CiberData. Núm. 1, 2025, pp. 29-33

ENTREVISTA CON BERNARDINO CORTIJO FERNÁNDEZ

Por Noelia Valenzuela García
Universidad de Cádiz - España
Orcid: 0000-0003-0851-9168

D. Bernardino Cortijo, Doctor en Derecho y Ciberingeniería, matemático e ingeniero civil. Fue Comisario de Policía Nacional y fundador de las Unidades de Ciberdelincuencia, además de representante de España en el Consejo de Europa. Actualmente es Director de Seguridad y Fraude de Telefónica y socio fundador de DACOR Intelligence. Profesor universitario, conferenciante y autor de diversas obras, es una de las figuras más reconocidas en el ámbito de la ciberseguridad y la investigación tecnológica.

P. Durante tu trayectoria en Telefónica, ¿qué tipo de incidentes o brechas de seguridad fueron más difíciles de contener o gestionar? ¿Qué aprendizaje crees que sigue siendo vigente hoy?

R. Lo más importante es tener una visión de riesgos en cada momento para poder priorizar por criticidad. Los intentos de ataque, el robo de datos y el ciberfraude son constantes a diario. No basta con herramientas tecnológicas: los procesos de prevención y control son tan importantes como las herramientas, y también la experiencia del personal experto en cada puesto.

Dado que muchos incidentes implican engaño al usuario, al empleado o al cliente, los casos más complejos son los que facilita el propio usuario sin saberlo. Por ejemplo: si con un simple toque se puede provocar el borrado de un disco, la decisión —inducida por engaño— nos deja poco margen salvo actuar preventivamente con formación y alerta.

También son muy complejos los ataques por persistencia. Sea cual sea la modalidad, cuando los intentos son repetitivos acaban causando brecha. Aquí, las acciones de defensa basadas en ciberinteligencia resultan muy eficaces.

Cada día veo distintos ciberriesgos y ataques, y me sorprende que la mayoría son los mismos de hace una década, aunque ahora cuentan con herramientas más accesibles, facilidad para programar malware e incluso uso de IA que los mejora o agiliza.

P. ¿Cuál dirías que es el mayor punto ciego actual en la seguridad digital de grandes infraestructuras o servicios críticos? ¿Qué está más expuesto de lo que la mayoría imagina?

R. Lo primero es diferenciar el área de la empresa crítica de la que hablamos, porque en todas hay cuestiones de seguridad digital. La más olvidada es la organizativa —gobernanza—. Dependemos de terceras partes (proveedores o incluso administraciones), el famoso "supply chain", que puede arruinarnos por el mal hacer de un proveedor: es el efecto mariposa.

Luego está la gestión del riesgo y, sobre todo, el apetito de riesgo: el umbral que fijan los responsables para mejorar resultados o cumplir mandatos. Por eso, siempre hay que hacer un mapa de riesgos específico para esa organización y ese momento, y contemplar la gestión de crisis dentro de la gobernanza.

En el plano tecnológico, en grandes empresas industriales con zonas robotizadas o automatizadas, todas las redes de datos deben separarse de las redes informáticas y auditarse por separado, sin parar producción y consdierando que es una empresa no crítica. Aquí hay muchos puntos ciegos: segmentaciones IP mal diseñadas, crecimientos sin planificación, híbridos cloud/SOC compartidos, y ofimática/aplicaciones internas basadas en servicios de terceros sin garantías de recuperación (hay que leer los contratos).

También fallan los sistemas internos de operaciones: aplicaciones desarrolladas deprisa que funcionan, pero con errores o puertas falsas y sin desarrollo seguro, pese a que la normativa europea lo exige. Añade la mala gestión de la información sensible: consejos de administración no protegidos, documentos que se pierden o roban, planes comerciales que acaban en la competencia. La solución pasa por un plan de control de la información, formación interna y uso adecuado de la tecnología. Además, NIS2 sanciona conductas irresponsables y DORA regula el sector bancario. Y la IA y los modelos generativos que se están incorporando sin conocimiento ni verificación generarán nuevos puntos ciegos.

Para un atacante, una infraestructura crítica es un laberinto con varias entradas: servicios multimedia, domótica, robótica, accesos de personal, móviles en la red, VPN remotas desde casas u hoteles, conexiones interno-externas.... Los detalles importan: la arquitectura de red debe diseñarse y respetarse, pero donde más vulnerabilidades hay es en los procedimientos. En servicios críticos, las rotaciones de personal, el diseño seguro y el manejo de datos son vitales. Y no pueden faltar revisiones constantes con red teams controlados.

