Documento
Opinión

20/2023 27 de febrero de 2023

David Corral Hernández *

Ciberdaños en los medios de comunicación

Ciberdaños en los medios de comunicación

Resumen:

En un mundo cada vez más digital y conectado los ciberataques tienen el entorno idóneo para demostrar la potencialidad de sus riesgos y la realidad, creciente en impacto y protagonismo, de los efectos de su acción. Anular, alterar, dañar, secuestrar, robar, suplantar, confundir, extorsionar… son múltiples las posibilidades, y en demasiadas ocasiones baratas y complicadas de atribuir, pero son aún peores los daños que causan en infraestructuras esenciales, en servicios, en sistemas financieros o de defensa, en la estabilidad de gobiernos y sociedades, como también en las empresas y profesionales de los medios de comunicación públicos y privados. Muy vinculados a la desinformación y a los conflictos híbridos, su paso no solo deja daños en la actividad, imagen o ingresos de los medios, también, aunque pase muy desapercibido, a la libre difusión de información y, sobre todo, por el posible daño que suponen para los sistemas democráticos por la denegación o alteración de información, contenidos o servicios imparciales y veraces. Con el constante aumento de las amenazas externas e internas a las democracias europeas, y a las instituciones que las sustentan, es cada vez más importante proteger el pluralismo y la independencia de los medios de comunicación de injerencias indeseadas y garantizar la libertad de expresión, cuestiones clave para asegurar el normal funcionamiento democrático y la libertad de los ciudadanos.

Palabras clave:

Cíber, medios de comunicación, democracia, derechos, desinformación.

Cyberdamages in the media

Abstract:

In an increasingly digital and connected world, cyber-attacks have the ideal environment to demonstrate the potential of their risks and the reality, growing in impact and prominence, of the effects of their action. To annul, alter, damage, hijack, steal, confuse, extort... there are multiple possibilities, and too often cheap and complicated to attribute, but even worse are the damages they cause to essential infrastructures, services, financial or defence systems, to the stability of governments and societies, as well as to companies and public and private media professionals. Closely linked to disinformation and hybrid conflicts, they not only damage the activity, image or income of the media, but also, although it may go unnoticed, the free dissemination of information and, above all, the potential damage to democratic systems through the denial or alteration of impartial and truthful information, content or services. With the constant increase in external and internal threats to European democracies, and to the institutions that sustain them, it is increasingly important to protect pluralism and the independence of the media from unwanted interference and to guarantee freedom of expression, key issues to ensure the normal democratic functioning and freedom of citizens.

Keywords:

Cyber. Media. Democracy. Rights. Disinformation.

Cómo citar este documento:

CORRAL HERNÁNDEZ, David. *Ciberdaños en los medios de comunicación*. Documento de Opinión IEEE 20/2023.
https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO20_2023_DAVCOR_Medios.pdf y/o enlace bie[3] (consultado día/mes/año)

DARPA, el origen

En 1969, en plena Guerra Fría, sucedieron, entre otros, dos hechos trascendentales para el ser humano. La Misión Apolo XI de la NASA estadounidense consiguió dar, en palabras del astronauta Neil Armstrong «un pequeño paso para un hombre, un gran salto para la humanidad», al convertirse en la primera persona en la historia en poner pie fuera de la Tierra dejando su huella en la Luna. Y a miles de kilómetros de distancia, en nuestro planeta, la Agencia de Proyectos de Investigación Avanzada del Pentágono enviaba y recibía un sencillo mensaje en una de las primeras redes informáticas, ARPANET. Fue otro pequeño paso, pero supuso el origen de Internet y de la revolución digital que, desde entonces, ha transformado el mundo, la economía y nuestras sociedades y en la que ahora, en lo que conocemos como internet de las cosas (IoT), vivimos con más de 10.000 millones de dispositivos conectados que podrían llegar a ser cerca de 30.000 millones en 2030. Si en aquel momento la carrera era entre dos superpotencias hoy, entre los múltiples desafíos y actores globales, el control o la manipulación del mundo digital, de los datos que por él circulan, de los dispositivos que hacen que sea posible y por mantener el liderazgo tecnológico es, de todas las carreras, una de las más disputadas.

Si la Defense Advanced Research Projects Agency, DARPA, dio el pistoletazo de salida de Internet también lo dio para el primer gusano, o virus, que circuló por aquella incipiente *red*. Un inocuo mensaje: «I'm the creeper, catch me if you can!» fue lanzado en 1971 por Bob Thomas, un técnico de ARPANET, para que viajara entre ordenadores de manera autónoma dejando a su paso un inocente mensaje en la pantalla. Dos años después un compañero de Thomas, Ray Tomlinson, informático e inventor del primer sistema de correo electrónico, también lo fue del primer antivirus de la historia, un *software* llamado Reaper, la «podadora» de la «enredadera». Y aunque tecnológicamente los ciberataques parecen una cuestión reciente su origen es más antiguo y analógico. En la Francia de comienzos del siglo XIX, en la que funcionaba un internet del siglo XVIII, el sistema de telégrafo inventado por el ingeniero Claude Chappe, dos hermanos banqueros, François y Joseph Blanc, lanzaron el primer ciberataque de la historia al alterar las informaciones y datos que circulaban por este sistema de uso exclusivo del gobierno.

Durante dos años beneficiaron su economía personal al contar con información *privilegiada* de las operaciones de bonos en el mercado tras romper el sistema por el eslabón habitualmente más débil, el humano, ya que sobornaron al operador de la ciudad de Tours. Ambas acciones quedaron sin castigo judicial al no existir un marco jurídico que contemplase este tipo de intromisiones en las redes y sistemas de comunicaciones. A partir de entonces la ciberdelincuencia ha crecido exponencialmente, marcada por una incesante evolución de tácticas, técnicas y procedimientos, todos ellos aplicados con fines habitualmente poco constructivos y lícitos.

Ofensivas en ascenso

Dos siglos después de los Blanc y medio siglo después de Thomas y Tomlinson el escenario tecnológico y normativo es completamente diferente. El inocente *Creeper* ha crecido y mutado hasta convertirse en una enredadera muy tupida y cargada de amenazas. Para el Foro Económico Mundial[1], en su *Global Risks Report 2023*, la ciberseguridad se encuentra entre los 10 principales riesgos severos para los próximos 2 o 10 años, ocupando en ambos casos la octava posición por detrás de cuestiones como el cambio climático, los desastres naturales, las crisis de recursos, las grandes migraciones, la polarización política y social, etc. Las grandes transformaciones tecnológicas supondrán grandes inversiones y avances, pero el informe también considera que agravará las desigualdades, la desinformación y otros peligros directos para las sociedades como el aumento de la ciberdelincuencia, los ciberataques contra infraestructuras, servicios y bienes esenciales y críticos como la sanidad, el agua, las comunicaciones, la seguridad, etc. Operaciones que, además, aunque suceda en democracias con regulaciones fuertes, debilitarán la soberanía digital individual y el derecho a la privacidad.

Con cada progreso tecnológico, y a medida que aumenta la cantidad de datos personales disponibles, crece notablemente la preocupación por la ciberseguridad. Cualquier dispositivo o sistema conectado es susceptible de ser atacado, dañado o usado indebidamente por cualquiera de las herramientas de un catálogo que no deja de desarrollarse y aumentar con nuevas formas de explotar dispositivos, sistemas o tecnologías para romper muros y acceder a los datos. Entre los más habituales y

[1] «Global Risks Report 2023», *World economic Forum*. 11/1/23. Disponible en: https://www.weforum.org/reports/global-risks-report-2023/digest (consulta: 2/2/23).

conocidos encontramos algunos de los recogidos en el *Glosario de términos de ciberseguridad* de INCIBE[2], el Instituto Nacional de Ciberseguridad de España, una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital que es referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos, para la prestación de servicios y la coordinación con los agentes con competencias en la materia con el fin de contribuir a construir ciberseguridad a nivel nacional e internacional.

