La SEI
School of Economic Intelligence & International Relations
Escuela de Inteligencia Económica y RRII
Universidad Autónoma de Madrid

01/2021

Vol. 3, n 2, pp. 11 - 23
ISSN 2659-9805
Editor in-Chief: Javier Oubiña

JOURNAL OF ECONOMIC & BUSINESS INTELLIGENCE

Universidad Autónoma de Madrid UAM

CIBERSEGURIDAD POSTCOVID: ¿QUÉ PAPEL JUGARÁ LA CIBERINTELIGENCIA FRENTE A LOS CISNES NEGROS DIGITALES QUE LLEGARÁN TRAS LA VACUNA?

José Manuel Vera*

Resumen

Quizá nada vuelva a ser igual. Se calcula que más del 40% de los trabajadores no volverán a pisar la oficina tras la Covid-19 y un 80% de los consumidores han descubierto la comodidad del comercio en línea. Los pilares del mundo que conocíamos han caído y el tsunami digital que estaba comenzando a levantarse ha cobrado metros de vida en solo unos meses de pandemia y confinamiento. Y esa carrera hacia un torbellino digital de consecuencias aún insospechadas ha hecho que la ciberseguridad también haya visto quebrantada sus principios esenciales. El perímetro, que nos suponía siempre a salvo, ha caído y las ciberamenazas se multiplican exponencialmente aprovechando fallos que se consideraban superados. Es lo que ha supuesto la explosión del teletrabajo.

Frente a esa nueva situación, la ciberinteligencia, como principal fuente para anticiparse a los incidentes, también ha cobrado un especial protagonismo de la mano de conceptos veteranos, aún por madurar, como los equipos de respuestas a incidentes. La inminente llegada de las redes 5G, y la aplicación intensiva de la robotización, la tecnología cuántica y la Inteligencia Artificial, precisarán de anticipación y proactividad. Por ello, muchos ven en la inteligencia económica y la ciberinteligencia unas herramientas imprescindibles para lograr resiliencia digital ante todo tipo de ciberamenazas, quizá incluso, ante los nuevos cisnes negros digitales que llegarán.

Palabras clave: Ciberseguridad, Covid-19, Seguridad de la Información, CISOs, protección digital, ciberinteligencia, Inteligencia Artificial, Enisa, Red Team, CSIRTs, SOC.

Abstract

Maybe nothing will be the same again. It is estimated that more than 40% of workers will not set foot in the office after Covid-19 and 80% of consumers have discovered the convenience of online commerce. The pillars of the world that we knew have fallen and the digital tsunami that was beginning to rise has claimed meters of life in just a few

* Periodista, Revista SIC (Ciberseguridad, Seguridad de la Información y Privacidad). El autor quiere mostrar un agradecimiento especial, por su colaboración, a Luis Fernández, José de la Peña y Ana Adeva de Revista Sic.

months of confinement. And that race towards a digital whirlwind of still unsuspected proportions has meant that cybersecurity has also seen its essential principles broken.

The perimeter, which always assumed us safe, has fallen and cyber threats are multiplying exponentially, taking advantage of bugs that were believed to be corrected. This is what the explosion of teleworking has meant. Faced with this new situation, cyber intelligence, as the main source to anticipate incidents, has also taken on a special role in the hands of veteran concepts, yet to mature, such as incident response teams (CERT / CSIRT). The imminent arrival of 5G networks, and the intensive application of robotization, quantum technology and Artificial Intelligence, will require anticipation and proactivity. For this reason, many see cyber intelligence as an essential tool to achieve digital resilience against all types of attacks and possible cyber threats maybe even, one day, before digital black swans.

Key words: *Cybersecurity, Covid-19, Information Security, CiSOs, digital protection, cyberintelligence, Artificial Intelligence, Enisa, Red Team, CSIRTs, SOC.*

1. Mundo hiperconectado… y vulnerable

Pocos conceptos son tan apasionantes para la inteligencia y, su rama más tecnológica, la ciberinteligencia y la economía como el de los cisnes negros. Presentado por Nassim Taleb, en 2007, en el libro del mismo nombre, se identifica con los "hechos fortuitos caracterizados por tener un efecto sorpresa, así como la imposibilidad de calcular las probabilidades de su ocurrencia y su repercusión a largo plazo "Lógicamente una pandemia, un ciberataque a nivel mundial o que una tormenta solar nos deje sin comunicaciones no lo son, porque son previsibles, pero lo cierto es que a lo largo de la historia se han identificado muchos como la I Guerra Mundial o los atentados contra las Torres Gemelas. Por supuesto, muchas de las grandes innovaciones que han revolucionado la historia pueden ser consideradas como tal.

Precisamente, el mundo que quedará tras la Covid-19 puede dar lugar a buen número de cisnes negros digitales, fruto de usar una tecnología de forma intensiva sin un conocimiento previo de sus consecuencias ni una higiene de seguridad básica. Frente a los que piensan que el mundo está preparado para garantizar la protección de personas y usuarios ante la popularización de las redes 5G, la Inteligencia Artificial y el Internet de las Cosas (IoT) -al que seguirá el Internet de las Personas (IoP)-, está el reducido grupo de profesionales que vive en su día a día una carrera sin freno para hacerlos seguros. Entre ellos están desde los responsables de ciberseguridad (CISOs), hasta investigadores y especialistas técnicos (hackers), responsables de tecnología (CIO), de privacidad (DPD), entre otros, trabajando al límite para evitar fallos que comprometan empresas, países y consumidores. Pero no pinta bien, según datos de la UE (2020), para 2025 estarán conectados en el mundo 25.000 millones de dispositivos. O, dicho de otra forma, cada ciudadano tendrá, de media, cuatro dispositivos conectados. Algo preocupante teniendo en cuenta que, a enero de 2021, no existe estándar nacional o internacional alguno que obligue a fabricarlos, usarlos y darlos de baja con unos mínimos estándares de seguridad, aunque en EE.UU. y Europa está previsto aprobarlos en breve. Sobre todo, en sectores críticos, ya que se considera que el número global de conexiones industriales de IoT alcanzará los 83.800 millones en 2025, desde los 17.700 millones en 2020, según Juniper Research (2020). Algo preocupante teniendo en cuenta que "o se hace con privacidad y seguridad" o la vida de los "milenial y no milenial domotizados terminará siendo como la de esos ratones de laboratorio en la que todo está dirigido para hacerlos crecer sanos y felices para luego poder hacer experimentos con ellos", alertó el profesor Jorge Dávila (2019), hablando de los retos de la IoT y la seguridad actualizable.

1.1 Carrera a contrarreloj

Por eso, regiones como EE.UU. y, también Europa, están en una carrera frenética para poner en marcha leyes que reduzcan la amenaza que representan estos dispositivos, incluso, dotados de cierta inteligencia. El mundo conectado brindará a los delincuentes y piratas informáticos mayores oportunidades para lanzar ataques y causar interrupciones al incrementar la superficie para hacerlo.

