Fundación Innovación Bankinter

FTF Future Trends Forum

25 Resumen Ejecutivo

Ciberseguridad, un desafío mundial

- Los cibercriminales se han vuelto mucho más sofisticados, organizados y peligrosos en sus ataques con los que obtienen enormes beneficios económicos.

P. 7

- El riesgo de un ciberataque serio en alguna planta nuclear está aumentando dada la vinculación cada vez mayor de dichas infraestructuras a sistemas digitales.

P. 10

- El objetivo sería globalizar la medida, es decir, que la seguridad de todos los productos hubiera sido probada antes de salir al mercado.

P. 16

- Se insta a crear una entidad "ciber" inspirada en el modelo de la Organización Mundial de la Salud (OMS) para educar a los ciudadanos a tomar precauciones.

P. 19

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 **Dª. 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 Konfidas, 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


#FTFCybersecurity

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.

El 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, muchas veces amparados en sus tropelías por sus propios gobiernos que no los castigan ni persiguen.

Nuevas capacidades informáticas y una "inteligencia artificial" cada día más poderosa están permitiendo automatizar los ataques y dotarlos de dimensiones masivas mediante redes de ordenadores autocontrolables y capaces de tomar decisiones propias.

Ciberguerra, ciberespionaje, vigilancia masiva son amenazas 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

Khoo Boon Hui
Ex presidente de INTERPOL.

Cibercrimen, redes pornográficas en internet, tráfico de armas en la "Web Profunda" (*"Deep Web"*) o ciberextorsion con consecuencias mortales para algunas víctimas son sólo algunas de las ciberamenazas que ganan peso en internet.

Chris Meyer
Consejero delegado de Nerve LLC y Patrono de Fundación Innovación Bankinter.

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.

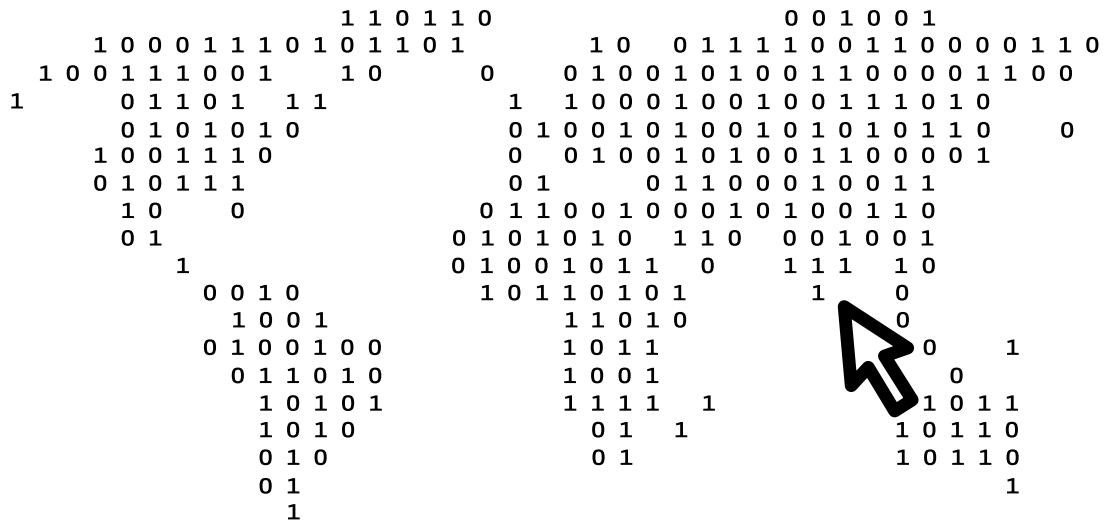
La industria de la ciberseguridad mueve presupuestos millonarios que crecen progresivamente. Anualmente este área moviliza entre 70.000 y 80.000 millones de dólares al año. Para el horizonte de 2020 las previsiones apuntan a que la cifra podría ser 2,5 veces mayor, según **Khoo Boon Hui**, ex presidente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

El ex presidente de INTERPOL forma parte de la treintena de expertos internacionales que ha 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, durante su vigesimoquinta edición, celebrada en Madrid en diciembre de 2015.