Distributed denial of service (DDoS): ataque a un sistema, aplicación o dispositivo para dejarlo fuera de servicio debido a una saturación de peticiones que se hacen desde diversos orígenes. De esta forma es más efectivo, y más complicado detener y determinar su origen. Se suelen utilizar miles de máquinas *host* infectadas con *bots* para enviar una cantidad abrumadora de tráfico de red, como mensajes de correo electrónico o solicitudes de conexión a un sistema objetivo, como el sitio web de una empresa o un servicio en línea. El objetivo es colapsar el sistema objetivo e inutilizarlo saturando sus recursos.

Bots (de «robots»): aplicaciones de *software* que ejecutan tareas automatizadas, generalmente de manera controlada, como es el control del tráfico web. Cuando son usados ilícitamente infectan ordenadores, envían información robada o *spam*, minan criptomonedas o atacan otros equipos de su red o entorno.

Malware: tipo de software malicioso que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: *malicious software*. Dentro de esta definición tiene cabida un amplio repertorio de programas maliciosos: virus, gusanos, troyanos, *backdoors*, *spyware*, etc. Los puntos en común de todos estos programas son su propagación en el disco duro o a través de una red y su carácter dañino o lesivo borrando, corrompiendo, inutilizando… datos, redes o dispositivos.

Phishing: técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio de confianza mediante un correo electrónico o mensaje (SMS o similar) para conseguir las

[2] *Glosario de términos de ciberseguridad*. INCIBE. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf (consulta: 2/2/23).

credenciales o información de la tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo.

Ransomware: *malware* cuya funcionalidad es *secuestrar* un dispositivo o la información que contiene dejando sin acceso a la víctima hasta que pague un rescate.

Clickjacking: ataques que suelen esconderse en una página web que contiene un botón que invita a pulsarse para ganar algo, como un premio o un regalo gratis. Cuando se pulsa activa un botón oculto tras una capa invisible debajo o encima del botón en pantalla que realiza una función maliciosa, como descargar *malware* en el ordenador.

Backdoors: se denomina *backdoor* o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema. Las puertas traseras pueden ser errores o fallos, o pueden haber sido creadas a propósito por los propios autores, pero al ser descubiertas por terceros pueden ser utilizadas con fines ilícitos. También se consideran puertas traseras a los programas que, una vez instalados en el ordenador de la víctima, dan el control de este de forma remota al ordenador del atacante. Aunque no son específicamente virus, pueden llegar a ser un tipo de *malware* que funciona como herramientas de control remoto. Cuentan con una codificación propia y usan cualquier servicio de Internet: correo, mensajería instantánea, http, ftp, telnet o chat.

Ingeniería social o *Social engineering*: quizá de los más preocupantes cuando se habla de usuarios y de una actividad como es la de los medios de comunicación dado que, a diferencia de la mayoría de las otras formas de ciberataques, implica la interacción humana. Son el conjunto de técnicas que los delincuentes emplean, jugando con la naturaleza social o curiosa de las personas, para engañar a los usuarios de sistemas/servicios TIC para que les faciliten datos que les aporten valor, ya sean credenciales, información sobre los sistemas, servicios instalados, información personal etc. Se basan en el engaño, el miedo, las motivaciones, los intereses…, en un perfil de la víctima que puede lograrse consultando sus redes sociales, la información que aparezca en buscadores, etc.

La digitalización forzada y el auge del teletrabajo que impulsó la pandemia, conflictos como el de Ucrania, tensiones geopolíticas entre grandes bloques, el preocupante

estado de la economía mundial… se está traduciendo en un aumento imparable de los ciberataques y de los actos de ciberdelincuencia contra personas, instituciones y países, como el que le sucedió a Costa Rica, que tuvo que declarar el estado de emergencia[3] tras sufrir un ataque masivo con el *ransomware* Hive contra organismos e instituciones por parte del grupo Conti, con base en Rusia. La guerra moderna, o los conflictos cada vez menos convencionales, comienzan a menudo con una ofensiva cibernética a gran escala y a través de diversos canales y medios, como la manipulación de la información, los ataques a las infraestructuras y servicios o a la estabilidad democrática, como en el caso de las injerencias electorales.

Según datos de la compañía Check Point Software[4], los ciberataques globales aumentaron un 38 % en 2022 con actores cada vez más ágiles que tienen en tecnologías como la IA o herramientas como ChatGPT unos aliados inmejorables para dañar la actividad, los ingresos, la cartera de clientes, la reputación o la sensación de seguridad, entre otras cuestiones, de los gobiernos, instituciones, empresas o personas atacados. La estimación recogida en el *Informe de Ciberpreparación de Hiscox 2022*[5] es de 105.655 euros de coste medio de la suma de los ciberataques sufridos por cada empresa española en 2021, casi el doble de los 54.300 euros del año anterior.

Los sistemas de detección del CCN-CERT, el Centro Criptológico Nacional (CCN), organismo adscrito al Centro Nacional de Inteligencia (CNI), han gestionado 55.695 ciberincidentes en 2022 en el sector público español, incluyendo aquellos notificados por los propios organismos, caso del CSIC, que sufrió un ataque de origen ruso con *malware* los días 16 y 17 de julio. De estos ataques los clasificados con una peligrosidad crítica ascienden a 75 y los clasificados como muy alto suman 3.749 ciberincidentes con orígenes muy variados destacando, por su peligrosidad, los patrocinados por Estados y los grupos del cibercrimen. Técnicamente, el tipo de ciberincidente más común es el

[3] «Estamos en guerra: 5 claves para entender el ciberataque que tiene a Costa Rica en estado de emergencia», *BBC.* 20/5/22. Disponible en: https://www.bbc.com/mundo/noticias-america-latina-61516874 (consulta: 2/2/23).

[4] «Check Point Software's Cybersecurity Predictions for 2023: Expect More Global Attacks, Government Regulation, and Consolidation», *Check Point.* 10/11/22. Disponible en: https://www.checkpoint.com/press-releases/check-point-softwares-cybersecurity-predictions-for-2023-expect-more-global-attacks-government-regulation-and-consolidation/ (consulta: 2/2/23).

[5] *Informe de Ciberpreparación de Hiscox 2022*. HISCOX. Disponible en: https://www.hiscox.es/sites/spain/files/2022-12/22161%20-%20Cyber%20readiness%20mini%20report%202022_SPA.pdf (consulta: 2/2/23).

contenido dañino (29 %), seguido del compromiso de información (8 %), la intrusión (8 %) y el fraude (7 %).

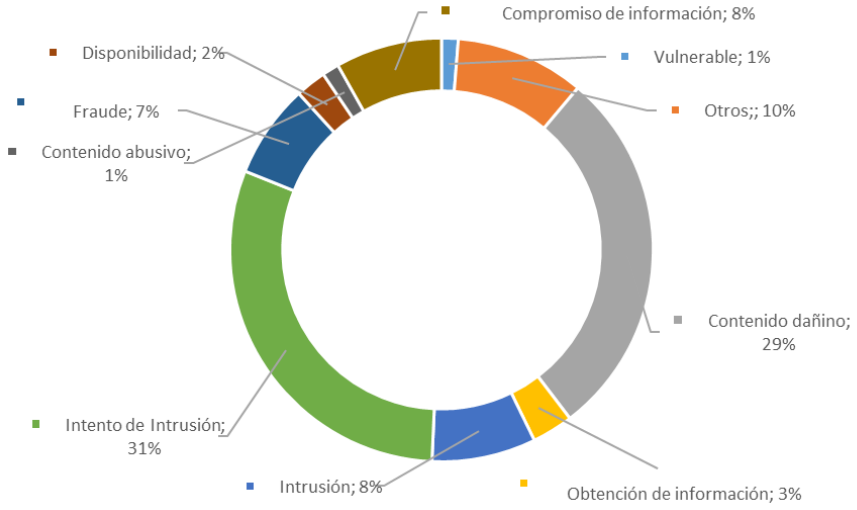

Ilustración 1. Clasificación de los incidentes gestionados por el CCN-CERT en 2022

1) Contenido dañino: troyanos, spyware*, etc.*

2) Contenido abusivo: contra la imagen.

