Informe de tendencias.

Ciberseguridad en tiempos post - Covid.

Evolución a través de los años y tendencias actuales.

Alba Campillo > Directora del Máster en Ciberseguridad en Three Points.

inesdi Digital Business School Madrid Barcelona Online
THREEPOINTS THE SCHOOL FOR DIGITAL BUSINESS
Digital Innovation Learning Hub
Planeta Formación y Universidades

Inesdi Digital Business School

Campus Barcelona:
C/ Mallorca, 27
08029, Barcelona
Teléfono: 932 27 81 50

Campus Madrid:
C/ del Príncipe de Vergara, 108
28002 Madrid
Teléfono: 914 11 80 36

e-mail:
info@inesdi.com

www.inesdi.com

Three Points, The School for Digital Business

Dirección:
C/ Mallorca, 27
08029, Barcelona

Teléfono:
932 27 81 50

e-mail:
info@threepoints.com

www.threepoints.com

Autora

Alba Campillo

> Directora del Máster en Ciberseguridad en Three Points.

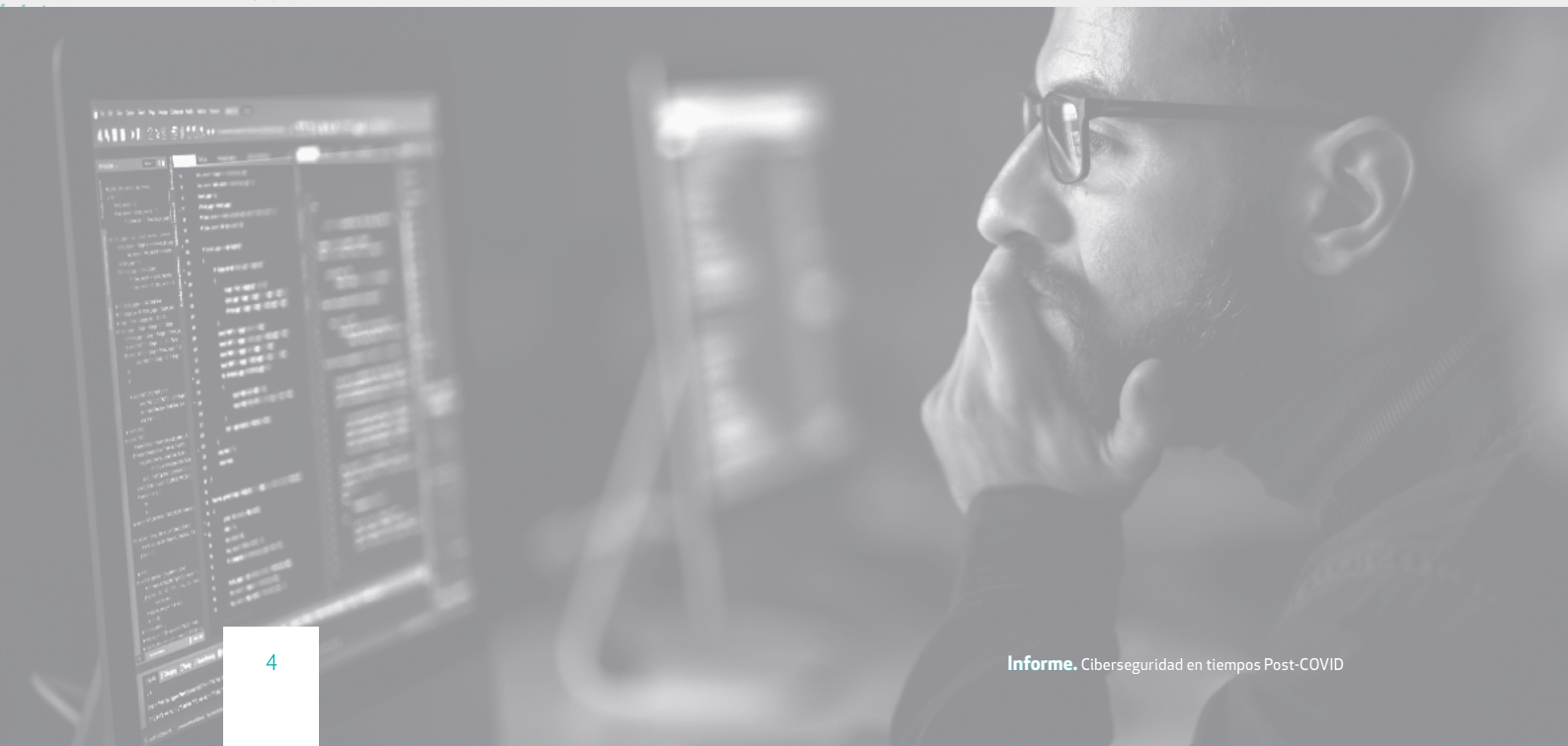
Consultora en Ciberseguridad en Indra, proveedor líder mundial de soluciones propias en segmentos específicos de los mercados de Transporte y Defensa y Directora del Máster en Ciberseguridad de Three Points.

Anteriormente, trabajó como Analista en Ciberseguridad e Inteligencia en el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), que forma parte del Ministerio del Interior de España.

También ha trabajado como Business Manager IT en empresas como Implemental Systems y Axpe Consulting.

Alba tiene un Máster en Relaciones Internacionales por la Universidad Autónoma de Madrid.

Contenido



CAP. 01

Introducción

La empresa Cisco define la ciberseguridad como:

> *La práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; extorsionar a los usuarios o los usuarios o interrumpir la continuidad del negocio.*[1]

Según el Departamento de Seguridad Nacional del Gobierno de España, "todas las actividades que se desarrollan en el ciberespacio son fundamentales para la sociedad actual. La tecnología e infraestructura que forman parte del ciberespacio son elementos estratégicos, transversales a todos los ámbitos de actividad, siendo la vulnerabilidad del ciberespacio uno de los principales riesgos como nación' [2] Por ello, la ciberseguridad es actualmente y desde hace algunos años, un **objetivo prioritario en las agendas de los gobiernos de todo el mundo.**

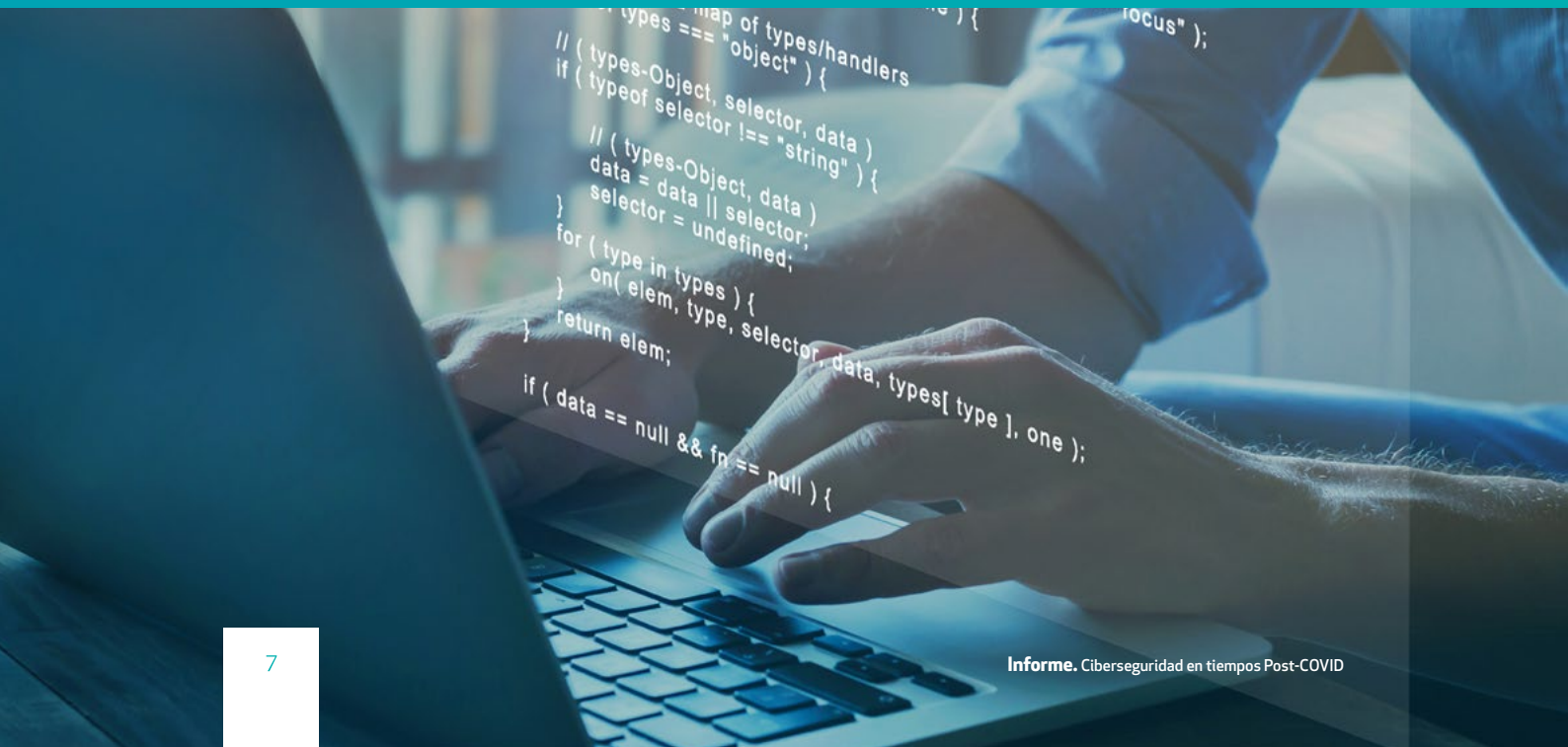
En el ámbito privado, las empresas tampoco se encuentran exentas de riesgos. La correcta adaptación de éstas a un entorno tecnológico en constante cambio aumenta su supervivencia. Tener una visión integral del entorno les ayuda a conocer los posibles riesgos identificando sus puntos débiles. En la actualidad la tecnología se encuentra presente en todos los procesos de negocio de cualquier empresa, por lo que la ciberseguridad es **elemento imprescindible para la generación de confianza** tanto en clientes como proveedores [3].

La ciberseguridad está cobrando cada vez más importancia, especialmente tras el estallido de la pandemia, aumentando la **necesidad de profesionales especializados.** No obstante, tanto empresas como instituciones públicas están detectando dificultades para encontrar candidatos que tengan formación en el sector. En este contexto, el mercado demanda cada vez más expertos que se hayan formado en materia de ciberseguridad y que puedan ayudar a identificar y prevenir posibles ataques.