Precisamente, este crecimiento será facilitado por la incipiente tecnología 5G -que según Marko Milijic (2019), de Leftronic se ofrecerá en un 40% del mundo para 2024. Ya se ha visto en los primeros meses de la Covid-19. "Los delincuentes no han dejado pasar la oportunidad y muchos de los incidentes que se vienen observando desde el inicio de la pandemia están relacionados directamente con una mala implementación de las políticas de seguridad y de una configuración incorrecta de los accesos remotos o los permisos

de los usuarios en una red corporativa", destaca el responsable de concienciación y laboratorio de Eset, Josep Albors (2020). "Con las transferencias de datos de alta velocidad, los piratas informáticos tendrán la capacidad de infectar paquetes de datos y realizar espionaje corporativo sin que se den cuenta. Eso es hasta que las empresas cambien su enfoque para estar atentos a esos intentos de violación maliciosos. Se requerirán niveles mucho más altos de seguridad y de monitorización una vez que 5G se convierta en la forma estándar de transferencia y comunicación de datos basada en la nube", destacan los expertos.

En su informe 'Future Series' (2020) el Foro Económico Mundial (WEF), destacó la creciente amenaza de los riesgos ocultos y sistémicos inherentes al entorno tecnológico emergente, que requerirá de un uso intensivo de la Inteligencia y un cambio significativo en la respuesta de las comunidades internacionales y de seguridad a la ciberprotección. Los días de la seguridad fragmentada han quedado atrás y la protección digital debe ser más proactiva y preparada para el futuro si queremos superar en innovación a los atacantes. "Las transformaciones tecnológicas críticas de las que depende la prosperidad futura (conectividad ubicua, inteligencia artificial, computación cuántica y enfoques de próxima generación para la gestión de identidades y accesos) no serán solo desafíos incrementales para la comunidad de seguridad", recuerda el WEF que al tiempo pide que "la transformación impulsada por la tecnología y las inversiones en ciberprotección deben avanzar juntas en este contexto", puesto que "las falsificaciones profundas ya se han aprovechado para crear nuevos vectores de ciberataques y se ha utilizado software de imitación de voz en robos importantes".

1.2 Sin fuerza laboral

Y a la incertidumbre que generarán las nuevas tecnologías se sumará la alarmante falta de personal cualificado para ofrecer suficiente ciberseguridad a ese mundo hiperconectado. Se calcula que, en los próximos años, habrá un déficit de hasta 3,5 millones de profesionales en ciberprotección. Una cantidad suficiente para llenar 50 estadios de la NFL, según Cybersecurity Ventures (2019), una cifra preocupante teniendo en cuenta que Cisco aseguró, en 2014, que ya rondaba el millón. Por eso, organizaciones como ISC², la europea Enisa o el NIST estadounidense, a través de su marco de trabajo Nice, creen que puede ser un factor determinante para esta década en favor de los ciberdelicuentes y han puesto en marcha diferentes iniciativas para formar más profesionales y retener a los que ya trabajan en el sector.

2. El Tsunami digital que está llegando

2020 pasará a la historia como el punto de partida de la carrera digital. Para los que tenían dudas de apostar por la automatización, la nube, la inteligencia artificial y la fuerza laboral 'líquida', fuera de la oficina, la Covid-19 ha quitado una venda que muchos no querían retirar. De hecho, el 62% de las empresas ha confesado recibir más ataques desde el comienzo de la pandemia, según datos de Deloitte (2020). Es más, se han incrementado en sectores tan vulnerables, en estos momentos, como el de la Sanidad, donde varias organizaciones han sufrido robos de información y ransomware (software malicioso que secuestra un dispositivo a cambio de un rescate) inutilizando sus sistemas.

Ello ha motivado que el 81% de las empresas aceleren sus procesos de modernización de TI debido a la pandemia. El 48% ha relanzado sus planes de migración a la nube y el 49% los de modernización de TI debido a la Covid-19. Según un informe de McKinsey & Company (2020), el 70% de los CISO también planean solicitar aumentos significativos en los presupuestos de ciberseguridad en 2021.

"Las conciencias de los riesgos cibernéticos están creciendo y más empresas están asignando recursos a la gestión de riesgos cibernéticos", explica el director de tecnología de NordVPN Teams, Juta Gurinaviciute (2020). Aun así, el gasto en ciberseguridad está lejos de donde debería estar, dada la escala monumental y la urgencia de la amenaza". Por ello, "se nos ciernen nubarrones de vigilancia digital, no ya sólo por la dichosa pandemia sino, además, por ese elefante que estrena cacharrería irrumpiendo desbocado en un tsunami telelaboral aún sin contornear", destacó el siempre incisivo editor de Revista SIC, Luis Fernández (2020), en la Revista Sic, la publicación, con casi 30 años, de referencia en ciberseguridad y privacidad en España.

2.1 Ciberpandemia por Covid-19

Quizá la pandemia pase, pero la que se quedará será la pandemia cibernética fruto de conectarlo todo y a todos sin una mínima seguridad. La Covid-19 no ha hecho sino agudizar el preocupante estado cibernético mundial. En su "Informe de riesgos globales 2020", el Foro Económico Mundial (WEF), establece que el cibercrimen será el segundo riesgo más preocupante para el comercio mundial durante la próxima década, el séptimo riesgo con mayor probabilidad de ocurrir y el octavo con mayor impacto.

De hecho, se calcula que, durante 2020, dos de cada cinco personas sufrieron problemas de ciberseguridad, en muchos casos motivados porque un 40% de los trabajadores cambiaron la oficina por el teletrabajo. Ello dio lugar a una carrera de los departamentos de TI y ciberseguridad por proteger millones de conexiones 'sacadas' fuera del entorno corporativo casi de un día a otro. Es más: en muchas ocasiones a través de dispositivos personales, de casa, sin la más mínima protección y compartidos con todo tipo de archivos y aplicaciones personales. Por eso se calcula que dos de cada seis empresas sufrieron ciberataques con éxito durante el confinamiento y los meses posteriores, según Deloitte (2020). Y todo parece evidenciar que esto no ha hecho más que comenzar.

En diciembre de 2020, la compañía SolarWinds[12] cuya plataforma usa la Administración estadounidense, el Fortune 500 y, por supuesto, el IBEX 35, descubrió que, precisamente durante los peores meses de la pandemia, había sido atacada, presuntamente, por un estado-nación, con un nivel de sofisticación pocas veces visto, para instalar software malicioso en una actualización validada por la empresa y cuyos clientes llevaban usando desde hace primavera. Sus consecuencias serán uno de los temas que, si transcienden, más dará que hablar en 2021.

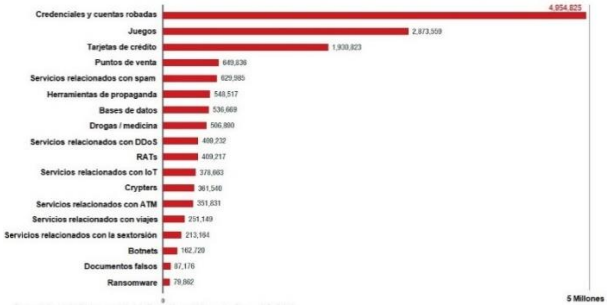
Sobre todo, porque el ciberespionaje está más en boga que nunca. Así, según Verizon (2020), se calcula que un 10% de los incidentes pertenecen a este tipo. Tras ellos están países que quieren robar datos confidenciales que permitan desestabilizar el orden mundial a su favor. "Estamos en una guerra fría, no de tipo nuclear, pero sí tecnológica. Según donde estés ves la película de una manera u otra, pero lo cierto es que todos hacen lo mismo y que lo hacen según sus capacidades, unos mejor y otros peor", explicaba recientemente el CEO de CounterCraft, David Barroso (2020).