3) Disponibilidad: daños de imagen y productividad (rendimiento).

4) Fraude: propiedad intelectual, protección de datos o suplantación de identidad (phishing).

5) Compromiso de información: acceso y exfiltración y/o borrado y publicación de información no pública.

6) Obtención de información: escaneo de redes (scanning), *análisis de paquetes* (sniffing), *ingeniería social.*

7) Intrusión: ataques dirigidos a explotar vulnerabilidades.

8) Intento de intrusión: explotación de vulnerabilidades conocidas, intento de acceso con vulneración de credenciales, ataque desconocido.

9) Vulnerable: servicios accesibles públicamente que puedan presentar criptografía débil (servidores web susceptibles de ataques), servicios accesibles públicamente que puedan emplearse para la reflexión o amplificación de ataques DDoS.

10) Otros: todo aquel incidente que no tenga cabida en ninguna categoría anterior.

En 2021 las fuerzas y cuerpos de seguridad del Estado tuvieron conocimiento de 305.477 ciberdelitos, el 15,6 % del total de las infracciones penales cometidas, es decir, uno de

cada seis delitos en España se cometió en el ciberespacio. En 2017 la cifra no llegaba a 6 %[6]. Desde su Centro de Respuesta a Incidentes de Seguridad (INCIBE-CERT), el Instituto Nacional de Ciberseguridad (INCIBE)[7], dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, gestionó 109.126 incidentes de ciberseguridad durante el año 2021. De ellos 90.168 afectaron a ciudadanos y empresas, 680 a operadores estratégicos y 18.278 a la Red Académica y de Investigación Española (RedIRIS). Por tipología el 29,88 % correspondió a *malware*, seguido de las distintas variantes de fraude con un 28,60 % y, en tercer lugar, destacan los ataques a sistemas vulnerables, con un 18,89 %.

A lo largo de 2021, según un informe de Deloitte[8] sobre el panorama de ciberseguridad en las principales organizaciones de España, el 94 % de las empresas ha sido víctima de, al menos, un incidente grave de ciberseguridad. El sector público, la sanidad, educación/investigación, y el ámbito económico y financiero han sido los más castigados. Las telecomunicaciones, los medios y la tecnología, aun no estando en cabeza, se sitúan por encima de la media y será probablemente peor en los próximos años. La Agencia de Ciberseguridad de la Unión Europea (ENISA) destaca entre las principales amenazas para 2030[9] asuntos tecnológicos como los ataques dirigidos mejorados por datos de dispositivos inteligentes, el auge de la inteligencia artificial, el aumento de amenazas híbridas avanzadas, entre otros, pero también en una lista de apenas diez puntos, las campañas de desinformación avanzada o el incremento del autoritarismo a través de la vigilancia digital y la pérdida de privacidad.

[6] «Uno de cada seis delitos en España se comete en el ciberespacio», *RTVE*. 26/10/22. Disponible en: https://www.rtve.es/noticias/20221026/aumentan-ciberdelitos-espana-ciberespacio/2407058.shtml (consulta: 2/2/23).

[7] «INCIBE gestiona más de 100.000 incidentes de ciberseguridad durante 2021», *INCIBE*. 12/05/22. Disponible en: https://www.incibe.es/sala-prensa/notas-prensa/incibe-gestiona-mas-100000-incidentes-ciberseguridad-durante-2021 (consulta: 2/2/23).

[8] «El estado de la ciberseguridad en España», *Deloitte*. Disponible en: https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html (consulta: 2/2/23).

[9] «Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride!», *ENISA*. 11/11/22. Disponible en: https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030 (consulta: 2/2/23).

Objetivo: los medios

La industria de los medios de comunicación y del entretenimiento desempeña un papel vital en la información y formación de la opinión pública de las sociedades, en la construcción de los discursos narrativos, en la proyección de los intereses y las visiones, en la definición de las agendas, en su participación como «poder blando» o, entre otras tareas, preservando, en sus archivos, la historia y memoria reciente de naciones, instituciones y personas. Los canales de comunicación y los medios de emisión y recepción son cada vez más, al igual que los actores y las tecnologías que están implicados en ellos y la diversidad de sus perfiles.

Los medios analógicos continúan trabajando en un ámbito tradicional, físico, con los medios impresos, la radio y la televisión como claros exponentes. Con la digitalización llegaron los nuevos medios al espacio *virtual* con los digitales y las redes sociales como protagonistas en un mundo en el que también destacan los *comunicadores* o *influencers* con una inmensa cantidad de seguidores, tecnologías como la *nube* o las emisiones en directo por *streaming*, el consumo bajo demanda de cualquier contenido en cualquier dispositivo, el acceso a múltiples recursos de comunicación cada vez más profesionales y baratos, etc. Pero clásicos y modernos, analógicos y digitales, nacionales e internacionales, públicos y privados, grandes y pequeños… si algo comparten, además de la actividad de comunicar, es que por ellos la desinformación intenta campar a sus anchas y que las intromisiones cibernéticas no son una simple amenaza inofensiva para empresas, profesionales o usuarios.

Los recursos o vectores de ataque y los puntos para llevarlos a cabo en toda la cadena de producción son casi incontables. *Ransomware, adware, spyware, phishing, pharming, spam, hijacking, stalkerware, exploit, worms, qrishing* (*phishing* oculto en códigos QR), las amenazas avanzadas persistentes... son distintos instrumentos diseñados para robar información privada o empresarial; datos personales o económicos de suscriptores y usuarios; nóminas de empleados o documentos confidenciales; identificar y localizar a periodistas y a sus fuentes poniendo en riesgo su integridad física; filtrar desinformación; acceder y manipular las redes de transmisión; eliminar o alterar bases de datos y archivos; usurpar la propiedad intelectual; secuestrar datos sensibles y extorsionar con su uso o devolución; ser suplantados; cometer fraudes; causar daños en los sistemas o equipos atacados; tomar el control de dispositivos (como ordenadores, teléfonos móviles,

programas de edición, cámaras, etc.); impedir el acceso a servicios o herramientas como la nube… entre otras interferencias maliciosas e ilegales que causan daños económicos, materiales, a la reputación, a la confianza de la sociedad y al papel de servicio público de los medios, a favor de la democracia, como transmisores de contenidos independientes y veraces.

Delincuentes de diversa naturaleza y distintas motivaciones han puesto a los medios en su punto de mira, entre ellos algunos españoles. Tal como se puede apreciar en la recopilación de KonBriefing Research solo los del primer semestre de 2022 duplicaron a todos los de 2021, 18, los mismos que constató la International News Media Association (INMA)[10].

