno a estos temas, resulta increíble "la idiotez" que uno detecta a veces, advierte por su parte Michael Schrage, del Centro de Negocios Digitales del Instituto Tecnológico de Massachusetts (MIT). Por un lado, se exige seguridad, pero paradójicamente por el otro, no se permite violar la privacidad

de la gente, añade. La cuestión aquí no tiene que ver con legislar o no, sino con los conflictos innatos entre unas normativas que compiten de forma inherente en sus objetivos y el propósito de garantizar una seguridad que, de algún modo "no infecte ni contamine otros valores". Esto, sin más, "no es sólo ingenuo sino un espejismo", precisa.

¿La tecnología cambia el comportamiento de las personas? ¿Cuál sería la mejor manera de promover la privacidad y la seguridad? ¿mediante nuevas soluciones tecnológicas o con el impulso de conductas diferentes? La mayoría defiende como clave del éxito la combinación de varias medidas. La solución tendría que pasar por la búsqueda de un equilibrio entre legislación, concienciación social y educativa, tecnología innovadora, etc.

Las regulaciones son importantes, asegura el vicepresidente de Constellation Research, **Steve Wilson**. Aunque en algunos países se discrepe, "por supuesto que las leyes cambian

---

**Michael Schrage** ▼  
Investigador del MIT Digital Lab.



# La solución tendría que pasar por la búsqueda de un equilibrio entre legislación, concienciación social y educativa, tecnología innovadora, etc.

el comportamiento de las personas a muy largo plazo", asegura. Para justificar sus argumentos pone de ejemplo los cinturones de seguridad en los vehículos cuyo uso obligatorio por ley impuesto en su día ha tenido mucho éxito a la hora de garantizar la seguridad en la automoción.

**Michael Schrage**, del MIT, precisa por su parte que la tecnología por sí misma es mucho más efectiva que cualquier ley que busque imponer determinados comportamientos incluso para la seguridad personal. Cita el caso de la tecnología que supone el "airbag" en los coches para proteger al pasajero en caso de accidente. Explica que el usuario no tiene que preocuparse de recordar si tiene que activarlo o no porque funciona automáticamente en caso de necesidad. El ciudadano no hace nada, es la tecnología la que se encarga de garantizarle la seguridad.

Añade que incluso ciertos pequeños defectos de la propia arquitectura de las tecnologías, incorporados premeditadamente por sus desarrolladores para activarse cada cierto tiempo garantizarían mejor, sin duda, la seguridad o la privacidad del usuario que muchas recomendaciones o leyes.

Si se pregunta a alguien, por ejemplo, que memorice una nueva contraseña cada seis semanas para

proteger así su identidad en internet, probablemente no será tan efectivo como la activación de algún tipo de mecanismo del propio sistema que cifre automáticamente las claves del usuario cada cierto tiempo para obligarle de ese modo a fijar unas nuevas por motivos de seguridad, agrega.

El libro "Nudge", traducido como "un pequeño empujón", al español, de los profesores Richard H. Thaler y Cass R. Sunstein, explica precisamente que se puede ayudar a la gente a tomar decisiones importantes de su vida con ese ligero codazo o empujón, como en este caso cifrar las contraseñas del usuario cada cierto tiempo, simplemente para forzar cariñosamente a cambiarlas.

**John Lyons**, de ICSPA, aprovecha el debate para destacar la importancia de la privacidad en internet no sólo para los ciudadanos sino también para las empresas y cuya trascendencia no debería subestimarse bajo el argumento de tener que anteponer otros requisitos como la seguridad, por supuesto también importantes. Advierte de que países de Sudamérica o algunos asiáticos, entre otros, podrían decantarse por los productos tecnológicos y por la innovación de determinadas áreas geográficas en el mundo, como Europa, por ejemplo, frente a otras, por el hecho de garantizar mayor compromiso con la privacidad en sus productos y servicios.



A portrait of Evan Wolff, a man with glasses and a light-colored shirt, smiling slightly. The background is a light, textured wall.

"Realmente no creo en la privacidad en internet. Creo que necesitamos autenticación más estricta para la privacidad y la seguridad en internet cuando sea necesario que así sea, pero cuando no, habría de prevalecer el anonimato"

---

**Evan Wolff**

Socio en Crowell & Moring.





## Prólogo de **Kevin Sale**

Especialista en Seguridad IT en la Universidad Abdullah de Ciencia y Tecnología.

### ● Los consumidores y los accionistas no parecen dar mayor importancia a la seguridad cibernética de una empresa.

**T**ras las filtraciones de datos que sufrieron Target y Home Depot, los clientes regresaron y el precio de las acciones de ambas empresas se elevó por encima de los niveles anteriores a esta violación de la seguridad. Ahora, algunos años después de estos hechos, ninguna de estas dos organizaciones parece sufrir ningún efecto negativo a largo plazo. La conclusión que extraigo de ello es que existen pocos incentivos que animen a las empresas a situar la seguridad cibernética en el centro de su estrategia organizativa.

Es necesario llegar a una situación en la que los consumidores basen sus decisiones de compra no solo en factores como el precio y el servicio al cliente, sino también en la actitud de las empresas respecto a la seguridad. Si se mentalizara a los clientes lo suficiente como para tener en cuenta la seguridad en sus decisiones de compra, esta impactaría directamente en las ventas. Así pues, las organizaciones de éxito e innovadoras deberían utilizar su seguridad como elemento diferenciador y, de esta manera, se produciría

una carrera armamentista entre organizaciones con la seguridad como argumento de venta.

Lograr que las fuerzas del mercado impulsen las mejoras en la seguridad no es un proceso rápido, pero, como todos los buenos proyectos de construcción, empieza por sentar una base sólida. El primer paso consiste en programas de educación pública masivos para informar a los consumidores acerca de cuestiones de seguridad básicas y del valor de sus datos. Deberíamos utilizar, para ofrecer educación sobre la salud digital de los ciudadanos, los mismos modelos de educación pública continua y coordinada que utilizan con éxito los gobiernos para informar al público de los peligros de fumar o de la propagación del VIH/SIDA. Actualmente, contamos con la Organización Mundial de la Salud; tomemos ejemplo y creemos la Organización Mundial de la Salud Digital. Una vez que el público adquiera una fuerte conciencia de su salud digital, tomará decisiones de compra y de estilo de vida basadas en el impacto para su salud digital y, en este momento, las fuerzas del mercado obligarán a las empresas a utilizar la seguridad como punto de venta.

A man with short dark hair, wearing a light-colored shirt with thin vertical stripes, stands with his arms crossed. He is smiling slightly and looking towards the camera. The background is a plain, light-colored wall.

**"Es necesario llegar a una situación en la que los consumidores basen sus decisiones de compra no solo en factores como el precio y el servicio al cliente, sino también en la actitud de las empresas respecto a la seguridad."**

---

**Kevin Sale**

Especialista en Seguridad IT en la Universidad  
Abdullah de Ciencia y Tecnología.



## Cómo mejorar la ciberseguridad

Los expertos proponen una serie de medidas en distintos ámbitos para ser adoptadas desde ya con el fin de mejorar la ciberseguridad global en el horizonte de 2020:

### 2.4

#### Cumplimiento de la Ley ▼

- ▶ Asegurar que las leyes tienen efecto sobre los cibercriminales.
- ▶ Castigar severamente a los ciberatacantes.

#### Industria tecnológica ▼

- ▶ Desarrollar sistemas de cifrado informático perfectos con computación cuántica.
- ▶ Reformar completamente los métodos de seguridad informática y el llamado Security Development Lifecycle (SDL) para garantizar la seguridad durante todo el desarrollo del *software*.

#### Educación ▼

- ▶ Ayudar a los ciudadanos a protegerse en el mundo digital como medida por excelencia más efectiva que podrían adoptar hoy los gobiernos.
- ▶ Definir claramente qué significa privacidad versus seguridad.