3. Negocio cibercriminal

Además, el delito a través de la Red sube, año a año, su rentabilidad. El ciberatacante de los años 90, que en muchos casos actuaba por pura curiosidad o por hacktivismo, ha dado lugar a un entramado mundial cibercriminal que la UE calcula que ha movido en 2020 en torno a 5,5 billones de euros, el doble que en 2015.

De hecho, desde hace un lustro las fuerzas y cuerpos de seguridad alertan de que resulta tan lucrativo este negocio para las mafias que han dedicado lo obtenido por el narcotráfico al crimen cibernético (ver Figura 1). Y todo ello con menos riesgo y de forma más lucrativa por realizarse desde países donde es muy complicado perseguirlo y, también, por la complejidad de una atribución cierta. Los datos no pueden ser más preocupantes. No extrañan, pues, los del informe de Crowd Strike (2020), que evidencian que siete de cada diez entidades atacadas… lo vuelven a ser en poco tiempo.

Figura 1.: Bienes y servicios más populares en la Dark Web (Basado en datos recogidos de 600 foros) (*Fuente: Informe de cibercriminalidad de Trend Micro. Adaptación: Revista SIC nº 140*)



Las cifras del cibercrimen apabullan. Según Steve Morgan, editor de Cybersecurity Ventures (2020), se prevé que el impacto global por *ransomware* alcance los 16.300 millones de euros en 2021, frente a los 265 de 2015. Algo que, desgraciadamente no es de extrañar teniendo en cuenta que, por ejemplo, los ataques contra el sector médico se cuadriplicaron durante la pandemia y que, según datos de la mencionada publicación, se espera que en 2021 se produzca un ataque de este tipo a una empresa, con éxito, cada 11 segundos en el mundo. A ello también ayudará el auge de las criptomonedas para 'mover' el dinero de la forma más discreta posible, ya que se calcula que el 70% de las transacciones de monedas digitales serán de actividades delictivas en 2021. "Los ciberdelincuentes están creando nuevos ataques e intensificando su ejecución a un ritmo alarmante, aprovechándose del miedo y la incertidumbre provocados por la inestabilidad de la situación socioeconómica a escala mundial. Al mismo tiempo, las medidas de confinamiento impuestas en el mundo han propiciado una mayor dependencia de la conectividad y las infraestructuras digitales, lo que aumenta las oportunidades de llevar a cabo intrusiones y ataques cibernéticos", alertó Interpol, en agosto de 2020, en su informe "Ciberdelincuencia: efectos de la Covid-19".

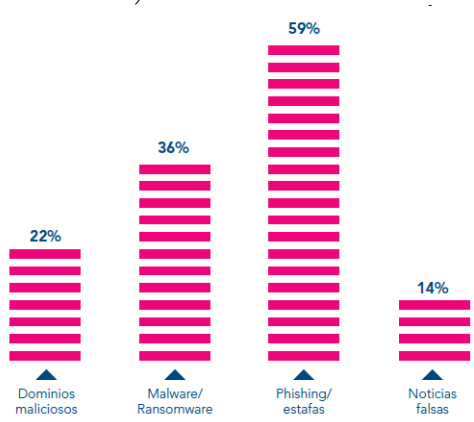
3.1 Ciberataques en 'modo Covid-19'

Como era de esperar, el mayor impacto del cibercrimen a lo largo del año, según un informe de Crowd Strike (2020),

ha sido por la masiva adopción del teletrabajo. Ello ha supuesto que, en el 30% de los incidentes, las soluciones de antivirus no estuvieran correctamente configuradas, tenían activada la seguridad más débil o ni siquiera protegían el entorno corporativo completo. Las soluciones tradicionales fallaron en la prevención del 40% de los incidentes, ya sea debido a errores de detección de *malware* o a que alguna secuencia del ataque no fue descubierta por la herramienta, destaca su informe.

Además, el repentino y masivo cambio hacia el trabajo en remoto aceleró la migración a la nube para el 76% de los altos ejecutivos de todo el mundo encuestados en el estudio 'C-Suite Perspectives' de Radware (2020).

Figura 1.: Proporción de las principales Ciberamenazas relacionadas con la Covid-19 (*Fuente: Interpol "Ciberdelincuencia: efectos de la Covid.19*)



3.2 Seguridad al límite

"Mientras trabajaban desde casa, los especialistas en ciberseguridad tuvieron que adaptar las defensas existentes a un nuevo paradigma de infraestructura, intentando minimizar la exposición a una variedad de ataques novedosos donde los puntos de entrada son el hogar de los empleados conectado a Internet y otros dispositivos inteligentes", indica el informe. "Al mismo tiempo y bajo una gran presión, tuvieron que implementar soluciones basadas en componentes que antes eran menos confiables, como el acceso remoto a través de la Internet pública, servicios en la nube, servicios de transmisión de video no seguros y dispositivos y aplicaciones móviles". Y es que el confinamiento por la pandemia "ha supuesto una verdadera puesta de largo de la disponibilidad en nuestros sistemas y datos como valor esencial de la seguridad, explica el analista de ciberseguridad, Alberto Partida (2020).

De hecho, la Agencia de Ciberseguridad de la UE (ENISA) destacó en su 'Informe Panorama de amenazas 2020' que "la resiliencia en ciberseguridad de la Unión Europea ha sido llevada al límite". Se culpa a la Covid-19 de un aumento del 238% en los ciberataques a sectores como el Fintech (tecnología aplicada a finanzas), con el 80% de las empresas en todo el mundo aumentando sus infraestructuras de seguridad digital (2020).

Sirva como ejemplo que, según un estudio de Symantec Internet Security (2020), el usuario ha recibido, de media, en el año pasado 16 correos electrónicos no deseados maliciosos cada mes. Y es que tanto el email como la ingeniería social (técnicas para engañar al usuario para que facilite el trabajo del atacante) han sido usadas de forma masiva por los atacantes aprovechando el 'caos' generado por la pandemia. Los investigadores de Kaspersky descubrieron un promedio de 360.000 nuevos archivos maliciosos cada día durante los últimos 12 meses, 18.000 más por día que el año anterior, un aumento del 5,2 por ciento, según su investigación 'Statistics of the Year Report' (Figura 2).

Y después del brote, "por razones existenciales, alrededor del 50% del mundo introdujo nuevas tecnologías para permitir comunicarse con los clientes de diferentes maneras, así como para facilitar el trabajo desde casa, y de ellos, alrededor del 60% implementó nuevas tecnologías sin seguridad", aseguró Kris Lovejoy, líder de ciberseguridad, EY Global Consulting (2020).

La situación de 2020 fue tan crítica que el 85% de los CISOs admitieron que sacrificaron la ciberseguridad para permitir que los empleados trabajaran de forma remota rápidamente, según una investigación de Netwrix también reveló que una de cada cuatro empresas considera que corre un mayor riesgo de ciberseguridad ahora que antes de la pandemia y el 54% de los CISO admitieron no tener la visibilidad necesaria para garantizar una protección de datos adecuada. Un problema teniendo en cuenta los principales patrones de amenaza que se detectaron, gran parte fruto de errores humanos: *phishing* o suplantación (48%), errores de administración (27%) e intercambio inadecuado de datos por parte de los empleados (26%). Los compromisos de la cadena de suministro se tardaron más en detectar: el 55% necesitó días, semanas o incluso meses para registrar estos incidentes.