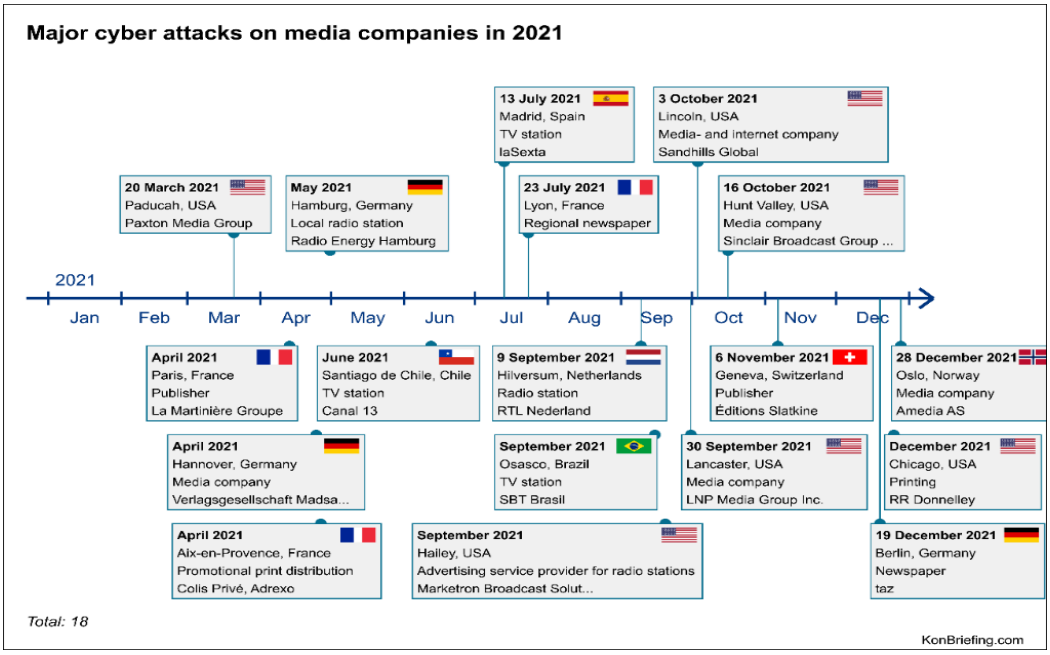

Ilustración 2. Ataques a medios en 2021. Crédito: KonBriefing Research

[10] «European media companies' share experiences of cyberattacks», *Moonshot*. 6/5/22. Disponible en: https://moonshot.news/news/media-news/european-media-companies-share-experiences-of-cyberattacks/ (consulta: 2/2/23).

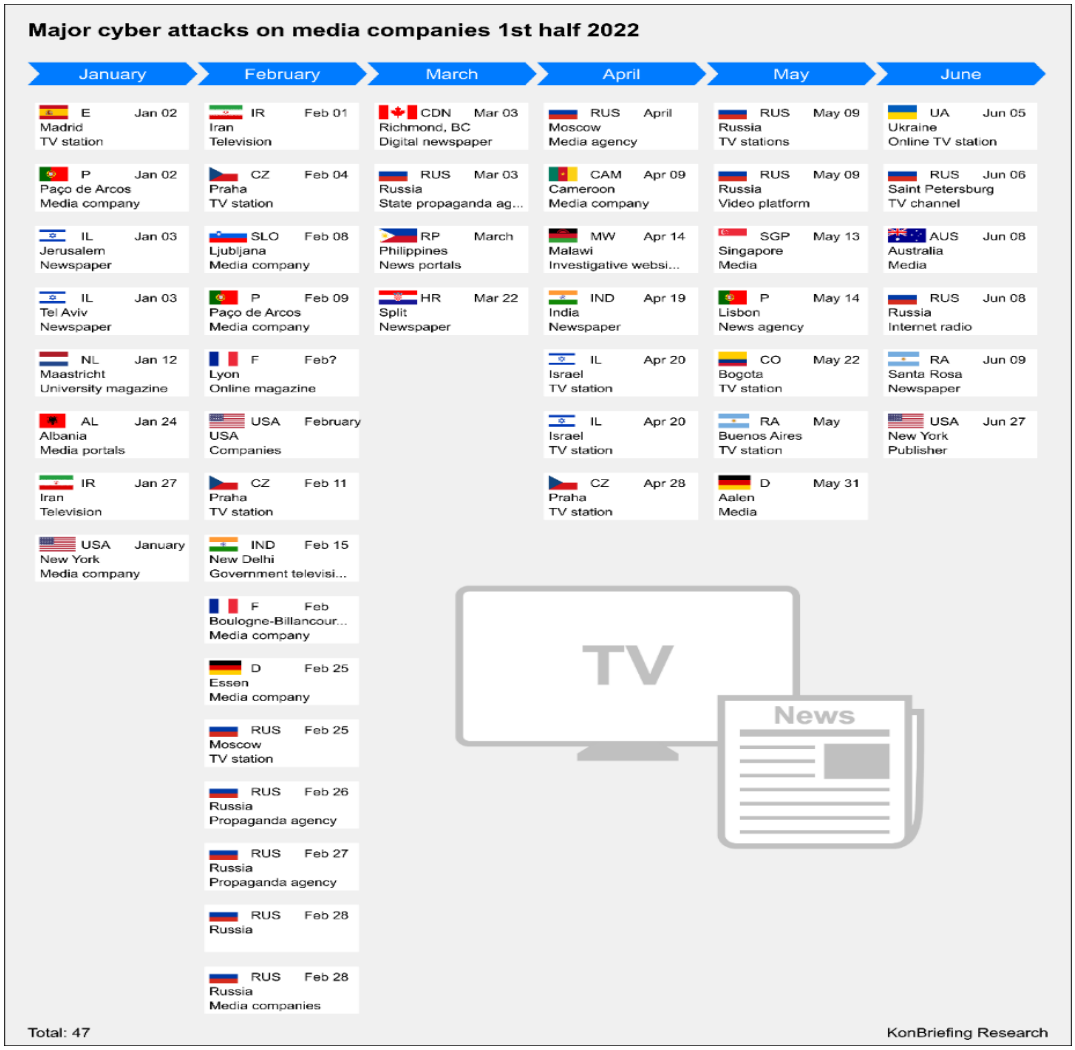

Ilustración 3. Ataques a medios en la primera mitad de 2022. Crédito: KonBriefing Research

Además de los que figuran en los gráficos, el pasado mes de abril la plataforma canadiense PressReader[11], el mayor proveedor de prensa digital a nivel mundial y que cuenta con cabeceras como *The New York Times*, *The Washington Post* o los medios de Prensa Ibérica en España, sufrió un ciberataque a sus servidores después de que fueran retirados decenas de periódicos rusos de su catálogo por la invasión de Ucrania. El bloqueo afectó a más de 7.000 publicaciones de las más importantes de todo el mundo. En diciembre[12], *The Guardian* sufrió un «ciberataque muy sofisticado que implicó el acceso no autorizado de terceros a partes de nuestra red», es decir, acceso a datos personales de la plantilla en Reino Unido. Sus periodistas, al igual que los de *Fox News*

[11] CAMARERO, José María. «Un ataque informático impide el acceso a miles de periódicos», *El Correo*. 4/3/22. Disponible en: https://www.elcorreo.com/sociedad/ataque-informatico-impide-acceso-periodicos-20220303184829-ntrc.html (consulta: 2/2/23).

[12] MILMO, Dan. «Guardian confirms it was hit by ransomware attack», *The Guardian*. 11/1/23. Disponible en: https://www.theguardian.com/media/2023/jan/11/guardian-confirms-it-was-hit-by-ransomware-attack (consulta: 2/2/23).

y otros medios, fueron víctimas de ciberespionaje entre 2021 y 2022. Un informe de Proofpoint[13] revela que recibieron ataques cibercriminales patrocinados por China, Corea del Norte, Irán y Turquía. En España los más destacados son los que afectaron a La Sexta o a la Televisión Autonómica de Castilla-La Mancha. Aunque es complicado afirmar el origen y autoría se podría decir que los fuertes vientos «llegan del Este» con el *phishing* y DDoS entre los más habituales.

Pero el ciberespionaje a los medios, como a políticos y activistas, tiene un nombre propio: Pegasus. Este *spyware*, desarrollado por la empresa tecnológica israelí NSO, infecta teléfonos móviles para tener acceso a la información personal del usuario. En teoría su venta solo está autorizada a Gobiernos y a servicios de inteligencia y seguridad oficiales, previa autorización del Ministerio de Defensa de Israel. Se estima que casi 200 periodistas de más de 20 países han sido espiados y visto comprometidos sus derechos individuales en los últimos años. El Supervisor Europeo de Protección de Datos (SEPD), distingue tres características importantes de Pegasus que le otorgan «el potencial de causar riesgos y daños sin precedentes no solo a las libertades fundamentales de las personas sino también a la democracia y el Estado de derecho». Otro sistema similar, Predator, ha sido utilizado por el Gobierno de Grecia para espiar la actividad de los periodistas en el pasado 2022[14].