#### Legislación y regulación ▼

- ▶ Impulsar la estandarización normativa y las regulaciones internacionales para mejorar la seguridad en el desarrollo de *software* y uso de datos cuando comparten información los gobiernos, y con el "Internet de las Cosas".
- ▶ Garantizar el equilibrio entre seguridad pública y posibles intrusiones e interferencias económicas de los gobiernos teniendo en cuenta que previsiblemente aumentarán sus órdenes de acciones preventivas al incrementarse los riesgos ciberterroristas.

#### Empresas ▼

- ▶ Impulsar certificados de seguridad del *hardware* y *software* y estándares obligatorios por parte de las organizaciones internacionales en estrecha cooperación con las empresas y los gobiernos. Los productos digitales habrían de pasar "tests" de ciberseguridad.

- ▶ Mejorar el equilibrio entre la gestión del riesgo y de la seguridad.

#### Individuos ▼

- ▶ Intentar equilibrar el conflicto público en torno a una posible aproximación distinta a temas de privacidad y seguridad por parte de una próxima nueva clase social que buscará otras formas de vida.

#### Colaboración multipartita ▼

- ▶ Promover un internet más seguro desde la autenticación, reglas de comportamiento, etc, de modo similar a cuando se construyen carreteras para las que se exige más seguridad con leyes y cumplimiento de normas.
- ▶ Buscar fórmulas creativas para incentivar el fomento de la ciberseguridad con la colaboración entre gobiernos, industria, universidades, etc.

#### Piratas informáticos ▼

- ▶ Estar vigilantes ante una "inteligencia artificial" con un nivel superior en capacidades para dirigir mejor sus ataques a partir del acceso a información personal identificable (PII) de usuarios en la red.
- ▶ Mejorar la cooperación con el sector privado.
- ▶ Atribuir los ataques a la fuente. Actualmente los ciberataques resultan prácticamente gratis a los atacantes y la Justicia debería hacerles "pagar" por sus delitos.
- ▶ Mejorar las técnicas de autenticación y establecer protocolos. Las contraseñas son cosa del pasado. La biometría tiene índices de fallo que no son ni mucho menos triviales.
- ▶ Empezar a trabajar en una arquitectura de referencia de ciberseguridad, dotada de mayor resiliencia. Podría empezarse con la banca.
- ▶ Proteger eficazmente las conexiones al "Internet de las Cosas", esa conexión de todo con todo (vehículos, hogares, etc), que constituirá la mayor fuente de vulnerabilidades en el futuro.
- ▶ Incorporar la cibereducación en todos los grados formativos tecnológicos.
- ▶ Educar y capacitar a los desarrolladores de *software* en técnicas de programación segura.
- ▶ Cambiar mentalidades.
- ▶ Impulsar una red de autoridades de registro de identidad digital para ayudar a los gobiernos y compañías a reconocer quién está detrás de cada transacción digital. También, dotar a cada individuo de una identidad digital única para cada interacción virtual basada en conceptos de confianza.

- ▶ Proteger las infraestructuras críticas de los países como reto urgente.
- ▶ Aumentar progresivamente la regulación y colaboración internacional en ciberseguridad.
- ▶ Vigilar que las regulaciones tradicionales no limiten la innovación ni el crecimiento económico.
- ▶ Anteponer en las estrategias de ciberseguridad la capacidad de recuperación rápida y lo menos dolorosa posible teniendo en cuenta que es inevitable que pasarán cosas "malas".
- ▶ Ser más conscientes de la situación de la ciberseguridad y dotarse de mejores medios a la hora de compartir la información más sensible de la organización.
- ▶ Desarrollar una sólida tecnología de autenticación digital y gobernanza por parte de la industria y los gobiernos.
- ▶ Diferenciar de forma más segura los accesos cifrados y permitir un uso común de bases de datos detalladas más ampliamente compartidas.
- ▶ Apostar por el tiempo real al hablar de ciberseguridad.
- ▶ Integrar la formación en ciberseguridad personal dentro de la educación superior.
- ▶ Estar atentos ante un nuevo nivel de control tipo "Gran Hermano" o vigilancia por los gobiernos que pudiera provocar resistencia popular.
- ▶ Implementar regulaciones internacionales por parte de organizaciones como Naciones Unidas para ser ratificadas por los países como leyes locales.

# Conclusiones

Cap. 2 – La seguridad del internauta

► **Cualquier ciudadano**, sin tener que ser famoso ni especialmente relevante en la esfera social, política o económica, despierta mucho más atractivo de lo que uno pudiera imaginar entre los ciberdelincuentes. Todo internauta supone para los ciberatacantes una posible víctima a la que sacarle el dinero en algún momento dado. Teniendo en cuenta la presencia cada vez mayor de la población en internet las probabilidades del individuo convencional de ser atacado serán progresivamente mayores.

El auge de soluciones comerciales que permiten fabricar fácilmente y por muy poco dinero dispositivos electrónicos que pueden ser conectados a internet dispararán las probabilidades de cada individuo de ser objetivo de ciberataques pero al mismo tiempo de convertirse en potencial atacante. Técnicamente es posible, según los expertos.

El "Internet de las Cosas", con todo conectado a la red, está disparando la circulación de datos privados de las personas y asimismo facilita el acceso a los

misimos desde cualquier lugar a ciberdelincuentes que pueden planificar mejor así sus ataques.

La privacidad personal se está viendo mucho más espoléada en el mundo digital que en el físico. Entre otros motivos, por la facilidad con la que las nuevas tecnologías de procesado y análisis inteligente de información, que permiten cálculos en tiempo real con millones de datos, establecen correlaciones entre ellos y logran desvelar a partir de información previamente inconexa no sólo la identidad de las personas sino características íntimas de ellas, en detrimento de su seguridad, entre otros aspectos.

En el tema de la autenticación, para verificar que las personas que interactúan en la red son realmente quienes dicen ser y evitar robos de identidad por parte de cibercriminales, por ejemplo, los retos son muchos y pasan, entre otros, por estandarizar sistemas que permitan comunicaciones completamente seguras al tiempo que se garantiza la privacidad de los mensajes transmitidos, según los expertos.



Fundación  
Innovación  
Bankinter

[fundacionbankinter.org](http://fundacionbankinter.org)

### Corporate Security Surveillance - Three main pillars: to detect, to respond to, and to remediate cyber attacks

#### Monitoring & Detection

- Monitoring of IT and OT systems
- Advanced cyber intelligence and threat intelligence (e.g., log correlation, SIEM, vulnerability assessments)
- Support & Engineering for Cyber Defense Centers (C2C2)

#### Incident Response

- Threat intelligence, analysis & detection & cyber incident response
- Security incident investigation & analysis
- Security incident response & containment
- Security incident response & recovery
- Security incident response & eradication
- Security incident response & lessons learned





# La ciberseguridad del futuro

---

3

---

**Richard Parry**

Fundador en Parry Advisory.

Las nuevas amenazas y riesgos de seguridad a los que se enfrenta el ciberespacio afectan al mundo entero, además de a todos los estamentos económicos y sociales. "Todos estamos bajo su amenaza", aseguran los expertos. Por tanto, las soluciones deben ser globales con medidas interdisciplinarias desde todo tipo de ámbitos: gobiernos, instituciones, empresas, industria, legisladores, educadores, etc.

Los peligros que acechan en el ciberespacio, cada vez más cruentos, sofisticados y peligrosos, alcanzarán tales dimensiones en los próximos años que los países deben plantearse ya como atajarlos. Deberían sentarse a negociar seriamente de forma conjunta y buscar soluciones entre todos para atajar el problema. Los expertos coinciden en que se necesitan foros de debate mundial para hablar de ciberseguridad de modo similar a como se discuten otros problemas internacionales en reuniones mundiales de alto nivel, como el cambio climático o la energía.

