Arcano Partners: “El CISO debe ser estratégico y táctico: ante una nueva amenaza o un nuevo riesgo, hay que actuar de inmediato”

Fernando Sanz de Galdeano Sanz, CISO de **Arcano Partners**

Hablamos con Fernando Sanz de Galdeano Sanz, CISO de Arcano Partners, para quien la gestión de terceros es uno de los mayores retos en ciberseguridad. Asegura que controles y capacidades de Zero Trust y otras plataformas como XDR o NDR son imprescindibles para la ciberseguridad del futuro, que DORA ha cambiado las reglas del juego, ya que ahora no sólo hay que demostrar seguridad, sino también resiliencia. Apuesta por enfoque Zero Trust para evitar fugas de información en el uso de IA, y tiene claro que, en un sector tan dinámico y competitivo, quedarse atrás en ciberseguridad no es una opción.

Con más de 15 años de experiencia, Fernando Sanz de Galdeano Sanz es, en la actualidad, el CISO de Arcano Partners, una firma internacional líder en asesoramiento financiero y gestor de activos alternativos con oficinas en España, Estados Unidos, Irlanda e Italia que, fundada en 2003, cuenta con un equipo de más de 250 profesionales.

IR A PÁGINA SIGUIENTE

La ciberseguridad se ha convertido en un elemento clave para las empresas del sector financiero, y Arcano Partners no es la excepción. Con la llegada del Reglamento de Resiliencia Operativa Digital (DORA), la compañía se enfrenta a nuevos retos para garantizar el cumplimiento normativo y la protección de su infraestructura digital. En una entrevista exclusiva, el directivo comparte su visión sobre la evolución del sector y los principales desafíos que enfrenta.

El responsable de seguridad de Arcano Partners destaca la importancia de la ciberseguridad en un segmento del sector económico financiero que tradicionalmente ha estado menos regulado en este aspecto. “Para nosotros, DORA es un cambio significativo. Hasta hace poco, nuestro subsector no estaba regulado en ciberseguridad, mientras que la banca y las aseguradoras, sí. Ahora, debemos cumplir con un marco normativo estricto y garantizar la resiliencia de nuestras operaciones y procesos, como grupo de entidades supervisadas por la CNMV”, asegura Fernando, señalando además la necesidad de concienciar a la sociedad sobre el papel de las entidades de inversión en el sector financiero: “Siempre se habla de los bancos y las aseguradoras, pero nosotros somos la tercera pata del sector. Gestionamos fondos y activos financieros, y la ciberseguridad es clave para mantener la confianza de nuestros clientes y la estabilidad del negocio”.

¿Qué cualidades debe tener un buen CISO?

Ser un buen comunicador es una de las cualidades que debe tener un buen CISO, asegura el directivo. Tiene claro que hay que saber explicar los riesgos en términos comprensibles para la alta dirección y para todos los empleados, además de “la importancia de mantener una perspectiva tanto estratégica como tác-

tica en ciberseguridad. La estrategia permite alinear las iniciativas de seguridad con los objetivos de negocio a largo plazo, garantizando una protección sostenible y coherente. Sin embargo, la dimensión táctica es igualmente crítica, ya que las amenazas evolucionan constantemente y exigen la capacidad de tomar decisiones rápidas y efectivas para mitigar riesgos en tiempo real".

Además, subraya durante la entrevista la importancia de la toma de decisiones basada en riesgos recordando que "el negocio cambia constantemente, surgen nuevas obligaciones, ya sea a través de nuevas regulaciones o requisitos de clientes institucionales, aparecen nuevas tecnologías que son utilizadas para generar amenazas cada vez más sofisticadas", y que un CISO "debe ser capaz de evaluar estos cambios y ajustar la estrategia de ciberseguridad en consecuencia".

Cierra esta pregunta señalando que "un buen CISO tiene que ser un engranaje dentro de la compañía e ir completamente a la par que todas las áreas de negocio, entendiéndolo perfectamente y siendo capaz de impulsar iniciativas alineadas con el crecimiento y la innovación, pero sin degradar el nivel de seguridad de la Compañía".