[1] https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
[2] https://www.dsn.gob.es/gl/file/2988/download?token=K4T9k3hV
[3] https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf

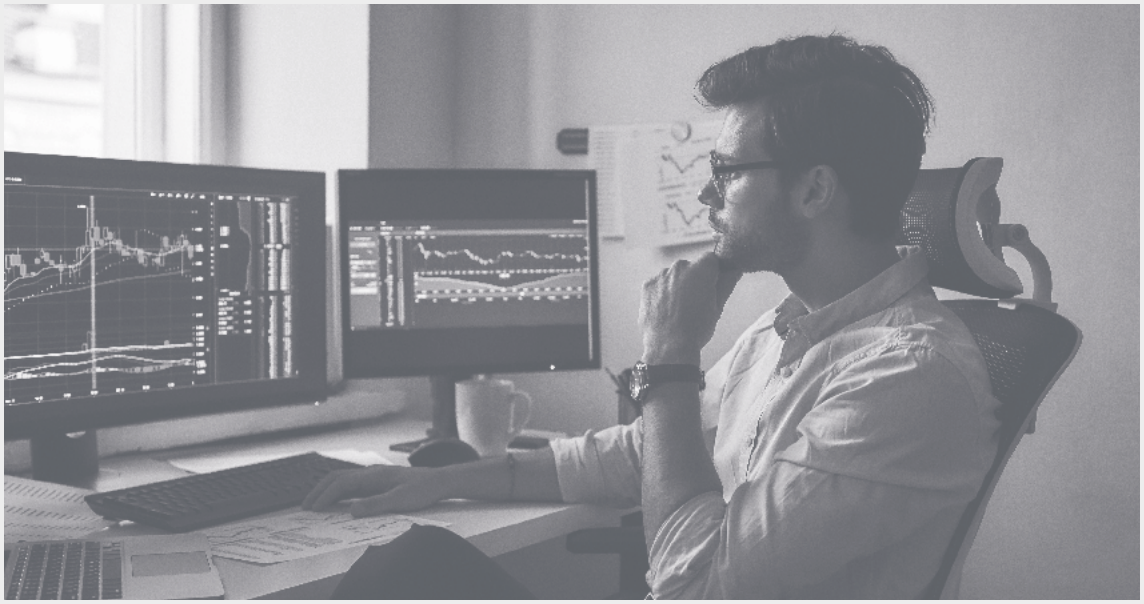
CAP. 02

Ciberseguridad antes de la pandemia



La primera *Estrategia Nacional de Ciberseguridad* en España se aprobó en el año 2013, su documento fijaba las líneas de actuación y directrices generales en términos de ciberseguridad. Un año después, durante el 2014, se creó el Consejo Nacional de Ciberseguridad con el objetivo de coordinar los organismos en materia de ciberseguridad. Asimismo, en los años posteriores se realizaron cambios notables a nivel jurídico, como la modificación en 2015 del Esquema Nacional de Seguridad para garantizar la seguridad de los sistemas del sector público y la entrada en vigor del Real Decreto- ley 12/2018 sobre seguridad de las redes y sistemas de información que traspone al ordenamiento jurídico español la directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo[4].

Durante el año 2017 se marcó un antes y un después dentro de la Estrategia de Seguridad Nacional, donde **se situó a la ciberseguridad en un lugar de vital importancia para la seguridad del país.** Para ello, se establecieron cinco puntos principales: la gestión de crisis; la cultura de Seguridad Nacional; los espacios comunes globales; el desarrollo tecnológico; la proyección internacional de España. A partir de este momento, la ciberseguridad no es únicamente vista como un vector tecnológico, sino que empieza a ser considerado como **imprescindible en otras esferas como la política, económica o social.**



El ciberespacio puede ser utilizado para múltiples finalidades, como influir en la opinión pública y en la forma de pensar de la población a través de campañas de desinformación y acciones de tipo híbrido. De esta manera, la instrumentalización del ciberespacio puede llegar incluso a influir en procesos electorales. De ahí que la ciberseguridad cada vez sea más importante[5].

En 2018 empieza a requerirse a las empresas que implementen la regla general de protección de datos (GPDR) aprobada en el año 2016. En cuanto a ciberseguridad, se exige que, cuando tenga lugar una brecha de datos, se realicen notificaciones dentro de las primeras 72 horas a la Agencia Española de Protección de Datos y, si son datos de carácter sensible, a los implicados.

[4] https://www.boe.es/eli/es/rdl/2018/09/07/12/dof/spa/pdf
[5] https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

Asimismo, también se empieza a solicitar que se defina la figura del Delgado de Protección de Datos y se exige que tenga lugar un consentimiento libre, informado y específico por parte de los usuarios para que el mismo sea 'inequívoco' [6]

Durante el 2019, el Consejo de Seguridad Nacional actualizó el plan de Estrategia Nacional de 2013. Para su diseño y redacción intervinieron únicamente representantes del Consejo, dejando al sector privado sin participación, aunque permitieran su visualización antes de la publicación. Esta nueva estrategia, entre otros aspectos, entendía a los ciudadanos como responsables de sus comportamientos y que, los mismos, pueden influir en la seguridad del ciberespacio. Por tanto, se le pide a la ciudadanía ser **consciente sobre los riesgos a los que se encuentran expuestos** (cultura de ciberseguridad).

Aunque muchos de los puntos tratados en esta actualización denotaran una madurez técnica por parte del Sistema de Ciberseguridad nacional, un notable número de expertos determinaron que el plan estaba más orientado a la protección ante riesgos e inseguridad, que el posible impacto que pudiera llegar a producirse ante un ciberincidente contra la actividad económica y el sector privado [7].

A finales de 2019, durante las jornadas XIII celebradas por el Centro Criptológico Nacional (CCN) se presentaron los datos de incidentes gestionados durante los últimos meses siendo 36 incidentes críticos y 1800 incidentes muy altos. Para que un ciberataque sea considerado como crítico debe tener una duración de más de una semana, ir dirigido contra infraestructuras críticas o estar originado por otros Estados. Según lo que fue compartido durante estas jornadas, se estimó que durante ese mismo año habían tenido lugar alrededor de 20 ciberataques dirigidos por parte de otros Estados contra España. [8] Por parte de INCIBE-CERT el total de incidentes gestionados fue de 107.397 de los cuales 72.858 de ciudadanos y empresas y 796 de operadores estratégicos. De estos datos se realizó un porcentaje de distribución por incidentes de los cuales un 29,7% eran fraude, 29,25% sistemas vulnerables, 25,47% Malware y el 15,11% de otros tipos[9].

Durante ese mismo año se elaboró el Informe Nacional del Estado de la Seguridad de los Sistemas de las Tecnologías de la Información y la Comunicación, en el cual en las últimas páginas se incluyó el Análisis de Riesgos para la Seguridad Nacional 2019/22. En el mismo, más de un centenar de expertos provenientes de la Administración, del sector privado e investigación, realizaron un apartado con el nivel de impacto y grado de probabilidad de las amenazas a la seguridad nacional de los cuales los riesgos tecnológicos predominaban por encima del resto. Especialmente se mencionaba el **mal uso del ciberespacio** y más concretamente los robos de datos, **ciberataques a infraestructuras críticas y desinformación** como riesgos de alto impacto y probabilidad[10].

[6] https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html
[7] https://www.realinstitutoelcano.org/analisis/la-nueva-estrategia-de-ciberseguridad-de-2019/
[8] https://www.europapress.es/nacional/noticia-espana-sufrido-20-ciberataques-parte-otros-estados-2019-cni-20191127150900.html
[9] https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2019_incibe.pdf
[10] https://www.redseguridad.com/actualidad/ccn-e-incibe-gestionan-mas-de-150-000-incidentes-de-ciberseguridad-en-2019_20200528.html

CAP.03

La ciberseguridad y el Covid-19

El año 2020 será recordado, no sólo por el comienzo de la crisis mundial provocada por la aparición del Covid-19, sino también por la transformación digital, la tendencia de teletrabajo en empresas de todo el mundo y, como consecuencia de ambos, el a**umento del riesgo en el ciberespacio.** A pesar del impacto positivo de la aceleración tecnológica, las repercusiones negativas en materia de ciberseguridad han llevado a muchos expertos a resumir los acontecimientos tecnológicos derivados de la crisis del Covid-19 como 'ciberpandemia'[11].

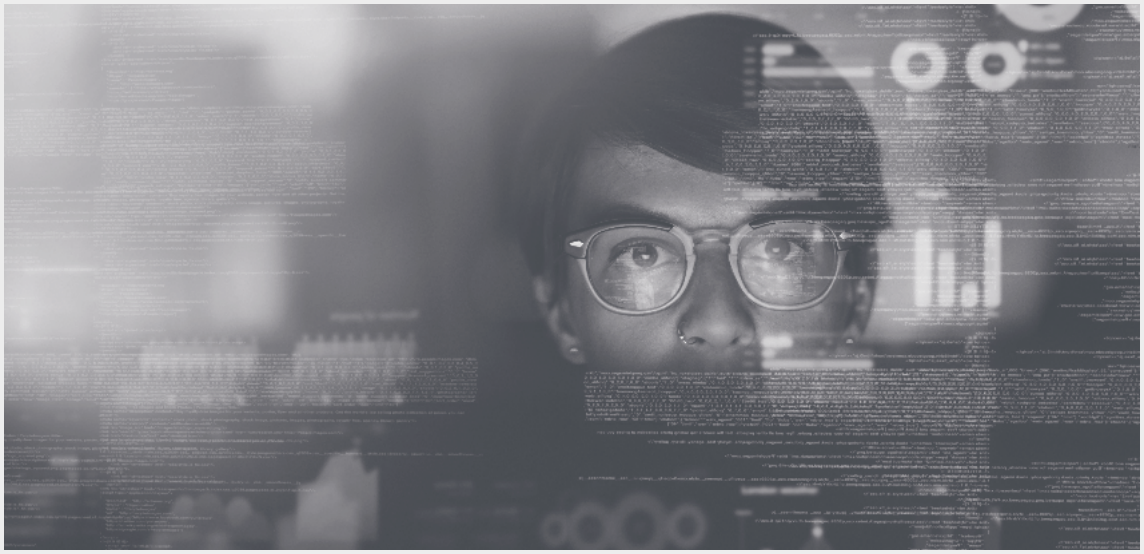
En días señalados como festivos (día de Navidad o Nochevieja) así como en situaciones de crisis (como terremotos o atentados) u horas de máxima audiencia (prime time), es cuando se produce un aumento de tráfico en las operadoras. Para este tipo de situaciones las redes se encuentran diseñadas para atender los picos de demanda y evitar el colapso de los sistemas. No obstante, las previsiones que pudieran haberse realizado respecto al Covid-19 fueron ampliamente superadas sin que hubiera precedentes. Según datos del Observatorio Nacional 5G recogidos por el Real Instituto Elcano, Nokia detectó un **incremento de hasta un 40% de crecimiento** en las zonas más castigadas por la pandemia[12]. Debido a esta alta afluencia en las comunicaciones, muchos servicios se vieron interrumpidos causando un alto impacto negativo sobre la población. Si en una situación normal esto ya es de por sí perjudicial, en un contexto de confinamiento de la población en el que las únicas vías de comunicación pasan por internet la situación es aún más crítica. Algunos de los ejemplos de situaciones que tuvieron lugar a consecuencia de la sobrecarga de internet fueron la imposibilidad por parte de algunos pacientes de contactar con los hospitales, dificultades para estudiantes para realizar exámenes o incluso problemas relacionados con el cobro de subsidios[13].

