EL PAÍS | Retina

eventos / retina

SÁBADO 13 DE MAYO DE 2023


**Imagen de la participación de tres agentes de las fuerzas de seguridad en el evento de Retina celebrado el martes pasado en Madrid.** SANTI BURGOS

# Foro Ciberseguridad

## La guerra en Ucrania, el aumento de ataques a infraestructuras críticas, un planeta fracturado en dos y unos criminales que manejan 8 billones de dólares sitúan la defensa digital en primera línea del frente

# La batalla de la ciberseguridad se recrudece

## Los ordenadores se han convertido en armas ofensivas y trincheras ante el exponencial aumento de los ataques telemáticos a lo largo y ancho del planeta

**En la foto superior, el general Miguel Ángel Ballesteros, director del departamento de Seguridad Nacional. Abajo, el general Rafael García Hernández, comandante del Mando Conjunto del Ciberespacio.** SANTI BURGOS

**Desde la izquierda: Félix Barrio, director del Incibe; Marina Nogales Fulwood, global head of Cyber External Engagement de Santander; y Miguel Ángel Thomas, socio para ciberseguridad de NTT Data.** S. B.

**Miguel Ángel García Vega**

Cuando unas jornadas tecnológicas las abre un general y las cierra otro, es una premonición de la gravedad del tema. Sin rehenes. El título es un estandarte. *Ciberseguridad: tecnología para proteger la transformación de las personas y las organizaciones.* La plataforma digital *Retina* ha planteado una narrativa que nos lleva a Ucrania, a un planeta fracturado en bloques, a la seguridad de las infraestructuras críticas, pero también a la protección del ciudadano frente a los delitos que proceden de ese lugar inasible que es el ciberespacio. Con la aportación de Banco Santander (impulsor), NTT Data (socio anual) y BeDisruptive (patrocinador), entre otros, el relato quizá sea la trama de una las mayores preocupaciones de nuestra era. ¿Hay una guerra si no se escuchan las bombas? ¿Existe un árbol que se desploma en medio del bosque si nadie lo oye? Esta es una industria del silencio y la discreción.

La cortinilla de *Retina* es un viaje de fractales, secuencias de números binarios, galaxias y el interior de un inquietante reloj que chasquea con un clic el tiempo. Es la hora de los números. Varían según las consultoras. Pero la raya del horizonte resulta muy parecida. El cibercrimen costará al mundo este año —acorde con la publicación *Cybersecurity Ventures*— unos ocho billones de dólares. Si fuese la economía de un país, sería la tercera mayor del mundo tras Estados Unidos y China. Cada segundo se *roban* 250.000 dólares. Es el negocio ilegal más rentable. La filósofa Hannah Arendt escribió que el ser humano solo puede apresar "momentos de verdad". Este mundo en su némesis. Una mentira continuada. Durante la pandemia aumentaron los intentos de robo de vacunas y patentes.

El director del Departamento de Seguridad Nacional, el general Miguel Ángel Ballesteros, es una persona sincera. Cuenta hasta donde puede contar. El material con el que trabaja es delicado, al igual que el cristal de Murano. "Tenemos en marcha un Plan Nacional de Ciberseguridad que se aprobó en marzo de 2022. No puedo describir en detalle cómo va esta estrategia, porque eso sería decirle a los criminales dónde estamos trabajando y dónde no, y revelaría nuestros puntos débiles", observa. Pero de memoria aporta unos datos que provocan más de un escalofrío. Solo el año pasado la Administración sufrió 55.695 ciberataques. El grado varía. Nivel alto (28.538), muy alto (3.744) y críticos, "que producían un daño tremendo" (75). Nueve contra la Administración central, 24 golpearon la autonómica y 42 afectaron a ayuntamientos. Uno de los nuevos objetivos de los delincuentes. "Ahí está el agujero y hemos desplazado presupuesto", afirma el general Ballesteros.