4. Gasto insuficiente

El problema es que "históricamente, la productividad de los trabajadores y la seguridad de los terminales empresariales han sido consideradas como prioridades en competencia", explica el director ejecutivo de Hysolate, Marc Gaffan (2020), "pero esto se agudizó en 2020 cuando los CISO,

que luchaban por escalar las operaciones de TI de su fuerza de trabajo remota en plena pandemia, vieron que la urgencia era la productividad de los trabajadores y que las soluciones heredadas como VPN, VDI y DaaS simplemente no pueden manejar las demandas de la nueva realidad *Remote-First*". Los datos del estrés laboral que está provocando esta situación son tales que incluso un 20% de los CISO confiesan en dicha investigación haber bebido más vino durante la crisis de la Covid-19, un 323% incrementó la ingesta de café e, incluso, un 8% de whisky… y un 40% "todo lo anterior".

Algo preocupante teniendo en cuenta que "existe una relación entre el presupuesto de una organización para ciberseguridad y los ciberincidentes que experimenta: las empresas que destinan menos de un 3% de su presupuesto de IT/OT a ciberseguridad -la media es 9,3%- sufrieron hasta dos amenazas cibernéticas con consecuencias significativas". De hecho, el documento confirmó una realidad terrible: solo el 52% de las empresas considera que su organización está preparada para hacer frente a un ciberataque.

Sin embargo, según datos del estudio, "a pesar de ello, la pandemia ha provocado la disminución de los presupuestos de ciberseguridad en el 57% de las empresas, con los consiguientes riesgos derivados de ello".

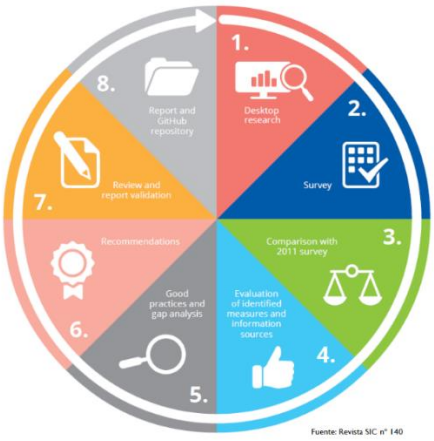
Pero con la popularización del teletrabajo, que en los meses de confinamiento supuso hasta el 70% de los empleados, y actualmente ronda el 30%, se calcula que cada trabajador tiene de media acceso a 10,8 millones de archivos, y las organizaciones más grandes tienen alrededor de 20 millones de archivos accesibles, según datos de Varonis (2020), el 64% de las organizaciones de servicios financieros tienen más de 1.000 archivos confidenciales abiertos para cada empleado. "La transición segura al trabajo remoto y el bloqueo de los datos expuestos para mitigar el riesgo de inicios de sesión remotos fueron dos de las mayores prioridades de seguridad para los equipos de TI en los servicios financieros", dijo una investigación de Varonis**.**

Esta mayor o menor adaptación a la modalidad laboral del teletrabajo es un factor o parámetro adecuado con el que medir la solidez de una organización y su resistencia a la incertidumbre. Un caso más que pone de manifiesto el valor que la Transformación Digital aporta al negocio o, si se prefiere, que ilustra la imposibilidad de supervivencia del negocio si no se acomete esta Transformación Digital, explica la empresa Tarlogic en un artículo (2020) sobre *insiders* y teletrabajo destacando esta amenaza como "un viejo conocido" y uno de los que más se podría evitar aplicando cibernteligencia en todos los niveles de la empresa.

5. En busca de la resiliencia

Frente a este tsunami digital que la pandemia ha acelerado, entidades como la Agencia Europea de Ciberseguridad (ENISA), aconsejan ser cada vez más proactivos y menos reactivos (Figura 3). Por eso, la UE ha acometido con intensidad un nuevo modelo de protección cibernética basado en su Ley de Ciberseguridad (Cybersecurity Act (2020), aprobada en 2020) que ha dado pie a la aprobada Estrategia de Ciberseguridad comunitaria 2020-2025, aprobada el 16 de diciembre, además de una nueva directiva de seguridad de redes (NIS 2), así como una propuesta de Directiva de Resiliencia (2020) para entidades críticas. "Todos deberían poder vivir su vida digital de forma segura. La economía, la democracia y la sociedad de la UE dependen más que nunca de las herramientas digitales seguras y fiables y la conectividad que debemos proteger", destacó la Comisión.

Figura 3.: Metodología para aplicar ciberseguridad proactiva, según ENISA (*Fuente: Revista SIC nº 140*)



La protección y contar con hegemonía para ejercerla según los parámetros de vida europeos se ha convertido en un reto prioritario para la UE. Por ello, también será impulsado de forma especial por su marco financiero plurianual 2021-2027, con un presupuesto de 2.000 millones de euros más la inversión de los Estados miembros y la industria. A los que se sumarán las inversiones de la UE en proyectos digitales que supondrán, al menos, al 20%, del mecanismo de recuperación y resiliencia de 672.500 millones de euros (unos 134.500 millones de euros). España, presumible-

mente, también incrementará su inversión en ciberseguridad. Sirva como ejemplo que el Instituto Nacional de Ciberseguridad (Incibe) contará con hasta 253 millones en los presupuestos de 2021, una cantidad notable teniendo en cuenta que en 2020 dispuso de poco más de 23.

Eso sí, "no debemos confundir la asignación presupuestaria para Incibe con lo que el Estado español, en base a los Presupuestos Generales del Estado, vaya a gastar y a invertir en ciberseguridad tanto en productos como en servicios", destacó en un análisis, en profundidad, el Director de Revista SIC, José de la Peña (2020).

Y es que gran parte de ellos debería ir a mejorar, de forma directa y con resultados comprobados, a las organizaciones españoles y su protección. Aunque también es "imprescindible que las empresas cuenten con una estrategia de seguridad centrada en las personas, ya que los ciberdelincuentes se dirigen cada vez más a los usuarios en lugar de a la infraestructura con el objetivo de robar credenciales, tomar el control de datos sensibles y transferir fondos de manera fraudulenta", explica el Country Manager de Proofpoint (2020) en España, Fernando Anaya, tras presentar la investigación de la compañía en la que el 36% de los líderes de TI en España consideraron que sus empleados convierten la empresa en vulnerable frente a ciberataques, por lo que la formación y la concienciación acerca de la seguridad, junto con controles y soluciones técnicas, pasan a ser una prioridad crítica que podría marcar la diferencia entre una tentativa de ataque y un ataque con éxito. "Los ciberdelincuentes tienen un objetivo claro y mejoran constantemente sus habilidades. Si las organizaciones no hacen lo mismo, solo puede haber un ganador", recuerda.

¿Se volverá a lo que había antes? Pues no lo parece, ya que, en una encuesta a 600 profesionales de seguridad de TI, realizada por Check Point (2020), el 47% de los encuestados dijo que la seguridad para los empleados que trabajan de forma remota será el principal desafío de cara a 2021, mientras que el 61% dijo que será una de las principales prioridades durante los próximos dos años. Y exactamente la mitad dijo que no habrá retorno a las normas de ciberseguridad pre pandémicas.