Aunque el Covid-19 ha traído numerosos nuevos retos y ha potenciado los ya existentes, los profesionales del sector han sabido responder rápidamente a los mismos al igual que los ciberdelincuentes han aprovechado esta 'tormenta perfecta' para tratar de **desestabilizar y atacar empresas e instituciones de todo el mundo 14.** Las medidas que se tomaron contra la pandemia, como el confinamiento, trajeron como consecuencia que las empresas que ya permitían el teletrabajo lo mantengan y aumenten y que aquellas que no contaban con ello, lo implementen. Este aumento del trabajo desde casa ha traído consigo nuevos retos de ciberseguridad que necesitaban respuestas urgentes. Muchas empresas, por tanto, han aplicado **controles de ciberseguridad más estrictos** y han promovido buenas prácticas de ciberseguridad para que sus plantillas puedan trabajar desde casa reduciendo, de esta manera, los posibles riesgos cibernéticos. Un gran número de organizaciones han acelerado la adopción de entornos multinube como una de las medidas para obtener beneficios en cuanto a costes y capacidad de soportar fuerzas de trabajo distribuidas para hacer frente a la situación derivada de la pandemia. Por esto, una de las tendencias más destacables en cuanto a ataques está siendo dirigida en contra de la nube.

Algunas disciplinas que también han tenido un gran desarrollo como consecuencia de la pandemia, como la Inteligencia Artificial o Machine Learning, han sido también

[11] https://www.computerweekly.com/es/cronica/Ciberpandemia-la-enfermedad-empresarial-que-tambien-requiere-vacuna
[12] https://www.realinstitutoelcano.org/analisis/ciberseguridad-en-tiempos-de-pandemia-repaso-a-la-Covid-19/
[13] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/341/58/PDF/G2234158.pdf?OpenElement
[14] https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-Covid-19-crisis-brought-a-cyber-pandemic.html

instrumentalizadas con mayor frecuencia en los ataques por parte de los ciberdelincuentes. De cara a un futuro próximo, los ataques serán más complejos debido a que los atacantes están aprovechando la automatización y la Inteligencia Artificial [15].



3.1. Ciberataques. Tipos de ciberataques que se han acentuado a consecuencia del Covid-19

Con el comienzo de la pandemia del Covid-19, las organizaciones se centraron en adaptar las condiciones de trabajo de los empleados con el objetivo de minimizar el riesgo de contagio lo máximo posible. Mientras que muchas empresas decidieron promover el trabajo a distancia o teletrabajo, muchas otras adaptaron las condiciones de la oficina para que sus empleados pudieran hacerlo in situ al ser considerados como personal esencial. Según lo compartido por parte de ISACA en una de sus publicaciones, los empleados que trabajan desde casa se encuentran sometidos a un nivel de estrés mayor y las probabilidades de distracción de los mismos aumentan. Esto se debe, entre otros motivos, a que desde casa se suele trabajar un mayor número de horas y los horarios suelen ser irregulares, lo que puede influir en el cansancio y estrés de los empleados. Teniendo en cuenta que el ánimo es determinante para el desempeño del trabajo, **el teletrabajo puede desembocar en un mayor número de errores de seguridad** como por ejemplo caer en estafas de phishing así como el compromiso de cuentas de los empleados despistados. El coste medio de una filtración de datos es de hasta 1,07 millones de dólares siendo el elemento del trabajo a distancia un encarecedor del coste de un suceso como este [16]. Las organizaciones tardan más tiempo en detectar y contener la filtración cuando la misma ha tenido lugar fuera de la oficina. De esta manera, aquellas organizaciones que tenían más del 50% de sus empleados trabajando a distancia **tardaron una media de 58 días más en identificar y contener la brecha** que las empresas con menos del 50% de empleados trabajando desde la oficina[17].

[15] https://www.tripwire.com/state-of-security/featured/Covid-19-pandemic-dominates-cybersecurity-world/
[16] https://www.ibm.com/downloads/cas/OJDVQGRY
[17] https://www.isaca.org/resources/isaca-journal/issues/2022/volume-2/cybersecurity-in-a-Covid-19-world

Durante los primeros 4 meses del año 2020 y, coincidiendo con el mayor periodo de propagación del Covid-19 a nivel mundial, se tuvo constancia por parte de Interpol de 907.000 mensajes de spam, 737 incidentes relacionados con malware y 48.000 URLs maliciosas. Desde la citada institución, se enviaron encuestas sobre el impacto de la crisis del Covid-19 a 194 países miembros de los cuales 48 contestaron. El análisis realizado como resultado de lo compartido por parte de los países fue complementado con información de Interpol Cybercrime Threat Response (CTR) y del Cyber Fusion Centre (CFC) [18] Algunas de las tipologías de criminalidad que más se han observado durante el periodo referido son los siguientes:

Estafas online y phishing

Durante la pandemia y al incrementarse el uso de internet para todas las actividades del día a día, aumentaron este tipo de ciberestafas. Asimismo, los delincuentes han aprovechado la situación de preocupación entre la población por el virus para utilizar temas relacionados con la pandemia como señuelo para, suplantando a gobiernos e instituciones, robar los datos de sus víctimas[19].

Malware disruptivo (ransomware y DDos)

El uso del malware se incrementó notablemente y, especialmente, contra infraestructuras críticas e instituciones sanitarias debido al alto beneficio y gran impacto de los ataques. Estos ataques pueden provocar interrupciones totales o parciales de operaciones comerciales así como pérdida de información relevante[20].

Malware recolector de datos

Los troyanos de acceso remoto, robos de información, spyware y troyanos bancarios están cada vez más en aumento. Como se ha mencionado anteriormente, la mayor parte del éxito por parte de los atacantes ha sido que han utilizado información relacionada con el Covid-19 para comprometer las redes, robar datos, desviar dinero y crear botnets[21].

[18] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-Covid-19
[19] https://www.welivesecurity.com/la-es/2020/11/25/crece-ecommerce-aumentan-estafas-incidentes-seguridad/
[20] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html
[21] https://www.redseguridad.com/actualidad/ciberseguridad-Covid-un-informe-de-interpol-alerta-sobre-la-alarmante-tasa-de-ciberataques-durante-el-Covid-19_20200810.html

Dominios maliciosos

Valiéndose del aumento de la demanda de suministros médicos e información sobre Covid-19 se ha producido un aumento notable sobre el registro de nombres de dominio que contienen palabras clave relacionadas con la pandemia. Estos websites fraudulentos señalan una amplia variedad de actividades maliciosas como servidores C2, despliegue de malware o phishing. Fue especialmente destacable el aumento de dominios maliciosos relacionados con la vacuna del Covid-19 [22]

Desinformación

Como consecuencia de la preocupación de la población por el avance de la pandemia, muchos actores han decidido compartir información falsa tanto para sembrar el caos como para la utilización de fines políticos. Según la Organización Panamericana de la Salud[23], esto ha tenido lugar debido a una infodemia masiva, es decir, una cantidad excesiva de información, que puede ser cierta o no, que dificulta que las personas encuentren fuentes correctas y fiables[24]

Respecto a la distribución de los ciberataques por países, el anteriormente citado informe de Interpol[25] señala que, aunque la ciberdelincuencia se ha disparado en los últimos meses, **las tendencias son diferentes según las regiones.**

En África, las noticias desinformativas han aumentado. Asimismo, algunos de los cambios dentro del comportamiento de los habitantes de esta zona, como el incremento de pagos electrónicos en detrimento del pago en cash, ha aumentado la exposición de la ciudadanía hacia los ciberataques[26]. Por otra parte, **el aumento del teletrabajo ha potenciado el phishing, las ciberestafas y la sextorsión** [27].

En las Américas, la campaña de ransomware llevada a cabo a través del malware LockBit fue especialmente dañina contra empresas medianas y tenía como objetivo bloquear el acceso de los usuarios a los sistemas informáticos y pedir el pago de un rescate para restablecerlo [28]. Por otra parte, el aumento de campañas de phishing y fraude con temática Covid-19 fue destacable, así como también lo fueron los problemas derivados del teletrabajo como el aumento de ataques para obtener el acceso remoto a las redes corporativas con el fin de robar información sensible. Respecto a las redes sociales, se ha incrementado su mal uso a través de los ciberdelincuentes que lo han utilizado para explotación sexual infantil en línea [29].

[22] https://haycanal.com/noticias/14304/dominios-registrados-como-coronavirus-la-otra-curva-del-Covid-19
[23] https://iris.paho.org/bitstream/handle/10665.2/52053/Factsheet-Infodemic_spa.pdf?sequence=16
[24] https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_es
[25] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-Covid-19
[26] https://www.bancomundial.org/es/news/press-release/2022/06/29/Covid-19-drives-global-surge-in-use-of-digital-payments
[27] https://www.muycanal.com/2020/04/29/espana-paises-mas-ciberataques-extorsion/amp
[28] https://latam.kaspersky.com/resource-center/threats/lockbit-ransomware
[29] https://www.uic.es/es/noticia/la-pandemia-por-Covid-19-ha-llevado-un-aumento-de-la-practica-del-sexting-especialmente

En los países asiáticos y del Pacífico Sur, las principales tendencias que incluyen el fraude relacionado con el Covid-19 fueron las campañas de phishing, la suplantación de identidad, así como venta ilegal en línea de suministro médico y equipos de protección personal falsos. Respecto al teletrabajo, se destaca la explotación de vulnerabilidades de seguridad de las herramientas de teleconferencia[30].

En Europa, dos tercios de los países informaron de aumentos significativos en la creación de **dominios maliciosos registrados con palabras clave como 'Covid' o 'Corona'** con el objetivo de confundir al creciente número de personas que buscaban información en internet sobre la pandemia. Por otra parte, también aumentaron los ataques hacia infraestructuras críticas e instituciones sanitarias encargadas de respuesta a Covid-19. Respecto a las administraciones públicas, se ha observado que durante los primeros meses de la pandemia se produjo el aumento de clonación de sitios web gubernamentales oficiales[31].

En las zonas de Oriente Medio y Norte de África (MENA), se observó al igual que en el resto del mundo, un aumento destacable de las noticias falsas relacionadas con el Covid-19. Como en otras regiones, también pudo observarse la utilización de medios sociales para la **venta ilícita de productos farmacéuticos y parafarmacéuticos contra el virus** y la proliferación de registros de dominios maliciosos que afirmaban proporcionar estadísticas sobre el Covid-19[32] .

[30] https://www.kaspersky.es/blog/videoconference-software-security/22549/
[31] https://www.bbc.com/mundo/noticias-38305426
[32] https://www.interpol.int/content/download/15305/file/20COM0356%20-%20IGGH_Covid-19%20threats%20to%20medicines_2020-05_SP.pdf?inLanguage=esl-ES

CAP.04

Evolución de la incidencia y la complejidad de los ataques en los últimos años

El primer virus informático de la historia surgió como parte de un experimento en el **año 1971** con el nombre de **'Creeper'**. Por aquel entonces, Internet aún era ARPANET, una relativa pequeña red de ordenadores que conectaba instituciones académicas y estatales. Al contrario de la complejidad y peligro que implican sus descendientes, el programa únicamente saltaba de un ordenador a otro llevando poco más que un saludo que citaba "Soy la enredadera" (creeper en inglés). A pesar de ser inofensivo, era considerado como un virus no por su maliciosidad pero sí por su capacidad para replicarse [33].