Ciberdelitos, redes pornográficas en internet, tráfico de armas en la "Web Profunda" ("Deep Web") o ciberextorsión con consecuencias mortales para algunas víctimas son sólo algunas de las ciberamenazas que ganan peso en un mundo como internet, cada vez más lucrativo para los criminales. Como grandes riesgos para el futuro vislumbran los ciberataques a dispositivos conectados a internet (coches, marcapasos); la ciberguerra internacional; la exposición pública de

información privada (salud, datos financieros); el robo de la identidad digital (incluida la financiera); los bioataques (contra la propia persona); los ataques físicos desde internet (atracos, intrusiones domésticas) y la vigilancia masiva de los gobiernos.

"El Internet de las Cosas" acabará siendo "el Internet de Todas las Cosas", según los expertos. Prácticamente nada ni nadie quedará libre de conexión. Este mundo con accesos infinitos a internet abre oportunidades inmensas a los cibercriminales y el problema será inabarcable si no se implementan soluciones coordinadas y contundentes, que ayuden a combatir de forma global el cibercrimen, según los expertos.

Previamente, los países deberían disponer de un mapa que determine cuál es la situación real de la ciberseguridad en el mundo y las amenazas más urgentes que habría que combatir en el ciberespacio, un mundo indiscutiblemente vinculado al mundo físico.



Los expertos han elaborado una detallada hoja de ruta con diez propuestas para avanzar hacia ese objetivo de un ciberespacio más seguro. Los internautas tienen que sentirse seguros a la hora de realizar transacciones financieras, comunicarse sin miedo a poder ser extorsionados y sin temor a que sus datos personales puedan ser manipulados o utilizados con fines ilícitos, según los intervinientes.

Las ventajas de internet son incalculables. La revolución digital ha abierto sus puertas a un mundo lleno de beneficios y las sociedades deben garantizar que todo esto sea seguro. La protección al internauta honesto tiene que estar asegurada mientras que el cibercriminal tiene que ser castigado. Actualmente "los malos" disponen en la red de un mundo sin fronteras para navegar a sus anchas y atacar cualquier parte del mundo desde su casa con sólo un ordenador, muchas veces amparado incluso por su gobierno y por sistemas que no siempre están preparados legalmente para castigar a los culpables.

En su decálogo, los expertos proponen una batería de medidas muy diversas: cooperación internacional; en el ámbito de la seguridad de los productos, que sean seguros desde su propio diseño; tecnologías de autenticación que exijan varios requisitos para verificar la identidad del usuario; campañas educativas a la población para aprender a protegerse en el mundo *online*; formación a las empresas y a los legisladores para concienciar a la sociedad en un consumo digital seguro; protección de los datos nacionales, como los países hacen con las divisas más allá de sus fronteras físicas.

Asimismo, se exige a la industria un *software* de calidad y seguro, y que se garantice por Ley que sus desarrolladores serán penalizados como en cualquier otra industria si el producto no cumple unos requisitos de seguridad. Además, se insta a determinar estándares globales homogeneizados a nivel internacional con las características que debería tener ese *software* seguro, y a promover una estrategia de ciberseguridad global con un mandato claro a los gobiernos, además de aportaciones de recursos económicos suficientes para la ciberseguridad y el impulso de alianzas público-privadas nacionales e internacionales frente al ciberdelito.

Los expertos han elaborado una detallada hoja de ruta con diez propuestas para avanzar hacia ese objetivo de un ciberespacio más seguro.



## Prólogo de **Richard Parry**

Fundador en Parry Advisory.

- Cuando los auges inflacionistas alcanzan su máximo y, a continuación, comienzan a desplomarse, uno normalmente se encuentra con un exceso de cualquiera que fuera la materia prima subyacente.

Numerosos ejemplos ilustran la historia, tanto lejanos como recientes, ya sean tulipanes en 1637, empresas de tecnología en la caída de las puntocoms en el año 2000, o viviendas en 2008. Algunos argumentan que estamos viviendo el colapso de un auge inflacionario en materia de ciberseguridad; sin embargo, no vemos un exceso seguridad por ninguna parte, más bien al contrario. Pero estamos inundados de tecnología de seguridad. Vemos algo parecido a una quiebra del mercado perpetua.

A pesar de la abrumadora inversión del sector público y privado en soluciones de seguridad, de un mejor hardware, de la mejora de los métodos, de los foros internacionales de cooperación, y del compromiso de hacer más y de gastar más, la letanía de violaciones de la seguridad, de ataques exitosos de piratas informáticos y de intercepciones sigue sin disminuir.

Cada año, el capital tanto financiero como humano destinado a seguridad aumenta hasta el punto de empañecer el del año anterior, mientras que los políticos temen por un posible fallo sistémico deliberado a manos de individuos, causas y estados o naciones. Mientras tanto, los consumidores / ciudadanos acaban por resignarse ante la idea de que

no se puede hacer nada, y de que, además, todo está bien porque todo es cada vez más conveniente.

2016 puede ser el año de los despidos, ya que los Directores de los Servicios Tecnológicos y los Directores de los Servicios de Seguridad de la Información concluyen que, con más servicios de suscripción a herramientas y más velocidad de reacción, pero sin prevención, cada vez es menos probable que conserven su puesto, o incluso que lo conserve su Director Ejecutivo.

Puede que ahora la atención se desvíe hacia las consecuencias de una infraestructura diseñada para otro momento y propósito. No es suficiente con poner tiritas en heridas de bala. Tampoco lo es un alud de nuevas empresas que deben recompensar a sus inversores con unos ingresos continuos procedentes de servicios basados en suscripciones que no acaban de resolver el problema.

¿Qué valor tienen para nosotros nuestras comodidades basadas en Internet, y qué estamos dispuestos a hacer para seguir disfrutando de ellas? Quizás sea necesario que sean los fabricantes de estructuras, y sus operadores, quienes lideren el proceso.

# Una "hoja de ruta con diez propuestas"

---

3.1

01 [ver propuesta](#) ➤

Reducir los costes globales del cibercrimen

---

02 [ver propuesta](#) ➤

Garantizar la integridad de las infraestructuras y soluciones tecnológicas

---

03 [ver propuesta](#) ➤

Extender el uso de la tecnología de autenticación de doble factor

---

04 [ver propuesta](#) ➤

Educar a los ciudadanos en ciberseguridad básica

---

05 [ver propuesta](#) ➤

Concienciar al consumidor digital en la seguridad

---

06 [ver propuesta](#) ➤

Proteger los datos nacionales en internet más allá de las fronteras territoriales

---

07 [ver propuesta](#) ➤

Responsabilidad penal para el *software* inseguro

---

08 [ver propuesta](#) ➤

*Software* de calidad

---

09 [ver propuesta](#) ➤

Impulsar una estrategia de ciberseguridad global

---

10 [ver propuesta](#) ➤

Colaboración público-privada

---



## 01 ▼

## Reducir los costes globales de los ciberataques

El objetivo sería modificar el tradicional equilibrio de costes en el ámbito de la ciberseguridad que hasta ahora, lamentablemente, resulta mucho más rentable para los cibercriminales que para los ciudadanos digitales honestos.

A los ciberdelincuentes les cuesta muy poco desde el punto de vista económico y operativo actuar en internet, donde logran fácilmente sus objetivos sin apenas recursos, muchas veces, con un simple ordenador y perpetrando sus tropelías desde cualquier país remoto pero causando víctimas a causa de sus ataques en cualquier parte del mundo.

Por el contrario, protegerse y defenderse de ciberataques resulta muy costoso y complicado a las víctimas. Para resolver este injusto desequilibrio los expertos instan a trabajar conjuntamente a nivel internacional. Se requiere una imagen global del conjunto de actores que suponen una amenaza para la ciberseguridad en el mundo. Se necesita luchar más eficientemente contra el cibercrimen y se insta a dar el visto bueno a un estándar tecnológico común de ciberseguridad.