Coordinados por **Chris Meyer**, consejero delegado de Nerve LLC y Patrono de Fundación Innovación Bankinter, los participantes han dialogado durante dos días 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.

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.

De hecho, son enormes las pérdidas que causa ya 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.

"Todo crimen internacional es un crimen local en algún lugar", asegura el ex presidente de INTERPOL. Cada país debería aplicar legislación contra los cibercriminales en sus fronteras y cooperar a nivel internacional cuando los delitos vayan más allá. También se necesitan alianzas público-privadas para compartir conocimiento y experiencias en ciberseguridad, añade.

Cibercrimen, redes pornográficas en internet, tráfico de armas en la "Web Profunda" *("Deep Web")* o ciberextorsion con consecuencias mortales para algunas víctimas son sólo algunas de las ciberamenazas que ganan peso en internet.

Como mayores riesgos para el futuro se perfilan los ciberataques contra 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, según los expertos.

El *software* se come el mundo

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".

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

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

Fabio Assolini
Analista de la empresa Kaspersky.

El riesgo de un ciberataque serio en alguna planta nuclear está aumentando dada la vinculación cada vez mayor de dichas infraestructuras a sistemas digitales.

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

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".

"El *software* siempre tendrá vulnerabilidades", asegura **Fabio Assolini**, analista de Kaspersky. Los cibercriminales lo saben y se aprovechan. Frente a ello, anima a las empresas a garantizar la seguridad de sus productos a lo largo de todo su desarrollo, como muchas ya están empezando a hacer.

Los ataques serán cada vez más peligrosos, según los expertos. 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, como pronostica **John Lyons**, presidente ejecutivo y fundador de Alianza Internacional de Protección de Seguridad Cibernética (ICSPA) en el Reino Unido.

En los próximos años se verán asimismo conflictos bélicos en los que se combinará la presencia de humanos y armas autónomas o "inteligentes", señalan los intervinientes. Sin embargo, aún no parecen probables las guerras ciber-ciber, o de máquinas contra máquinas, con desenlaces significativos.

Los riesgos de conectar las infraestructuras críticas a internet

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 consciente de las cibervulnerabilidades a las que se exponen.

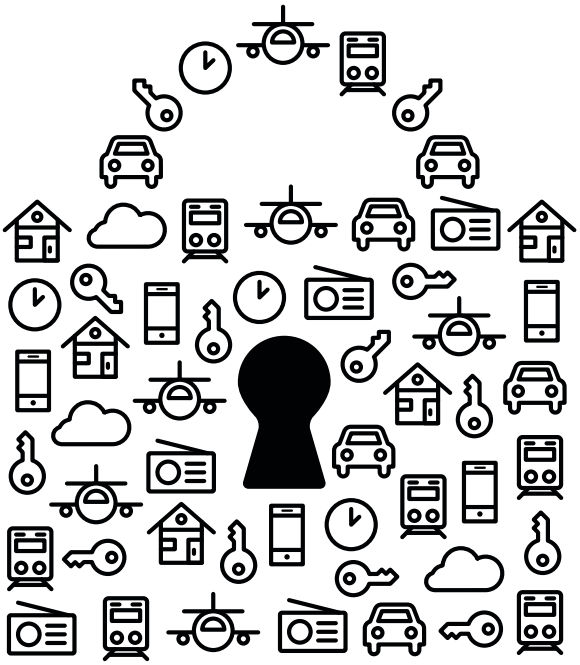
Así se desprende de un informe publicado en octubre de 2015 del Instituto de Relaciones Internacionales británico, conocido como Chatham House. **Caroline Baylon**, coautora de la publicación, ha advertido de que antes de 2020 podría producirse algún

cibermacroataque contra alguna red eléctrica que dejaría sin servicio a áreas importantes del país afectado durante al menos un día. Para ese mismo horizonte, añade, algún grupo terrorista podría juntarse con un equipo de ciberatacantes profesionales a los que pagarían por sus servicios para atacar alguna infraestructura crítica.