6. Ciberinteligencia como vacuna digital

Decía Immanuel Kant que "la inteligencia del individuo se mide por la cantidad de incertidumbres que es capaz de soportar". Precisamente, la ciberinteligencia como parte de la ciberseguridad es lo que ayuda a reducir dicha incertidumbre y el 'suspense' que, parafraseando a Alfred Hitchcok similar a un "hombre sentado en el sofá favorito de su casa. Debajo tiene una bomba a punto de estallar. Él lo ignora, pero el público lo sabe. Esto es el suspense". Y "en circunstancias como las actuales la Inteligencia es una herramienta de gran utilidad, pero ¿qué entendemos por Inteligencia? La Inteligencia podríamos definirla como "Capacidad de entender, asimilar, elaborar información y utilizarla adecuadamente, siendo la capacidad de procesar información, estando íntimamente ligada a otras funciones mentales como la percepción, o la capacidad de recibir la citada información, y la memoria, junto la capacidad de almacenarla", pero resumiendo esta definición más todavía, podemos llegar a definir la Inteligencia como Información procesada con vista a la acción que pretende reducir la incertidumbre en la toma de decisiones", destaca el responsable de ciberinteligencia en Internet Security Auditors, Carlos Seisdedos en el diario La Razón (2020) a la vez que recordaba que "en situaciones como la actual, la inteligencia y la elaboración de escenarios ayudan en el asesoramiento, elaboración y planificación de escenarios de futuros, cuya finalidad es la creación de planes de contingencia en el ámbito de la ciberseguridad, pero también en el ámbito sanitario, logístico o de seguridad, que nos permitan prever y afrontar los diferentes escenarios plausibles y los menos probables que serían dañinos en el caso de materializarse, para favorecer la anticipación mediante la proactividad".

Figura 4.: Porcentaje de empresas que tienen un plan de respuesta (*Fuente: The Hidden Costs of Cybercrimen –McAfee 2020*)

6.1 El poder de ser reactivos

En definitiva, según Zane Ryan**,** CEO de DotForce (2020) "el poder de anticipar una incidencia está directamente relacionado con la cantidad de información que se pueda analizar en tiempo real. Por eso, la ciberinteligencia pone al servicio de las organizaciones la máxima seguridad ofreciéndoles la posibilidad de ver más allá de sus fronteras o de sus parámetros de red, con el fin de detectar los ataques, así como anticiparse a las posibles intrusiones y mitigarlas" (Figura 4).

Por eso contar con visibilidad de lo que ocurre e información patrones e indicadores de compromiso es la única garantía que permitirá anticiparse a las amenazas digitales pasando de una ciberseguridad reactiva a anticipativa. Algo decisivo en un mundo cada vez más complejo, cambiante que, como una bola por un tablero inclinado, está cobrando velocidad ante la inminente explosión de tecnologías que pueden terminar provocando la cuarta revolución industrial –o mejor dicho digital-. Y la Covid-19 ha hecho que, cambios que iban a tardar una década, se hagan en poco menos de dos o tres años.

"Un buen modelo de amenazas hace más que decirle a una organización cómo los adversarios atacarán sus sistemas y activos. También puede identificar vulnerabilidades previamente desconocidas, medir cuánto riesgo está incurriendo una empresa, permitir juegos de guerra de diferentes escenarios de seguridad y estimar los efectos colaterales de diferentes estrategias de mitigación por adelantado, en lugar de sobre la marcha durante un ataque en curso. Pero las empresas no pueden cosechar esos beneficios si no tienen un modelo en primer lugar, o si desarrollan uno en las condiciones incorrectas", destaca una encuesta de Deloitte de 2010, en la consta que solo el 47% de los líderes de C-Suite dijeron que están haciendo análisis de amenazas y modelado al menos una vez por trimestre.

"Todos tenemos dificultades para lograr que se adopte el modelo de amenazas por su verdadero valor", dijo Alyssa Miller (2919) investigadora de seguridad. Precisamente, un estudio realizado por SafeGuard sugiere que las empresas deberían fortalecer los sistemas contra los vectores de ataque no convencionales. "Existe una desconexión y tensión significativas entre la seguridad percibida y las necesidades de cumplimiento y el nivel de planificación organizacional. El mayor desafío de seguridad y cumplimiento es el uso de aplicaciones no autorizadas (52%), seguido de intentar monitorizar las comunicaciones comerciales en entornos multirregionales (43%), lo que sugiere que las empresas globales están experimentando más fricciones en la adaptación de sus procesos al nuevo espacio de trabajo digital en un mundo post-Covid".

7. España ciberinteligente

Por eso, la ciberinteligencia cobró especial importancia en 2020. Incluso llegó a celebrarse desde España un congreso multitudinario, IntelCON (2020), organizado por la comunidad Ginseg, que congregó a miles de asistentes y más de medio centenar de ponentes para profundizar en las diferentes técnicas y su aportación a la seguridad corporativa. También el evento de ciberseguridad técnica más veterano de España, RootedCON, coordinado, entre otros por Román Ramírez**,** mostró muchos aspectos imprescindibles de ciberseguridad e inteligencia.

La ciberinteligencia también tiene mucho que ver con la labor de los equipos de respuesta a incidentes (CERT / CSIRT), que nacieron para ofrecer capacidades de reacción al gran primer ciberataque mundial, causado por el 'Gusano Morris', en 1988, y que hoy se está convirtiendo en una herramienta imprescindible para las empresas y organizaciones más maduras en ciberprotección. "Un concepto cada día más importante por cuanto, además de permitir responder de forma eficiente a las amenazas también resulta fundamental para anticiparse a los incidentes actúan de forma proactiva con tecnologías, procesos y ayudando a formar a los empleados frente a los principales ataques de ingeniería social, los que buscan que los empleados cometan errores para acceder a la información más crítica de la empresa", destaca la periodista Ana Adeva, (2020) que ha escrito sobre su situación y retos. También en España, que lidera el ranking europeo en número de equipos de este tipo.

De hecho, compañías punteras españolas como S2 Grupo, entre otras, cuentan desde 2018 con un departamento, el Lab52, especializado en ciberinteligencia, que fue reforzado en 2020. "Estar prevenidos, de verdad, significa, estudiar sus intereses de forma continua, analizar TTPs para preparar nuestros sistemas defensivos, etc. y de ahí la importancia de compartir y aglutinar esta información", recuerdan desde la compañía a la vez que destacan que desde la web de LAB52 (2018) se ofrece, de forma gratuita, capacidades de ciberinteligencia como son: responder a los usuarios que lo precisen, sobre cuáles son los posibles grupos APT (Amenazas Persistentes Avanzadas) que pueden estar interesados en la información de su compañía, es decir, sus posibles ciberatacantes. Se trata de una de las muchas iniciativas españolas que hay en marcha para ofrecer protección anticipativa y por la que está apostando de forma muy especializada empresas con un fuerte crecimiento y personal muy especializado como Zerolynx o Blueliv, con fuerte proyección internacional, entre otras.

8. Protección digital total

En 2016, EE.UU. activó su conocido escudo antimisiles, en el que participa España a través de tres fragatas en la base naval de Rota. Un proyecto que busca proteger a cualquier

país de la OTAN en caso de ser atacado con misiles intercontinentales. Lo cierto es que este tipo de defensa no deja de causar perplejidad respecto a la inversión que supone frente a lo que se está haciendo en proteger el ciberespacio. El principal problema es que este es un dominio incipiente y, por lo tanto, al margen de no pocas leyes. Muchos lo han comparado con el salvaje Oeste, otros con el mar antes que se aplicara el derecho naval. Sin embargo, aún hoy, hay vastas extensiones de océano consideradas 'aguas internacionales' aprovechadas por el crimen y el terrorismo para realizar y coordinar todo tipo de actos.