La pandemia, la guerra en Ucrania y la creciente polarización han empeorado drásticamente la seguridad de los profesionales de los medios. Trabajan en condiciones cada vez más peligrosas y son objeto de ataques físicos y en línea, con oleadas de abusos en las redes sociales. Pamela Morinière, jefa del Departamento de Comunicación y Campañas de la Federación Internacional de Periodistas, destaca que uno de los principales amenazados es el pluralismo ya que «los abusos en línea conducen a la autocensura, algunas voces dejan de oírse y grandes historias mueren. Como consecuencia, el derecho del público a saber no se cumple y la democracia se resiente porque la gente no puede tomar decisiones con conocimiento de causa. En cuanto a los

[13] «Periodistas de *The Guardian, Fox News* y otros medios fueron víctimas de ciberespionaje entre 2021 y 2022», *CSO España*. 15/7/22. Disponible en: https://cso.computerworld.es/cibercrimen/periodistas-de-the-guardian-fox-news-y-otros-medios-fueron-victimas-de-ciberespionaje-entre-2021-y-2022 (consulta: 2/2/23).

[14] «States should impose a moratorium on spyware such as Pegasus and Predator», *European Federation of Journalists*. 30/1/23. Disponible en: https://europeanjournalists.org/blog/2023/01/30/states-should-impose-a-moratorium-on-spyware-such-as-pegasus-and-predator/ (consulta: 2/2/23).

periodistas, estar en línea es una extensión de estar fuera de línea. Forma parte del trabajo. Estar en silencio en las redes sociales significa no ser visible, dificulta la promoción y repercute en el trabajo, la reputación y, en última instancia, en los ingresos».

Muros en una carrera imparable

Desde 1988, cada 30 de noviembre se celebra el Día Internacional de la Seguridad de la Información, una fecha en la que se recuerda el primer caso de *malware* mundial, los «gusanos de Morris». Otra fecha para recordar es el 7 de febrero, Día Internacional de Internet Segura, una efeméride que sirve para recordar datos como los recogidos por Surfshark[15] en su informe sobre censura digital 2022. Después de investigar los cierres parciales y totales de Internet y redes sociales en 196 países han llegado a la conclusión de que la censura digital, para dificultar la difusión de información entre otros objetivos, afectó a 4.200 millones de personas en 2022, «más de la mitad de la población mundial». En esta carrera sin fin entre el gato y el ratón los asaltantes, cada vez mejor organizados y sofisticados, deben encontrar delante muros que sean, en lo posible, difíciles de salvar.

Internacionalmente algunos de los principales *arquitectos* son la ONU y algunas de sus agencias específicas, la OTAN[16], la OSCE[17], la UE u organizaciones no gubernamentales internacionales como el Foro Económico Mundial, para el que la ciberdelincuencia representa un grave riesgo para la prosperidad mundial en la Cuarta Revolución Industrial. Naciones Unidas considera como delitos el fraude informático, la manipulación de ordenadores, datos y programas, los sabotajes y espionajes informáticos, los virus o los hackeos, entre otros. En conversaciones internacionales está la que podría ser, aún con muchas reticencias, la Convención de las Naciones Unidas sobre la Ciberdelincuencia. Su fin debería ser combatir el uso de las tecnologías de la información y la comunicación con fines delictivos sin poner en peligro los derechos fundamentales de aquellos a los que pretende proteger, para que las personas puedan disfrutar y ejercer libremente sus derechos, en línea y fuera de línea.

[15] «4.2 billion people experienced internet censorship in 2022», *Surfshark.* 17/1/23. Disponible en: https://surfshark.com/blog/internet-censorship-2022 (consulta: 2/2/23).

[16] «Cyber defence», *NATO*. 23/3/22. Disponible en: https://www.nato.int/cps/en/natohq/topics_78170.htm (consulta: 2/2/23).

[17] «Cyber/ICT Security», *OSCE*. Disponible en: https://www.osce.org/cyber-ict-security (consulta: 2/2/23).

La política de la Unión Europea en materia de ciberdefensa está basada en cuatro pilares: actuar juntos para ser más fuertes y con mejores mecanismos de coordinación; proteger el ecosistema de defensa de la UE reforzando la estandarización y certificación de la seguridad cibernética para proteger los dominios militares y civiles; aumentar significativamente las inversiones y hacerlo utilizando las plataformas de cooperación y los mecanismos de financiación disponibles, como PESCO, el Fondo Europeo de Defensa, así como Horizonte Europa y el Programa Europa Digital; y asociarse para abordar desafíos comunes. Un conjunto en constante adaptación de medidas políticas, legislativas, jurídicas, organizativas y técnicas debe garantizar, con sello europeo, la transformación digital de nuestras sociedades a la vez que se deben proteger los derechos fundamentales, la democracia y el Estado de derecho junto a los sistemas, redes y servicios de las Administraciones públicas, entidades privadas y de los ciudadanos.

En su discurso sobre el estado de la Unión de 2021 la presidenta Ursula Von der Leyen pidió[18] el desarrollo de una política europea de ciberdefensa después de que, en 2020 la Comisión Europea y el Servicio Europeo de Acción Exterior (SEAE) presentasen una nueva Estrategia de Ciberseguridad[19] de la UE. Tomando el testigo de su predecesora, la Agencia de Seguridad de las Redes y de la Información de la Unión Europea, aunque manteniendo su nombre, ENISA[20] proporciona, con un mandato permanente, apoyo a los Estados miembros, las instituciones de la Unión y otras partes interesadas frente a los ciberataques. Con la directiva de seguridad en redes de la Unión Europea (NIS 2.0) se pedirán medidas de ciberseguridad para los 16 sectores establecidas en la misma, no siendo los medios de comunicación uno de ellos.

Un ciberespacio seguro y fiable es preciso para garantizar la digitalización y transformación de las economías, las Administraciones públicas y las sociedades, como la española. La ciberseguridad es uno de los pilares de las actuales políticas de Estado y su garantía es el Esquema Nacional de Seguridad, actualizado en Real Decreto 311/2022 de 3 de mayo, y la actividad de instituciones y organismos como son el

[18] «Discurso sobre el estado de la Unión de 2021 pronunciado por la presidenta Von der Leyen», *UE*. 15/9/21. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/SPEECH_21_4701 (consulta: 2/2/23).

[19] «The Cybersecurity Strategy», *UE.* Disponible en: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (consulta: 2/2/23).

[20] ENISA. Disponible en: https://www.enisa.europa.eu/ (consulta: 2/2/23).

Departamento de Seguridad Nacional (DSE); el Centro Criptológico Nacional (CCN-CERT), responsable de controlar los ciberataques a sistemas clasificados de las Administraciones públicas y de empresas y organizaciones de interés estratégico para el país, y de coordinar la red de centros de operaciones de ciberseguridad (SOC); el Instituto Nacional de Ciberseguridad (INCIBE), institución de referencia para la ciberseguridad; el Centro de Operaciones de Ciberseguridad (COCS); la Agencia Española de Protección de Datos (AEPD), encargada del cumplimiento en nuestro país de la protección de datos de carácter personal a través del RGPD (Reglamento Europeo de Protección de Datos); la División de Planificación y Coordinación de Ciberseguridad de la Secretaría General de Administración Digital (SGAD); la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS); la Unidad de Coordinación de Ciberseguridad y el Grupo de Delitos telemáticos de la Guardia Civil; la Brigada central de Investigación Tecnológica (BCIT) de la Policía Nacional; el Mando Conjunto del Ciberespacio (MCCE) del Ministerio de Defensa; junto a los servicios propios de comunidades autónomas y otros actores públicos y privados.

