por **Sandra Par Cebrián**

Laura Caballero

Directora de la Agencia de Ciberseguridad de Cataluña

"Las instituciones de control aportan una visión independiente y rigurosa sobre el cumplimiento de las medidas de seguridad"

Laura Caballero Nadales (Barcelona, 1985) es ingeniera de Telecomunicaciones y ha pasado por diferentes empresas del sector de las tecnologías de la información antes de aterrizar en el sector público. El pasado 7 de enero fue nombrada directora de la Agencia de Ciberseguridad de Cataluña, entidad pionera en España en este ámbito. Sobre la mesa de su nuevo despacho, Caballero se ha encontrado con un sector de una elevada importancia estratégica –557 empresas con una facturación global estimada de más de 1.400 millones de euros anuales–, pero también con un incremento exponencial de la actividad delictiva a través de las redes de telecomunicaciones. En julio de este año la Sindicatura de Comptes firmó un convenio con la Agencia para garantizar la asistencia técnica y la implantación de medidas de ciberseguridad.

- ***Auditoría Pública.*** Fue designada directora de la Agencia de Ciberseguridad de Cataluña en enero de este año. ¿Cuáles son los principales objetivos que se ha marcado al frente de la Agencia ante los importantes retos que plantea la ciberseguridad?

Laura Caballero. La Agencia de Ciberseguridad de Cataluña tiene como objetivo principal garantizar la resiliencia digital del país, protegiendo infraestructuras públicas consideradas esenciales e importantes, según la clasificación de la normativa europea. En concreto, centramos esfuerzos sobre todo en proteger el entorno sanitario, la infraestructura digital, las universidades y las administraciones locales.

Nuestro modelo de ciberseguridad es estratégico, transversal y con visión de futuro. Por lo tanto, no nos quedamos en la parte estrictamente técnica. Para nosotros es muy importante fomentar la cultura de ciberseguridad entre la ciudadanía y las empresas, con acciones de formación, sensibilización y recursos específicos. Las personas pueden ser el caballo de Troya o la primera gran defensa de los sistemas de las organizaciones con las que nos relacionamos y, por lo tanto, tener conocimientos en ciberseguridad nos convierte en una sociedad mejor protegida.

Además, promovemos la innovación y la colaboración con el ecosistema tecnológico para reforzar la gobernanza digital e impulsar el sector de la ciberseguridad en el territorio, con formación de profesionales especializados en ciberseguridad, así como la consolidación de un tejido empresarial competitivo.

- ***AP.*** Según los datos de que disponen, ¿cuántos incidentes de ciberseguridad ha sufrido Cataluña el último año? La evolución de los datos, ¿dibuja un escenario preocupante?

LC. Durante 2024, la Agencia gestionó 3.372 incidentes de ciberseguridad, lo que representa un incremento del 26% respecto al año anterior. De estos incidentes, 33 se consideran complejos; en este sentido, observamos un aumento de la sofisticación de las amenazas.

Más que preocuparnos, tenemos que estar alerta y aplicar las medidas necesarias para protegernos. La evolución de los ataques nos muestra un escenario lleno de retos y esto nos tiene que mantener proactivos. No podemos quedarnos quietos: las ciberamenazas son cada vez más globales, más sofisticadas y han llegado para quedarse.

Herramientas innovadoras como las inteligencias artificiales utilizadas por los ciberdelincuentes han aumentado la complejidad de los ataques y pueden llegar a ser especialmente sofisticadas en casos de estafas. Para que se hagan una idea: en Cataluña, el 15% de las infracciones penales están vinculadas al cibercrimen y el 95% de estas son estafas digitales (ciberestafas), según datos de los Mossos d'Esquadra.

Por este motivo, como ciudadanía tenemos que estar alerta y dejar atrás la idea de que la ciberseguridad no va con nosotros. Tener buenos hábitos

"El sector público tiene que adoptar un modelo de gestión integral basado en la prevención, la protección y la resiliencia"

digitales nos ayudará a estar prevenidos ante las estafas que circulan y las que vendrán.
Por otro lado, como instituciones tenemos que trabajar en la mejora constante y en dotarnos de recursos para intentar situarnos por delante de los ciberdelincuentes.

- ***AP.*** ¿Cuáles son los tipos de ciberincidentes más comunes y cuáles los que más han crecido en los últimos años?