Cualquier manual de batalla, y esta lo es, describe las tácticas propias y del enemigo. En el principio lo habitual era la denegación de servicio. La página web queda inaccesible durante un tiempo. El problema es que accedan a la plataforma, consigan privilegios de administrador, encripten la información, la revendan a otro *hacker* o bien chantajeen al propietario. A veces, las fórmulas más sencillas son las que mejor funcionan. La primera medida que se adoptó cuando Rusia invadió Ucrania fue que en 48 horas todos los funcionarios cambiaran sus claves. Porque el departamento de Seguridad Nacional llevaba más de un mes largo, antes de la contienda, estudiando las consecuencias que podría tener para España el enfrentamiento. Comerciales, agrícolas, militares o en

**Abajo, de izquierda a derecha: Elia Fernández Granados, productora ejecutiva de Branded Podcast en Prisa Audio; Manuel Bartual, guionista de Titania; Marta Cabello Cid, responsable de Contenidos en Banco Santander; y Andrés Arias Cortés, head of Secure Online Experiences and Content de Grupo Santander .** SANTI BURGOS


las relaciones entre territorios. Toda guerra es un fracaso. "Pero esta es vergonzosa y entra dentro de los crímenes contra la humanidad. No existe ninguna guerra humana, sin embargo esta la supera", lamenta.

En el otro extremo del diálogo. Aunque las palabras nunca se crucen. El encuentro lo cierra la voz, cargada de experiencia, del general Rafael García Hernández, comandante del Mando Conjunto del Ciberespacio (MCCE). Es la unidad conjunta más joven de las Fuerzas Armadas. Se creó en mayo de 2020. Días de pandemia. Y de inquietud. "Cada vez hay más preocupación con las infraestructuras críticas que dependen de las Fuerzas Armadas", admite el militar. El campo de batalla son trincheras de tecnología. Aviones, tanques, proyectiles, barcos. Imaginen —explica— que atacan los sistemas de navegación por GPS de los barcos que cruzan el estrecho de Gibraltar. "En el ciberespacio parece que la guerra es constante. Aunque no estamos mal. No somos lobos pero tampoco corderos", resume García Hernández. Los nuevos barcos —avanza— se están creando con su gemelo digital y esto "hay que protegerlo". "E intentamos siempre buscar proveedores, pensemos en *software*, españoles. Es la primera opción. Los hay, y muy buenos". Encaja con la estrategia de soberanía digital.

En la cortinilla de comienzo otra de las imágenes de la presentación es una galaxia en espiral. Algo muy lejano. Hace falta viajar años luz. Pero el futuro es ahora. Un modelo de guerra

**Carlos López Blanco, presidente de la Fundación ESYS (Empresa, Seguridad y Sociedad Digital); y Olga Forné, CISO Global de Abertis.** S. B.

**Jose Ángel Delgado, fundador y CEO de BeDisruptive (izquierda); y Xabier Mitxelena, CEO de Cybertix.** S. B.

## El 'podcast' de la conciencia virtual

El primer gran *podcast* de la historia fue *La guerra de los mundos* (1938), protagonizado por el genio Orson Wells, que avanza la llegada de unos hostiles marcianos al planeta. El pánico que generó en una advenediza sociedad estadounidense todavía se recuerda.

Actualmente, el formato *podcast* vive su Edad de Oro y se ha convertido en una herramienta que, define con acierto Elia Fernández, productora ejecutiva de *branded podcast* en Prisa Audio, es "cine para los oídos".

Pero dónde entra en escena la ciberseguridad. Prisa Audio junto con el Banco de Santander han creado *Titania*. Un *thriller* sonoro escrito por Manuel Bartual, ganador del Ondas Global del Podcast 2023, y Juanjo Ramírez, guionista de la serie *La casa de papel*.

El relato comienza con una voz en *off* y sus, entre frías y cálidas, palabras.

—Muchas veces la rutina es lo único que nos aleja de lo que realmente queremos—.

—Pasamos nuestros días atrapados en una vida que no nos deja tiempo para disfrutar, pero esto va a cambiar con Ada—.

—Gracia a Ada podrás olvidar el estrés y la complicación de la planificación diaria—.

—Nuestro asistente va a organizar tu tiempo de manera eficaz y segura-segu-segu-segur…—. La voz se rompe.

(De fondo, una música dramática).

—Acabo de hablar con Rebeca, ha perdido a Lucas—, asegura, espantada, una mujer.

—¿Cómo va a perder a Lucas?, su hijo—, replica un hombre. Estate tranquila va a salir todo bien. Esto no es más que un susto, ya verás—.

(…)

La trama continúa con una superposición de inquietantes frases y ruidos.

Es el arranque. No se puede llegar más lejos. Se estrena el 23 de mayo, entre otras, en la plataforma *Podium*.