Por eso, el objetivo de la UE esta década será "intensificar el trabajo con socios internacionales para avanzar y promover un ciberespacio global, abierto, estable y seguro donde se respeten el derecho internacional, los derechos humanos, las libertades fundamentales y los valores democráticos".

A pesar de las nuevas tecnologías de ciberseguridad, de la mayor concienciación mundial y del trabajo de Agencias, organismos y sector, lo cierto es que "el escenario de ciberriesgos prepandemia continúa, puesto que las empresas siguen enfrentándose al mismo tipo de amenazas, como el *phishing* o el *ransomware,* que ha crecido un 50% en los últimos tiempos. Sin embargo, las compañías tienen ante sí un nuevo reto: hacer más seguras las infraestructuras y el acceso remoto a su información", destacó en su evento anual Check Point a través de su responsable, Gil Shwed (2020). "Estamos atravesando un cambio de paradigma, puesto que no hace mucho la mayoría de la carga de trabajo se desarrollaba en entornos físicos estables, pero la pandemia nos ha obligado a adaptarnos y comenzar a trabajar online de forma mayoritaria. El gran problema es que el 40% de las empresas no cuenta con seguridad básica", añadió.

Cada cierto número de décadas la humanidad se 'resetea'. A veces ocurre por una innovación que lo cambia todo destaca FireEye en su informe 'Un reinicio global: predicciones de seguridad cibernética 2021, pocas semanas antes de descubrirse uno de los mayores ataques a la compañía de ciberseguridad, a finales de año. De cualquier forma, cada vez las empresas comprenden mejor "el valor de mantener sus sistemas seguros y tomar iniciativas contra posibles fugas querrán invertir en ciberseguridad. Refuerce al equipo y haga nuevas contrataciones si es necesario. En general, las empresas han apoyado a sus equipos de seguridad durante este tiempo, pero si la seguridad no es una prioridad, conviértala en una," resaltó Elias Manousos**,** director ejecutivo de RiskIQ (2020).

Y en el mundo de la Inteligencia y la seguridad, también será determinante la identidad y su protección como garante del negocio en un entorno cambiante y disruptivo. Precisamente, en su edición de 2020, IdentiSIC tuvo, entre sus grandes conclusiones, la necesidad de contar con más control, visibilidad, preparación estratégica y prioridad la información y datos más críticos que hay que proteger, además de las cuentas privilegiadas, con una clara apuesta por la seguridad basada en conceptos de 'Confianza cero'. Parece que llevemos muchos años en el mundo digital, pero a la vista del incremento del cibercrimen y de los ataques durante 2020 se puede decir que esto "no ha hecho más que empezar".

¿Descubrirá el mundo la 'piedra filosofal' que haga el entorno digital seguro? Es poco probable porque, más allá de la tecnología, tendría que apostar por la colaboración y el entendimiento, a nivel mundial, creando unos 'cascos azules', preparados para intervenir en cualquier parte del mundo, con un centro global de protección mundial y con seguridad por diseño en cada dispositivo conectado, incluso con capacidades ofensivas. En cierto modo, la red de redes que es Internet se podría extrapolar y crear una red de nodos de protección digital, gestionados por *bots* que hagan las veces de ciberpolicías, para garantizar que el delito no se aprovecha de las mismas 'carreteras' que usan empresas y ciudadanos para mejorar su vida digital. Pero hay 'demasiados ratones' que piensan que ellos saben más que el 'gato'…

9. Inteligencia y ciberinteligencia para mitigar y reducir riesgos económicos y digitales

Por eso, la inteligencia económica y la ciberinteligencia cobrarán un protagonismo nunca conocido esta década. Su capacidad para ofrecer información que reduzca el riesgo y anule las amenazas las hará determinantes para parar el tsunami tecnológico que viene a nosotros y cuya velocidad no ha hecho sino acrecentarse por todos los cambios que ha supuesto la Covid en la forma de trabaja y acometer el día a día.

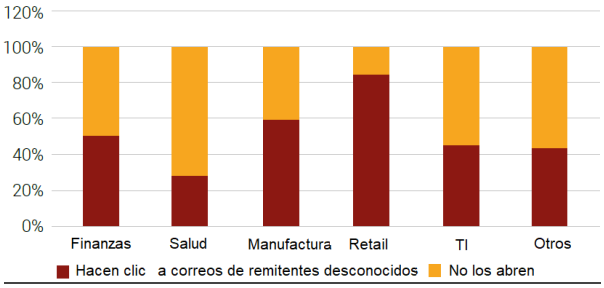
En definitiva, estos años estarán marcados por el poder de anticipación a las amenazas, tanto económicas como sociales y tecnológicas. Esa será la labor de la Inteligencia económica y de la ciberinteligencia que serán determinante para reducir el riesgo o, en caso de incidente, gestionarlo de forma eficiente siendo lo más resilientes posibles.

De hecho, un estudio de PWC (2020) recuerda que "los mecanismos de gestión de riesgos tradicionales no han sido suficientes para enfrentar la crisis, y las funciones de aseguramiento deberán tener un rol protagonista". Por eso, cree "necesario construir resiliencia en las organizaciones para una gestión de riesgos inteligente que permita contar con una mejor preparación ante futuras posibles disrupciones". PWC señala que "han sido pocas las funciones de riesgos y aseguramiento que han podido enfrentar la crisis". Dicho de otra forma: si algo ha quedado claro ya con la crisis por la Covid-19 es que no hay mecanismos clásicos que aseguren la anticipación ante los cisnes negros, salvo contar con capacidad de anticipación al riesgo, y la inteligencia económica y la ciberinteligencia, en conjunción, son una parte fundamental. Ello supondrá también que "las funciones de aseguramiento deberán posicionarse como protagonistas en la alta dirección y consejería, y así evitar el riesgo de volverse invisibles", destacan desde la consultora que recuerda que "la crisis económica del coronavirus ha tenido como resultado que muchas empresas se enfoquen en amenazas externas para mantener su viabilidad, según KPMG[44]. Algo de lo que también sabe mucho el sector asegurador que basa su negocio en valorar y cuantificar el impacto de los riesgos, también con ciberinteligencia.

Por eso, se ha observado una disminución en la atención en el control interno, lo cual incrementa el riesgo en áreas críticas como fraude, cumplimiento normativo y sistemas de reporte internos. Sin embargo, aunque algunos reguladores han relajado sus requisitos y plazos de presentación de informes debido a la crisis económica, las obligaciones impuestas a las organizaciones siguen vigentes, por lo que las responsabilidades fundamentales de las empresas se mantienen igual". Sus consejos para gestionar esta década pasan por "dar prioridad a las actividades clave de control", así como apostar por una "adecuada segregación de funciones, delegación de responsabilidades y líneas de reporte definidas, adecuados niveles de autorización, acceso a sistemas que garanticen la confidencialidad, integridad y disponibilidad de los datos ante amenazas internas y externas, y optimizar el uso de datos y técnicas analíticas" (Figura 5).