  LC. Los incidentes más comunes son las fugas de credenciales, los accesos ilegítimos y los ataques de *ransomware* –ataques en los que se exige un rescate económico–. Y de todos ellos, el *ransomware* crece año tras año de manera constante.
  Además, el robo de datos supone una actividad muy lucrativa para los delincuentes y por eso buscan constantemente vulnerabilidades y puntos de acceso a los sistemas. En este sentido, el tipo de *malware* –programa maligno– que conocemos como *infoestealer* es una amenaza creciente que afecta tanto al sector público como al privado.
  También destacan los ataques de denegación de servicio (DDoS), que han aumentado en 2024 un 170% respecto al año 2023. A menudo se relacionan con conflictos geopolíticos y, en función de la evolución de estos conflictos, los ataques pueden llegar a fluctuar.

- ***AP.*** La Agencia, de acuerdo con la ley, tiene por objeto garantizar la ciberseguridad en el territorio de Cataluña. ¿Cuál es su diagnóstico de la salud del sector público catalán en términos de ciberseguridad?

  LC. La Agencia trabaja para la protección de la ciberseguridad del territorio desde sus instituciones de gobierno y su sector público. A partir de esta premisa, hablar de todo el sector público catalán, por un lado, representa una extensión muy heterogénea, y por otro, nosotros solo tenemos la visión de una parte.
  No obstante, podemos afirmar que el sector público catalán muestra una mejora en la madurez de la ciberseguridad respecto a los últimos años, si bien es cierto que aún hay retos importantes.
  Hay que invertir en la mejora continua de la protección de datos sensibles, la continuidad operativa y el cumplimiento normativo. Por eso también hemos iniciado una carrera intensa para que el sistema público se adecúe al Esquema Nacional de Seguridad (ENS).

- ***AP.*** Precisamente la Sindicatura y otros órganos de control externo del Estado han hecho los primeros

informes de controles básicos de ciberseguridad. Detectamos que la implantación del ENS es una asignatura pendiente en muchas administraciones y entidades públicas. ¿Qué medidas están llevando a cabo para mejorar esta realidad?

LC. La Agencia actúa como Organismo de Auditoría Técnica (OAT) para facilitar el asesoramiento y la certificación en el Esquema Nacional de Seguridad. Se acompaña a las entidades públicas en la adecuación normativa y se promueven planes de seguridad personalizados.
Además, este año hemos firmado un convenio con Localret, que podremos hacer extensivo al mundo local de manera eficiente. Mediante este convenio, se hará un diagnóstico de la postura actual de ciberseguridad de estos organismos, proponiendo mejoras a implementar. Se realizarán también acciones de formación y soporte específico en el cumplimiento normativo. Para este proyecto en concreto destinamos 3,3 millones de euros, que financiamos junto con los fondos Next Generation de la Unión Europea, dentro del marco del Plan de Recuperación y Resiliencia.

"Centramos esfuerzos sobre todo en proteger el entorno sanitario, la infraestructura digital, las universidades y las administraciones locales"

- ***AP.*** En su opinión, ¿cuál puede ser la aportación de las instituciones de control como la Sindicatura en esta materia?

LC. Las instituciones de control aportan una visión independiente y rigurosa sobre el cumplimiento de las medidas de seguridad. Son la gran defensa de los derechos de la ciudadanía y una herramienta democrática, en primer lugar.
En segundo lugar, nos pueden ayudar a identificar áreas de riesgo y a promover buenas prácticas.
Gracias a organismos como la Sindicatura se garantiza una mejor transparencia, la rendición de cuentas y la mejora continua en las políticas, como las de ciberseguridad, en este caso.

- ***AP.*** ¿Diría que en el sector público vamos atrasados respecto al sector privado?

LC. Yo no diría que vamos más atrasados. En algunos ámbitos, el sector público ha ido más lento que el privado en la adopción de medidas de ciberseguridad y en otros hace tiempo que desplegamos un modelo integral de prevención y respuesta.
Además, la exigencia para el sector público en temas éticos y en la protección de datos nos deja escaso margen para no aplicar medidas que pongan el foco en la protección de la información de la ciudadanía, por ejemplo.
La falta de recursos específicos afecta al sector público, que es muy heterogéneo, pero también afecta a un sector privado en el que la PIME representa una parte muy importante del tejido empresarial. Las empresas más grandes suelen tener recursos y expertos que apuestan por la protección de sus sistemas, pero en las empresas más pequeñas la inversión en ciberseguridad no se ha priorizado y están en el punto de mira de les redes de cibercrimen precisamente por eso.