## Trabajar conjuntamente frente al cibercrimen

Se propone a las organizaciones actuar coordinadamente y no de forma individual frente a este problema, bajo el paraguas de alguna entidad no gubernamental, que permita difuminar riesgos de posibles represalias individualizadas por parte de ataques de cibercriminales.

Se plantea otorgar inicialmente ese papel líder a la Agencia Europea de Seguridad de las Redes y de la Información (Enisa) <https://www.enisa.europa.eu/>, una organización que actualmente ayuda a la

UE a equiparse y prepararse mejor para prevenir o responder a los problemas de seguridad de la información. La idea es que trabaje en colaboración con los Equipos de Respuesta ante Emergencias Informáticas (CERT) de los países, en donde se integran los expertos del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en sistemas de información de los estados.

Cuando los países actúan conjuntamente bajo la tutela de alguna organización, como sería Enisa, tienen más fácil mantenerse teóricamente al margen como diana u objetivo particular, en caso de alguna posible acción ofensiva contra ellos, según los expertos. Esta organización "paraguas" sería elegida de forma consensuada por sus miembros.

El éxito de las medidas vendría definido por la reducción del tiempo de exposición de las organizaciones a las amenazas, es decir, por la agilidad para la detección del ataque desde que se produce. Los retos serían aminorar los impactos e identificar a los criminales. También, la posibilidad de recuperación de las pérdidas causadas mediante la implementación de procesos judiciales.

Los desafíos pasarían por definir los términos de participación y colaboración de los países en este modelo de ciberprotección. El primer paso se daría en una mesa redonda para debatir el protocolo y la ejecución del plan.

Protegerse  
y defenderse  
de ciberataques  
resulta muy costoso  
y complicado a  
las víctimas.

## 02 ▼

# Garantizar la integridad de las infraestructuras y soluciones tecnológicas

Se insta a crear un estándar diferencial para el escrutinio de seguridad y promoverlo, así como la privacidad y la seguridad desde el diseño, es decir, aseguradas éstas desde el inicio del proceso de creación del producto, además de inculcarse transparencia y responsabilidad en valores corporativos.

La entidad que lideraría esta propuesta sería de nuevo Enisa <https://www.enisa.europa.eu/>, en colaboración con organizaciones ya establecidas, o sus equivalentes, y que comparten información sobre procesos de estandarización como la Organización Internacional de Normalización (ISO) <http://www.iso.org/iso/home.html> y asimismo con los ISAC <http://www.isaccouncil.org/memberisacs.html> o equivalentes, es decir, los centros que suministran información sobre ciberamenazas a infraestructuras críticas a las autoridades en EEUU.

El éxito de la iniciativa vendría determinado por la confirmación de la reducción de vulnerabilidades o CVE de los productos de las empresas que se comprometieran con estos estándares de seguridad. Asimismo por los niveles de participación de estas empresas y demostrando que las medidas adoptadas permiten reducir brechas de seguridad.

El estímulo de las empresas para unirse a la iniciativa sería importante dado que les permitiría probar ante sus clientes que sus productos son mejores que muchos de la competencia tras haber pasado una serie de pruebas de seguridad que lo corroboran, y a las que los de otras compañías no han sido sometidos o al menos de forma menos exhaustiva.

Uno de los retos de la propuesta tiene que ver con la aspiración de globalizar las soluciones. El objetivo

sería que todos los productos hubieran sido probados desde el punto de vista de la seguridad antes de salir al mercado, y también las infraestructuras. Cuando un nuevo software se hace tan popular que alcanza a una masa crítica, se deben tener garantías de que es seguro, señalan los expertos.

Para el impulso de esta propuesta habría de identificarse a un líder industrial a modo de "evangelista", que no sería tanto una organización sino otro tipo de entidad. El desafío exigiría colaboración por parte de varias entidades y no se podría llevar a cabo de forma independiente.

## Huir de trabas normativas

Lejos de procedimientos regulatorios que pudieran resultar excesivamente burocráticos, la implementación de la propuesta vendría impulsada por los propios mecanismos del mercado que incentivarían la demanda de ciertos productos una vez demostrado que permiten mayor seguridad. Se confía en los mecanismos del mercado y no tanto en decretos del Gobierno, según los expertos.

En el debate se ha destacado asimismo el papel prioritario de las empresas del sector asegurador a la hora de impulsar indirectamente niveles de calidad de la industria y la exigencia a las empresas

Crear un estándar del proceso de creación del producto, además de inculcarse transparencia y responsabilidad en valores corporativos.

Se plantea otorgar inicialmente ese papel líder a la Agencia Europea de Seguridad de las Redes y de la Información (Enisa), una organización que actualmente ayuda a la UE a equiparse y prepararse mejor para prevenir o responder a los problemas de seguridad de la información.

de cumplir unos niveles de seguridad para obtener una póliza, que las motiva para elevar sus estándares, explican.

### 03 ▼

## Extender el uso de la tecnología de autenticación de doble factor

---

Se pretende mejorar la seguridad de las transacciones *online* mediante tecnologías que verifican dos veces la identidad (2FA). Este tipo de técnicas exige al usuario además de la contraseña habitual algún otro identificador que corrobore que la persona es realmente quien dice ser.

Muchos bancos, por ejemplo, ofrecen esta tecnología para las transacciones de sus clientes

cuando les exigen confirmar una orden, más allá de claves o coordenadas, con los dígitos recibidos directamente en su móvil personal.

¿Cómo podría impulsarse el uso de esta tecnología? Se preguntan los expertos. La realidad no incentiva demasiado a algunas organizaciones para emprender solas este camino hacia la tecnología multifactor, más segura. Por tanto, deberían ser estimuladas a dar el salto juntas con un esfuerzo colectivo, y además amparadas por algún tipo de legislación.

La tecnología que finalmente se decidiera generalizar debería ser "agnóstica", suficientemente amplia. Debería fijarse además alguna fecha límite para su implantación por parte de las organizaciones.

Se propone que la medida fuera liderada por el Gobierno, en colaboración con los principales bancos centrales de los países y las compañías de tarjetas de crédito.

El foco se fijaría preferentemente en la industria financiera, sobre todo en los pagos digitales, debido al gran atractivo que supone para los cibercriminales este área al involucrar enormes cantidades de dinero.

¿Cómo se definiría el éxito de su implementación? Básicamente con métricas de uso, niveles de adopción pública, indicadores sobre la seguridad *online* que garantiza un sistema concreto y, especialmente, con mediciones sobre los ciberdelitos asociados a fraude penal.

## El reto de popularizar esta tecnología multifactor

Uno de los objetivos de la propuesta es conseguir que se extienda realmente el uso de esta tecnología 2FA. Ello exigiría un esfuerzo coordinado nacional pero también entre países, para implantarse de forma sincronizada por territorios concretos, por ejemplo, a nivel europeo. De ese modo, se evitarían desequilibrios regionales como consecuencia de que unos países agilizaran drásticamente su uso frente a otros.

La implantación de algún sistema de autenticación multifactor implicaría grandes desafíos en

Se pretende mejorar la seguridad de las transacciones *online* mediante tecnologías que verifican dos veces la identidad (2FA).

sectores muy concretos porque transformaría la forma de muchas empresas a la hora de llevar sus negocios. Por ejemplo el comercio minorista *online*, cuyo modelo de compra se basa en un "clic" sobre el producto.

Para generalizarse esta tecnología habría de identificarse en primer lugar qué grupos podrían hacer "lobby" para presionar juntos y concienciar al Gobierno y también a nivel internacional. Los grupos de presión podrían ser asociaciones de consumidores, industrias, etc. Habrían de animar a promover regulaciones y legislaciones que exigieran la implementación de esta tecnología más segura.

## 04 ▼

### Educar a los ciudadanos en ciberseguridad básica

---

En general, la población tiene escasos conocimientos sobre ciberseguridad y sobre cómo protegerse en internet. Habitualmente los ciudadanos velan menos por su identidad personal en internet que en su vida real, recuerdan los expertos.