El "Internet de las Cosas" dispara las alarmas

El imparable fenómeno de conexión de todo con todo traerá inevitablemente sorpresas en temas de seguridad no siempre gratas, como ya está ocurriendo. Ningún sector parece librarse de la seducción de internet, coinciden los expertos. Cualquier ciudadano, sin tener que ser especialmente relevante en la esfera social, política o económica, despierta más atractivo de lo que uno pudiera imaginar entre los ciberdelincuentes. Determinados ámbitos serán 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 la red, bajo el riesgo de ser accesibles por cualquiera y poner en jaque la intimidad de sus dueños.

Frigoríficos inteligentes que informan al dueño cuando falta algo, automóviles autónomos y semiautónomos, que alertan al conductor si se está durmiendo, y un sinfín de dispositivos, como televisores, pulseras o relojes están ya conectados a internet. Cualquiera puede crearse fácilmente, por muy poco dinero, su propio dispositivo y conectarlo a internet. El problema de esta conectividad omnipresente es que "todos nos convertimos en posibles atacantes, y asimismo todos nos convertimos en posibles víctimas de ciberamenazas", asegura **Inbar Raz,** vicepresidente de PerimeterX. La seguridad de internet debería regularse como un servicio básico por el gobierno, como la electricidad, añade.



La autenticación de la identidad digital

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. Aunque existen atributos asociados a la identidad digital del individuo, estos pueden ser modificados, enmascarados e incluso sustituidos por otros de forma fraudulenta.

Drew Dean ▲
Director de Programas en SRI International.

Steve Wilson ▲
Vicepresidente de Constellation Research.

"Se necesitan protocolos de autenticación seguros para un futuro en confianza", asegura **Drew Dean**, director de programas en SRI International. Por su parte, el vicepresidente de Constellation Research, **Steve Wilson**, precisa que es una utopía pensar que en el mundo digital se pueden hacer negocios con cualquier extraño.

Privacidad versus seguridad

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) 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.

La seguridad de internet debería regularse como un servicio básico por el Gobierno.

Ciertos gobiernos recurren a técnicas de ciberguerra para espiar bajo el argumento de garantizar la seguridad ciudadana, según los expertos. En sus debates, han destacado las visitas de muchos de ellos a los mercados de venta de vulnerabilidades *0-day* para aprovecharse de esas "puertas traseras", que es como funcionan, para acceder a los sistemas informáticos y realizar vigilancia masiva. El problema de dar vía abierta a esas entradas es que también pueden utilizarlas los cibercriminales, según los ponentes.

Cómo avanzar hacia un mundo más seguro

De cara al 2020, los expertos confían en que se hayan logrado ciertos hitos en materia de ciberseguridad. Por ejemplo, la generalización de *software* seguro en la industria con unos estándares de calidad; mejores estrategias de seguridad en el trabajo; mayor protección para el consumidor y concienciación sobre ciberseguridad entre los estudiantes; un comercio digital seguro en todo tipo de transacciones; mejores técnicas de autenticación digital para garantizar la privacidad, por ejemplo, de los registros médicos; cooperación global y leyes internacionales que exijan el cumplimiento de penas por parte de los cibercriminales.

Mirando más allá, hasta 2025, se espera que las empresas se responsabilicen más y se apoye a los consumidores en temas de seguridad *online*. Sería deseable además que los gobiernos interactuaran virtualmente con mayor normalidad con el ciudadano. Para 2030, se habría de garantizar un consumo financiero seguro en la red, con ciudadanos menos vulnerables a posibles sabotajes.