Que la seguridad es una condición imprescindible para el crecimiento del ser humano y el normal desarrollo de nuestra vida cotidiana, cuya protección requiere el esfuerzo y la corresponsabilidad de todos, ha quedado recogido en la Ley 36/2015 de Seguridad Nacional[21], texto que destaca la importancia de promover una cultura de seguridad nacional «que favorezca la implicación activa de la sociedad en su preservación y garantía, como requisito indispensable para el disfrute de la libertad, la justicia, el bienestar, el progreso y los derechos de los ciudadanos». El actual marco de referencia es la *Estrategia de Seguridad Nacional de 2021*[22], en la que las ciberamenazas constituyen uno de los mayores riesgos y desafíos a los que tenemos que hacer frente por su peligrosidad e impacto por el aumento en el uso del ciberespacio y, consecuentemente, el aumento de la frecuencia y magnitud de los ciberincidentes que menoscaban los derechos y las libertades de los ciudadanos y el progreso socioeconómico.

[21] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, *BOE*. 29/9/15. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10389 (consulta: 2/2/23).

[22] *Estrategia de Seguridad Nacional 2021*. DSN. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021 (consulta: 2/2/23).

Hay que destacar, entre otras medidas previstas en la Estrategia Nacional de Ciberseguridad, la creación de dos foros específicos impulsados y presididos por el Departamento de Seguridad Nacional: el Foro Nacional de Ciberseguridad[23] y el Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional[24]. En ambos participan, entre otros, representantes de la sociedad civil, expertos independientes, sector privado, académicos, asociaciones y organismos sin ánimo de lucro y, reseñable por el tema en cuestión, profesionales de los medios de comunicación. La finalidad es potenciar y crear sinergias público-privadas, fundamentalmente en la generación de conocimiento sobre las oportunidades y amenazas para la seguridad o en casos específicos como podría ser el análisis de los riesgos que los ciberataques a los medios y periodistas pueden tener como vehículo para la difusión de campañas de desinformación. El DSN destaca que «existe cada vez más relación entre los ciberataques/cibercrimen y la desinformación, desde el uso de ciberataques para filtrar información (ataques al partido republicano en 2016, a Macron en 2017, o a la EMA durante la COVID-19) incluyendo la alteración de documentos o su publicación sacados de contexto. Por otro lado, campañas como la de *ghostwriters* han aflorado este nexo entre desinformación y ciberataques. Por último, la proliferación de la desinformación como servicio, con la venta, por ejemplo, de redes de *bots* en los mercados cibercriminales, facilitan el empleo de técnicas para no solo promocionar contenido desinformativo, sino que, además, pueden usarse para acosar y silenciar a voces discrepantes, entre ellas a periodistas».

Ramón Ortiz, responsable de Seguridad IT Mediaset, recalca que «hay normativas generales aplicables, pero no hay ninguna específica sectorial de medios de comunicación. Existe un Código de Derecho de la Ciberseguridad, publicado en el *Boletín Oficial del Estado* y modificado en mayo de 2022, que contiene la referencia a todo el marco jurídico en la materia, desde la propia *Constitución española* a los principales reglamentos europeos aplicables, además de leyes orgánicas y leyes, reales decretos, resoluciones y órdenes relacionadas con la seguridad. Se mencionan todas las normativas respecto a los siguientes aspectos: seguridad nacional, protección de

[23] «Estrategia Nacional de Ciberseguridad», *Foro Nacional de Ciberseguridad*. Disponible en: https://foronacionalciberseguridad.es/index.php/estrategia-nacional-de-ciberseguridad (consulta: 2/2/23)

[24] «Creación del Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional», DSN. 2/6/22. Disponible en: https://www.dsn.gob.es/es/actualidad/sala-prensa/creaci%C3%B3n-foro-contra-campa%C3%B1as-desinformaci%C3%B3n-%C3%A1mbito-seguridad-nacional (consulta: 2/2/23).

infraestructuras críticas, seguridad física, respuesta a incidentes de seguridad, ciberseguridad, telecomunicaciones y usuarios, protección de datos personales y ciberdelincuencia». Considera, además que «en caso de materializarse alguna de las amenazas que supusiera un grave impacto, las repercusiones serían grandes y la sociedad se vería muy afectada en el caso de discontinuidad o falta de acceso a los medios de comunicación. Otra cuestión relevante es la posibilidad y el riesgo que supone la difusión por parte de los medios de noticias no verificadas, cuyo origen y motivaciones sean malintencionados».

En el ámbito de los medios uno de los principales referentes es EBU/UER, la Unión Europea de Radiodifusión. La principal alianza mundial de medios de comunicación de servicio público del mundo, con más de cien organizaciones, mantiene activas diversas iniciativas y actividades de ciberseguridad para aumentar la concienciación y la capacidad de defensa frente a los riesgos de seguridad, en continua evolución, que afectan a todo el sector y a su actividad. Entre otras acciones hay encuentros, como los que mantienen todos los meses los CISO[25] de los miembros para debatir los ataques, sus proyectos actuales, las mejores prácticas o para elaborar recomendaciones destinadas a los organismos de radiodifusión y a los vendedores de sistemas de medios de comunicación, aunque, por motivos de confidencialidad, no se revelan sistemáticamente los ataques y vulnerabilidades sufridos. De manera continuada hay grupos de trabajo específicos[26] que, por ejemplo, emiten recomendaciones que tienen por objeto alinear las prácticas de ciberseguridad en los medios con las adoptadas en el entorno TI.

Con la vista puesta en tecnologías punteras y en las innovadoras cuestiones de seguridad que traerán el HbbTV, 5G, IP, Metaverso, web distribuida o computación cuántica, la EBU y sus miembros trabajan junto a proveedores de sistemas e instituciones para mejorar la ciberseguridad. En términos de ataques, destaca Lucille Verbaere, *senior project manager* en el área de Tecnología e Innovación de EBU, «no es tan diferente de lo que les sucede a otras empresas que dependen de Internet. La diferencia es que las redes de los medios de comunicación han estado aisladas y

[25] «Media Cybersecurity CISO. Dedicated to security experts from EBU Members», *EBU/UER*. Disponible en: https://tech.ebu.ch/groups/cybersecurity_ciso (consulta: 2/2/23).

[26] «Media Cybersecurity. Shaping a more secure media industry», *EBU/UER*. Disponible en: https://tech.ebu.ch/groups/mcs (consulta: 2/2/23).

protegidas del exterior durante mucho tiempo y los medios de comunicación no están acostumbrados a aplicar la ciberseguridad, aunque ahora están cambiando a IP».

Tampoco se quita el ojo a la actividad cotidiana y a los flujos y equipos de trabajo en uso, con un gran impacto de la digitalización que ha creado nuevas oportunidades para la producción y distribución, pero también ha abierto las puertas a nuevas amenazas. Los productos analógicos o *legacy* no se pueden actualizar porque ya no reciben soporte de los proveedores o porque, al no haber redundancia, significaría interrumpir los servicios. Proteger los sistemas, las infraestructuras y los procedimientos utilizados en la cadena de producción, distribución y archivo contra ataques potencialmente dañinos; salvaguardar la reputación y los contenidos frente a la desinformación y la piratería para mantener la confianza del público en los medios y los ingresos de los proveedores de servicios legítimos; cumplir con la normativa vigente de la UE y mantenerse actualizados en el ámbito legal al igual que sobre las últimas tecnologías, herramientas y prácticas en materia de ciberseguridad; fijar y exigir requisitos de ciberseguridad para los productos; descubrir vulnerabilidades; establecer entornos de colaboración dedicados, por ejemplo, a amenazas, herramientas o mejores prácticas; fomentar la concienciación sobre ciberseguridad en los miembros de EBU y en la industria de los medios de comunicación en su conjunto, etc. Son algunos de los objetivos y ámbitos de trabajo para garantizar la ciberseguridad de las organizaciones y sus profesionales y, como fin último, garantizar la continuidad y calidad de los medios de comunicación públicos y sus contenidos, esencialmente los informativos.