Frente a ello, se propone promover campañas de educación dirigidas a la población para concienciarla globalmente sobre los riesgos de no protegerse en internet. Instan a que dicha misión esté a cargo de una ONG independiente, lejos del influjo directo de los gobiernos, que trabajaría en cooperación con ellos, sí, pero asimismo con las grandes empresas y la red académica, incluidos profesores de colegios.

## Concienciar desde la infancia

Es precisamente hasta ese nivel de escolares en edades muy tempranas hasta donde se quiere llegar con los mensajes que se lancen para concienciar de la necesidad de protegerse en el mundo virtual.

Las organizaciones involucradas en la puesta en marcha de la iniciativa actuarían de forma

voluntaria y conjuntamente, bajo el estímulo común de sentirse partícipes de la posible aceleración de una agenda de acciones. La clave de esta iniciativa sería precisamente dicha colaboración. alguna de las entidades involucradas lideraría el proceso de presionar para la implementación de las medidas.

¿Cómo llegar realmente a los ciudadanos con los mensajes? La percepción de lo que cada uno considera información privada varía mucho de país a país, de cultura a cultura. Difiere mucho también el grado de confianza en un gobierno o escuela dependiendo de cada sociedad o individuo. De ahí que se proponga a una organización no gubernamental independiente que lidere el proceso de intentar educar a la población en temas de ciberseguridad.

Es precisamente hasta ese nivel de escolares en edades muy tempranas hasta donde se quiere llegar con los mensajes que se lancen para concienciar de la necesidad de protegerse en el mundo virtual.

## Los medios de comunicación, el gran aliado

Los mensajes emitidos tendrían que ser muy sencillos. Muy accesibles al público. Fáciles de llegar a la gente. Para ello, se priorizarían las inversiones en canales de comunicación de uso habitual (televisión, juegos, etc.). También la radio e incluso el teléfono, con mensajes sobre cómo protegerse en la red, que escucharía el ciudadano y que permitirían ser oídos incluso en zonas remotas en donde el móvil es la única infraestructura de telecomunicación.

A veces, se diseñan webs muy bonitas con mensajes cuidadosamente elaborados, pero sin embargo poco productivas en su misión formativa para las que fueron concebidas, simplemente porque el usuario no sabe cómo llegar a ellas, advierten.

Para determinar el nivel de éxito de la implementación de la medida se propone algún tipo de valoración de impactos sobre el conocimiento general de la población a partir de algún nivel de referencia, así como métricas que determinen si la gente se maneja de forma segura en el mundo *online*.

Como retos se destaca la identificación del tipo de emisor en el que la gente confiaría, para asignarle la misión de comunicar los mensajes con los que se buscaría impactar al público e instarlo a protegerse. Asimismo habría de determinarse cuáles serían concretamente los canales apropiados para calar en la población.

Para arrancar con las acciones de concienciación global propuestas habría que desarrollar en primer lugar métodos y materiales educativos sobre ciberseguridad. Se debería diseñar asimismo algún plan de implementación, junto con indicadores para medir la evolución de la aplicación de las medidas.

Habría de disponerse de financiación a largo plazo, teniendo en cuenta que los ciclos formativos requieren continuidad para llegar a distintos grupos con consejos adaptados en cada fase a las nuevas



amenazas del momento, porque evolucionan imparables. Concienciarse de ciertos hábitos suele requerir tiempo y de ahí que las campañas educativas exijan inversiones prolongadas, añaden los expertos. Habría que identificar las carencias de cada colectivo en cuanto a conocimientos sobre ciberseguridad para focalizar mejor las acciones.

## 05 ▼

### Concienciar al consumidor digital en la seguridad

---

El objetivo es educar en ciberseguridad básica al consumidor para hacerle cambiar conductas de compra poco seguras en internet. La iniciativa habría de abordarse con un enfoque piramidal. Por un lado, con campañas educativas a la población, pero asimismo, a nivel superior, con medidas dirigidas a las empresas y los legisladores con la idea de contribuir a concienciar sobre ciberseguridad y con acuerdos internacionales a nivel institucional.

El objetivo es educar en ciberseguridad básica al consumidor para hacerle cambiar conductas de compra poco seguras en internet.

## La OMS, un modelo a seguir

Desde el punto de vista de la concienciación ciudadana, se plantea la creación de una entidad para liderar el proceso, que sería una versión "ciber" de la Organización Mundial de la Salud (OMS) <http://www.who.int/es/>. Se propone trasladar al ámbito de internet y al uso que hace la población de los productos y servicios tecnológicos la estrategia de trabajo de la OMS sobre prevención en temas de salud.

La idea sería concienciar a la sociedad de la necesidad de protegerse en el mundo digital y se haría con un modelo similar al de la OMS cuando intenta educar a los ciudadanos para tomar precauciones ante ciertas prácticas sexuales de riesgo y evitar el contagio de enfermedades como el sida.

La versión ciber de la OMS tendría como socios principales a las grandes empresas tecnológicas, tipo Google o Apple, pero también serían claves los medios de comunicación públicos como canal de transmisión de los mensajes con los que se quiere concienciar a la población.

La Organización Mundial de la Salud representa un modelo no opresivo. No se trata de una entidad reguladora ni obliga a nada. Simplemente contribuye a concienciar al público, señalan los expertos. Además facilita la coordinación de distintos de actores, y no sólo estatales, que precisamente son una minoría. En la entidad *ciber* planteada podrían incluirse expertos en ciberdelitos, centros de investigación, empresas y ONG.

Su estructura sería como la de la OMS, que cuenta con una red de organizaciones de investigación tanto públicas como privadas en distintos países que contribuyen al conocimiento de enfermedades, y que en este caso de la ciberseguridad aportarían información sobre vulnerabilidades informáticas.

Posteriormente, en el caso de la OMS, la organización distribuye esa información a los estados, que lanzan respectivas acciones educativas nacionales

# Desde el punto de vista de la concienciación ciudadana, se plantea la creación de una entidad para liderar el proceso, que sería una versión "ciber" de la Organización Mundial de la Salud (OMS).

para incrementar la concienciación pública sobre nuevas amenazas y para prevenir epidemias.

No se buscaría que el consumidor tuviera que entender sobre nuevos virus ni analizarlos técnicamente, sino sólo saber adoptar determinadas conductas, algunas estandarizadas, ante determinados indicios susceptibles de afectar a su ciberseguridad.

Como ejemplo de éxito de campañas de educación ciudadana, aunque en el ámbito de la salud, los expertos rememoran una iniciativa contra el sida en la década de los ochenta en el Reino Unido con enorme impacto social que se sirvió de todos los canales de comunicación disponibles para concienciar sobre los riesgos de ciertas prácticas sexuales.

Cuando al público se le dota de información suficiente se le capacita para tomar decisiones

rápidas más acertadas, explican los expertos. Por ejemplo, para decidir de forma sencilla sin poner en jaque su seguridad personal ni sus datos privados si sigue adelante con una transacción digital en función de los datos que posee.

La sencillez del contenido del mensaje que se quiera difundir es esencial para llegar con éxito a las masas, destacan. Se ha recordado también una antigua campaña muy popular en Australia para concienciar sobre el cáncer de piel y asimismo se ha destacado una actual iniciativa en Estados Unidos, bajo el lema "Stop. Think. Connect" <https://www.stopthinkconnect.org/> para concienciar sobre ciberseguridad.

## Las particularidades regionales requieren especial atención

Uno de los grandes desafíos de esta propuesta tendría que ver con la adaptación de los mensajes a las particularidades locales. La propia definición de privacidad varía enormemente en las distintas partes del mundo. Así, es muy distinto cómo ve la privacidad un chino respecto de un estadounidense o un británico. También es diferente el nivel de concienciación de unos y otros sobre cómo podrían utilizarse por terceros sus datos personales para lucrarse con ellos. Por eso, el mensaje para concienciar sobre ciberseguridad en una parte del mundo u otra del planeta debería ser distinto y adaptado a cada contexto concreto.