A partir del **2 de noviembre de 1988** la historia y la seguridad en internet cambió radicalmente. El conocido como **"gusano Morris",** y antecesor de los ataques DDoS[34], fue liberado ese mismo día y llegó a paralizar Internet aprovechando las vulnerabilidades de miles de ordenadores que detuvieron sus sistemas. Anteriormente no se había producido una incidencia similar ya que 600 de las 6000 computadoras de Internet (alrededor de un 10%) estuvieron infectadas durante 72 horas. En los directorios de algunas máquinas se llegaron a descargar archivos inusuales y los sistemas comenzaron a funcionar cada vez más lento a medida que los procesos se iban ejecutando [35]. El creador de este malware fue el universitario Robert Tappan Morris, quien decidió medir el tamaño de Internet creando un programa lo suficientemente complicado para que nadie lo pudiera borrar y también con la capacidad de replicarse a lo largo de la red. A pesar de que su intencionalidad no fuera la de producir daño alguno, un error de programación hizo que se multiplicaran las infecciones desde un ordenador único y que, como se ha mencionado antes, se sobrecargara el servidor.

En el **año 2000** apareció el virus conocido como **"ILoveYou"** en Filipinas, llegando a infectar a millones de ordenadores de importantes instituciones tales como la CIA, el Pentágono y el Parlamento Británico. En España el 80% de los ordenadores sufrieron el ataque de este virus. El gancho para que los usuarios abrieran el mail era una supuesta carta de amor y, de esta manera, cuando el usuario abría el archivo, además de infectar ordenador, se obtenía información confidencial del equipo infectado y se lo enviaba a su autor. Esto trajo consecuencias especialmente perjudiciales en entornos corporativos[36].

En el **año 2003** tiene lugar el nacimiento de **Anonymous**, concretamente en el foro de internet de '4chan' que había sido creado en la década de los 2000. Dentro de este foro, específicamente en 'Random', es donde nace el nombre de Anonymous donde los usuarios solían subir imágenes extrañas, textos sin sentido o cualquier cuestión que les interesara. En este caso, para publicar un mensaje se solicitaba, de manera opcional, un seudónimo o correo electrónico que si no se completaba aparecía como 'Anonymous' o, en otras palabras, usuario anónimo. Como muchas personas empezaron a esconderse tras el anonimato para realizar comentarios ofensivos o controvertidos empezó a extenderse la idea de que todos los 'Anonymous' eran la misma persona. Aunque en muchas ocasiones sea considerado a 'Anonymous' como un colectivo hacktivista, muchas personas sostienen que esta acepción sería incorrecta y que son más bien

[33] https://elpais.com/tecnologia/2021-05-20/atrapame-si-puedes-el-inocente-primer-virus-informatico-de-la-historia-cumple-50-anos.html
[34] https://www.kaspersky.es/blog/el-gusano-morris-cumple-25-anos/1836/
[35] https://www.welivesecurity.com/la-es/2016/11/08/retrospectiva-gusano-morris/
[36] https://www.pandasecurity.com/es/mediacenter/malware/virus-iloveyou/

un grupo de personas. Esto se debe a que no tienen una jerarquía concreta ni un líder y su modus operandi es el de decidir si llevar a cabo o no lo propuesto por un usuario[37].

En el **año 2009** tuvo lugar un ataque masivo contra varias corporaciones como Google, Adobe, Juniper, Rackspace y 30 más en la conocida como **"Operación Aurora".** Una de las hipótesis sobre la motivación del ataque fue la de robar información de propiedad intelectual a grandes compañías y, otra, la de robar cuentas de Gmail de activistas de Derechos Humanos en China. Se llegó a la conclusión de que el autor fue probablemente de origen chino ya que el código fuente de algunos componentes se encuentran en el idioma chino simplificado[38].

En **enero de 2010** tuvo lugar la aparición de la primera arma digital de historia, el **virus Stuxnet**. Durante la visita de unos inspectores de la Agencia Internacional de Energía Atómica a una planta nuclear en Natanz, Irán, notaron que las centrifugadoras usadas para enriquecer uranio habían dejado de funcionar sin poderse determinar el por qué. Cinco meses después, el fenómeno volvió a repetirse y logró determinarse la causa, un virus informático[39]. Según pudo determinarse por los investigadores de este ataque, el virus utilizaba hasta cuatro vulnerabilidades de zero day, lo cual era inusual hasta ese momento. Además, el software malicioso incluía líneas de SCADA cuya tecnología para ordenadores permitía controlar y supervisar procesos industriales a distancia lo cual no había sido visto anteriormente por expertos de ciberseguridad. El virus era también capaz de dirigir los PLC, controladores lógicos programables, computadoras usadas para automatizar procesos electromecánicos. Teniendo en cuenta la complejidad del ataque y el código utilizado para el mismo, se estima que se necesitaron entre 5 y 10 personas trabajando durante 6 meses para llevarlo a cabo. Por otra parte, los ciberdelincuentes debían tener conocimiento y acceso a los sistemas de control industrial para realizar las pruebas de calidad denotando, de manera, que tuvieron una gran organización, infraestructura y recursos económicos detrás. Este ciberataque fue el primero de la historia en tener consecuencias en el mundo físico consiguiendo, por parte de los atacantes, control total sobre una infraestructura crítica[40]. Según se confirmó posteriormente [41], la autoría del ataque provenía de Estados Unidos e Israel, cuyas razones eminentemente políticas, tuvieron que ver con el desarrollo armamentístico nuclear por parte de Irán.

En **2013** tuvo lugar otro hito en la historia de la ciberseguridad, el ataque contra la cadena de grandes almacenes Target. Como resultado de este, 40 millones de números de tarjetas de crédito y 70 millones de registros fueron robados[42]. La modalidad de malware utilizada para el ataque recibió el nombre de **BlackPOS**, cuya tipología es denominada como 'Malware point of sale', que afecta a los lectores de tarjetas de crédito y cajas registradoras[43].

El **12 de mayo de 2017** tuvo lugar un secuestro de equipos a escala mundial como consecuencia de la explotación de la vulnerabilidad de SMB (MS17 – 101). En concreto, el ransomware **WannaCry** infectó las redes mediante el 'exploit' EternalBlue aprovechándose de la vulnerabilidad antes

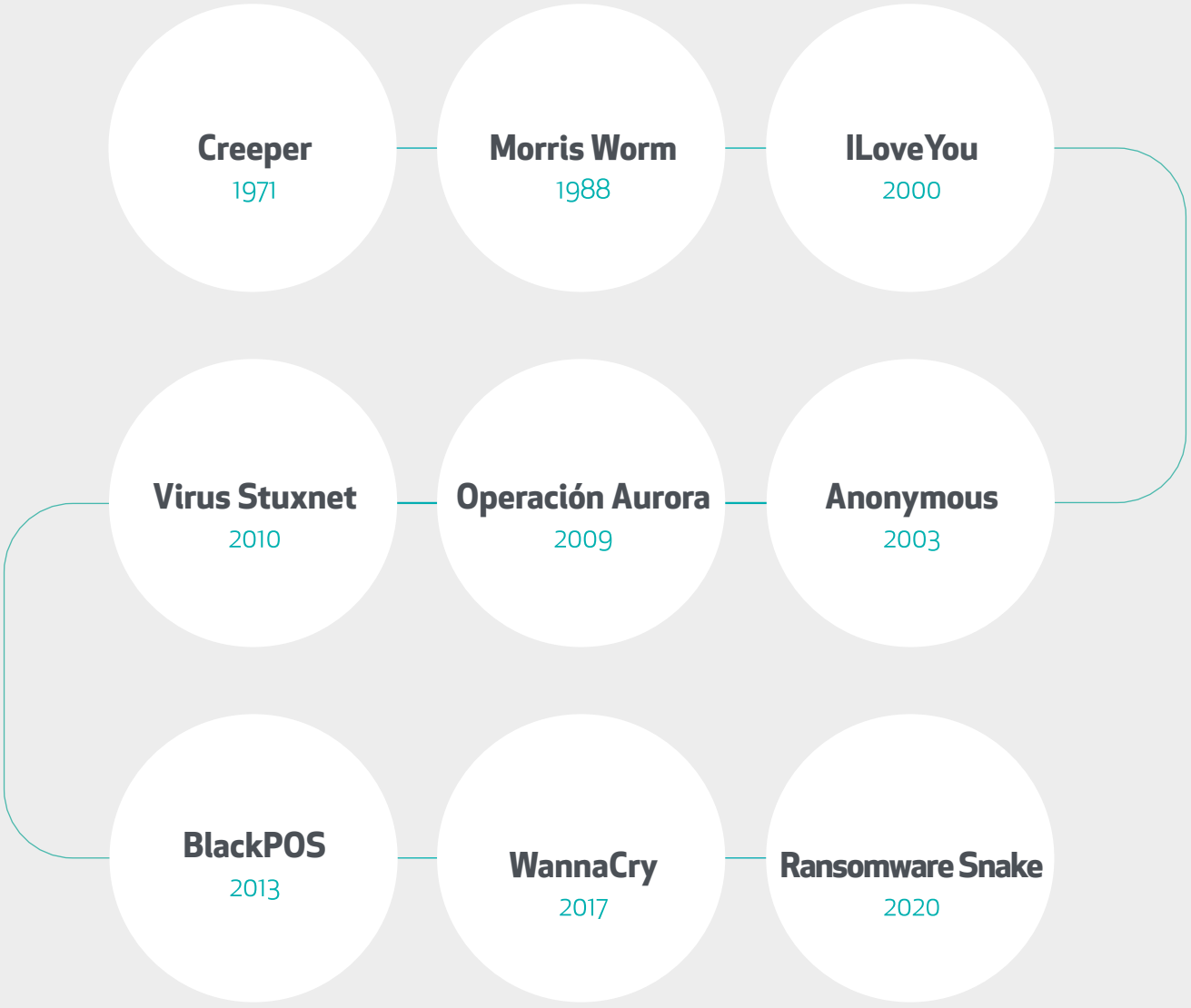
[37] https://www.ucm.es/data/cont/docs/506-2015-04-16-tfmbattocchio-seguridad.pdf
[38] https://www.welivesecurity.com/la-es/2010/01/21/que-es-operacion-aurora/
[39] https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet
[40] https://cronicaseguridad.com/2018/05/16/stuxnet-primera-ciberarma-historia/
[41] https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html
[42] https://cso.computerworld.es/tendencias/trend-micro-alerta-del-aumento-de-las-brechas-de-datos-y-del-malware-ram-scrapers-contra-el-sector-retail
[43] https://www.kaspersky.es/blog/malware-pos-y-raspadores-de-ram/2304/

mencionada del sistema operativo Microsoft Windows e instalando el backdoor 'DoublePulsar' que fue instalado en los ordenadores para ejecutar el ataque. Por tanto, fueron infectadas todas aquellas versiones anteriores de Windows en las que los operadores de la red no habían instalado las actualizaciones recomendadas oportunamente[44]. Los atacantes exigieron un rescate en bitcoins por un valor de 300 dólares y, más tarde, aumentaron el rescate en bitcoins a 600 dólares que debía ser pagado en el plazo de tres días si no querían que sus archivos fueran eliminados de forma permanente. En cuanto a esto, por parte de las Fuerzas y Cuerpos del Estado, recomiendan no sucumbir y pagar a los ciberdelincuentes ya que no hay garantía de que se devuelvan los archivos y se motiven más ataques de este tipo en un futuro. Respecto a esto, pudo comprobarse posteriormente que la codificación para realizar el ataque era defectuosa y que cuando algunas de las víctimas pagaban el rescate los atacantes no tenían forma de asociar el pago con el ordenador de una víctima específica. El impacto del ransomware provocó la paralización de los sistemas informáticos de 150 países que desembocó en pérdidas de 4.000 millones de dólares en todo el mundo[45]. Uno de los primeros países donde se reconoció que hubo ataques fue España, debido al ejercicio de transparencia por parte de la operadora Telefónica que confirmó que había sido atacado. Posteriormente, se conocieron paralizaciones en varios hospitales del sistema público sanitario de Reino Unido, la infección de numerosos equipos en la compañía estadounidense de FedEx y problemas en varias cadenas de montaje de los fabricantes de vehículos Nissan y Renault. Los países más afectados por el ataque fueron China y Rusia debido a la utilización de una copia pirata de Windows no registrada y licenciada, al no poder realizarse las actualizaciones pertinentes a productos piratas, no se podían proteger a los equipos[46]. La autoría del ataque fue reclamada por Shadow Brokers[47].