"Construir la capacidad de resiliencia de las organizaciones requiere aumentar la confianza en la inteligencia basada en datos de gestión de riesgos y modelar escenarios que permitan tomar decisiones inteligentes sin sesgos emocionales. Al contar con una mejor preparación y prevención ante posibles disrupciones, las empresas se adaptarían más rápido, beneficiando a todas sus áreas", destacan en un interesante análisis desde Aserta (2020). A la vez que recuerdan la importancia que tendrá el "desarrollo de soluciones y plataformas de Inteligencia Artificial (AI) en el posicionamiento competitivo post COVID-19 de las empresas. Se espera que los servicios basados en esta tecnología sean más integrados en procesos críticos de negocio a partir de la crisis, tales como la gestión de riesgos".

Figura 4.: ¿En qué sectores se abren más enlaces de correo electrónico de remitentes desconocidos? (*Fuente: Informe Gurucul / Revista SIC nº 139*)



En definitiva, se trata de sobrevivir a los cisnes negros digitales que llegarán, más que nunca, con la explosión tecnológica que supondrá la popularización, tanto 'en el lado del bien como del mal' de la Inteligencia Artificial, la automatización, la robótica, la tecnología cuántica, el 5G y 6G y, por supuesto, el *big data*. Por eso, es más importante que nunca "aportar prospectiva y no solo retrospectiva", como destacó Richard Chambers, presidente del Global Institute Internal Auditors. Y, por supuesto, como recordó el precursor del concepto de cisnes negros, Taleb Assib, en 2018, en una conferencia en KPMG, será fundamental tener claro que "para tener éxito, lo primero es sobrevivir". O sea que hay que centrarse primero en reducir riesgos y luego en generar el negocio. Eso teniendo en cuenta que la clave para afrontar los riesgos actuales, más dinámicos que nunca, es entenderlos y para eso será determinante contar con la inteligencia económica y la ciberinteligencia por su capacidad de anticipación.

En definitiva, "se prevén eventos lejanos…y …mediante procesos de Ciberinteligencia, embebidos en el departamento de ciberseguridad o en el de Inteligencia económica. Es la única forma de ir más rápido que los *Threat Actors*, o actores maliciosos", destaca Hugo Zunzarren (2018), CEO de ArmadatA, que recuerda que "la ciberseguridad en la inteligencia económica es, de hecho, uno de los factores más importantes. Y, además, un valor diferencial, porque es un cambio de óptica radical". No hay que olvidar que, en definitiva, "la ciberinteligencia se pone al servicio de la ciberse-

guridad y actúa antes que se produzca un ataque cibernético, reuniendo toda la información necesaria para prevenir esos ataques y tomar decisiones con un alto nivel de certeza"[47]. El tiempo dirá si el mundo ha usado de forma eficiente las herramientas que tenía para no adentrarse en los peores augurios que muchos estudios vaticinan si no se actúa de forma coordinada frente a las ciberamenazas previsibles y, con ciberinteligencia, nos preparamos para las imprevisibles, los cisnes negros.

ANEXO A: LISTA DE LAS 15 PRINCIPALES AMENAZAS DE ENISA

Los 15 informes de amenazas cibernéticas principales son de naturaleza técnica e incluyen hallazgos, incidentes importantes, estadísticas y más. Los informes de amenazas son los siguientes:

1. Software malicioso (malware)
2. Ataques basados en web
3. Suplantación de identidad (phishing)
4. Ataques a aplicaciones web
5. Correo no deseado
6. Denegación de servicio distribuida (DDoS)
7. El robo de identidad
8. Filtración de datos
9. Amenaza interna
10. Botnets
11. Manipulación física, daño, robo y pérdida
12. Fuga de información
13. Secuestro de datos
14. Espionaje cibernético
15. *Cryptojacking* (minería maliciosa de criptomonedas)

(*Fuente: ENISA, Threat Landscape -ETL, 2020*)

ANEXO B: LOS CINCO MALWARE MÁS PELIGROSOS DE 2020, SEGÚN ESET

Los ataques de malware más comunes durante 2020, según su Informe de Amenazas para el tercer trimestre fueron:

1. Archivos torrent maliciosos. En septiembre se descubrió una familia de malware no conocida hasta la fecha llamada KryptoCibule, que utiliza criptominería y técnicas de secuestro del portapapeles para robar criptomonedas y extraer archivos relacionados con criptomonedas en los equipos infectados.

2. Amenazas en Android. Las aplicaciones ocultas en Android han dominado la mayor parte del año. Este tipo de amenaza consiste en utilizar aplicaciones falsas disfrazadas de aplicaciones legítimas, sobre todo utilidades o juegos, que esconden su icono después de la instalación y que muestran anuncios a pantalla completa en el dispositivo.

3. Amenazas en IoT. Los dispositivos IoT siguen diseñándose sin pensar en la seguridad, por lo que son un blanco fácil para los delincuentes. Los atacantes pueden infectar estos dispositivos e integrarlos dentro de una botnet que puede ser utilizada para realizar ataques a gran escala.

4. Malware en Mac. A principios de 2020, la aplicación de trading Kattana, diseñada para ordenadores Mac, fue replicada y 'tuneada' por un grupo de cibercriminales que insertó un software malicioso (malware) utilizado para robar información como las cookies del navegador, carteras de criptomonedas o capturas de pantalla.

5. Correos maliciosos. El malware distribuido a través de correo electrónico tuvo especial incidencia después del verano, sobre todo con ataques usando *exploits* (programas que se aprovechan de un fallo de seguridad) para Microsoft Office.

10. Referencias

Albors, J.: "Tendencias 2021: ¿qué nos depara un futuro incierto en materia de ciberseguridad?" https://blogs.protegerse.com/2020/12/04/tendencias-2021-que-nos-depara-un-futuro-incierto-en-materia-de-ciberseguridad. Diciembre.

Anant, V., Caso J. y Schwarz A (2020): "La crisis de COVID-19 cambia las prioridades y los presupuestos de ciberseguridad". www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cyber-security-priorities-and-budgets#. Julio

Aserta (2020): "Preparar las compañías ante "cisnes negros". aserta.com.es/teoria-cisne-negro-economia. Julio.

Busselen, M.(2020): "Por qué el ciberdelito sigue siendo un desafío empresarial preocupante en un mundo bloqueado por COVID". www.crowdstrike.com/blog/why-cybercrime-remains-a-worrying-business-challenge-in-a-covid-lockdown-world. Septiembre.

CheckPoint (2020): "CheckPoint Secure" www.checkpoint.com/events. Noviembre

Checkpoint (2020: "La 'nueva normalidad' llegó para quedarse durante algún tiempo: una nueva encuesta revela

las prioridades de seguridad de las organizaciones para 2021 y más allá".blog.checkpoint.com/2020/12/08/the-new-normal-is-here-to-stay-for-some-time-new-survey-reveals-organizations-security-priorities-for-2021-and-beyond. Diciembre.

Darkreading (2020): "Encuesta: Las mayores preocupaciones sobre la seguridad de la infraestructura digital incluyen COVID, aplicaciones no autorizadas, plataformas de colaboración, tecnología de marketing". www.darkreading.com/risk/survey-biggest-concerns-about-securing-digital-infrastructure-include-covid-unsanctioned-apps-collaboration-

Dávila, J. (2019): "La IoT y la seguridad actualizable". Revista SIC nº 138, 'En Construcción'. Febrero

De la Peña, J (2020): "Ciberseguridad: a veces, vemos euros". Revista Sic nº 142 / revistasic.es/revista-sic-numero-142-pdf-cop. Noviembre.