Conseguir cambiar el comportamiento del consumidor a la hora de elegir un producto u otro de acuerdo a los niveles de seguridad que aporta sería determinante a la hora de determinar el éxito o no de la iniciativa, según los expertos.

Por otra parte, se proponen indicadores de calidad en temas de ciberseguridad para identificar por ejemplo qué proveedores cumplen determinados requisitos. También se incluirían parámetros para medir la concienciación en ciberseguridad

La clave es que los productos y servicios digitales deberían ser seguros de por sí como factor indispensable para ser comercializados, comentan varios de los intervinientes.

para determinar si las medidas están siendo efectivas. El análisis sería a largo plazo teniendo en cuenta que lleva tiempo cambiar conductas.

El primer paso para esto sería lograr que el conjunto de las grandes empresas tecnológicas se comprometiera con este tipo de medidas. Habría que hacerles ver que es preferible que se sumen a esto de forma voluntaria porque, de lo contrario, el Gobierno podría imponerles en un momento dado cómo deben actuar.

## Mayor respaldo al consumidor en temas de ciberseguridad

Aunque el comportamiento del usuario tiene impacto directo en su seguridad y no es un tema que debería ignorarse, no habría de otorgarse responsabilidad única en el tema de la ciberseguridad ciudadana a la conducta de los individuos. La clave es que los productos y servicios digitales deberían ser seguros de por sí como

factor indispensable para ser comercializados, comentan varios de los intervinientes.

La seguridad por diseño debería estar garantizada. Se ha puesto el ejemplo de la seguridad en la industria del automóvil. El coche se comercializa con unos requisitos básicos de seguridad exigidos por ley. Otra cosa es que luego el consumidor elija libremente el modelo que mayor reputación tenga en temas de seguridad. El peso de la seguridad tendría que extenderse también a los vendedores sin poner todo el peso de la balanza en el consumidor.

## 06 ▼

### Proteger los datos nacionales en internet más allá de las fronteras territoriales

---

Este objetivo pone el foco en la protección de los datos, una "commodity" en esta nueva era digital, dado que se producen en masa. Su proliferación se debe al auge de tecnologías innovadoras y sensores conectados a la red, junto con la expansión del "Internet de las Cosas", que han disparado la circulación mundial de información y la accesibilidad a la misma en todo momento y lugar.

Los expertos instan a los países a ser capaces de preservar los datos que sean de su propiedad en el entorno sin fronteras que es internet, completamente global. Los estados necesitan comprender los límites digitales de su información y protegerla como hacen en el ámbito financiero con sus divisas, por ejemplo.

Se propone crear una entidad "ciber" que sería equivalente al Grupo de Acción Financiera para combatir el lavado de dinero (FATF) <http://www.fatf-gafi.org/> La idea sería extender a la protección de los datos el modelo utilizado por los países en esta entidad, cuando intentan mantener más allá de sus fronteras la integridad de su sistema financiero, independientemente de si su moneda se usa en Estados Unidos, Rusia o cualquier otro territorio.

## Quiénes integrarían este organismo "ciber"

Estaría formado por distintos países, por sus ciberorganizaciones; algunas de nueva creación y otras ya existentes. Sería clave la cooperación con las organizaciones internacionales de tecnologías de comunicación e información (ICT) y grandes empresas como PayPal, Amazon o Google, involucradas asimismo en transacciones financieras y muy interesadas en el enjuiciamiento de los cibercriminales.

Se insta a que los datos puedan ser monitorizados por el país que los posee o sus empresas más allá de los límites territoriales nacionales. El modelo del FATF es un ejemplo de buenas prácticas por parte de organizaciones relacionadas con temas de aplicación legal en la lucha contra el fraude financiero extraterritorial, según los expertos. Alegan que la experiencia en otras industrias puede contribuir a plantear propuestas en el ámbito de la ciberseguridad fáciles de debatir y susceptibles de ser implementadas rápidamente.

El éxito de las medidas planteadas en el ámbito de la preservación de datos vendría definido por el grado de participación de los estados en esa organización "ciber" equivalente al FATF. Asimismo por su tipo de acciones, ideas, etc. Los niveles de concienciación y prevención en protección de datos que se consiguiera impulsar sería también determinante. Para ello, habrían de establecerse previamente métricas de valoración del impacto de las medidas. El primer paso tendrían que darlo los propios países, apoyados por las grandes empresas tecnológicas internacionales.

## Los países son reticentes al intercambio de información

Los expertos advierten de que, en general, arrancar compromisos internacionales de los países para

Los expertos instan a los países a ser capaces de preservar los datos que sean de su propiedad en el entorno sin fronteras que es internet, completamente global.

trabajar conjuntamente en el ámbito de internet es muy complicado, y por supuesto también compartir datos, incluso para combatir el cibercrimen. De hecho, muchos estados lo patrocinan, como se ha destacado varias veces en el debate. Aunque la mayoría de los países se manifiesta públicamente en contra del cibercrimen, a la hora de la verdad muchos de ellos lo apoyan, lo que complica la idea de compartir datos. A ese problema se añade que algunos de los que sí luchan contra ese tipo de delitos no están todavía suficientemente preparados para intercambiar información ni involucrarse en nada parecido a nivel internacional.

## 07 ▼

### Responsabilidad penal para el software inseguro

El objetivo de esta medida es animar a que se legisle sobre responsabilidad penal en el caso del *software*. Se propone seguir el ejemplo de otras industrias en cuanto a responsabilidad legal en temas de seguridad.

Los expertos reconocen que es especialmente complicada su regulación por la complejidad para establecer parámetros globales de estandarización de lo que sería un *software* seguro y por la falta de coordinación internacional en este objetivo.

¿Cómo debería legislarse? Los intervinientes instan a mirar como ejemplo a otras industrias. Recuerdan que en ámbitos como la seguridad de los coches o en temas de contaminación, la gente va a la cárcel cuando incumple ciertas exigencias de seguridad en procesos de fabricación.

## La falta de indicadores de valoración de la calidad del *software*

Se necesitan métricas que permitan determinar y establecer objetivos para determinar con rigor si un *software* es realmente bueno o no y su seguridad. Asimismo, estándares legales frente a ciertos comportamientos. No tanto estándares técnicos sino "mejores prácticas", aunque admiten que es complicado determinar cuál debería ser el punto de referencia que marcara la frontera entre lo seguro o no en este ámbito del *software*.

Se advierte de que los "tests" actuales para comprobar su calidad "son insuficientes" y asimismo son "escasas" las verificaciones que se realizan antes de ser lanzados los programas al mercado o integrarse en nuevos sistemas dentro del llamado "Internet de las Cosas". Tampoco existe homogeneización, añaden los expertos.

Una legislación que exigiera responsabilidades penales en temas de seguridad del *software* contribuiría a reducir vulnerabilidades en los sistemas informáticos y su uso por grupos como los cibercriminales en beneficio propio. Desde el punto de vista de la implementación resultaría asimismo complejo determinar con rigor si las nuevas medidas serían o no exitosas en su propósito de poder confirmar en qué

medida contribuyen a reducir el número de ciberataques, advierten los participantes.

## El reto de la coordinación internacional de los gobiernos

Este objetivo resulta fundamental. Como en cualquier otro esquema de seguridad se necesitaría además una entidad encargada de implementar lo adoptado a nivel estatal. Esta autoridad para la ciberseguridad sería creada en cada país bajo norma parlamentaria, en el marco de la legislación nacional. Trabajaría en colaboración con la industria, la red académica y las entidades de estandarización. Cuando se dispone de procedimientos nacionales de actuación se está en disposición de pasar a la esfera de la coordinación internacional. De hecho, nada es tan internacional como el *software* e internet, recuerdan los expertos.