Mediaset, como ejemplo de medio privado en nuestro país, no tiene «ninguna herramienta de protección específica para los activos y tecnología de TV, pero sí que, para la infraestructura multiplataforma existe algún servicio concreto para el aseguramiento de la distribución de contenidos por Internet. En general se trabaja con tecnologías ajenas de fabricantes especializados, aunque existe alguna herramienta desarrollada internamente», según su responsable de Seguridad IT, Ramón Ortiz. En el caso público, RTVE emplea «herramientas tanto propias como ajenas, siempre teniendo como referencia lo recomendado por el Centro Criptológico Nacional, algunas de ellas desarrolladas por organismos de la Administración y en algunos casos específicas para medios», explican desde su Dirección de Ciberseguridad.

Pensando en la seguridad, empezando por uno mismo

Se estima que el coste anual de la ciberdelincuencia en el mundo superará los 20 billones en 2026 siendo en 2022, según Cybersecurity Ventures[27], de unos 8 billones, lo que supondría el equivalente a ser la tercera economía mundial después de Estados Unidos y China. Gobiernos, instituciones, medios y asociaciones profesionales no son en absoluto ajenos al problema de los ciberataques, aunque las principales víctimas, ya sean periodistas o ciudadanos, aún no tengan una consciencia del impacto y la extensión que tiene en sus vidas, por ajenos o inocuos que los ataques puedan parecer. Los escudos tecnológicos y normativos encuentran su «talón de Aquiles» en el desconocimiento o descuido de personas o trabajadores ya que, el factor humano, es el elemento clave en garantizar la estructura de seguridad y, a la vez, el principal activo al que proteger.

Tener un *poco* de cultura de empresa y un *poco* de conciencia y disciplina personal, que no deja de ser un beneficio, no supone ni un gran gasto económico ni de tiempo y tampoco afecta a la cadena de producción. Incrementar la seguridad puede repercutir beneficiosamente en el producto final, tanto en calidad como en confianza. Recursos hay múltiples y muy accesibles, especialmente en fuentes oficiales como el INCIBE, que pone a disposición de los ciudadanos y empresas guías, consejos y buenas prácticas en seguridad de la información y de los sistemas que la gestionan al igual que su Oficina de Seguridad del Internauta (OSI), con la *Guía de ciberataques*[28]. Además ofrecen un servicio[29] nacional, gratuito y confidencial, a través del teléfono 017, WhatsApp (900 116 117) y Telegram (@INCIBE017), para ofrecer información y asesoramiento sobre ciberseguridad o cómo poder solucionar un ciberincidente. En la página web del CCN-CERT[30] y en ÁNGELES[31], el portal de formación del Centro Criptológico Nacional, se publican diferentes recursos como documentos de buenas prácticas aplicables a la protección del correo, la navegación web, el uso de redes sociales o la protección de teléfonos móviles.

[27] MORGAN, Steve. «Top 10 Cybersecurity Predictions and Statistics For 2023», *Cybercrime Magazine*. 10/12/22. Disponible en: https://cybersecurityventures.com/stats/ (consulta: 2/2/23).

[28] *Guía de ciberataques*. OSI. Disponible en: https://www.osi.es/es/guia-ciberataques (consulta: 2/2/23).

[29] «Tu ayuda en ciberseguridad», *INCIBE*. Disponible en: https://www.incibe.es/linea-de-ayuda-en-ciberseguridad#linea (consulta: 2/2/23).

[30] CCN-CERT. Disponible en: https://www.ccn-cert.cni.es/ (consulta: 2/2/23).

[31] ÁNGELES. *CCN-CERT*. Disponible en: https://angeles.ccn-cert.cni.es/index.php/es/ (consulta: 2/2/23).

Reporteros Sin Fronteras ofrece gratuitamente en su web el *Manual de seguridad para periodistas*[32], una guía práctica editada en español, inglés, francés y árabe para todos aquellos que se enfrentan a situaciones peligrosas mientras llevan a cabo su tarea informativa. La primera versión data de 1992 y ha ido actualizándose según se han transformado los contextos y las amenazas físicas y psíquicas. Recoge consejos prácticos para salvaguardar la integridad del periodista, ya sea física, como un secuestro, o virtual, como la ciberseguridad, y también aporta las prácticas implantadas en grandes medios y agencias de información. CPJ, el Committee to Protect Journalists, de la John S. and James L. Knight Foundation Press Freedom Center, ofrece dos guías de recomendada lectura. El *Digital Safety Kit*[33] es un manual general para los profesionales de los medios que quieran aumentar su seguridad digital para protegerse a sí mismos, a sus contactos y fuentes y a la información con la que trabajan con un buen repertorio de herramientas e información útil. La segunda publicación es el *Manual de seguridad para periodistas*. *Cubriendo las noticias en un mundo peligroso y cambiante*[34], un texto mucho más amplio pero que ya cuenta con un capítulo específico dedicado a la tecnología. El International Center for Journalists (ICFJ), en asociación con el Border Center for Journalists and Bloggers (BCJB), ofrece capacitación[35] sobre seguridad digital para periodistas y representantes de la sociedad civil, para que sepan cómo proteger su información, datos, dispositivos y comunicaciones contra intromisiones de seguridad digital. La Fundación para la Libertad de Prensa (FLIP), una organización sin ánimo de lucro creada en Colombia para proteger a los periodistas amenazados tiene en su web a disposición de cualquier persona su *Manual antiespías: Herramientas para la protección digital de periodistas*[36], una lectura muy completa y recomendable.

---

[32] *Manual de seguridad para periodistas*. Reporteros Sin Fronteras, 27/1/20. Disponible en: https://www.rsf-es.org/download/manual-de-seguridad-para-periodistas/ (consulta: 2/2/23).

[33] «Digital Safety Kit», *Committe to Protect Journalists*. 30/7/19. Disponible en: https://cpj.org/2019/07/digital-safety-kit-journalists/ (consulta: 2/2/23).

[34] *Manual de Seguridad para Periodistas. Cubriendo las noticias en un mundo peligroso y cambiante.* Committe to Protect Journalists. Disponible en: https://cpj.org/es/2012/04/manual-de-seguridad-para-periodistas-del-cpj/ (consulta: 2/2/23).

[35] *Fortalecimiento de la Seguridad Digital para Periodistas y Organizaciones de la Sociedad Civil.* International Center for Journalists y Border Center for Journalists and Bloggers. Disponible en: https://digitalsecurity.training/courses/course-v1:ICFJ-BCJB+DS-ES+22/about (consulta: 2/2/23).

[36] *Manual antiespías*. Federación para la Libertad de Prensa. Disponible en: https://flip.org.co/index.php/es/publicaciones/manuales/item/download/14_acc75253172a7a207401074633ef88bb (consulta: 2/2/23).

Los medios, públicos y privados, además de poder contar con unidades cíber propias y participar activamente en distintos foros nacionales e internacionales, como es el caso de la Dirección de Ciberseguridad RTVE, proporcionan «haciendo un esfuerzo considerable», formación específica a sus empleados. «El eslabón humano es el más débil», aseguran, «por eso es imprescindible la concienciación y la formación que permita evitar y reducir el impacto de ataques y amenazas». También facilitan a los que realizan coberturas en el exterior, caso de las áreas técnicas, recomendaciones sobre desplazamientos de personal para la protección de sus conexiones y equipos como las recogidas en el *Digital Safety for Field Journalists* de EBU. Este conjunto de recomendaciones, herramientas y prácticas pretende garantizar, en lo posible dado que se trabaja en entornos hostiles e inciertos, mantener el mayor nivel de seguridad viable, proteger el anonimato y la huella digital, garantizar una comunicación continua con sus sedes y permitirles captar, editar, producir y enviar sus contenidos con seguridad desde el terreno a sus redacciones. Además, para el público general, la Corporación ofrece en la web un resumen de consejos[37] elaborados por su Lab y su departamento de verificación, RTVE Verifica.