> "Un CISO debe ser un buen comunicador, capaz de trasladar los riesgos de ciberseguridad en un lenguaje comprensible para la alta dirección y para toda la organización"

Los principales riesgos para Arcano Partners

Preguntado por los retos que afronta Arcano Partners destaca Fernando Sanz de Galdeano Sanz el cumplimiento normativo. Recuerda que la compañía "está entrando actualmente en el juego de la regulación y cumplimiento normativo de ciberseguridad y resiliencia", ya que no ha sido hasta el 17 de enero de 2025, la fecha en la que entra en vigor Dora, cuando se enfrentan "no sólo a un marco de regulación que debemos aplicar, sino ser capaces de trabajar junto con el supervisor que nos va a exigir tener un entorno de control y un entorno de gobierno que garantice el cumplimiento de los objetivos de gestión de riesgos tecnológicos que se han establecido en la propia regulación de resiliencia operativa digital".

Otro de los riesgos a los que deben enfrentarse es la gestión de terceros. "Tenemos proveedores en distintos países y cada uno está sujeto a normativas diferentes. Garantizar la seguridad en toda la cadena de suministro es un reto enorme, especialmente con proveedores pequeños que no siempre pueden cumplir con los requisitos exigidos", asegura el responsable de ciberseguridad de Arcano Partners.

Asegurando que la digitalización y la inteligencia artificial traen muchas ventajas, pero también

aumentan los riesgos, señala que, “por último, el mayor riesgo que quizás puedo identificar en nuestros sectores no es la transformación digital en sí, sino la velocidad a la que avanza. Este ritmo acelerado de innovación y adopción tecnológica a menudo supera la capacidad de las organizaciones para gestionar adecuadamente la seguridad, exponiéndolas a vulnerabilidades, brechas de privacidad y nuevas amenazas por lo que aquí es crítica la labor del CISO, que haya sido capaz de generar una cultura de seguridad dentro de la compañía para que la seguridad esté presente desde el momento en el que se comienza a planificar una nueva iniciativa tecnológica o de negocio.”

Tecnologías y cadena de suministro

El mercado de la ciberseguridad está saturado de soluciones y fabricantes y escoger la propuesta adecuada no es sencillo. Según el CISO de Arcano, la clave está en que los proveedores entiendan el negocio: “Nuestro modelo se parece más al de una consultora que al de un banco. Necesitamos proveedores con recorrido que comprendan nuestras necesidades y adapten sus soluciones en consecuencia. Además, los servicios gestionados son fundamentales para empresas como la nuestra, ya que permiten optimizar recursos y garantizar una gestión eficiente de la seguridad”, asegura.

A la hora de responder qué tecnologías de seguridad son imprescindibles, asegura que “no hay una respuesta correcta” ya que dependería de los procesos de negocio de cada compañía y amenazas a las que cada empresa se viera más afectada. Para un negocio como Arcano Partners apuesta por “tecnologías de tipo XDR, que te permitan integrar, detectar y responder a amenazas en tiempo real de una forma semiau-

> “El mayor reto con DORA ha sido la ejecución de pruebas de resiliencia operativa. Sobre el papel, se nos exigen el mismo nivel de exigencia que a un banco o una aseguradora, cuando nuestro modelo de negocio es completamente distinto”

tomatizada”, además de plataformas con enfoque Zero Trust, procesos de gestión de identidades y, fundamental, plataformas que analicen el comportamiento de usuarios, como UEBA y plataformas que también detecten y respondan a amenazas basadas en tráfico de red y comportamiento de dispositivos, como NDR (Network Detection and Response).

A la hora de gestionar la cadena de suministro, Arcano Partners ejecuta un proceso de gestión del riesgo para evaluar a los proveedores antes de su incorporación. Se realiza un análisis inicial para determinar el nivel de riesgo, diferenciando entre, por ejemplo, servicios con acceso limitado a información o aquellos que operan directamente en la infraestructura tecnológica. Según el nivel de riesgo, se establecen contractualmente controles específicos alineados con DORA y la Política de Seguridad de Arcano, y se exige el cumplimiento de estándares como ISO27001 o ISO 22301. Si el riesgo es alto, se realizan auditorías más exhaustivas. Si el riesgo tecnológico del servicio que ofrece el proveedor no puede mitigarse, el proveedor no puede ser contratado. Una vez contratado, el proveedor es sometido a auditorías periódicas, generalmente anuales, para asegurar el cumplimiento continuo. En caso de incidentes o alertas, se refuerzan las evaluaciones para confirmar que los controles de seguridad siguen activos y efectivos y, en definitiva, el riesgo tecnológico de la compañía, sigue controlado.