Lo apasionante es que a la vez enseña a los clientes de Banco Santander sobre los riesgos de la ciberseguridad mientras se desliza una apasionante historia. "Desde el banco tenemos la idea de que la gente puede mejorar en todos los aspectos, incluido el digital. Por eso para llevar la ciberseguridad más lejos hay que traerla más cerca", observa Andrés Arias Cortés, *head of Secure Online Experiences and Digital Content* de la entidad.

*Titania* mezcla la parte divulgativa (*branded content*) con lo lúdico. "Es un vehículo perfecto para trasladar nuestros mensajes", admite Marta Cabello, responsable de Contenidos en Banco Santander. Y, también, emplea alquimia. Con los guionistas. Hicieron su trabajo de campo. Reunir toda la información posible y entrevistar a *hackers* que se "habían vuelto buenos". "La ciberseguridad es un problema pero es un caramelito para la ficción porque genera infinidad de posibilidades narrativas", sostiene Bartual. La intriga siempre es un género atractivo.

Anthony Burgess (1917-1993) publicaba en 1962 su famosa novela *La naranja mecánica* y también un texto distópico, *The Wanting Seed*, que definió como "un cómic malthusiano". Gran Bretaña está superpoblada. Se fomenta la homosexualidad. Los embarazos son ilegales y los heterosexuales están discriminados. El país inventa guerras falsas con el único propósito de matar a los jóvenes que sobran. Pero el final aporta esperanza a tanta desolación. La pareja central, cuyas vicisitudes construyen la trama, se encuentra en una playa. "Y ella rezó por alguien, y la plegaría fue atendida de inmediato. Ella se aferró a él". Burgess cierra el relato con un verso del poeta francés, Paul Valéry: "El viento se levanta. Debemos tratar de vivir".

híbrida. Ucrania ha abierto esa escotilla. "Es una guerra que mezcla pasado y vanguardia. No existe un único ciberespacio: sino una síntesis del espacio físico y digital", prevé el general. Y el planeta se parte con la facilidad de la madera de balsa. "Existen dos grandes bloques, los que aceptan las reglas democráticas y los que no. Ese es el futuro: lo aceptas o no", recalca. Ante tantas incertidumbres, la ciberdelicuencia opera a la carta. Grandes empresas —con criminales muy preparados— que aceptan encargos.

Los dos generales han llevado a la audiencia al río y les han hecho contemplar el reflejo. Sin distorsiones. "Esta es la realidad, no imaginen otra". Guerra, miles de ataques, billones de dólares robados, vidas más difíciles de vivir. En el Instituto Nacional de Ciberseguridad (Incibe) estas aguas las han remontado muchas veces. Su cometido es sobre todo defender a empresas y ciudadanos. Sobran los motivos. "Los ciberataques son cada día mayores", cuenta su director, Félix Barrio. Europa necesitará 160.000 nuevas pymes que den servicios de ciberseguridad al tejido digital, ciudadanos y administraciones. Hasta 2026, el Incibe invertirá 520 millones de euros en mejorar las capacidades del tejido empresarial. Quieren proteger, entre otros sectores, las finanzas o la energía, donde, diríase, buscan cobijo los estafadores. Son ámbitos prósperos. Y estos criminales son ladrones de prosperidad. Nadie está a salvo. Marina Nogales Fulwood, *Global Head of Cyber External Engagement* de Banco Santander, revela que incluso colaboran con competidores directos. Un endemismo en la competitiva soledad del dinero. Comparten información, sistemas de defensa y detección. "Esto llega a los proveedores y los clientes", admite. Porque los intrusos han des-

*Pasa a la página 4*

*Viene de la página 3*

cubierto que es un hueco en el tronco del árbol de *Alicia en El País de las Maravillas*, por donde descender y llegar a la fuente original. "Tenemos que proteger el ecosistema *ciber*", subraya Nogales. Un banco global, una seguridad global. Especialmente cuando mucha información se guarda en la nube. "La inteligencia artificial y la automatización nos ayudarán", prevé Miguel Ángel Thomas, socio de ciberseguridad de la firma de integración de sistemas NTT Data. "Pero también hay que intentar asfixiar a los criminales con sanciones económicas". El analista trae a la memoria que genera más dinero que el narcotráfico. Es una lucha que también implica a organizaciones como Interpol o Europol. "He estado en incidentes grandes y ayuda la simplicidad. Tener una visión precisa de la compañía porque, si no, incluso adquirir una mirada de tu propia firma se complica mucho. Aunque existen herramientas que te pueden ayudar", incide Thomas.