En **enero del 2020**, se notificaron los primeros ataques por parte del **ransomware 'Snake'** también conocido como 'Ekans'. Al igual que otros ransomware de su clase, encripta programas y documentos en las máquinas infectadas eliminando además todos los archivos infectados imposibilitando la recuperación de archivos por parte de las víctimas. Especialmente, se ha señalado a este ransomware como uno de los más peligrosos debido a su capacidad de destruir todos los procesos relacionados con los sistemas de control industrial y SCADA[48]. Los primeros objetivos fueron Honda y Enel Group, un conglomerado energético italiano[49]. Posteriormente y con la llegada de la pandemia por Covid-19, el ransomware Snake atacó a una de las empresas sanitarias del sector privado más grandes de Europa y propietaria de QuirónSalud[50]. En medio de la situación de desconcierto provocado por la pandemia, los ciberdelincuentes se aseguraban causar el máximo daño posible a los países atacados imposibilitando la utilización de medios digitales para acceder a la sanidad. En ese mismo año, en el año 2020, se produjo el hackeo masivo a cuentas de Twitter entre las que se encontraban grandes personalidades como Jeff Bezos, Bill Gates, Elon Musk y Obama.[51] Una vulnerabilidad zero day fue utilizada para hackear 5,4 millones de cuentas cuyos datos, posteriormente, fueron colgados en internet

[44] https://www.proofpoint.com/es/threat-reference/wannacry
[45] https://www.kaspersky.es/resource-center/threats/ransomware-wannacry
[46] https://elpais.com/tecnologia/2017/05/18/actualidad/1495108825_274656.html
[47] https://cso.computerworld.es/alertas/shadow-brokers-planea-vender-mas-exploits-de-equation-y-datos-de-ciberespionaje
[48] https://www.itdigitalsecurity.es/infraestructuras-criticas/2020/02/snake-un-ransomware-destructivo-que-ataca-a-sistemas-de-control-industrial
[49] https://www.comparitech.com/net-admin/snake-ransomware/
[50] https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/grupo-sanitario-fresenius-victima-ransomware-snake
[51] https://www.bbc.com/mundo/noticias-53426108

y, en concreto, en el foro 'BreachedForums'[52]. La filtración de datos personales puede causar un gran impacto posterior ya que pueden ser utilizados para casos de phishing y usurpaciones de identidad[53].



[52] https://www.elgrupoinformatico.com/noticias/hackeo-twitter-filtradas-millones-cuentas-t84266.html
[53] https://www.elespanol.com/omicrono/software/20220808/twitter-confirma-millones-cuentas-contrasena-ajustes-seguridad/693930614_0.html

CAP.05

Nuevas tendencias de ciberataques

A partir de la crisis sanitaria por el Covid-19, se ha tenido que forzar el traspaso de lo analógico hacia lo digital debido al aumento de compras por internet, comunicación por videollamadas y fomento del teletrabajo. No obstante, el avance tecnológico ha traído consigo el aumento de la ciberdelincuencia.

Ransomware

El ataque ransomware, si bien es cierto que no es una amenaza nueva, se ha convertido en **uno de los delitos más comunes y que más ha aumentado tras el surgimiento de la pandemia** del Covid-19. En la actualidad, se estima que existen más de 120 familias distintas de ransomware. Se destaca especialmente una nueva generación de ransomware más dirigido y sofisticado que los anteriores conocidos como 'Human Operated Ransomware' (HOR), en los que el ransomware se convierte en el último estadio de un proceso de infección en el que los atacantes llevan varios días dentro de la red. Respecto a otras innovaciones llevadas a cabo por los ciberatacantes para realizar el máximo daño posible, se ha observado el aumento significativo de cooperación de grupos de ciberdelincuentes que comparten sus plataformas de dataleaks utilizadas para la extorsión generando, por tanto, el aumento de conocimiento sobre estrategias, tácticas y conocimientos sobre los ciberataques[54].

Los ransomware suponen una de las amenazas más significativas debido al **alto contenido de datos confidenciales en riesgo y el impacto económico** que puede suponer un ataque de este tipo. Es precisamente por su componente económico que está teniendo más auge ya que para los ciberdelincuentes resulta 'relativamente fácil' obtener dinero de esta manera. En concreto, los hackers han promovido el pago con criptomonedas de manera que éstos sean difíciles de rastrear. Es entonces que se está pudiendo ver un aumento de la competititivad entre grupos de ransomware por ver quién genera más beneficios.

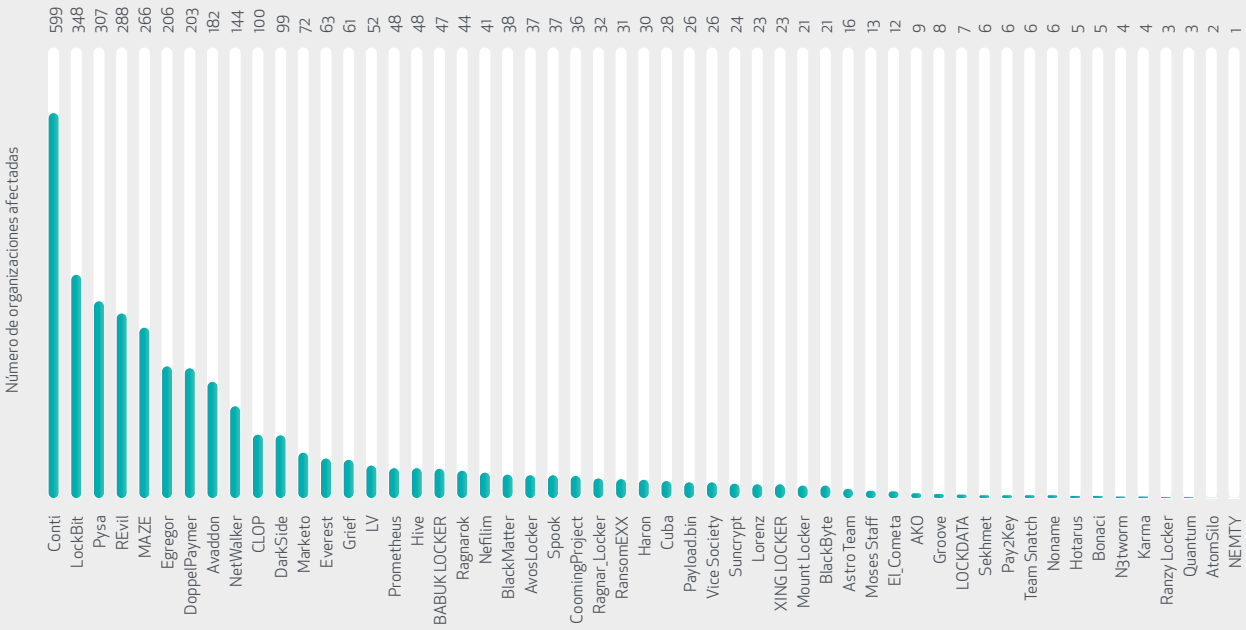
A raíz de esto, una de las líneas a seguir más importantes por parte de las empresas es la **creación periódica de back-ups, el desarrollo de planes de contingencia** entre los empleados para saber cómo responder ante un ciberataque o **mantener los sistemas, programas y aplicaciones constantemente actualizados**[55].

Entre los ransomware más activos entre 2020-21, se encuentran Maze, LockBit, RagnarLocker, Ragnarok, NetWalker, Nemty, Tycoon, SNAKE, Avaddon, Thanos, Phobos, BlackKingdom, DoppelPaymer, REvil, TinyCryptor, Ryuk, RansomExx, Conti, Egregor, Pay2Key o Zeppelin [56].

[54] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html
[55] https://cybersecuritynews.es/el-incremento-de-los-ciberataques-en-el-sector-sanitario-no-cesa-despues-de-dos-anos-de-pandemia/
[56]

Ilustración 1. Los tipos de ransomware más usados[57]

Fuente: DarkTracer.com



IoT

El internet de las cosas (IoT por sus siglas en inglés) está cada vez más presente en nuestras vidas y se ha intensificado aún más con la llegada del 5G a dispositivos que se encuentran presentes en nuestro día a día como pueden ser los altavoces, asistentes de voz, enchufes o bombillas. En la actualidad, se estima que **un 33% de los dispositivos ya han sufrido algún tipo de incidente de seguridad.** Este crecimiento sin precedentes se debe principalmente a factores como el aumento exponencial de uso de estos objetos y a su implementación insegura, con un acceso a internet fácil, falta de actualizaciones, y uso de contraseñas débiles, quedando expuestos a exploits[58].

Además de poner en riesgo la seguridad de los usuarios, los dispositivos IoT están siendo utilizados por los ciberdelincuentes para formar una botnet que está formado un conjunto de dispositivos controlados por ellos para llevar a cabo ataques tales como **spam, lanzamiento de ataques de denegación distribuida de servicio** o DDoS, distribución de malware y otros[59].

Se estima que la cifra de dispositivos que estarán conectados a internet seguirá creciendo hasta llegar en 2030 a los 125.000 millones de dispositivos en comparación con los 27.000 millones de 2017[60].

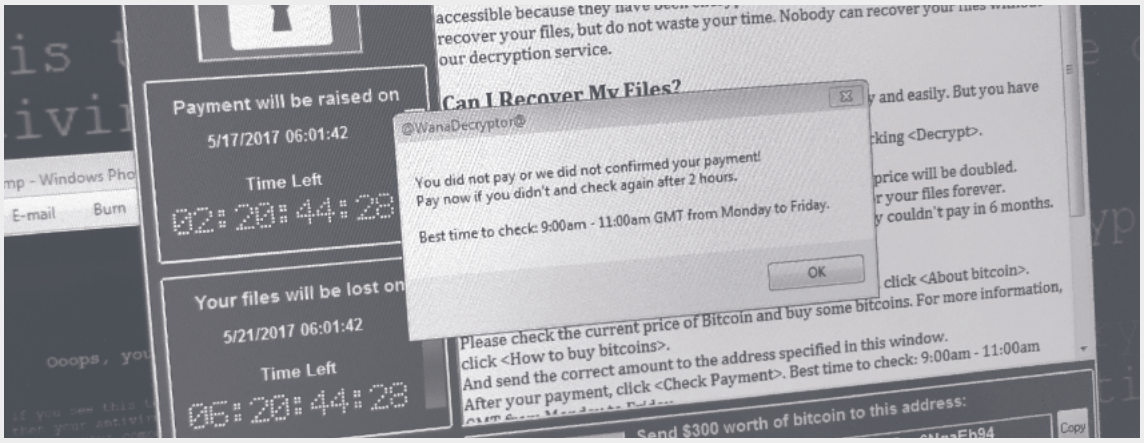
[57] https://www.welivesecurity.com/la-es/2021/12/20/ransomware-2021-datos-ataques-grupos-mas-activos/
[58] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html
[59] https://www.incibe.es/protege-tu-empresa/tematicas/iot
[60] https://www.europarl.europa.eu/news/es/headlines/priorities/transformacion-digital/20211008STO14521/por-que-hay-que-reforzar-la-ciberseguridad-de-la-ue

Código dañino avanzado

En el caso del código dañino, se están observando nuevas técnicas y amenazas que están desembocando en un mayor nivel de avance y sofisticación en los ataques. Los grupos de ciberdelincuentes se sirven de situaciones de riesgo para aprovechar y realizar ataques como, por ejemplo, la pandemia por Covid-19 y el desarrollo de vacunas. Las vulnerabilidades están siendo utilizadas por parte de los ciberdelicuentes para explotarlas antes de que salgan los posibles parches. Una de las tendencias observadas en los últimos meses es la del **aumento de desarrollo de malware en .NET.** Uno de los motivos de esto es el poco conocimiento por parte de las soluciones de seguridad para detectar código malicioso que se haya desarrollado en este lenguaje[61].

Ataques sistemas remotos

Con la pandemia de Covid-19, muchas instituciones y empresas han adoptado el teletrabajo, lo cual incluye el acceso remoto a sistemas y datos sensibles de las organizaciones. Como anteriormente se ha mencionado, los ciberdelincuentes aprovechan las circustancias, especialmente, si son críticas para sacarle la mayor rentabilidad a un posible ataque. Debido a la manera inesperada con la que llegó la pandemia del Covid-19, muchas empresas e instituciones tuvieron que adaptarse a la situación a marchas forzadas habilitando infraestructuras de acceso remoto no auditadas ni bastionadas correctamente. Por tanto, debido a la descentralización del trabajo y el surgimiento de las vulnerabilidades asociadas al mismo, se han intensificado los ataques a sistemas remotos[62]. A pesar de que por parte de las empresas se promueve el **doble factor de autentificación** para limitar posibles ataques, los actores maliciosos están desarrollando nuevas técnicas para poder burlar este mecanismo[63].



[61] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html
[62] https://www.imf.org/-/media/Files/Publications/Covid19-special-notes/Spanish/sp-special-series-on-Covid-19-cybersecurity-of-remote-work-during-pandemic.ashx
[63] https://www.forbes.com/sites/forbestechcouncil/2020/08/21/how-threat-actors-are-bypassing-two-factor-authentication-for-privileged-access/?sh=2818e1da649e

5.2. Ciberseguridad por sectores

El aumento de los ciberataques tras la llegada de la pandemia fue exponencial, de manera que, mientras en 2020 un 37% de empresas se vieron infectadas por estos ataques, en 2021 la cifra aumentaba al 66%. Esta cifra alcanzó hasta el 71% en el caso de países como España [64], 75% Ecuador, 71% Perú, 60% Panamá, 43% Guatemala y 29% Venezuela[65].

Educación

El sector educativo ha sido, con el estallido de la pandemia, el más atacado por los ciberdelincuentes. Esto ha sido principalmente, porque antes del Covid-19 la mayor parte de las clases eran impartidas de manera presencial siendo, las clases online, minoritarias dentro del panorama internacional [66]. Una de las amenazas principales que ha sufrido este sector ha sido el ransomware. El día 11 de octubre de 2021 tuvo lugar un ciberataque contra la Universidad de Barcelona que dejó inutilizados durante 30 días sus sistemas informáticos. El responsable del ataque fue 'PYSA', cuyos ciberdelincuentes pidieron 60 bitcoins (3,5 millones de euros) para descifrar y no distribuir las 650.000 carpetas y ficheros[67]. El 24 de febrero de 2022 algunas universidades españolas fueron atacadas con motivo de la guerra entre Rusia y Ucrania. La Universidad Oberta de Cataluña sufrió un ciberataque el día 3 de enero de 2022 con motivo del cierre de semestre y coincidiendo con la mayor actividad de la universidad en su campus virtual. Al igual que en el caso de la UAB, los ciberdelincuentes atacaron con un ransomware la universidad para, posteriormente, pedir un rescate para permitir la reanudación de la actividad de sus sistemas. El Govern se comprometió a dar 3,5 millones de euros a la Universidad

[64] https://cybersecuritynews.es/media-retail-y-energy-fueron-los-sectores-mas-afectados-por-ramsomware-en-2021/
[65] https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/
[66] https://cso.computerworld.es/cibercrimen/el-sector-educativo-acosado-por-los-ciberataques-en-2021
[67] https://es.ara.cat/sociedad/autores-ciberataque-uab-amenazan-publicar-informacion_1_4177249.html

para la recuperación de daños de la institución[68]. El 24 de febrero de 2022 la Universidad de Oviedo sufrió un ataque de denegación de servicio (DDoS) realizando múltiples inicios de sesión que, como resultado, provocaron el colapso de su sistema. En este caso, el ciberataque se cree que pudo haber sido perpetrado por actores rusos al observar un gran número de tráfico proveniente desde el citado país[69]. Si bien es cierto que la actuación por parte de las universidades fue rápida, se cometieron algunos errores, como fue en el caso de la UAB, que apagaron las máquinas en vez de desconectarlas que hubiera sido lo correcto en ese caso[70]. A raíz de estos ataques, se ha fomentado la **formación de ciberseguridad entre los empleados** y se han realizado algunos cambios en la operativa como segmentar los servicios dentro de la institución con el fin de minimizar los posibles riesgos de un ciberataque. En Latinoamérica también se han reportado casos de **ciberataques contra universidades** como el que tuvo lugar el 27 de junio de 2021 contra la Universidad El Bosque de Colombia que no sólo afectó a su cuenta de Twitter, sino también a otros sistemas informáticos como los correos institucionales[71].

Sanidad e investigación

Uno de los sectores críticos más amenazados por los ciberataques tras la pandemia ha sido el de la Sanidad. En el caso de España, se considera que ha sido el **tercer país en recibir más ataques en el sector sanitario** por detrás de Canadá, que ha reportado un incremento en los ataques del 250%, y Alemania, con un 220% más. Respecto a regiones, en Europa Central los incidentes han crecido un 145%, Asia Central 137% y América Latina un 117%.[72]

Una de las razones por las cuales el sector sanitario es tan sensible a posibles ataques es por el **alto número de dispositivos que pueden servir como vector para un posible ciberataque.** En el caso de los equipos de mamografía, que son administrados por un ordenador a través de un firmware, el hacker únicamente necesitaría una contraseña para reprogramar la máquina. Los dispositivos cardíacos contienen numerosas vulnerabilidades debido a que, en muchas ocasiones, los proveedores compran componentes software o hardware a terceros. Las máquinas de imágenes por resonancia magnética resultan fácil de ser atacadas porque muchas mantienen sus contraseñas predeterminadas. En el caso de los desfibriladores implantados y las bombas de insulina también contienen vulnerabilidades que pueden ser utilizadas por los atacantes[73]. Una mala instrumentalización de los citados dispositivos por parte de actores maliciosos podrían desembocar en pérdidas de vidas humanas. Al respecto, se han notificado el **fallecimiento de dos personas que pueden encontrarse vinculados con ciberataques**[74].

Incluso antes de la pandemia, las instituciones sanitarias era un objetivo lucrativo para los ciberdelincuentes. Una prueba de esto, fue el ataque al Sistema Nacional de Salud (NHS) del

[68] https://www.elperiodico.com/es/sociedad/20220102/uoc-ciberataque-impide-acceso-campus-virtual-13051750
[69] https://www.lavozdeasturias.es/noticia/asturias/2022/02/26/universidad-oviedo-afectada-ciberataque-procedente-rusia/00031645877244831842414.htm
[70] https://www.ull.es/portal/noticias/2022/universidades-exponen-casos-de-ciber-ataques/
[71] https://www.eltiempo.com/vida/educacion/universidad-el-bosque-sufre-ataque-informatico-599303
[72] https://cso.computerworld.es/cibercrimen/el-sector-sanitario-espanol-el-tercero-mas-atacado-del-mundo-en-los-ultimos-meses
[73] https://www.consalud.es/saludigital/292/sector-sanitario-enfrenta-ciberataques-plena-escalada-amenazas_112231_102.html
[74] https://www.businessinsider.es/bebe-muere-ciberataque-hospital-nacia-941145

Reino Unido durante el 2017[75]. Según se pudo saber, al menos los ordenadores y dispositivos de 16 hospitales de Londres, Nottingham, Heredforshire, Blackburn y Cumbria fueron infectados por el ransomware Wannacry.[76] El coste del impacto de este ataque fue estimado en más de 90 millones de libras[77]. El 14 de mayo de 2021, el Health Service Executive (HSE) de Irlanda fue atacado por el ransomware Conti después de que un empleado abriera un documento excel malicioso recibido en su mail [78]. En este caso, los ciberdelincuentes consiguieron pasar desapercibidos durante ocho semanas en las que estuvieron recopilando información sensible hasta que se detectó lo que estaba ocurriendo. La recuperación tras el ataque duró más de cuatro meses y se estima que se invirtieron más de 600 millones de dólares en la misma[79]. Respecto la situación en España, entre 2020 y 2021, se tiene constancia de más de 3.300 incidentes de seguridad en el sector. Por parte del Estado Español, se ha compartido con la Comisión Europea la necesidad de destinar más fondos para la lucha contra los ciberataques dirigidos hacia sector sanitario e investigación[80]. Esto ha tenido lugar como consecuencia del ataque ransomware contra el Consejo Superior de Investigaciones Científicas (CSIC) de España perpetrado el 16 de julio que fue reivindicado por ViceSociety. Durante dos días los 149 institutos que componen esta institución estuvieron inoperativos. Al igual que en otros ataques de este mismo tipo, los ciberdelincuentes han cifrado muchos archivos del CSIC para pedir un rescate. Posteriormente y al no recibir pago del rescate, **compartieron en la Dark Web los datos de carácter sensible** que han conseguido sustraer[81].

[75] https://cybersecuritynews.es/protegiendo-la-sanidad-una-revision-del-estado-de-la-ciberseguridad-en-el-sector-sanitario/
[76] https://elpais.com/tecnologia/2017/05/12/actualidad/1494602389_458942.html
[77] https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled
[78] https://www.irishtimes.com/news/crime-and-law/opening-of-email-attachment-led-to-hse-cyber-attack-report-finds-1.4752043
[79] https://www.scmagazine.com/analysis/ransomware/ransomware-post-mortem-ireland-hse-cyberattack-recovery-dogged-by-missteps
[80] https://isanidad.com/223193/el-problema-de-los-ciberataques-a-los-centros-sanitarios-llega-al-parlamento-europeo/
[81] https://cronicaglobal.elespanol.com/creacion/vida-tecky/banda-vice-society-reivindica-ciberataque-csic_709124_102.html

Finanzas

El sistema financiero, al igual que el resto de sectores, ha notado el aumento de ciberataques contra sus infraestructuras y clientes en los últimos años. Una de las razones de esto ha sido la irrupción del Covid-19 en el panorama internacional y, por tanto, el cambio a marchas forzadas hacia lo digital. Otra, de las principales, la especifidad del sector de contar con el uso de banca online. Asimismo, la ciudadanía ha resultado especialmente damnificada con el crecimiento de estafas en el sector. A través de técnicas de phishing, los ciberdelincuentes obtienen **información confidencial de los clientes así como números de cuenta y contraseña** que desembocan en transferencias fraudulentas de dinero y suplantación de números de tarjeta[82]. En muchas ocasiones, tras la obtención de información sensible, tiene lugar una llamada de voz fraudulenta con el fin de conseguir el token o la clave SMS del usuario en lo que se denomina 'vishing' que es la mezcla entre 'voice' y 'phishing'[83]. Así como se utilizan las llamadas de voz, también se utilizan los sms en lo que se denomina como 'smishing' que tratan, mediante SMS o WhatsApp, recopilar información de la víctima o compartirles URLs a webs fraudulentas[84].