Uno de los principales desafíos es la gestión de proveedores pequeños, que a menudo no cuentan con los recursos para cumplir con las exigencias de seguridad de grandes compañías. Desde el Departamento de Seguridad de Arcano, se trata de equilibrar la proporcionalidad de las medidas sin comprometer la seguridad de los activos, pero algunos proveedores quedan fuera debido a la complejidad de cumplir con los estándares requeridos, especialmente en lo relacionado con la seguridad de su propia cadena de suministro (subcontratados)

La irrupción de la inteligencia artificial en la ciberseguridad

La inteligencia artificial ha supuesto una revolución en la ciberseguridad, tanto en la prevención como en la detección de amenazas. Arcano Partners ha tomado medidas para adaptarse

a esta nueva realidad “reforzado la concienciación de los empleados, porque la IA ha hecho que los ataques de ingeniería social sean más sofisticados. Por otro, hemos mejorado nuestras tecnologías de detección y respuesta, trabajando con proveedores especializados para mitigar la materialización de un ciberataque”, explica el directivo.

Además, la compañía ha implementado estrictas políticas de control sobre el uso de la IA en el entorno corporativo: “Aplicamos principios de Zero Trust, restringiendo el acceso a herramientas de IA no homologadas y monitorizando el tráfico de datos para evitar fugas de información”, asegura Fernando Sanz de Galdeano Sanz. “El compromiso de la Dirección con la ciberseguridad ha sido un apoyo fundamental a la hora de implementar nuevos controles y nuevas políticas”.

DORA y su impacto en Arcano Partners

Tiene claro el responsable de ciberseguridad de Arcano Partners que DORA “ha llegado para aportar claridad y fortalecer la seguridad y continuidad de negocio en las organizaciones”, entre otras cosas, porque exige que el Consejo de Administración supervise y apruebe la estrategia de resiliencia operativa digital, asegurando que la ciberseguridad sea una prioridad a nivel de la Alta Dirección y se integre en la estrategia global de negocio.

A pesar de ello, el cumplimiento de esta normativa está suponiendo un desafío, especialmente en lo referente a las pruebas de resiliencia operativa, que requieren un nivel de exigencia similar al de bancos y aseguradoras, a pesar de que su modelo de negocio es diferente. “La mayor dificultad la hemos encontrado en la ejecución de estas pruebas, ya que la normativa nos exige el mismo nivel de cumplimiento que una entidad bancaria o aseguradora, cuando nuestro sector nunca había estado regulado en ciberseguridad ni en continuidad de negocio”,

> “Todos los empleados reciben formación en ciberseguridad. No se trata solo de cumplir con normativas, sino de crear una cultura de seguridad dentro de la organización”

explica el director de seguridad de Arcano Partners. “Nos enfrentamos a auditorías, simulaciones de ciberataques y pruebas de recuperación sin tener claro aún cuál es el criterio de proporcionalidad que aplicará el supervisor a la hora de evaluarnos. Sin duda las primeras revisiones que se realicen en el sector, serán un feedback valiosísimo para confirmar que nuestro enfoque y nuestras medidas son las adecuadas”, comenta el directivo.

Otro reto importante es la gestión del registro de información, que DORA exige mantener actualizado con datos detallados sobre todas las compañías del grupo, proveedores tecnológicos y los servicios que prestan.

Formación y servicios

En Arcano, la concienciación de los empleados es una prioridad. Explica Fernando que “nuestro enfoque es partir de la base de que todos los empleados tienen un perfil de riesgo muy alto, por lo que todos reciben formación anual obligatoria, complementada con casos prácticos y numerosas simulaciones de ataques como phishing, llamadas fraudulentas y SMS maliciosos, diseñados para evaluar su nivel de preparación. Este nivel de riesgo se va adaptando y se planifican formaciones y ejercicios específicos para cada colectivo”.

Además, “medimos la efectividad de la formación con simulaciones realistas de ciberataques, identificando vulnerabilidades antes de que se conviertan en amenazas reales, incluyendo a la Alta Dirección”, explica el responsable de seguridad, dejando claro que la ciberseguridad está integrada en la cultura de la empresa.

Para el CISO de Arcano Partners, un servicio gestionado debe estar alineado con los objetivos de la empresa y ser capaz de anticipar riesgos, más allá de simplemente ejecutar tareas técnicas o de mantenimiento. “El sector cambia constantemente, y un proveedor que no sea capaz de detectar amenazas emergentes no nos aporta valor”, explica. “Adicionalmente, un proveedor no puede convertirse en una fuente de riesgo”.