Se insta a que los datos puedan ser monitorizados por el país que los posee o sus empresas más allá de los límites territoriales nacionales.



Para que la propuesta se lleve a cabo se necesitaría "la típica cascada": un patrocinador político en el país concreto y hacer "lobby". Se requiere activismo para que las entidades existentes piensen distinto y sean algo más agresivas al respecto.

A largo plazo se augura un largo camino en el mundo de la ingeniería del *software*, con intensos debates sobre aspectos metodológicos, desarrollo de ciclo de vida de los programas o distintos lenguajes de programación.

## 08 ▼

### Software de calidad

El objetivo es alcanzar un acuerdo en el ámbito de la ingeniería para avanzar hacia un *software* de calidad. La medida sería liderada por alguna entidad ya existente, a la que se le otorgaría dicha competencia para promover un acuerdo en este sentido.

Si se preguntara a las asociaciones vinculadas a la industria informática cómo colaboran con la seguridad del *software*, probablemente dirían que están haciendo todo lo posible por mejorarlo desde el punto de vista de su ingeniería. Por ejemplo, pronunciando conferencias, escribiendo libros, etc. indican los expertos.

El objetivo de esta medida es animar a que se legisle sobre responsabilidad penal en el caso del *software*.

Se habla de cierta complacencia por parte de esos profesionales del *software* y de la informática, quienes probablemente disfrutaban mucho con conferencias y están haciendo una muy buena investigación, pero sin embargo no se interesan del mismo modo en lo que se refiere a crear legislación.

## Se necesita un acuerdo sobre qué significa ingeniería de *software*

Habría que alcanzar algún tipo de consenso o pacto con argumentos razonables que ayuden a decidir sobre especificaciones, requisitos, algún tipo de medida de referencia sobre ingeniería de *software*. Ello contribuiría a paliar dificultades en torno a la resolución de casos judiciales controvertidos a la hora de determinarse o no supuestos usos negligentes del mismo. Ciertas entidades profesionales deberían poner el foco de sus actuaciones precisamente en este objetivo de determinar qué es un *software* de calidad.

Se podrían tomar de referencia listas actuales con vulnerabilidades ampliamente aceptadas como las que publica SANS <https://www.sans.org/>, una organización sobre certificación de seguridad informática, para medir el éxito o no de las supuestas actuaciones. Podría mostrarse realmente si un producto concreto o algún tipo de implementación ha mejorado o no respecto a las 25 principales vulnerabilidades, por ejemplo. El gran reto sería la innovación.

Uno de los desafíos sería lograr una estabilidad en la ingeniería del *software*, aunque hay desacuerdo en el sector. No sólo se puede cambiar el código todo el tiempo, sino los lenguajes de programación continuamente. Por qué no dejar de sacar continuamente nuevos lenguajes y programar todo en uno solo, pero muy cuidado, se plantean los expertos. El primer paso para implementar las medidas exigiría cierto activismo que animara a las entidades profesionales a hacer algo diferente.

El objetivo es alcanzar un acuerdo en el ámbito de la ingeniería para avanzar hacia un software de calidad.

## 09 ▼

### Impulsar una estrategia de ciberseguridad global

---

Se observa mucha actividad a nivel de gobiernos en temas de ciberseguridad. Cada uno intenta hacer las cosas lo mejor que puede pero falta una estrategia global de todos ellos. Se insta a impulsar una iniciativa de este tipo que podría ser liderada por Naciones Unidas (ONU) <http://www.un.org/es/index.html>. Como socios claves estarían la Policía Internacional (INTERPOL) o la Oficina Europea de Policía (Europol) <https://www.europol.europa.eu/>. En los trabajos colaborarían otras entidades como los ISAC o el Foro Económico Mundial (WEF) <http://www.weforum.org/>.

### Se necesita un mandato claro a los gobiernos

Según los expertos, el primer paso sería disponer de una resolución a nivel global, que otorgara a los socios una orden clara de apoyo a los países para establecer sus propias estrategias y

ayudarles a implementarlas. Muchos países no lo tienen todavía claro. Algunos necesitan que se les exija ese compromiso. Sería fundamental además algún tipo de concienciación sobre la situación actual de la ciberseguridad para establecer las prioridades correctas.

El desafío sería atajar la falta de confianza entre las empresas, por un lado, y de los gobiernos, por otro. Es necesario crear una especie de "sentido de urgencia" así como mecanismos para establecer el nivel de confianza suficiente para entender este problema de dimensiones globales, en el que todos deben trabajar.

Uno de los elementos claves consistiría en ir reduciendo el foco de las prioridades a combatir. Lo fundamental sería hacer frente al ciberdelito, así como sus vinculaciones políticas y nacionales como ocurre en determinados casos. Esta lucha no debería limitarse al deseo de hacerlo sino que la estrategia habría de incluir asimismo inversiones de dinero, presupuestos específicos. Por ejemplo dirigidos a INTERPOL <http://www.interpol.int/es/Internet>, entre otras organizaciones.

¿Cuáles serían los pasos a adoptar? Habría que establecer los canales correctos con los gobiernos y también con el sector privado para crear una masa crítica en torno a estos problemas y concienciar de que es prioritario manejar esto. Se espera del sector privado que discuta cuál podría ser la organización para conseguir los objetivos marcados.

## 10 ▼

### Colaboración público-privada

---

Este tipo de alianzas son claves en el ámbito de la ciberseguridad. El sector privado habría de liderar dicha cooperación dado que es parte especialmente perjudicada en los ciberataques. ¿Quién sufre más daños? se preguntan los expertos. Los ciudadanos se pueden ver agredidos por el ciberdelito, por supuesto, pero las empresas son víctimas de pérdidas económicas millonarias.

Una de las claves de este tipo de cooperación sería mejorar el intercambio de información sobre seguridad de los distintos servicios de inteligencia.

Por eso, lo lógico es que fuera el sector privado el que liderara las alianzas, junto con los grandes vendedores de *software*, que juegan un papel importante en este ámbito. Y por supuesto con la colaboración del sector público.

Una de las claves de este tipo de cooperación sería mejorar el intercambio de información sobre seguridad de los distintos servicios de inteligencia. Esto no debería limitarse sólo a comunicar el número de incidentes diarios, que es algo muy abstracto, sino a facilitar información concreta de ciberproblemas que ayude a comprender cuál es la situación real de las amenazas. Una mejor comprensión de la situación real permitiría a todos priorizar mejor las medidas que se tuvieran que implementar.

Se necesita cooperación además para garantizar una mayor seguridad desde el diseño de los productos. Modelos, prototipos, con vistas a establecer unos estándares globales. Están surgiendo muchos de ellos a nivel local en distintas industrias aunque lejos de avanzarse en algo global.

Una iniciativa de este tipo que podría ser liderada por Naciones Unidas (ONU)

## Indicadores para valorar el éxito de la medida

Se necesitan datos que demuestren acciones coordinadas concretas: alguna operación conjunta, resolución de vulnerabilidades o el intercambio de información sobre problemas que suponen un desafío.

Cuanto mayores son los grupos de trabajo de los gobiernos, más abstracta suele ser la información que se plantean compartir con otros. Sin embargo, grupos más pequeños suelen tener mayor predisposición a intercambiar datos sensibles, y de ahí que sean más productivos, recuerdan los expertos.

Es fundamental hacer comprender a las partes implicadas que existe un verdadero beneficio para todos en ese objetivo de compartir información. Se trata de establecer confianza entre los distintos actores. Se advierte además de la conveniencia de no caer en regulaciones excesivas que pudieran matar la innovación antes de llegar a término.

El primer paso sería realmente apremiar al sector privado a que entendiera realmente el valor de todo esto. Hacerle ver que implica ventajas para todos. La puesta en marcha de la medida arrancaría con un enfoque a nivel nacional en cuanto a fortalecimiento de esas relaciones de confianza. Superada esa fase la implementación se llevaría a la esfera global.