Entre las prioridades de EBU se encuentra la formación para mejorar la madurez de la ciberseguridad en las organizaciones, la mejor gestión de los riesgos de ciberseguridad, escanear equipos, etc. ya que en muchas ocasiones «los profesionales de los medios no están acostumbrados ni formados para configurar correctamente los sistemas (en particular los servicios en la nube) y no creen que la ciberseguridad sea un problema para los medios de comunicación (porque antes no lo era)». Para suplir la escasez de personal de los equipos de ciberseguridad proponen campañas de concienciación y formación y están estudiando la posibilidad de elaborar una guía más detallada para los periodistas.

En el ámbito privado, tomando como ejemplo a Mediaset, los profesionales tienen a su disposición la política de seguridad corporativa y sus normativas y procedimientos de seguridad aplicables, que incluyen recomendaciones sobre el uso de los recursos y los servicios IT. Coinciden en que «el factor humano es crítico. La vertiente del usuario final por una parte y, por la otra, la necesidad de técnicos y proveedores de servicios de

[37] «Consejos para tu ciberseguridad de VerificaRTVE», *RTVE*. 17/5/21. Disponible en: https://www.rtve.es/noticias/20210517/consejos-para-tu-ciberseguridad/2090665.shtml (consulta: 2/2/23).

seguridad suficientemente capacitados y entrenados. Mediaset planifica y desarrolla planes de formación en materia de seguridad y privacidad y además lleva a cabo campañas de concienciación con el objetivo de prevenir ataques de *phishing* y de ingeniería social por medio de iniciativas de llamadas de *vishing, media droping*, campañas de *phishing*, etc. Por otra parte, se informa mediante el envío de SMS y emails, así como presencia en la intranet corporativa de campañas constatadas de *phishing* y *smishing*».

«Probablemente el "talón de Aquiles" sean más los humanos que las máquinas», considera Pamela Morinière, jefa del Departamento de Comunicación y Campañas de la Federación Internacional de Periodistas (FIP), «y probablemente lo sean porque no se presta gran atención al fenómeno y el personal está muy poco formado. Una encuesta de la FIP realizada en 2018[38] mostró que solo la mitad de las víctimas de abusos en línea (53 %) denunciaron los ataques a la dirección de su medio, al sindicato o a la policía, y en dos tercios de los casos no se hizo nada (las encuestadas eran mujeres periodistas). En otra encuesta, de 2022[39], dos tercios de los encuestados afirmaron que el acoso en línea no era una prioridad para su empresa de comunicación y el 44 % dijo que ni siquiera se hablaba del tema. Consideramos que no es "parte del trabajo" y que el personal debe recibir la formación adecuada para hacer frente a los abusos en línea y proteger su seguridad digital».

Prevención, detección y respuesta son las tres fases básicas del ciclo de ciberseguridad. Pensar, con la cantidad de dispositivos conectados, que se es invulnerable o que los ataques nunca llegarán es una muestra de confianza en el prójimo loable pero que puede terminar siendo, con una alta probabilidad, una mala experiencia. Trabajar en el ámbito de la prevención puede permitir, con las tecnologías adecuadas, que los ataques incluso más avanzados pueden evitarse sin que afecten a la actividad regular. Un resumen de consejos básicos para proteger nuestra privacidad y la actividad que hacemos con nuestros dispositivos conectados, que son ordenadores, teléfonos, tablets… pero también coches, aspiradores o asistentes de voz, es:

[38] «You are NOT alone», *International Federation of Journalists*. Disponible en: https://www.ifj.org/actions/ifj-campaigns/online-trolling-you-are-not-alone.html (consulta: 2/2/23).

[39] «Time to end media inaction over online abuse, says IFJ», *International Federation of Journalists*. 8/3/22. Disponible en: https://www.ifj.org/media-centre/news/detail/category/stop-gender-based-violence-at-work/article/time-to-end-media-inaction-over-online-abuse-says-ifj.html (consulta: 2/2/23).

- Sentido común, espíritu crítico y un punto de escepticismo, nadie regala nada y si algo parece sospechoso puede que tenga muchas posibilidades de serlo. Es tener «la ciberseguridad en mente» para no ser víctimas de un ataque por abrir archivos adjuntos de fuentes desconocidas, correos electrónicos, SMS, mensajes de WhatsApp o Telegram extraños o marcados como *spam*, por conectar dispositivos USB contaminados a los ordenadores propios o de la red de las empresas, etc. O por descargarnos y abrir *software* malicioso, un clásico del *ransomware*.

- Ante un incidente, o con dudas razonables, contactar con los servicios de ciberseguridad de nuestras empresas, especialistas de las Administraciones públicas (INCIBE o cuerpos y fuerzas de seguridad) o con empresas especializadas, para contar con una solución o una opinión profesional antes de tomar cualquier decisión o acción.

- Los datos personales son lo que son, personales, si se van a dar que sea en sitios en los que se pueda confiar por su seguridad. Hay que tener prevención con los sitios que piden nuestras biografías completas o todos los datos biométricos. Tampoco se deben difundir ni exponer datos profesionales o personales, como cuentas de correo, números de teléfono, en listas de distribución o páginas web que ofrezcan pocas garantías y que agiganten nuestra huella digital y nuestra trazabilidad.

- Intentar diferenciar o separar equipos, cuentas, etc. profesionales de los personales, que sean lo más ajeno y aislados que sea posible. No todos los trabajos o los archivos digitales tienen el mismo riesgo, pero es importante que los periodistas, según sea su actividad o el lugar en el que la llevan a cabo, cuenten con equipos específicos para sus vidas personales y profesionales. Revisar y ajustar en ellos la configuración de seguridad.

- No utilizar contraseñas fáciles (cumpleaños), que sean iguales o similares en todos los dispositivos o servicios y diferenciar las profesionales de las personales. En lo posible, emplear doble factor de autenticación y periódicamente hacer cambios de contraseñas, incluso contando con un administrador de contraseñas.

- Regularmente hacer copias de seguridad de los datos (documentos, imágenes, etc.) en dispositivos externos no conectados (discos duros) o en una nube segura

para evitar su robo o, simplemente, su pérdida. Si es posible, con un programa o por la prestación de servicios en la nube, cifrar los datos.

- Actualizar el sistema operativo y el *software*, especialmente las actualizaciones de seguridad, y proteger todos los dispositivos conectados con cortafuegos y un antivirus. Hay muchos buenos gratuitos (y no hay que olvidar que cuanto más actualizados más garantías de protección). Y se debe recordar que el teléfono móvil, al que tanto uso se da y tanto nos conecta, también es un ordenador y protegerlo con un antivirus es una prevención muy eficaz. Tener correos electrónicos y perfiles digitales *alternativos* en redes para determinados trabajos no deja de ser otro cortafuegos que proporciona un mínimo anonimato y evita, o retrasa, recibir visitas indeseadas en las cuentas personales y profesionales.

- Evitar navegar por entornos web no confiables y en lo posible navegar con el protocolo de transferencia de hipertexto seguro (HTTPS), en lugar de HTTP, y empleando una red privada virtual (VPN), un servicio encriptado de pago que también se puede encontrar disponible gratuitamente en navegadores como Opera con el que se protege la actividad e información personal de injerencias de terceros. Cuidado también con las wifis gratuitas, o los ordenadores de cibercafés, y por dónde navegamos en ellos o los datos que dejamos que circulen. Borrar los historiales de navegación, o hacerlo en modo privado, evita dejar algunos rastros.

- Si no se recibe formación, intentar adquirirla en fuentes oficiales o especializadas, hay una gran cantidad de ellas accesibles y, en general, sin coste.

Nadie está exento de sufrir una intromisión, pero está claro que la mejor defensa… empieza por uno mismo. Puede parecer un paso pequeño, pero es fundamental para que la democracia pueda seguir funcionando sin miedo, con voces independientes, abierta al pluralismo de opiniones y fuentes en debates libres y abiertos para servir, como medios y profesionales, al fin al que nos debemos: una ciudadanía bien informada.

*David Corral Hernández**
Periodista RTVE