- ***AP.*** ¿Qué acciones cree que debe poner en práctica el sector público para prevenir y evitar los ciberataques?

LC. El sector público tiene que adoptar un modelo de gestión integral basado en la prevención, la protección y la resiliencia. Para esto, es necesario, por un lado, implementar protocolos de ciberseguridad, sistemas de monitorización y detección 24x7 y elaborar planes de respuesta a incidentes, y por otro lado, ofrecer formación continua al personal.
Asimismo, es esencial aplicar el modelo de confianza cero y reforzar la seguridad en la cadena de suministro.
Estas acciones requieren inversión y recursos. Para conseguir más con menos, es imprescindible utilizar las tecnologías disruptivas a nuestro alcance como la inteligencia artificial (IA) para la mejora de las operaciones y la capacidad de protección de las herramientas de seguridad.

- ***AP.*** Si bien de forma aún incipiente, la mayoría de las organizaciones empiezan a plantearse la introducción de estas herramientas para optimizar procesos. Ante el aumento de ciberestafas que apuntaba antes, ¿cree que la IA nos hace más vulnerables?

LC. La inteligencia artificial tiene una doble vertiente: puede ser una aliada en la detección y respuesta a las ciberamenazas, pero también es una herra-

"En 2024, el 60% de las fugas de datos en el sector público fueron a causa de errores humanos"

mienta para cometer ataques y estafas. En este sentido, sí: nos vuelve más vulnerables. Los ciberdelincuentes utilizan la IA para generar contenidos malintencionados, cada vez más realistas y difíciles de detectar.
Pero por otro lado, en Cataluña, el 42,7% de las empresas de ciberseguridad ya utilizan la IA para reforzar la protección digital. Por lo tanto, la innovación siempre nos ofrece oportunidades.

- ***AP.*** En Cataluña, recientemente instituciones de la envergadura del Hospital Clínico o la Universidad Autónoma de Barcelona han sido objeto de graves ciberataques. ¿Qué papel desempeña la Agencia en estos casos? ¿Cuál es el nivel de recuperación de la información?

LC. La Agencia actúa con rapidez siempre que las entidades y organismos nos piden ayuda. Les ayudamos a contener el incidente, a hacer análisis forenses y les damos apoyo técnico y asesoramiento en todo lo que puedan necesitar, desde el marco normativo hasta acciones de comunicación.
Se analizan los vectores de entrada, se coordina la respuesta con las entidades o organismos afectados y se trabaja para recuperar la información y minimizar al máximo el impacto.
La recuperación depende de la capacidad que haya tenido previamente cada entidad para hacer copias inmutables de la información de manera regular y guardarlas en entornos aislados.

- ***AP.*** ¿Cree que la ciudadanía está suficientemente concienciada de los riesgos a los que están expuestos los sistemas de telecomunicaciones? ¿Hay cultura de la ciberseguridad?

"Los incidentes más comunes son las fugas de credenciales, los accesos ilegítimos y los ataque de ransomware, que crecen año tras año"

LC. La concienciación ciudadana ha mejorado, pero aún hay margen para consolidar una cultura de ciberseguridad.
Muchas estafas se producen por engaños que aprovechan errores humanos, como el *phishing* (la pesca de información haciéndose pasar por entidades legítimas) o el *smishing* (la estafa de pesca de información mediante los SMS). De hecho, según datos de la Autoridad Catalana de Protección de Datos (APDCAT), en 2024 el 60% de las fugas de datos en el sector público fueron a causa de errores humanos.

- ***AP.*** Dado el carácter transnacional de los incidentes de ciberseguridad, ¿con qué organismos europeos y estatales cooperan de forma regular?

LC. La Agencia coopera regularmente con todos los actores posibles. Nos coordinamos con las entidades autonómicas y estatales de ciberseguridad y también colaboramos con organismos europeos como ECSO, ENISA, Europol e Interpol. También participamos en redes de coordinación internacional para compartir información sobre amenazas y buenas prácticas.
Tenemos claro que el cibercrimen no tiene fronteras y la colaboración es clave para reforzar la seguridad colectiva.