# Conclusiones

Cap. 3 – La ciberseguridad del futuro

► **El ciberespacio** ha evolucionado exponencialmente en muy poco tiempo. Las tradicionales barreras contra el ciberdelito se han quedado completamente obsoletas. Los sistemas de defensa tipo ciberfortalezas o muros de contención para repeler ciberataques son cosa del pasado, porque los cibercriminales han saltado a otro nivel y utilizan técnicas significativamente sofisticadas para traspasar los sistemas informáticos aprovechándose de alguna vulnerabilidad o simplemente mediante ingeniosas técnicas persuasivas para robar datos personales o claves de usuarios. La protección por sí sola en internet ya no es suficiente porque los criminales lograrán atacar.

Lo fundamental ahora para protegerse es estar siempre vigilantes. Se requieren avanzados sistemas de monitorización de datos para detectar situaciones de alarma e identificar peligros en tiempo real para prevenirlos. Asimismo, herramientas y soluciones mucho más sofisticadas para frenar a tiempo las amenazas y tecnologías de última generación para reponerse cuanto antes en caso de ataques, entre otras muchas cosas. Pero por encima de todo, lo que se necesita es cooperación mundial.

Los expertos insisten en que el esfuerzo en esta gesta de la ciberseguridad tiene que ser colectivo. De hecho, en su decálogo de propuestas se anima a trabajar conjuntamente a todo un sinfín de actores: organizaciones internacionales que velan por la seguridad, equipos de respuesta ante emergencias informáticas; organizaciones de normalización y estandarización, centros nacionales que suministran información sobre ciberamenazas a los países, gobiernos, empresas, entidades financieras, grupos de presión (consumidores, industrias), legisladores, proveedores de internet, ciudadanos, tecnólogos, académicos, profesores, ONG, medios de comunicación, etc.

El desafío es mundial y el compromiso debe ser global. El reto es enorme, pero como dice un proverbio oriental: "Hasta el camino más largo comienza siempre con un primer paso".

# Ciberseguridad, un desafío mundial Predicciones

|              | Hogar ▼                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Ciudadano ▼                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Techin ▼                                                                                                                                                                                                                                                                                                                                                                                                           | Trabajo ▼                                                                                                                                                                                                                                                                                                                                                                    |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2015         | <ul style="list-style-type: none"> <li>Seguir optimizando mi vida. Reclamar más tiempo para mi mismo. Reducir mi distracción con las máquinas.</li> </ul>                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>Mejorar el intercambio de información alentando a las empresas a recortar los "indicadores de compromiso" de forma anónima.</li> </ul> <p>Proporciona un tipo de "sistema de aviso temprano" sobre ataques actuales, qué vulnerabilidades se están utilizando, etc. Ello permite a las empresas aplicar defensas donde es preciso.</p>                                      | <ul style="list-style-type: none"> <li>Educación: concienciar</li> </ul>                                                                                                                                                                                                                                                                                                     |
| 2015<br>2020 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>Para los niños: Del mismo modo que se le explica a un niño que no debe aceptar dulces de un extraño, también hay que explicarle que no debe aceptar golosinas virtuales de sitios web extraños.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                              |
| 2017         | <ul style="list-style-type: none"> <li>Montar una competición de ámbito nacional sobre un juego de simulación de ciberdefensa y ofensiva en China, y proporcionar formación certificada en línea para todo el mundo.</li> </ul>                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                              |
| 2018         | <ul style="list-style-type: none"> <li>MAGFA calificará automáticamente la calidad del software que utilizo.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                              |
| 2019         | <ul style="list-style-type: none"> <li>2FA y otros mejores métodos de autenticación mejoran la privacidad en línea.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                              |
| 2020         | <ul style="list-style-type: none"> <li>IoT hará que estemos más conectados y menos seguros, y no hay nada que hacer contra ello.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>Capacidad para hacer seguras las transacciones electrónicas informadas, sabiendo que tu transacción es segura y que tu información de identificación personal (PII) será tratada de forma adecuada.</li> </ul> <p>Un mundo conectado y seguro para un futuro mejor.</p> <p>Capacidad para tener una vida digital segura similar a la vida real (transparente, habitual, ...)<br/>(comercio electrónico, administración electrónica, ...).</p> <p>Proporcionar ventajas a los ciudadanos digitales a la vez que se incrementan los recursos y las dificultades para los delincuentes digitales.</p> <p>Mis hijos estudiarán ciberseguridad en la escuela.</p>                                                                                                                                                                                                                                                                                                               | <ul style="list-style-type: none"> <li>Innovación. Incremento significativo de normativas y mínimos obligados para las empresas hasta 2020. Organismos internacionales. Verificaciones anuales de diseño del software. Acciones ejecutivas gubernamentales. Las empresas de software e Internet estarán reguladas como lo están actualmente.</li> </ul>                                                            | <ul style="list-style-type: none"> <li>Desarrollar un grupo de práctica jurídica para llevar la acusación en litigios de ciberseguridad.</li> </ul> <p>Industria tecnológica: priorizar la seguridad en el desarrollo de software y ayudar a las empresas a conseguir ese objetivo.</p> <p>Abandonar mi chute de adrenalina diario, dejando de ver series continuamente.</p> |
| 2020<br>2025 | <ul style="list-style-type: none"> <li>Gustosamente dispondría de historia clínica electrónica. Registro de comidas / ejercicio físico / consultas.</li> </ul> <p>Soy pesimista en cuanto a un mañana mejor sin pasar por un todavía indefinido acontecimiento catastrófico tipo evento del cisne negro que obligará a MAGMA a replantear prioridades para un bien más amplio que los mantenga.</p>                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>Mejores estándares derivan en software más seguro pero pueden suponer una carga económica y burocrática para las PYMES. Organización internacional de ciberseguridad reconocida, que otorgará certificados obligatorios (conformidad de seguridad) y que garantizará que los productos de seguridad cumplen las directivas y estándares de seguridad aplicables.</li> </ul> | <ul style="list-style-type: none"> <li>Transformación de la industria del software. Los negocios serán más seguros.</li> </ul>                                                                                                                                                                                                                                               |
| 2025         | <ul style="list-style-type: none"> <li>La responsabilidad por la inseguridad hará del mundo en el que vivo un lugar ligeramente más seguro, y cabe esperar que transforme la brújula moral en las empresas y apoye a los consumidores.</li> </ul> <p>Internet será tan seguro para mí como un abuelo para mis nietos cuando todos seamos particularmente vulnerables a las ciberamenazas y todavía altamente dependientes de la red (dondequiera que elijamos estar en el mundo).</p> <p>Más + sueño de calidad.</p> | <ul style="list-style-type: none"> <li>Mejora de la ciberseguridad como resultado de cualquiera de sus acciones.</li> </ul> <p>Trabajo más leal, más eficiente, incluso más enganchado a la red por encima de cualquier otra cosa. El Ciberis se convertirá en la mayor amenaza a la estabilidad y la seguridad internacional.</p> <p>Aparecen nuevos medios de comunicación y sube el nivel educativo de la gente en todos los continentes.</p> <p>Los gobiernos dependerán más de los ciudadanos y serán más populistas. Campañas populistas de ámbito nacional amenazarán los sistemas políticos pero habrá más participación ciudadana.</p> <p>Los ciudadanos en línea serían menos vulnerables a las pérdidas financieras y a la vez se sentirían más seguros en su uso de Internet. Felices de realizar operaciones en línea, mediante dispositivos móviles con confianza, seguridad y protección.</p> <p>Mejor salud gracias al intercambio de datos médicos estadísticos y al creciente conocimiento.</p> |                                                                                                                                                                                                                                                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>Me sentiré como pez en una red invisible. La vida nunca me ha sido tan irreal como un juego.</li> </ul> <p>Iniciaré un sistema de enseñanza para futuros monjes o un campo de refugiados para los que necesitan encontrar su sitio espiritual y su sanación emocional.</p>                                                            |