Deloitte (2020): "El estado de la ciberseguridad en España: Digitalización, teletrabajo y ciberataques en tiempos de pandemia". www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html

Dotforce (2020): "Anticipando los ciberataques, las empresas rentabilizan la inversión en seguridad hasta un 740%" aslan.es/dotforce-anticipando-los-ciberataques-las-empresas-rentabilizan-la-inversion-en-seguridad-hasta-un-740. Julio.

ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf.

Enisa (2020): "Panorama de amenazas de ENISA a través de los años". www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape.

Fernández, L. (2020). "Sin Comentarios: Every breath you take". Revista Sic nº 140. / revistasic.es/revista-sic/sic-140/sin-comentarios/ Junio

Fireeye (2020): "Un reinicio global: predicciones de seguridad cibernética 2021" www.fireeye.com/current-threats/annual-threat-report.html

Freeze, D (2019): "Desde Piratear Juguetes Hasta Threat Hunter y Soccer" cybersecurityventures.com/from-hacking-toys-to-threat-hunter-and-soccer-ref. Octubre.

Fuentes Guerrero, R.Solar (2020): "Winds sufre un ataque de cadena de suministro". unaaldia.hispasec.com/2020/12/solarwinds-sufre-un-ataque-de-cadena-de-suministro.html Diciembre.

Gaffan, M. (2020): "Cómo desarrollar una sólida estrategia de seguridad BYOD para su creciente fuerza de trabajo remota".

García, M. A. (2020): "David Barroso (CounterCraft): "Estamos en una guerra fría, no de tipo nuclear, pero sí tecnológica". escudodigital.com/expertos/entrevistas/david-barroso-estamos-en-una-guerra-fria-no-de-tipo-nuclear-pero-si-tecnologica. Diciembre.

Ginseg (2020).ginseg.com

Hartley, R (2020):."2021 será el año de la puesta al día".securityboulevard.com/2020/10/2021-will-be-the-year-of-catch-up. Octubre.

Higgins D., Lovejoy, K.. Albang, K. (2020): "Se necesita una estrategia tecnológica proactiva, empática y centrada en el ser humano para dotar a las organizaciones de una ventaja competitiva más sólida".

Identisic (2020): "Identisic". revistasic.es/identisic/que-es-identisic Noviembre.

Iniseg (2020): "Ciberinteligencia y ciudades inteligentes". www.iniseg.es/blog/ciberseguridad/ciberinteligencia-y-ciudades-inteligentes. Febrero.

Juniper Research (2020): "Las conexiones de iot alcanzarán los 83 mil millones en 2024, impulsadas por casos de uso industrial en proceso de maduración", www.juniperresearch.com/press/press-releases/iot-connections-to-reach-83-billion-by-2024-driven. 31 de marzo

Kaspersky, AMR (2020): "Boletín de seguridad de kaspersky 2020. Estadísticas securelist.com/kaspersky-security-bulletin-2020-statistics/99804". Diciembre.

KPMG (2018): "Sobrevivir a los cisnes negros" www.tendencias.kpmg.es/2018/10/cisnes-negros-gestion-riesgos. Octubre.

Manousos, E (2020): "Deje de pensar en la ciberseguridad como un problema: considérelo como un juego". www.helpnetsecurity.com/2020/11/11/cybersecurity-game. Noviembre.

Milijic, M (2019): "Estadísticas 5G (El INCREÍBLE poder de la velocidad)". leftronic.com/5g-statistics. Noviembre.

Morgan S. (2019): "La Reducción del talento en ciberseguridad creará 3,5 millones de puestos de trabajo Ssn cubrir en todo el mundo para 2021". cybersecurityventures.com/Jobs. Octubre.

Morgan, S. (2020): "El Ciberdelito costará al mundo $ 10,5 billones anuales para 2025". cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021. Noviembre.

Netwrix (2020): "Encuesta: el 85% de los CISO admiten que sacrificaron la ciberseguridad para permitir que los empleados trabajen de forma remota".

Ortiz, M. (2020): "Teletrabajo e Insider Threats. Nuevas oportunidades para un viejo conocido". www.tarlogic.com/blog/teletrabajo-e-insider-threats-nuevas-oportunidades-para-un-viejo-conocido. Agosto.

Partida, A.(2020): "Cavilaciones seguras. El patito feo de la seguridad"Revista Sic nº 140/ revistasic.es/revista-sic/sic-140/cavilaciones-seguras/1dsdsds. Junio.

Proofpoint (2020): "El 87% de las organizaciones españolas sufrió al menos un ciberataque en los últimos 12 meses.www.proofpoint.com/es/newsroom/press-releases/el-87-de-las-organizaciones-espanolas-sufrio-al-menos-un-ciberataque-en-los. Diciembre.

PWC (2020): "Impacto del COVID-19 en la ejecución de los planes de auditoría interna". www.pwc.com

Radware (2020): "Perspectivas de C-Suite: migración acelerada a la nube pero infografía de seguridad rezagada".www.radware.com/documents/infographics/2020-csuite-perspectives-infographic. Septiembre.

Revista SIC (2020) "CSIRT. Al pie del cañón". Nº 142.

revistasic.es/revista-sic-numero-142-pdf-cop Junio

S2 Grupo. (2018): "Threat Intelligence". s2grupo.es/soluciones/threat-intelligence

securityboulevard.com/2020/10/how-to-spin-up-a-robust-byod-security-strategy-for-your-growing-remote-workforce/. Octubre.25 Sobers, R (2020): "El mundo de las filtraciones de datos". www.varonis.com/blog/the-world-in-data-breaches. Marzo.

Seisdedos, C.(2020): "Inteligencia al servicio de la Ciberseguridad". La Razón. www.larazon.es/tecnologia/20201110/dbtjm4ad4nh4pas3xt6bo2jhym.html. Noviembre.

The European (2020): "La falta de preparación mundial contra la ciberseguridad está acabando con el crecimiento económico". the-european.eu/story-20895/lack-of-global-preparedness-against-cybersecurity-is-killing-economic-growth.html. Septiembre.

UE (2020): "Directive of the european parliament and of the council"

UE (2020): "La estrategia de ciberseguridad de la UE para la década digital", ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade. 16 de diciembre

UE (2020): "Ley de ciberseguridad de la UE" ec.europa.eu/digital-single-market/en/eu-cybersecurity-act. Febrero.

Verizon (2020): "Cazar. Detectar. Responder. Ciberespionaje". www.verizon.com/business/resources/reports/cyber-espionage-report. Noviembre.

World Economic Forum (2020: "Future Series: Ciberseguridad, tecnología emergente y riesgo sistémico" www.weforum.org/reports/future-series-cybersecurity-emerging-technology-and-systemic-risk. Noviembre.

www.ey.com/en_gl/consulting/how-can-technology-at-speed-create-competitive-advantage. Agosto.

www.netwrix.com/netwrix_survey_cisos_admit_they_sacrificed_cybersecurity_to_quickly_enable_employees_to_work_remotely.html. Septiembre.

Zunzarren, H. (2018): "Seis claves para entender la ciberinteligencia y la ciberseguridad". hackercar.com/seis-claves-para-entender-la-ciberinteligencia-y-la-ciberseguridad