P. La ha irrumpido en todos los sectores, también en el delictivo. ¿Qué uso de la IA por parte de atacantes te preocupa especialmente? ¿Y cómo puede aprovecharse desde la defensa?

R. La inmersión en IA por parte de organizaciones y personas sin entender qué implica será un problema inmediato. Se han puesto en manos de todos herramientas espectaculares, pero no se enseña a usarlas ni a comprender sus implicaciones.

Te cuento algo: he hablado con asociaciones que representan a cientos de empresas y miles de ciudadanos. Muchas usan ChatGPT, Perplexity, Arc, Copilot, etc., y les proporcionan datos personales, financieros o de expedientes —a menudo en servicios gratuitos— para que les ayuden en sus trabajos. Eso habla por sí solo.

Además, hoy es fácil programar sin saber programar, así que es sencillo crear rutinas de troyanos o malware que confundan a usuarios e incluso a programas de seguridad, cambiando

código para hacerse invisibles y ampliar alcance. Algunos estarán protegidos, pero muchos no.

En defensa, estamos preparando modelos de IAG y monitorizaciones activas con lenguajes naturales y multimodales (tipo GPT o Gemini) para automatizar decisiones con grandes volúmenes de datos, reglas e instrucciones. Lo clave hoy no es solo detectar, sino automatizar respuestas: cambiar parámetros, limitar IP, restringir conexiones salientes, balancear accesos ante DoS, etc. Un sistema de contramedidas autónomo (o asistido) con todo preconfigurado es posible, parecido a los sistemas expertos clásicos (en un portaviones, por ejemplo, ante un incendio, un humano no procesa todo en segundos; un sistema experto sí).

Esto exige una capa de toma de datos con acceso a todos los sistemas, filtrado y preparación, un modelo IAG/LLM (p. ej., GPT-5, Falcon, Llama), código de eventos de seguridad y una capa operativa (SOAR) integrada con SIEM, IDS, firewalls, GRC, para playbooks y control de incidentes, todo ello auditado (evidencias). Hay plataformas comerciales que lo orquestan, pero hay que adaptarlo a cada caso.

P. ¿Estamos preparados para ataques combinados, como ciberataques coordinados con desinformación o suplantación de identidad mediante deepfakes? ¿Qué brechas ves en la respuesta institucional o empresarial?

R. No creo que estemos preparados; casi siempre los ataques son combinados. En los masivos o indiscriminados, una buena configuración hecha por profesionales y formación reducen más del 75 % de los riesgos.

Pero los casos graves que sufren los ciudadanos —derivados de ataques a empresas que custodian sus datos— sí suelen ser mixtos. El ser humano es el eslabón más débil (y también el más fuerte): puede ser engañado con facilidad, y entonces el sistema queda expuesto.

Por eso, prefiero procedimentar, documentar, formar al personal y a los usuarios, y después monitorizar e implantar modelos sencillos. Las herramientas funcionan y son importantes, pero hay que crear procesos auditables y comprensibles.

P. ¿Qué tipo de perfil profesional falta hoy en los equipos de ciberseguridad? ¿Formamos bien en la dimensión humana, estratégica y ética de la seguridad?

R. Hay técnicos estupendos, con una capacidad bestial, pero son pocos. Es difícil encontrar expertos verdaderos en modelos de seguridad. Dirijo un máster en Ciberdelincuencia centrado en lo investigativo y forense, e incidimos en lo jurídico: 50 % de los contenidos son jurídico-procesales. No solo por su uso en procedimientos, sino para comprender la actividad del ciberdelincuente y cómo operan las organizaciones criminales. No todo vale para todo: como en medicina, un cardiólogo no tiene que saber de psiquiatría.

Otra carencia es la visión global y estratégica. Muchos empresarios contratan a “informática” para diseñar la seguridad, cuando debe hacerlo un experto en ciberseguridad (o seguridad global) y luego tecnología implanta. Ejemplo: hay que saber si un empleado hace entradas remotas un fin de semana sin justificación o descargas masivas: eso debe vigilarlo un experto en seguridad; el responsable de informática facilita la información o automatiza reglas.