### Delincuencia global

Quizá uno de los grandes "descubrimientos" que dejan la crisis económica mundial en 2008, la pandemia de covid durante 2020 y la guerra en Ucrania es que las sociedades son más frágiles de lo que se pensaba. Este descubrimiento también lo han hecho quienes se mueven en la noche más oscura del alma. "Los ciberdelincuentes son globales. Hay gente que ha creado plataformas a las que le encargas el delito. Esto es fascinante, si no fuera terrible", relata Carlos López Blanco, presidente de la fundación ESYS (Empresa, Seguridad y Sociedad Digital). Esta fragilidad preocupa especialmente en las infraestructuras o entidades consideradas, según algunas voces, críticas. Un silogismo básico propone que un problema global exige una respuesta global. Pero también hay una geopolítica del desacuerdo. Las respuestas generales chocan contra la soberanía nacional. Bruselas está ahí. Inactiva, dirán unos. Protegida, aseverarán otros. También trazan bisectrices comunes. La seguridad en la red 5G resulta esencial.

Los límites se han fracturado. La velocidad resulta enorme. Las autopistas —cada vez más digitales— sufren mayores ataques. Buscan información de tráfico o números de clientes. Y roban *software* y *hardware*. La polémica público-privada las ha situado cerca del frente. Ninguna gran compañía puede abarcarlo todo. Los presupuestos son finitos. "La estrategia debe ser sencilla, eficaz y eficiente", desgrana Olga Forné, *Chief Information Security Office* (CISO) global de Abertis. Y añade: "Tienes que plantearte qué riesgos quieres asumir y cuales no; y trazar tu estrategia de ciberseguridad". Nadie duda de la implicación de estas siglas. Pero, ¿y otras? ¿Los CEO? ¿Los consejeros delegados? ¿Les preocupa este riesgo? "Sin duda, la letra con sangre entra. La crisis de seguridad es un daño reputacional y eso les importa mucho. Además, los consejos de administración son responsables si no han actuado con diligencia", avisa López Blanco. La tecnología empezó midiendo los cielos y, últimamente, mide las sombras.

# Ertzaintza: "Las estafas digitales nos están machacando"

## El año pasado, el 48% de los delitos se sufrieron en el ámbito de internet y uno de cada cinco se comete a través de las redes. Casi cualquier fraude se pude construir a través de las TIC

**M. Á. García Vega**

Vasos comunicantes. Quizá sea una de las conexiones más vibrantes que puede establecer hoy la tecnología. La que lleva del emprendedor ciberdigital a los cuerpos y fuerzas de seguridad del Estado que, como describen ellos con realismo, "pisamos todos los días el barro del delito". Por medio hay frases y palabras sobre inversión, talento, formación. Xabier Mitxelena, consejero delegado de Cybertix —una consultora de ciberseguridad destinada a autónomos y pequeñas empresas—, es bien conocido en el mundo emprendedor. Comenzó en los albores de internet allá por 1995, y sabe que emprender es decidir y nunca resulta fácil. No son fondos de inversión que entran y salen en un máximo de cinco años y manejan un holgado balance. "Como inversor particular es bastante complejo. Hay que calcular un análisis muy exhaustivo. Hallar un valor añadido. Nosotros lo encontramos en los servicios de seguridad gestionado [antivirus, *firewalls*, detección de intrusos, actualizaciones, auditoría de seguridad…]", admite.

El ecosistema de las cifras parece la carrera de *Alicia en El País de las Maravillas*: hay premio para todos. Este año, el sector facturará, a nivel mundial, 219.000 millones de dólares y crecerá un 12%. Y la consultora Gartner estima que durante 2026 el 70% de las juntas directivas tendrán que conocer el entorno ciberseguridad. Es la estrella de David guiando al portal de Belén. ¿O amanecen nubes que la ocultan? Hace falta talento que empiece ya a trabajar (existen unos 120 másteres de seguridad, una diáspora educativa), simplificar todo este escenario y que los consejeros delegados entiendan que no hablamos de coste, sino de inversión. Y concretar los oficios: ser, por ejemplo, experto en seguridad financiera o energética.