En España se destacó durante el 2020, el ataque de la familia de troyanos bancarios 'Grandoreiro' a 22 entidades bancarias[85]. La campaña utilizaba vídeos con temas de coronavirus enviados a través de mensajes de spam para que, mediante el engaño, los remitentes abrieran una URL. Una vez los usuarios se encontraban en la página, se les ofrecía la opción de descarga de un archivo .MSI que en realidad era el cargador de Malware. Una vez se encontraba la descarga realizada, el Malware enviaba información sobre la máquina y la posibilidad de acceso remoto cuando la víctima accedía a una web bancaria[86]. En enero de 2021, tuvo lugar la publicación del data leak de 10.000 cuentas de American Express de Mexico en un foro de internet. Según la intencionalidad de la misma, únicamente se compartió la información para que aquellos que la compraran pudieran realizar marketing. Llegaron a asegurar también que tenían en su poder información de otros bancos como Santander o Banamex[87].

Durante ese mismo año, uno de los bancos más importantes de Ecuador, el Banco Pichincha, llegó a sufrir hasta dos ciberataques en el mismo año. El primero, en febrero, cuando 'Hotarus group' publicó la filtración de datos tanto de clientes como de empleados de este banco. Unos meses después, en octubre, se produjo otro cibertaque que dejó como resultado la inoperatividad de la banca online, la aplicación móvil, la página web, etc[88].

Industria

Durante el mes de mayo de 2021 tuvo lugar un ciberataque contra la empresa 'Colonial Pipeline' llegándose a considerar una amenaza contra la seguridad nacional de Estados Unidos. El oleoducto comprende más de 8.000 kilómetros de tuberías que comienzan en Texas y terminan en Nueva Jersey suministrando casi la mitad de combustible de la Costa Oeste de EEUU[89]. El

[82] https://www.tendencias.kpmg.es/2014/06/ciberamenazas-en-el-sector-bancario-espanol/
[83] https://www.20minutos.es/tecnologia/ciberseguridad/phishing-smishing-vishing-y-spoofing-que-son-y-por-que-debemos-preocuparnos-5023735/
[84] https://www.bbva.com/es/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/
[85] https://www.ituser.es/seguridad/2021/05/un-troyano-ataca-a-22-entidades-bancarias-espanolas
[86] https://www.itdigitalsecurity.es/actualidad/2020/04/el-malware-bancario-grandoreiro-ataca-a-usuarios-espanoles
[87] https://www.bleepingcomputer.com/news/security/hacker-posts-data-of-10-000-american-express-accounts-for-free/
[88] https://securityaffairs.co/wordpress/123465/cyber-crime/ecuadors-banco-pichincha-cyberattack.html
[89] https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

ataque constó de varias fases y se cree que los ciberatacantes conocidos como DarkSide pudieron haber penetrado dentro de los sistemas unos meses antes sin que nadie hubiera tenido constancia de ello. Previamente, en febrero de ese mismo año, el acceso de un hacker a los sistemas de agua de la ciudad de Florida pudo haber causado un grave impacto. En concreto, se pretendió **programar el vertido de un producto químico en las aguas potables de la ciudad** que fue evitado por un empleado que pudo parar el ataque antes de tiempo[90].

En el caso del ataque a Colonial Pipeline, se cree que pudo haber sido la filtración de una contraseña VPN lo que propició el ciberataque y que, debido al uso de la misma contraseña para varios accesos, se pudieron comprometer las cuentas[91]. Se llegaron a robar alrededor de 100 gigabytes que, posteriormente, fueron utilizados para realizar el ataque ransowmare que afectó a diversos departamentos de la empresa. La finalidad de los atacantes no era la de comprometer la economía sino **obtener un beneficio económico a través de la extorsión.** No obstante, la difusión de noticias falsas provocó que la empresa decidiera desconectar el oleoducto desencadenando, de esta manera, el pánico entre la población. La imagen de ciudadanos americanos realizando colas por la obtención de gasolina generaba una imagen negativa en el exterior que, unido al miedo a consecuencias mayores, hizo intervenir al Presidente Joe Biden. Junto con el cierre de los oleoductos, otro de los grandes errores cometidos tras el ataque, fue el hecho de pagar los 5 millones de dólares que pedían los rescatadores, lo cual no impidió que se descrifraran muchos de los archivos ni que el sistema reanudara su normal funcionamiento. Muchos expertos en materia de ciberseguridad consideran que, en caso de haber tenido separada la operativa diaria de los sistemas informáticos de la empresa, no se hubiera producido la disrupción en el servicio que tuvo lugar tras el ataque[92].

[90] https://www.bbc.com/news/technology-57063636
[91] https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know#:~:text=The%20pipeline's%20operational%20technology%20systems,within%20a%20two%2Dhour%20window.
[92] https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html

Otros sectores

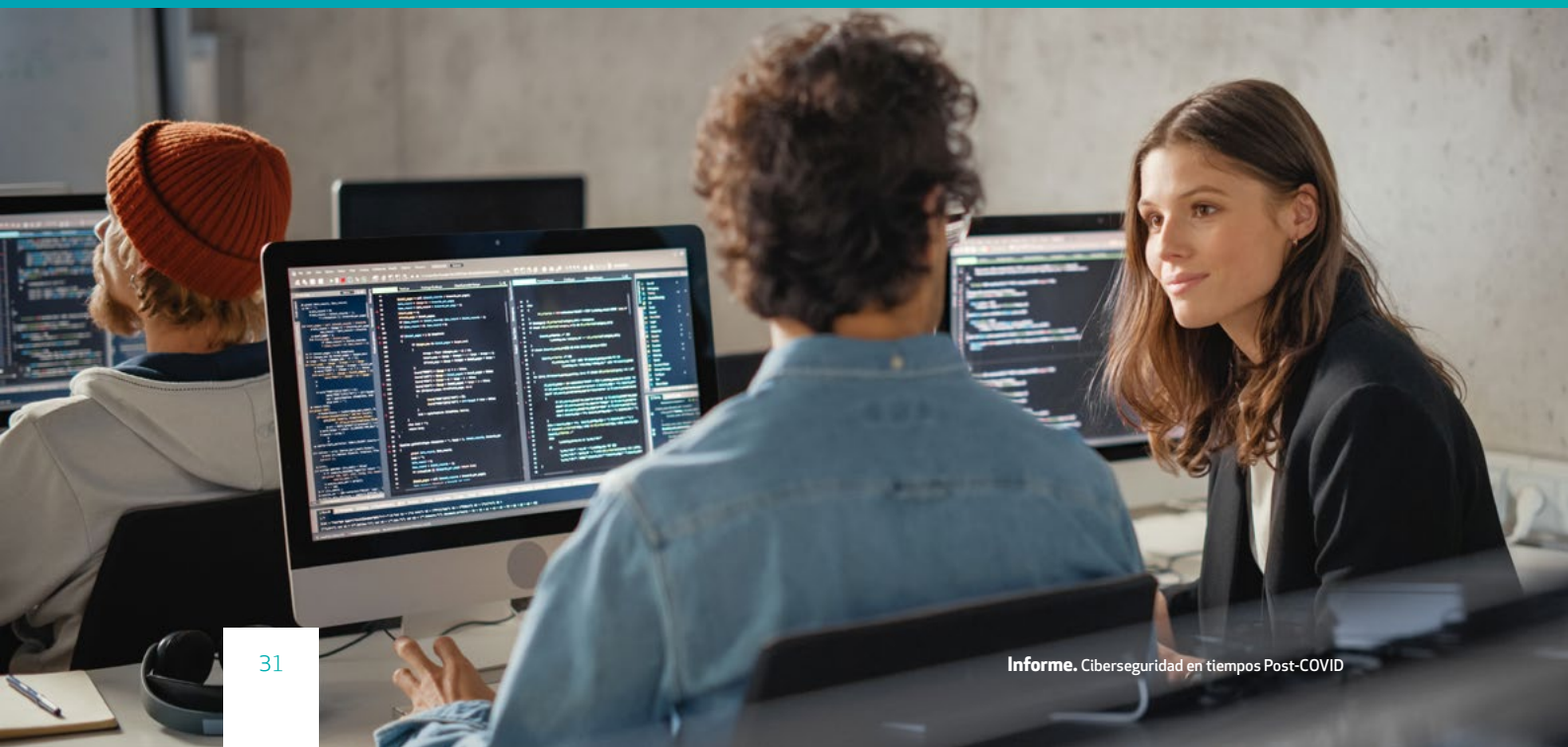
En la actualidad, ni las empresas dedicadas al sector IT se encuentran exentas de recibir un ataque. Uno de los casos más sonados por su complejidad, fue el que tuvo lugar el 13 de diciembre de 2020 contra la empresa estadounidense SolarWinds, dedicada al desarrollo de software e infraestructura de redes. La autoría del ataque fue reclamada por Cozy Bear también conocidos como APT29, de origen ruso. Los hackers instalaban el malware Surbunst en Orion permitiendo el acceso a la información de más de 18.000 clientes. Al igual que en el caso de otros ataques, pudo identificarse mala praxis en esta empresa como **el uso de contraseñas débiles en sus servidores o ausencia de protocolos de ciberseguridad**[93].

En el mes de julio de 2021, Microsoft advirtió sobre la existencia de una campaña de ciberataques específicamente dirigidos contra compañías aéreas y de viajes. Los ciberatacantes querían robar credenciales, hacer capturas de pantalla y de webcams y extraer información a través de 'Spear Phishing'[94]. Esta técnica es cada vez más utilizada entre los delincuentes y se basa en una **estafa de correo electrónico o comunicaciones dirigida contra personas u organizaciones específicos.** Aunque mayormente el objetivo es robar datos para fines delicitivos, los cibercriminales también pueden intentar instalar malware en el ordenador de la víctima.

[93] https://es.digitaltrends.com/computadoras/que-es-ataque-solarwinds/
[94] https://www.watchguard.com/es/wgrd-news/blog/troyanos-de-acceso-remoto-rats-que-amenazan-al-sector-aereo

CAP.06

Talento: escasez de perfiles vs demanda en España y Latinoamérica



Según la Oficina de Estadísticas Laborales de EEUU se prevee que el analista de seguridad de la información será la **décima ocupación que más crecerá en la próxima década.** La estimación de la tasa de crecimiento del empleo es del 31% mientras que la tasa promedio del resto de las ocupaciones es de un 4%[95]. Aunque a nivel global la necesidad de profesionales se ha reducido notablemente en el último pasando de 3,12 millones a 2,72 millones, la brecha aún sigue siendo notable[96]

En España, durante el 2021 se alcanzó la cifra de 149.774 trabajadores que se dedicaban a la ciberseguridad siendo de 24.119 la brecha de talento. Según estimaciones realizadas por parte del Instituto Nacional de Ciberseguridad (INCIBE) y el Observatorio Nacional de Tecnología y Sociedad, el mayor reto por parte de las distintas instituciones es atraer y retener talento en el sector de ciberseguridad.

Al menos, **2 de cada 10 profesionales de la ciberseguridad no han recibido la formación adecuada para el desempeño de su trabajo en el sector**[97]. Alrededor del 40,1% de las organizaciones confiesan reciclar talento con el uso de profesionales de otros departamentos para introducirlos en ciberseguridad, para lo cual en muchas ocasiones, no tienen la formación específica necesaria [98] En la actualidad hay alrededor de 1**20.000 puestos tecnológicos en España sin cubrir,** estando muchos de ellos relacionados con la ciberseguridad. Este dato, conlleva atractivos sueldos ofrecidos dentro del sector de la ciberseguridad que, en las grandes empresas, oscilan entre los 25.000 y 60.000. En las pymes, aunque la cifra pueda disminuir, los sueldos siguen siendo igual de competitivos ya que los profesionales son imprescindibles para disminuir los posibles riesgos de un ciberataque[99]. El informe 'Análisis y diagnóstico del talento de ciberseguridad en España' elaborado por ObervaCiber determinó que durante el 2021 había un déficit de 24.119 empleados lo que se traduce en un 16%. La cifra, continúa en aumento llegando durante el 2022 a los 63.191 especialistas en ciberseguridad. Se estima que durante el 2024 la cifra llegará hasta los 83.000 lo que supondrá un gran reto a la hora de atraer y retener talento[100].

En Latinoamerica la necesidad de profesionales está incrementando al igual que en el resto del mundo. El cibercrimen le cuesta 90.000 millones de dólares a América Latina de los cuales los países más afectados están siendo Brasil y México seguidos por Colombia, Argentina y Perú. Ante estas amenazas, se requieren perfiles que no sólo prevengan, monitoricen y anticipen ataques, sino también, que tengan los **conocimientos suficientes para interpretar y analizar los datos recolectados** que son claves para la toma de decisiones[101]. De acuerdo con algunos informes, el 70% de las empresas ha indicado haber sufrido de una a cuatro brechas de seguridad en los últimos dos años cuyo impacto se ha llegado a traducir en 1 millón de dólares

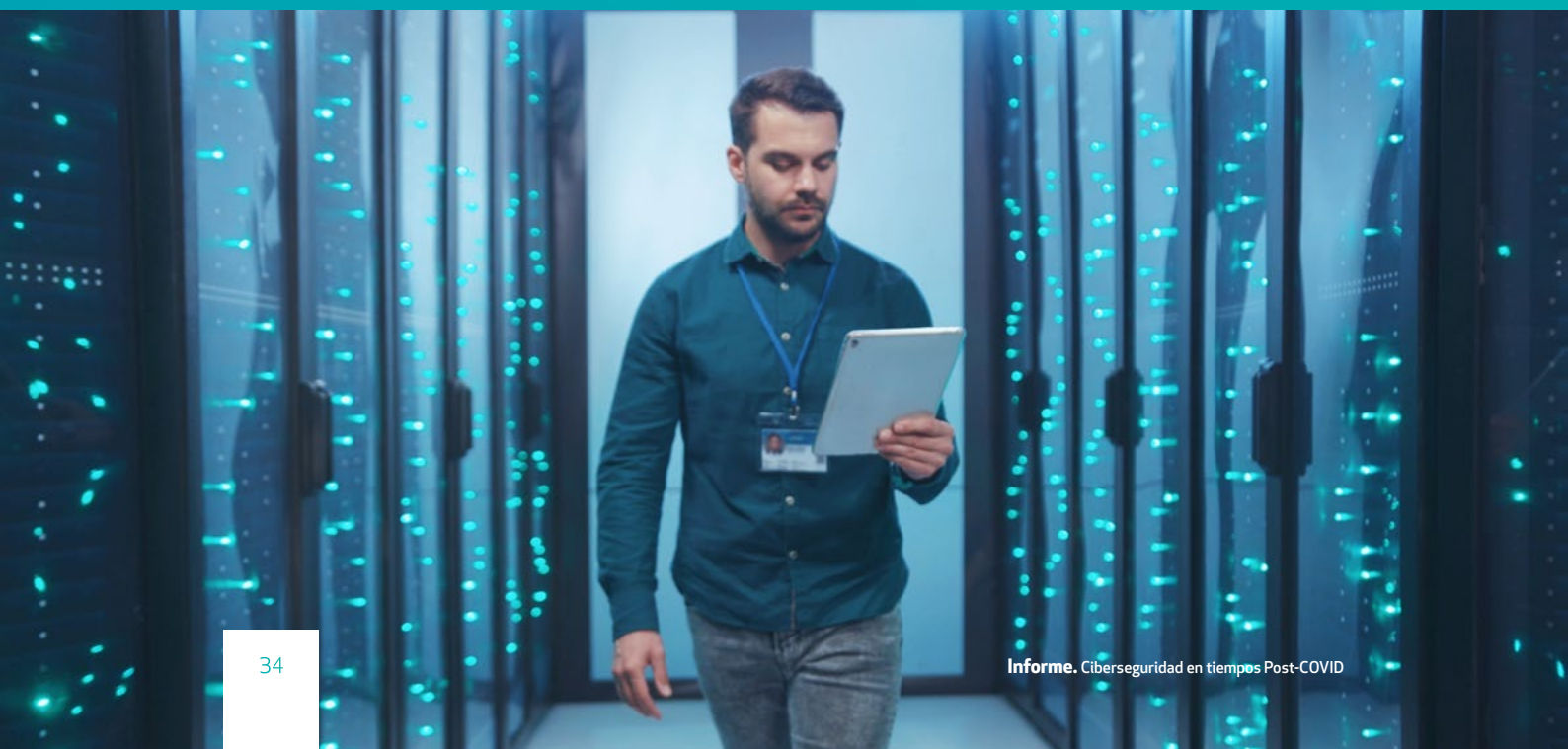
[95] https://cnnespanol.cnn.com/2021/05/30/se-busca-millones-expertos-ciberseguridad-salario-trax/
[96] https://www.estrategiaynegocios.net/tecnologia-cultura-digital/fortinet-escasez-de-profesionales-en-ciberseguridad-pone-en-riesgo-a-las-empresas-BM7925355
[97] https://www.channelpartner.es/seguridad/noticias/1131831002502/faltan-84000-profesionales-de-ciberseguridad-espana-segun-incibe.1.html
[98] https://www.lavanguardia.com/economia/20220401/8161871/espana-deficit-expertos-ciberseguridad-demanda-sigue-aumentando-nuclio-brl.html#:~:text=El%20informe%20An%C3%A1lisis%20y%20diagn%C3%B3stico,brecha%20que%20seguir%C3%A1%20en%20aumento.
[99] https://www.20minutos.es/tecnologia/emprendimiento/existe-escasez-de-talento-tecnologico-en-espana-los-especialistas-no-cubren-ni-el-25-de-la-oferta-actual-5053732/
[100] https://www.lavanguardia.com/economia/20220401/8161871/espana-deficit-expertos-ciberseguridad-demanda-sigue-aumentando-nuclio-brl.html#:~:text=El%20informe%20An%C3%A1lisis%20y%20diagn%C3%B3stico,brecha%20que%20seguir%C3%A1%20en%20aumento.
[101] https://forbes.co/2022/07/14/capital-humano/se-acabo-la-especializacion-la-demanda-de-perfiles-hibridos-se-acelera-en-latinoamerica%EF%BF%BC/

para sus negocios. Uno de los motivos principales de este alto impacto en los ataques tiene que ver con la falta de habilidades en ciberseguridad. La brecha de habilidades en el sector se ha convertido en los últimos tiempos en una de las principales preocupaciones de los ejecutivos y las juntas directivas de las empresas latinoamericanas y de países de otras regiones[102]. Según el Cyber Workforce Report de 2021 de (ISC)2, el número de empleados y expertos en materia necesita **crecer al menos un 65% para cubrir los posibles riesgos** a los que todos los países del mundo se están enfrentando. En el caso de LATAM, esto se traduce en la necesidad de 701.000 profesionales [103].

[102] https://www.estrategiaynegocios.net/tecnologia-cultura-digital/fortinet-escasez-de-profesionales-en-ciberseguridad-pone-en-riesgo-a-las-empresas-BM7925355
[103] https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

CAP.07

Conclusiones



Desde la creación del primer virus informático conocido como 'Creeper' han ido surgiendo y aumentando las ciberamenazas. Por ello, tanto las empresas como la Administración Pública se han tenido que adaptar a las nuevas tendencias para evitar, en la medida de lo posible, las ciberamenazas. Actualmente, el aumento del uso de nuevas tecnologías como IoT han **aumentado la sofisticación de los ataques.**

Asimismo, se ha tenido que legislar, partiendo de 0, sobre nuevos retos que han surgido derivados del desarrollo tecnológico que han provocado el aumento de riesgos en materia de ciberseguridad. A raíz del surgimiento de la pandemia por Covid-19 se han intensificado las amenazas en el ciberespacio consiguiéndose, en muchas ocasiones, incluso a afectar al mundo físico hasta el punto de causar muertes (como se cree que ha sido el caso de los ciberataques contra algunos hospitales). Por ello, todos los sectores están expuestos a posibles ciberincidentes que únicamente pueden ser paliados con la **incorporación de profesionales que sepan de ciberseguridad.**

Aunque los ciberataques afectan a todo el mundo, las tendencias detectadas han sido diferentes dependiendo de la región así como se han podido identificar algunos países que han sufrido más ataques de ciberdelincuentes. La tipología de los ciberincidentes también han variado entre regiones aunque se han encontrado coincidencias entre territorios. Tras los ataques, además de que se sigue aumentando la sofisticación de los mismos se descubren **nuevos métodos que son explotados por los ciberdelincuentes.** A pesar de ello, en muchas ocasiones los atacantes aprovechan simples detalles como la **falta de actualización de los sistemas** para llevar a cabo su intrusión en las instituciones tanto de ámbito público como privado. Además, la **falta de cultura de ciberseguridad** hace que los empleados no estén alineados con la estrategia de la empresa y que, en muchas ocasiones, también sirvan como vectores de ataque.

Por todo lo anterior, la experiencia en ciberataques tiene que servir como ejemplo para el resto de profesionales que deben aprender de este tipo de incidentes y tratar de evitarlos en la medida de lo posible. Estos mismos empleados, tienen que encontrarse actualizados con formaciones de ciberseguridad y seguir los **protocolos determinados por las empresas**. Por su parte, los responsables de las empresas que lleven a cabo la estrategia de ciberseguridad, tienen que **actualizarse constantemente para estar al día de las nuevas tendencias.** Cuando tiene lugar un incidente de este tipo, las pérdidas económicas por parte de las empresas afectadas pueden llevar incluso a la quiebra a las organizaciones por lo que es imprescindible **minimizar los posibles riesgos** y contar con los mejores profesionales del sector que ayuden a ello.

inesdi Digital Business School Madrid Barcelona Online

THREEPOINTS THE SCHOOL FOR DIGITAL BUSINESS

Digital Innovation Learning Hub

Planeta Formación y Universidades