La ética es clave: no es postureo. También afecta al empresario o político que usa datos pero no pone medios para protegerlos: eso también es ética.

P. ¿Detectas una desconexión entre el avance técnico y la cultura digital de la población? ¿Qué errores repetimos por falta de alfabetización en seguridad?

R. No lo veo como desconexión, sino como exceso de innovación para todos —dispositivos, comunicaciones rápidas, programas intrusivos, necesidad de usarlos a diario— con muchos riesgos y pocos avances legislativos y operativos: desprotección de la ley en datos (a pesar del GDPR), exceso de necesidad de uso (recordemos el apagón global), administraciones no preparadas, delincuentes muy activos, globalización de comunicaciones y datos.

Hay desconocimiento, sí, pero también exceso de digitalización. Muchas veces obligan a usar sistemas incomprensibles (impuestos por Internet, certificados o firmas electrónicas poco amigables), cuando técnica y organizativamente sería posible hacerlo sencillo. En cambio, impiden ir físicamente o hablar por teléfono con una persona. No estoy en contra de la digitalización —me dedico a ello—, pero no vale todo. La alfabetización no es solo del usuario: también del que pone los sistemas y de la administración. Y esto es global.

P. En términos de coordinación entre entidades privadas, administraciones públicas y cuerpos policiales, ¿dónde ves más debilidades? ¿Qué tipo de cooperación real es posible?

R. Sin trabajo conjunto entre administración y empresas, mal asunto. Y la Policía ya no puede ser independiente: debe trabajar con el ciudadano, la empresa y los técnicos, y estos deben ayudar. También al revés. Hay medidas que pueden tomarse antes de la judicialización para evitar males mayores.

El problema es que muchas veces depende de personas, no de la institución. Existe coordinación entre policías. En su momento fui representante en el Convenio de Cibercrimen (Consejo de Europa). Hoy casi todos los países lo han incorporado y se ha avanzado más. Europol funciona bien en coordinación operativa. Ahora toca coordinar con la sociedad civil. Hay avances, pero insuficientes. También los órganos judiciales deben mejorar: el ciberespacio va muy rápido y no podemos seguir los plazos de la sociedad del "derecho romano".

Seamos positivos: todo ha mejorado mucho en esta década. La coordinación y los medios policiales son mejores. Algunas compañías colaboran bien, pero carecen de defensa jurídica a veces; por eso hace falta legislación y aplicación judicial que sostenga esa colaboración.

P. Si mañana tuvieras que diseñar una estrategia nacional urgente contra los riesgos digitales, ¿qué tres prioridades marcarías sin dudar?

R. Sería pretencioso hacerlo solo: hay muchas áreas y se hace con equipo. Pero me mojo.

Debe alinearse con la UE (legislaciones y estándares). Alcance temporal: 5 años, con dos premisas: prevención proactiva (ciberinteligencia y medidas prospectivas) y ciberresiliencia (capacidad de recuperación automática al estado inicial). Ámbito: administración, servicios críticos y regulados, y pymes —algunas críticas—.

Modelo basado en zero trust ("nunca confíes, verifica siempre") y análisis de riesgos, guardando evidencias y corporación.

Áreas: gobernanza, regulación, sistemas de alta protección (críticos), detección-respuesta, ciberinteligencia y ciberdelito, capacitación y formación, IAG, cooperación nacional e

internacional (empresa-administración), plan de ciudadanía, indicadores y un observatorio de la realidad digital. Priorizaría:

1. Gobernanza digital operativa: CERT nacional; equipos responsables de NIS2, DORA, IA, GDPR, cibercrimen y judicial; procedimientos de desescalado y ejecución; autoridad de ciberresiliencia; estrategia y planes sectoriales de detección-respuesta; gabinete de crisis.

2. Protección de servicios e infraestructuras críticas y suministros.

3. Cibercrimen y seguridad: prospectiva (ciberinteligencia), mecanismos de coordinación y control, seguimiento horizontal y empresas; unidad de IA/IAG.

Y medición, auditorías y ciudadanía (planes de formación).

En mi experiencia, he pasado por Administración, Policía, ciberdelitos, gran empresa, ingeniería, consejos y pyme especializada: todas son importantes en la seguridad de un país. Hay que proteger al Estado y a las infraestructuras, pero también a las pymes y al ciudadano, que es el principal afectado.