**De izquierda a derecha: Elsa Vicario, responsable de delitos estratégicos en la demarcación del Duranguesado (Bizkaia); Diego Alejandro Palomino, inspector jefe Policía Nacional; y Rosalía Machín Prieto, capitán de la Guardia Civil.** SANTI BURGOS

Recuerda aquella frase de Neruda. "Nosotros, los de entonces, ya no somos los mismos". La diferencia puede ser el formato. BeDisruptive se define como una *boutique* tecnológica. La semántica resulta importante. Trabajan —sostiene— a medida del cliente y le acercan las últimas soluciones. En un mapa tachonado de destinos y oficinas. Roma, Madrid, Milán, Panamá y Washington. Esta es la interpretación de José Ángel Delgado, fundador y consejero delegado de la compañía. Los dos expertos tienen fe y esperanza en los cambios. Todas las empresas españolas de *software* que han tenido éxito (¿recuerdan Panda?) han sido compradas o bien trabajan fuera. "Debemos conservar esta industria. Es un tema cultural. Falta que cale la idea de que se trata de una urgencia y necesitamos confianza", resume Mitxelena.

Tal vez debería trascender el concepto de soberanía digital. Y una vez más la palabra talento. Un punto y seguido que transcurre por una carretera interminable. "Creo que no andamos tan mal. Tenemos gente muy preparada. Pero faltan deberes. Debemos avanzar con la Administración pública para formar a los jóvenes", aconseja Delgado. Cursos cortos, inteligencia artificial, cuidar a las personas, dotarlas de un plan de carrera, chicos y chicas que estén estudiando Formación Profesional o entren en la Universidad y hallen en este mundo un propósito de vida.

### Vocación contra el cibercrimen

Ese es el barro de Elsa, Rosalía y Diego. La calle, la comisaria, las oficinas estatales. Gran parte de los estratos de esa tierra arcillosa donde el delito toma forma. Los tres (se aprecia en las fotos) visten sus uniformes respectivos. Representan una generación joven, con dos mujeres, de la seguridad del Estado. Faltan sus apellidos y sus historias. Elsa Vicario es responsable de Delitos Estratégicos en la demarcación del Duranguesado (Bizkaia). Ha pasado siete años en tecnología y ha vuelto a trabajar en el día a día. Pelo castaño recogido en una colecta, manga corta y un discurso a los ojos.

"No os hacéis una idea de la cantidad de estafas que estamos viendo. Es el delito que más se comete. Tanto a empresas como a particulares, les están puliendo. Es una barbaridad", avisa. "Tal vez no genere tanta alarma social como la pornografía infantil o la pederastia, pero las estafas nos están machacando". Y advierte de que hay chicos de 20 años capaces de organizar en un fin de semana una estafa y ganar de 150.000 a 200.000 euros sin trabajar y desde casa. "Son jóvenes nativos digitales resultado de la era que vivimos y persiguen, solo, dinero", revela Vicario.

**Hay chicos de 20 años capaces de organizar en un fin de semana un timo *online* y ganar hasta 200.000 euros desde casa**

El paisaje es bastante oscuro, casi negro. El año pasado, el 48% de los delitos se sufrieron en el ámbito digital y "uno de cada cinco se comete a través de las redes. Casi cualquier fraude se pude construir a través de las TIC". Quién duda ahora del infinitivo "machacar". Esta última declaración procede de Diego Alejandro Palomino, inspector jefe de Policía Nacional. Transmite un relato seguro. Es vocacional. Y también comenta el asombro. Confirma eso que en el argot llaman *modus operandi*. "Las organizaciones criminales están trabajando como empresas. Incluso reinvierten sus ganancias ilícitas en mejorar su tecnología. Han aprovechado la pandemia para ser más eficientes", revela.

Rosalía Machín se disculpa. "Hablo mucho", sonríe tras una coleta rubia y una enorme empatía. Es capitán de la Guardia Civil y jefe de proyectos TIC-IA (Inteligencia Artificial). "Estamos en un espacio sin fronteras y los delitos no tienen nacionalidad. Hay que reforzar la cooperación internacional. Y la relación público-privada".

Dos frases directas que no precisan ni comas. Pero conviene armar alguna cuenta. Para no perderse como Teseo (sin Ariadna) en laberinto de las cifras inimaginables. El coste medio de una *ciber-breach* (cíber-brecha) que dura 200 días o más es de 4,86 millones de dólares. Son los datos del informe *Cost Of A Data Breach*, publicado el año pasado por IBM. Quizá sean las grietas más caras del mundo.