LA CIBERSEGURIDAD COMO **ASIGNATURA PENDIENTE**

La creciente digitalización de la sociedad hace necesario analizar hasta qué punto son seguros los sistemas que están detrás de las estructuras que lo permiten. De ello trata este artículo.

Álvaro Saavedra Montejo
Colaborador de Proyecto
Universidad Pública de Navarra

La preocupación por la ciberseguridad está siendo cada vez mayor, tanto a nivel nacional como internacional, dado el incremento de casos de ciberamenazas que reciben no solo las empresas, sino también las propias personas que conforman la sociedad. La tecnología supone y seguirá suponiendo una herramienta con la que avanzar hacia un futuro donde se trate de mejorar determinados aspectos que respondan a nuestras necesidades y deseos como ciudadanos. Venimos de una pandemia donde se ha acelerado la simbiosis entre sociedad y tecnología debido al aumento del teletrabajo y de las clases online, entre otros motivos. Esto se traduce en un mayor uso del *cloud computing*, que es en esencia la posibilidad de trabajar de manera colaborativa con otras personas y desde distintos dispositivos. En este momento se hace necesario ver hasta qué punto son seguros los sistemas que están detrás de estas estructuras digitales.

Pero primero, es importante mencionar qué se entiende por ciberseguridad. "La ciberseguridad es la protección de los sistemas conectados a internet, como el hardware, el software y los datos, frente a las ciberamenazas. Esta práctica es utilizada por particulares y empresas para protegerse contra el acceso no autorizado a los centros de datos y otros sistemas informáticos". Varios artículos e informes, como CCN-CERT (2021) y Rojas (2022), han determinado que la ciberseguridad es una asignatura pendiente de nuestro país. A esta conclusión se ha llegado debido al gran número de casos de ciberamenazas que se han producido a lo largo de 2020 y 2021, ya que no solo han incrementado su número, sino también su efectividad en términos de intrusión.

Tal es la preocupación que se espera que para este año 2022 el 25% de las empresas españolas incrementen el doble del presupuesto destinado a aumentar la seguridad. Así ha quedado

evidenciado tras el informe publicado por una de las principales consultoras, Price Waterhouse (Pwc, 2022), donde han realizado una encuesta a más de 3.500 responsables de ciberseguridad, CEOs y altos directivos. Si el periodo 2021 se consideró como año récord de ciberataques, este curso 2022 se plantea como uno de los años más intensos en términos de blindaje de ciberseguridad, ya que se espera que el número de ciberataques se incremente considerablemente.

La ciberseguridad nunca ha sido un tema baladí y, no solo afecta al tejido empresarial sino también al nivel de los ciudadanos. Es decir, tanto empresas como ciudadanos son objeto de ciberataques. En el informe realizado por The Cocktail Analysis encargado por Google (The Cocktail Analysis, 2020), se realizó una radiografía de cómo se perciben estas cuestiones relacionadas con la privacidad (con una muestra de 817 encuestas a distintos perfiles sociodemográficos de usuarios). En torno al 75% de los encuestados manifiestan que la ciberseguridad se considera un tema de especial relevancia, dadas las implicaciones que tiene en el día a día el uso de las tecnologías de la información y comunicación. Desde el punto de vista de la experiencia con la seguridad, afirma que 6 de cada 10 usuarios han tenido algún tipo de incidencia, ya sea actividad sospechosa en la cuenta personal, suplantación de la identidad o fraude, entre otros. De manera general, se entiende que hay una conciencia elevada en relación al riesgo que supone operar en los entornos digitales. Además, una buena noticia es que una amplia mayoría de la muestra conoce uno de los principales mecanismos para evitar ciberataques a nivel usuario: el sistema de verificación en dos pasos (2SV).

Por otro lado, es importante tener en cuenta cuáles son los hábitos de comportamiento de los ciudadanos en internet. En el último informe de abril

ESPAÑA LIDERA CON GRAN DIFERENCIA RESPECTO AL SEGUNDO EN LA LISTA, ITALIA, EN NÚMERO DE ATAQUES AL ESCRITORIO EN REMOTO

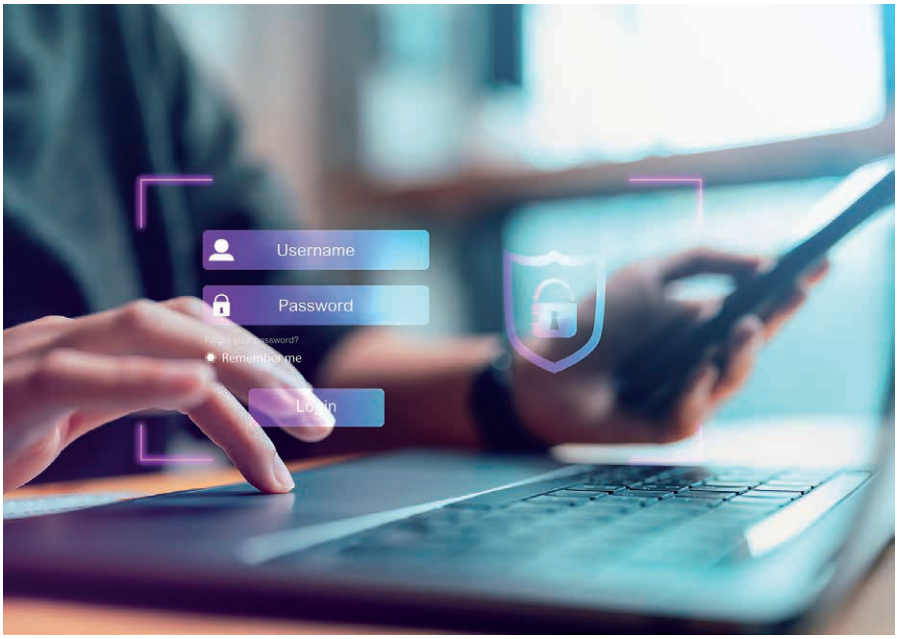
PRINCIPALMENTE, EL SECTOR DE LA BANCA, LA ADMINISTRACIÓN PÚBLICA Y LAS COMPRAS ONLINE SON LOS QUE SE CONSIDERAN ENTORNOS MÁS SEGUROS EN CUANTO AL TRATAMIENTO DE DATOS PERSONALES. MIENTRAS QUE EN EL LADO OPUESTO ENCONTRARÍAMOS EL CAMPO DE LAS REDES SOCIALES, PERCIBIDO COMO UN ENTORNO MENOS SEGURO