Una hoja de ruta con diez propuestas

01 ver propuesta
Reducir los costes globales del cibercrimen

02 ver propuesta
Promover desde el diseño la seguridad y la privacidad en el software

03 ver propuesta
Generalizar la autenticación de doble factor

04 ver propuesta
Educar a los ciudadanos en ciberseguridad básica

05 ver propuesta
Concienciar al consumidor digital en seguridad

06 ver propuesta
Proteger los datos nacionales

07 ver propuesta
Exigir responsabilidad penal a los responsables de software inseguro

08 ver propuesta
Avanzar hacia un software de calidad

09 ver propuesta
Impulsar una estrategia de ciberseguridad global

10 ver propuesta
Colaboración público-privada

El objetivo sería globalizar la medida, es decir, que la seguridad de todos los productos hubiera sido probada antes de salir al mercado.

En su decálogo, los expertos proponen una batería de medidas muy diversas frente al ciberdelito: cooperación internacional; productos seguros desde su propio diseño; tecnologías de autenticación con varios requisitos para verificar la identidad; campañas educativas a la población para aprender a protegerse en el mundo *online*; formación para concienciar de un consumo digital seguro o protección de los datos nacionales.

Asimismo, se exige a la industria un *software* seguro y responsabilidades penales como en otras industrias en caso de fallos en la seguridad. También se insta a determinar lo que es un *software* seguro con estándares globales homogeneizados a nivel internacional, promover una estrategia de ciberseguridad global e impulsar alianzas público-privadas nacionales e internacionales frente al ciberdelito.

Las diez propuestas son las siguientes:

01
Reducir los costes globales del cibercrimen

Se insta a trabajar conjuntamente a nivel internacional bajo el liderazgo de Enisa, como organización "paraguas" que ayude a los participantes a difuminar la posibilidad de convertirse en objetivo de posibles represalias cibercriminales. Trabajaría en cooperación con los Equipos de Respuesta ante Emergencias Informáticas (CERT) de los países.

Los retos serían aminorar los impactos de los ataques e identificar a los criminales. También, la posibilidad de recuperación de las pérdidas causadas mediante la implementación de procesos judiciales de los culpables. 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.

02
Promover desde el diseño la seguridad y la privacidad en el software

Se insta a garantizar el cumplimiento de unos estándares claros de seguridad. La medida sería impulsada por Enisa, junto con entidades internacionales de estandarización y de vigilancia de ciberamenazas.

El objetivo sería globalizar la medida, es decir, que la seguridad de todos los productos hubiera sido probada antes de salir al mercado. Se exigiría colaboración de varias entidades. La implementación de la propuesta vendría impulsada por los propios mecanismos del mercado, lejos de burocracias legales.

Habría de identificarse a un líder industrial a modo de "evangelista". El éxito de la iniciativa vendría determinado por la reducción de vulnerabilidades de los productos comprometidos con estos estándares de seguridad.

03
Generalizar la autenticación de doble factor

Se trata de una tecnología con la que se verifica dos veces la identidad digital para aumentar la seguridad. Se promovería su uso por cada Gobierno, en colaboración con los bancos centrales y las compañías de tarjetas de crédito. El foco se fijaría preferentemente en la industria financiera, los pagos digitales, debido al gran atractivo que supone para los cibercriminales.

Se exigiría un esfuerzo coordinado nacional y también de los propios países para sincronizar su implantación. Eso evitaría desequilibrios regionales como consecuencia de que unos estados fueran más ágiles que otros. Habría que identificar qué grupos podrían hacer *"lobby"* para concienciar al Gobierno, también a nivel internacional para generalizar la tecnología multifactor.

04
Educar a los ciudadanos en ciberseguridad básica

Se proponen campañas de concienciación global de la sociedad. La medida sería liderada por una ONG en cooperación con los gobiernos, las grandes empresas y la red académica, incluidos profesores de colegios.

Se trata de una tecnología con la que se verifica dos veces la identidad digital para aumentar la seguridad.

La clave sería dicha colaboración. Alguna de las entidades lideraría el proceso de presionar para su implementación. Los medios de comunicación serían el gran aliado, con mensajes muy sencillos y accesibles al público. Asimismo, habría de disponerse de financiación a largo plazo, teniendo en cuenta que los ciclos formativos requieren continuidad.

05
Concienciar al consumidor digital en seguridad

Se insta a crear una entidad "ciber" inspirada en el modelo de la Organización Mundial de la Salud (OMS) para educar a los ciudadanos a tomar precauciones frente a ciertas prácticas de riesgo. Tendría como socios principales a las grandes empresas tecnológicas tipo Google o Apple, y también serían claves los medios de comunicación públicos en la labor de concienciación.

La OMS representa un modelo de organización no opresivo. No se trata de una entidad reguladora ni obliga a nada. Además facilita la coordinación de distintos de actores y no sólo estatales, señalan los expertos.

Uno de los grandes desafíos 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.

06
Proteger los datos nacionales

Se propone implantar una entidad "ciber" intergubernamental con un modelo equivalente al del Grupo de Acción Financiera para combatir el

lavado de dinero FATF cuyos países buscan mantener su integridad financiera más allá de sus fronteras.

Este organismo "ciber" estaría formado por distintos países, por sus ciberorganizaciones; algunas de nueva creación y otras 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 los países a ser capaces de preservar los datos que sean de su propiedad en el entorno sin fronteras que es internet. Los estados necesitan comprender los límites digitales de su información y protegerla como hacen en el ámbito financiero con sus divisas, por ejemplo. El primer paso tendrían que darlo los propios países, apoyados por las grandes empresas tecnológicas internacionales.

07
Exigir responsabilidad penal a los responsables de software inseguro

Establecer unos estándares legales en cuanto a seguridad del *software*, impulsados por una autoridad para la ciberseguridad creada bajo norma parlamentaria en cada país, junto con la industria, red académica y entidades de estandarización.

Se propone seguir el ejemplo legal que se impone en otras industrias. Se recuerda 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.

Se necesitarían métricas y parámetros concretos para determinar con rigor si un *software* es realmente seguro o no. La coordinación internacional de los gobiernos sería fundamental. En cada país se necesitaría un patrocinador político, y hacer *"lobby"* y "activismo".

08
Avanzar hacia un software de calidad

Se insta a estandarizar unos requisitos y especificaciones concretas sobre calidad del *software* tras lograr algún pacto sobre su ingeniería. La propuesta sería implementada por alguna entidad ya existente, a la que se le otorgaría dicha competencia.

Para demostrar si un producto o implementación ha mejorado podrían tomarse de referencia listas actuales con vulnerabilidades ampliamente aceptadas como las que publica SANS.

Uno de los desafíos sería lograr una estabilidad en la ingeniería del *software*, aunque hay desacuerdo en el sector. Se exige cierto "activismo" que anime a las entidades profesionales a hacer algo diferente a lo de ahora.

09
Impulsar una estrategia de ciberseguridad global

Se exige un mandato claro de dicho compromiso a los gobiernos con algún tipo de resolución en ese sentido. La iniciativa sería liderada por la ONU, junto con INTERPOL o Europol como socios claves. Colaborarían con otras entidades como los ISAC o el Foro Económico Mundial (WEF).

El desafío sería atajar la falta de confianza en el ciberespacio de las empresas y los gobiernos, mediante mecanismos para ganar confianza y entender que hay que trabajar de forma urgente

Se insta a crear una entidad "ciber" inspirada en el modelo de la Organización Mundial de la Salud (OMS) para educar a los ciudadanos a tomar precauciones frente a ciertas prácticas de riesgo.

todos juntos contra el cibercrimen, un problema de dimensiones globales. Las estrategias habrían de incluir presupuestos específicos. Por ejemplo dirigidos a INTERPOL, entre otras organizaciones.

10
Colaboración público-privada

Esta cooperación sería liderada por el sector privado como víctima de pérdidas millonarias por el ciberdelito, acompañado de los grandes vendedores de *software*, y con la colaboración del sector público.

La cooperación sería clave para mejorar el intercambio de información sensible. No debería limitarse a incidentes diarios, que es algo muy abstracto, sino a datos concretos de ciberproblemas.

También se insta a garantizar una mayor seguridad desde el propio diseño de los productos, y establecer estándares globales mediante modelos, prototipos, etc. El primer paso sería apremiar al sector privado a que entendiera realmente el valor de todo esto. Hacerle ver que implica ventajas para todos.

Conclusiones

El ciberespacio ha evolucionado exponencialmente en muy poco tiempo. Las tradicionales barreras contra el ciberdelito se han quedado completamente obsoletas. Los cibercriminales han saltado a otro nivel y utilizan técnicas significativamente más sofisticadas para traspasar cualquier sistema informático.

Esta nueva fase en la ciberseguridad exige para defenderse sistemas de monitorización de datos para detectar situaciones de alarma e identificar peligros en tiempo real para prevenirlos. Asimismo, herramientas mucho más sofisticadas para frenar a tiempo las amenazas, tecnologías de última generación para reponerse cuanto antes de los ataques y sobre todo cooperación internacional. El desafío es mundial y el compromiso debe ser global.

Ciberseguridad, un desafío mundial Predicciones

	Hogar	Ciudadano	Techin	Trabajo
2015	Seguir optimizando mi vida. Reclamar más tiempo para mi mismo. Reducir mi distracción con las máquinas.		Mejorar el intercambio de información alentando a las empresas a recortar los "indicadores de compromiso" de forma anónima. 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.	Educación: concienciar
2015 2020		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.		
2017	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.			
2018	MAGFA calificará automáticamente la calidad del software que utilizo.			
2019	2FA y otros mejores métodos de autenticación mejoran la privacidad en línea.			
2020	IoT hará que estemos más conectados y menos seguros, y no hay nada que hacer contra ello.	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. Un mundo conectado y seguro para un futuro mejor. Capacidad para tener una vida digital segura similar a la vida real (transparente, habitual, ...) (comercio electrónico, administración electrónica, ...). Proporcionar ventajas a los ciudadanos digitales a la vez que se incrementan los recursos y las dificultades para los delincuentes digitales. Mis hijos estudiarán ciberseguridad en la escuela.	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.	Desarrollar un grupo de práctica jurídica para llevar la acusación en litigios de ciberseguridad. Industria tecnológica: priorizar la seguridad en el desarrollo de software y ayudar a las empresas a conseguir ese objetivo. Abandonar mi chute de adrenalina diario, dejando de ver series continuamente.
2020 2025	Gustosamente dispondría de historia clínica electrónica. Registro de comidas / ejercicio físico / consultas. 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.		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.	Transformación de la industria del software. Los negocios serán más seguros.
2025	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. Internet será tan seguro para mi 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). Más + sueño de calidad.	Mejora de la ciberseguridad como resultado de cualquiera de sus acciones. Trabajo más leal, más eficiente, incluso más enganchado a la red por encima de cualquier otra cosa.El Ciberisis se convertirá en la mayor amenaza a la estabilidad y la seguridad internacional. Aparecen nuevos medios de comunicación y sube el nivel educativo de la gente en todos los continentes. 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. 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. Mejor salud gracias al intercambio de datos médicos estadísticos y al creciente conocimiento.		Me sentiré como pez en una red invisible. La vida nunca me ha sido tan irreal como un juego. 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.


Fundación
Innovación
Bankinter
fundacionbankinter.org