Históricamente, los servicios gestionados se limitaban a la externalización de personal (BPO), pero hoy en día se espera más: “No sólo buscamos eficiencia operativa y cumplir con los objetivos, sino también que el proveedor actúe como un observatorio del mercado, alertándonos sobre nuevas amenazas antes de que impacten a la empresa. En definitiva, dado que un ciberataque ya sea a cliente o a proveedor, afecta a ambos, en nuestros proveedores esperamos encontrar socios para plantar cara conjuntamente a nuevas amenazas”.

¿Qué te haría fracasar como CISO?

“Principalmente, falta de alineación con el negocio y funcionar como un silo. No tener sensibilidad por el negocio y no ser capaz de identificar soluciones proporcionales y adaptadas a lo que me está requiriendo mi propio negocio, sin aumentar el nivel de riesgo o degradar los indicadores de seguridad o de continuidad”, responde Fernando

Explica que un CISO que no comprende las necesidades del negocio y no adapta las soluciones de ciberseguridad a sus riesgos y objetivos” está condenado al fracaso” ya que la ciberseguridad “no puede ser un ente aislado, sino un elemento integrado en la estrategia empresarial”.

La comunicación es otro pilar fundamental, comenta el directivo, recordando que es clave “saber explicar los riesgos tecnológicos a la alta dirección y al resto de empleados en un lenguaje comprensible. Muchas empresas no priorizan la ciberseguridad hasta que ocurre un incidente, y ahí es donde la concienciación previa ha marcado la diferencia en las empresas que no han sufrido un incidente y por tanto deben trabajar desde un punto de vista preventivo”.

Además, el CISO debe estar preparado para responder de manera inmediata ante amenazas emergentes. “Si se produce un incidente en una empresa del sector, ya sea un competidor o un proveedor comprometido, es esencial actuar con rapidez y tomar decisiones estratégicas para minimizar el impacto. La ciberseguridad es un entorno dinámico y en constante evolución, donde la falta de reacción oportuna puede derivar en consecuencias significativas”, enfatiza.

Para ello, es fundamental contar con procesos robustos respaldados por métricas que pro-

porcionen una visión continua del estado de seguridad. Estos indicadores incluyen tanto KPIs (Key Performance Indicators), que permiten medir el desempeño en seguridad, como KRIs (Key Risk Indicators), esenciales para identificar posibles riesgos emergentes. La implementación y supervisión de estos indicadores permiten mantener un enfoque de mejora continua, garantizando que la organización pueda adaptarse y responder de manera ágil ante cambios en la exposición al riesgo.

> "No buscamos proveedores que simplemente vendan herramientas. Necesitamos socios estratégicos que entiendan nuestro negocio y que puedan anticiparse a los riesgos emergentes"

Las tecnologías del futuro en ciberseguridad

El CISO de Arcano Partners destaca varias tecnologías que considera imprescindibles para reforzar la seguridad en las empresas, con un enfoque especial en la inteligencia artificial y la automatización.

Comenta que "Zero Trust evolucionado es una de las claves" ya que "no basta con un modelo tradicional, necesitamos que las decisiones se tomen en tiempo real, idealmente con el apoyo de IA. Hay compañías que aún no pueden reaccionar con suficiente rapidez ante amenazas emergentes o nuevas plataformas que continuamente aparecen", señala.

Además, enfatiza la importancia de soluciones basadas en inteligencia artificial avanzada: "Las herramientas antimalware tradicionales ya han quedado obsoletas. Ahora buscamos plataformas que combinen lo mejor de SIEM, XDR y EDR, pero con IA que permita una respuesta autónoma y proactiva ante amenazas".

Otra de las tecnologías en su radar es UEBA (User and Entity Behavior Analytics), que analiza patrones de comportamiento de usuarios y entidades para detectar anomalías. "Es una tecnología que ya lleva tiempo en el mercado, pero ahora se está potenciando con inteligencia artificial avanzada, lo que mejora su capacidad de detección y reduce los falsos positivos", destaca Fernando Sanz de Galdeano Sanz.

Por último, destaca el papel del MDR (Managed Detection and Response) y el Threat Hunting: "El enfoque MDR refuerza la seguridad al combinar la monitorización continua con capacidades avanzadas de detección y respuesta. Sin embargo, dado que ninguna solución puede garantizar una detección del 100% de los ataques, complementar con un equipo de expertos que realice Threat Hunting, analice proactivamente los logs, ejecute consultas avanzadas y verifique posibles incidentes resulta clave para una defensa eficaz concluye".