de 2022 del Observatorio Nacional de Tecnología y Sociedad (Observatorio Nacional de Tecnología y Sociedad, 2022), se recogen los principales hábitos de comportamiento tanto en la navegación como en el uso de internet. La amplia mayoría de los encuestados conocedores de los riesgos de internet han reconocido que vigilan periódicamente los movimientos en la cuenta bancaria *online,* cierran sesión al terminar la consulta y evitan el uso de equipos públicos. Pero, sin embargo, no hay tanto consenso a la hora de crear tarjetas prepago o 'monedero' como medida para efectuar transacciones más seguras.

Si bien todas las cuestiones relacionadas con la privacidad son cruciales para empresas y ciudadanos, es importante explicar en qué ámbitos se manifiesta una cierta sensibilidad a esta problemática. Entendemos por sensibilidad aquellas actividades que pueden conllevar un riesgo potencial. Principalmente, el sector de la banca, la Administración Pública y las compras online son los que se consideran entornos más seguros en cuanto al tratamiento de datos personales. Mientras que en el lado opuesto encontraríamos el campo de las redes sociales, percibido como un entorno menos seguro.

Por lo que respecta a las empresas, el estudio de CCN-CERT (2021) ha clasificado los principales sectores afectados en función de la tipología de ciberataque. *Ransomware* es una de las ciberamenazas que más ha afectado a nivel sanitario, logístico, educacional y pymes. El BEC (*business email compromise*) o *phishing*, ha sido más utilizado por los ciberdelincuentes tras el auge del teletrabajo debido a la pandemia de la Covid-19. Aunque hay una mayor tipología de ciberataques, de manera general, el mayor número se ha concentrado en el ámbito gubernamental, como también en defensa, en el ámbito energético, y entretenimiento digital (CCN-CERT, 2021). Entre los ataques que se prevén que más van a crecer se sitúa en primer lugar al anteriormente mencionado, *ransomware*.

Haciendo alusión a uno de los lemas en este contexto, "un sistema de seguridad es tan fuerte como su eslabón más débil", es importante tener en cuenta que en cuestión de dos años se ha producido un proceso de digitalización forzosa dadas las circunstancias sanitarias. ¿Por qué entonces la ciberseguridad es una asignatura pendiente en el territorio español? Solo debemos acudir al informe realizado por ESET, una empresa especializada en protección



antivirus y pionera en cuestiones relacionadas con la ciberseguridad en Europa. En dicho informe hace referencia a la mayor extracción y facilidad de adivinación de las contraseñas de los usuarios por los ciberdelincuentes. Pues bien, España lidera con gran diferencia respecto al segundo en la lista, Italia, en número de ataques al escritorio en remoto (ESET, 2021). Para ir terminando podemos recurrir a las palabras de César Martín Lara, socio de Risk Advisory además de responsable de ciberseguridad (Deloitte, 2021): "En el momento actual, la ciberseguridad es más que nunca una necesidad para las organizaciones. Esto se aprecia en que ha aumentado la concienciación de las empresas con respecto a la importancia de los riesgos digitales, lo que ha derivado en que las organizaciones destinen un mayor presupuesto a la ciberseguridad y a la sensibilización de sus empleados. A pesar de este avance, no obstante, todavía queda un largo camino por recorrer".

Al final, estas practicas llevadas a cabo por las distintas empresas supondrán una mayor seguridad para los ciudadanos de nuestro país. En esta línea, la Unión Europea ha liberado los famosos fondos *Next Generation* para la digitalización y el desarrollo de planes de ciberseguridad de las empresas. El 'futuro' tan incipiente viene repleto de cuestiones que deben ser abordadas desde la óptica de la ciberseguridad, como la cuarta revolución industrial (Industria 4.0), el *big data o* la ampliación del 5G, entre otras cuestiones. ■

Referencias

CCN-CERT. (2021). Ciberamenazas y Tendencias. Edición 2021. Centro criptológico nacional. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1.html.

Deloitte. (2021). Encuesta Future of Cyber 2021. https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html.

ESET. (2021). Threat report 3o Trimester 2021 (p. 59). https://www.welivesecurity.com/wp-content/uploads/2022/02/eset_threat_report_t32021.pdf.

Observatorio Nacional de Tecnología y Sociedad. (2022). Cómo se protege la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España. https://www.ontsi.es/index.php/es/publicaciones.

Pwc. (2022). Digital Trust Survey 2022. https://www.pwc.es/es/publicaciones/transformacion-digital/global-digital-trust-insights-2022.html.

Rojas, J. (2022, agosto 29). El reto de la ciberseguridad en España: Un país vulnerable. Telefónica. https://www.telefonica.com/es/sala-comunicacion/blog/un-pais-vulnerable-el-reto-de-la-ciberseguridad-en-espana/.

The Cocktail Analysis. (2020). Panorama actual de la Ciberseguridad en España. https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf.