DEBATES ciberseguridad TIC

Menos riesgos, más control: Descubre cómo simplificar la gestión de proveedores

IR A PÁGINA SIGUIENTE

Menos riesgos, más control: Descubre cómo simplificar la gestión de proveedores

El almuerzo-debate "Menos riesgo más control: Descubre cómo simplificar la gestión de proveedores", organizado por Ciberseguridad TIC con el patrocinio de Mastercard, reunió hace unas semanas a responsables de ciberseguridad y cumplimiento del sector público y financiero para debatir sobre uno de los desafíos más urgentes de la ciberseguridad empresarial: cómo responder a la creciente presión regulatoria y a la sofisticación de los ciberataques sin comprometer la agilidad operativa.

Rosalía Arroyo

La cita sirvió para analizar cómo tecnologías como la automatización, la inteligencia artificial o las herramientas de *scoring* pueden ayudar a reforzar la protección de datos, fortalecer la ciberresiliencia y facilitar el cumplimiento de normativas como NIS2, DORA o el Esquema Nacional de Seguridad (ENS). Se puso el

foco en el riesgo creciente asociado a la cadena de suministro, donde las organizaciones se enfrentan al doble reto de controlar proveedores cada vez más numerosos y garantizar que todos ellos cumplen unos estándares mínimos de seguridad.

Este resumen recoge las principales aportaciones de los participantes, agrupadas por intervención, para ofrecer una visión ordenada y completa del debate. Un debate marcado por el intercambio de experiencias reales, el reconocimiento de obstáculos comunes y la voluntad de avanzar hacia modelos más inteligentes de gestión del riesgo en el ecosistema de proveedores.

Mastercard

Juan Rodríguez, director regional España y Portugal, Mastercard

“Queremos daros herramientas que os permitan dormir tranquilos”

Juan Rodríguez abrió el coloquio destacando que Mastercard, a pesar de ser conocida principalmente por sus servicios de pago, es “la segunda empresa a nivel mundial que más ha invertido en temas de ciberseguridad”, solo por

> “La ciberseguridad no es una foto fija, hay que mantenerla y actualizarla constantemente”
>
> **Juan Rodríguez,**
> director regional España y Portugal, **Mastercard**

detrás de Cisco. Señaló que el grupo lleva décadas desarrollando e incorporando capacidades avanzadas en protección de datos, privacidad y análisis de inteligencia, incluyendo adquisiciones clave como Recorded Future.

Reivindicó el papel de Mastercard como actor relevante en ciberseguridad, con soluciones que van desde detección de fraude en tiempo real hasta servicios de pentesting con inteligencia integrada. “Imaginaos si yo esto lo mezclo con análisis de inteligencia de Recorded Future... voy a tiro hecho donde sé que se encuentran los puntos vulnerables”.

Además, compartió iniciativas orientadas a ayudar a entidades públicas a incorporar herramientas de *scoring* en licitaciones sin romper con el principio de concurrencia: “Estamos trabajando en certificados gratuitos para que la cadena de suministro se pueda certificar... y el *scoring* sea un proceso más”.

Rodríguez defendió también la integración de indicadores multidimensionales en la evaluación de riesgo, no sólo ciber: “La herramienta va a tener también ESG, privacidad y factores económicos... para que puedas elegir cómo analizar tu cadena de suministro”.

Asitur Asistencia

Israel Díaz, CISO, Asitur Asistencia

“Nos cuesta mucho convencer a los intermediarios para que cumplan normas de seguridad”

> “Llegamos a tener que justificar preguntas con línea de código y enviarlas al cliente para que las vea”
>
> **Israel Díaz,**
> CISO, **Asitur Asistencia**

Desde Asitur, Israel Díaz expuso con franqueza las dificultades de aplicar políticas de seguridad en un entorno dominado por proveedores de muy pequeño tamaño, como profesionales tipo fontaneros o grúas. “Nuestros proveedores no son muy grandes… nos cuesta mucho convencer a los que intermedian con estos profesionales para que cumplan con normas de seguridad”. Señaló que están intentando adaptar las exigencias regulatorias a su red de colaboradores mediante cuestionarios simplificados, aunque admitió que el proceso es arduo y de difícil comprensión: “Nosotros intentamos trasladar los requerimientos de seguridad a nuestros proveedores de un tamaño mucho más pequeño”.

Destacó Israel Díaz la utilidad de la regulación como palanca de cambio como DORA, pero también lamentó la falta de madurez tecnológica de muchos proveedores: “La gente confía en las IP contra IP… pero nunca nadie ha puesto un *logging power*”.

De forma gráfica, describió el nivel de exigencia al que están sometidos por sus propios clientes: “Llegamos a tener que justificarauditorias llegando a línea de código y enviarlas al cliente para que las vea”.

Aresbank

Manuel Rodríguez, CIO, Aresbank

“Nos comprometemos a monitorizar a nuestros proveedores directos, pero es difícil llegar más allá”

> “La participación de los usuarios en la elaboración de los mapas de riesgos supone un cambio de paradigma en la organización”
>
> **Manuel Rodríguez,**
> CIO, **Aresbank**

Manuel Rodríguez compartió la visión de una entidad financiera de tamaño medio que, aunque no actúa como proveedor para terceros, debe cumplir con exigencias regulatorias como

Explora cómo la IA y automatización transforman la ciberseguridad, fortalecen resiliencia y aseguran cumplimiento normativo

las establecidas por DORA y el Banco de España, especialmente en lo relativo a la externalización de servicios tecnológicos críticos como el core bancario.

Reconoció que el control efectivo de toda la cadena de suministro es complejo: “Nuestro proveedor tiene literalmente decenas de subproveedores… y no siempre es viable supervisar todo ese ecosistema con los recursos disponibles”. Además de contar con garantías contractuales, apuntó que “en la práctica, nos centramos en asegurar que nuestros proveedores directos cumplen con los requisitos establecidos”.

También señaló que se está trabajando para que el riesgo tecnológico tenga una presencia más transversal.

Finalmente, subrayó la importancia de avanzar hacia una mayor concienciación y colaboración entre áreas: “No siempre es fácil implicar a los usuarios o al negocio en la identificación de riesgos, pero es algo que establece la normat y que debemos seguir promociendo”.

CESCE

Enrique Cervantes – Dir. de Seguridad e Infraestructura Tecnológica, CESCE

“Adaptar los contratos heredados a nuevas exigencias no siempre es sencillo”

Enrique Cervantes aportó la visión de una empresa estatal que combina las exigencias del sector público con las del mundo asegurador. Subrayó que, aunque los pliegos de contratación ya incorporan cláusulas de cumplimiento y seguridad, una de las principales dificultades está en la rigidez de algunos contratos firmados años atrás, que ahora deben revisarse para adaptarse a nuevas normativas y realidades del entorno de riesgo.

“Todo lo que sacamos va por pliego, y eso implica contratos muy definidos… volver a abrirlos

“Hay una tensión real entre exigir seguridad y garantizar la concurrencia”

Enrique Cervantes,
Dir. de Seguridad e Infraestructura Tecnológica**, CESCE**

para introducir cambios puede ser complejo”, explicó. Aun así, destacó que contar con ese marco cerrado también tiene ventajas, ya que “nos da cierta garantía de cumplimiento desde el inicio”.

También hizo hincapié en la tensión que a veces existe entre las exigencias de seguridad y los principios de concurrencia que rigen la contra-

tación pública. “Poner ciertos requisitos puede limitar la participación de pequeñas empresas, y eso hay que gestionarlo con cuidado”, comentó, apuntando a la necesidad de equilibrio entre protección y apertura.

Cervantes valoró positivamente la posibilidad de contar con herramientas que faciliten la evaluación objetiva de proveedores, siempre que se adapten a los requisitos del sector público. “Tiene sentido si se articula bien… no es tan distinto de otras referencias que ya usamos, como puede ser un informe de analistas”.

Ministerio del Interior

Francisco Alonso – CISO, CETSE / Ministerio del Interior

“Trabajamos con perfiles sensibles, y eso requiere medidas adicionales de control”

Francisco Alonso aportó la perspectiva del Ministerio del Interior, donde la sensibilidad de la información y los entornos gestionados exige medidas de seguridad reforzadas. Explicó que, en determinados contratos, se aplican controles específicos como la habilitación personal

“No es sólo tener herramientas, es usarlas bien, mantenerlas y actualizarlas”

Francisco Alonso,
CISO, CETSE / **Ministerio del Interio**

de seguridad o la comprobación de antecedentes del personal externo: “Comprobamos antecedentes para asegurarnos de que quienes prestan ciertos servicios tienen un historial adecuado”.

También señaló que, en función de la naturaleza del proyecto, se recurre a diferentes niveles de habilitación o cláusulas contractuales de confidencialidad, adaptadas al nivel de criticidad. “No es lo mismo trabajar en una oficina que dar soporte a sistemas de ámbito nacional”, puntualizó.

Respecto a herramientas de evaluación o modelos de *scoring*, se mostró abierto a su uso como complemento, aunque remarcó la importancia de garantizar su objetividad y encaje con el marco legal. “Me parece una buena herramienta, pero es importante saber quién está detrás, cómo se construye y cómo se articula para que no afecte a la libre concurrencia”.

Por último, valoró el papel del Centro Criptológico Nacional (CCN) y su catálogo de productos como un marco útil de referencia asegurando que da ciertas garantías en la selección de soluciones.

CNMV

Miguel Tomás, Subdirector de Ciberseguridad, CNMV

“Aplicamos criterios de riesgo, aunque el marco de contratación pública impone ciertos límites”

"¿Cómo le vas a pedir al fotógrafo que evidencie que ha borrado los datos? Pero hay que hacerlo"

Miguel Tomás, Subdirector de Ciberseguridad, **CNMV**

Miguel Tomás expuso los retos que enfrenta un organismo regulador como la CNMV en la gestión de terceros, en un contexto marcado por la Ley de Contratos del Sector Público, que condiciona tanto los procedimientos como los tiempos de evaluación. Explicó que, en ocasiones, la posibilidad de valorar aspectos técnicos de seguridad antes de adjudicar un contrato está limitada, y que en esos casos se trabaja con planes de acción posteriores: "Muchas veces, la evaluación más detallada se hace después de adjudicar, porque el marco legal no permite otra cosa", aseguraba.

Aun así, subrayó que la CNMV aplica criterios de riesgo para adaptar el nivel de exigencia al tipo de servicio contratado. "No se pide lo mismo a un proveedor de servicios críticos que a uno con un impacto menor... usamos baremos que nos ayudan a graduar el nivel de control".

También mencionó el desafío que supone trabajar con proveedores muy pequeños o autónomos, que no siempre disponen de procedimientos formales de seguridad: "Hay casos donde es difícil exigir ciertas prácticas, pero aun así tratamos de concienciarles y mantener unas mínimas garantías".

En relación con herramientas externas de evaluación o *scoring*, valoró su utilidad como complemento para determinados casos, especialmente si ayudan a mantener una supervisión continua sin incrementar excesivamente la carga administrativa.

Banco Inversis

Manuel Fernández, director de Riesgo Tecnológico & Cumplimiento, Banco Inversis

"Estamos reforzando la función de terceros para afrontar los nuevos requisitos normativos"

"El propietario del riesgo es el área que contrata, y nosotros damos soporte al seguimiento"

Manuel Fernández, director de Riesgo Tecnológico & Cumplimiento, **Banco Inversis**

Manuel Fernández compartió la experiencia de Banco Inversis en la adaptación organizativa que están llevando a cabo para cumplir con los requisitos de normativas como DORA, que exigen un mayor control sobre los terceros y una visión más integrada del riesgo tecnológico.

Explicó que han creado una función específica para reforzar la gestión de proveedores TIC, con personal dedicado exclusivamente a ello. “Hemos empezado incorporando dos personas nuevas en esta función… y seguimos trabajando para consolidarla”. Señaló que uno de los principales retos es coordinar a las distintas áreas implicadas y lograr que la responsabilidad del riesgo no recaiga solo en los equipos de cumplimiento o tecnología. “Es importante que toda la organización entienda que esto no es solo un tema del área de riesgos”.

Destacó durante el debate que ya cuentan con un proceso formal de homologación, en el que participan diferentes departamentos como protección de datos, cumplimiento o prevención de blanqueo, pero reconoció que aún están trabajando en homogeneizar metodologías para evaluar el riesgo técnico de manera más sistemática. Subrayó la necesidad de fomentar una mayor concienciación interna y de avanzar hacia modelos de gestión más compartidos: “Requiere un esfuerzo constante explicar que esto afecta a todos… y que no es una tarea que podamos abordar en solitario”.

FUNDAE

Carlos Juarros, CISO, FUNDAE

“Ahora llega el shadow AI… esa IA oculta que nadie sabe que se está usando”

Carlos Juarros abordó el debate desde la perspectiva de una fundación estatal que gestiona fondos públicos y colabora con distintos organismos y proveedores. Subrayó que uno de los principales desafíos no es solo técnico o normativo, sino cultural. “El mayor reto que tenemos en las organizaciones es la cultura y hacer ver la importancia que tiene esto, no sólo a los de negocio que lo ven más claro, sino a toda la organización”.

Explicó que la aparición de nuevas normativas como NIS2 y la irrupción de tecnologías como la inteligencia artificial exigen una adaptación

> “Tenemos que hacer ver a toda la organización la importancia de la gestión de riesgos”
>
> **Carlos Juarros,** CISO, **FUNDAE**

constante de los marcos de riesgo. “Tienes que empezar a inyectar todo esto nuevo que va entrando… tener eso al día es imposible si no se interioriza desde todas las áreas”.

Compartió el caso concreto de proyectos adquiridos que, en algunos momentos, no habían pasado por los canales habituales de super-

visión técnica: “A veces te encuentras con soluciones ya implantadas que no han sido evaluadas previamente, y hay que trabajar a posteriori para garantizar la seguridad y el cumplimiento”.

Juarros valoró positivamente las herramientas que puedan facilitar la evaluación de proveedores de forma más objetiva y sencilla, y afirmó que ya están explorando su posible integración en los flujos de contratación y seguimiento. “Estamos empezando a incorporar este tipo de análisis desde el inicio del proceso y también en la fase de producción”.

IGAE / Ministerio de Hacienda y Función Pública

Mª Jesús Casado, Responsable de Seguridad de la Información, IGAE / Ministerio de Hacienda y Función Pública

“Llevamos años trabajando para integrar la seguridad en todos los niveles de la organización”

Mª Jesús Casado ofreció una visión respaldada por una amplia trayectoria en el ámbito de la seguridad de la información dentro de la Administración General del Estado. Destacó que, en la IGAE, la seguridad no es algo nuevo, sino una práctica integrada desde hace más de dos décadas. “En junio de 2002 ya teníamos un comité de seguridad... y desde 2003 soy la responsable”, explicó.

> “Hacemos campañas de phishing y enviamos informes anonimizados a los responsables jerárquicos”

Mª Jesús Casado,
Responsable de Seguridad de la Información,
IGAE / Ministerio de Hacienda y Función Pública

Subrayó que el Esquema Nacional de Seguridad (ENS) ha sido una herramienta clave para estructurar los procesos de control y facilitar el trabajo con proveedores. “El ENS nos ha ayudado mucho... y ahora las empresas quieren certificarse porque les interesa trabajar con la Administración”. En los pliegos de contratación, exigen la conformidad con el ENS y el uso de productos del catálogo del CCN, lo que reduce muchas complicaciones operativas.

Mª Jesús Casado también puso en valor el avance cultural dentro de la organización, logrando que áreas de negocio se impliquen en los análisis de riesgos continuos: “Hemos conseguido que los responsables participen activamente... ahora incluso asumen riesgos formalmente cuando hay decisiones que lo requieren”.

Además, compartió su experiencia en campañas internas de concienciación: “Realizamos simulaciones de phishing y elaboramos informes anonimizados que se comunican a los responsables jerárquicos... eso ayuda a visibilizar los puntos de mejora sin generar fricción”.

Conclusión

El debate dejó claro que la gestión del riesgo en la cadena de suministro se ha convertido en una prioridad estratégica para organizaciones tanto públicas como privadas. Ya no se trata únicamente de cumplir con la normativa, sino de hacerlo de forma eficiente, sostenible y alineada con las necesidades reales del negocio. Frente a un panorama regulatorio cada vez más exigente —con normativas como NIS2, DORA o el Esquema Nacional de Seguridad—, todos los participantes coincidieron en que los modelos tradicionales de supervisión y control de proveedores están quedando obsoletos.

Uno de los grandes consensos fue la necesidad de combinar agilidad operativa con una mayor visibilidad sobre los terceros implicados en los servicios críticos. Esto implica, por un lado, mejorar la coordinación interna entre áreas técnicas, jurídicas y de negocio; y por otro, establecer mecanismos de evaluación más dinámicos, proporcionales al nivel de riesgo real y sostenibles en el tiempo.

Aunque las condiciones varían entre el sector privado y el público —especialmente en lo relativo a los marcos de contratación—, el debate evidenció que los retos son compartidos: dificultad para evaluar proveedores muy pequeños, presión creciente desde los órganos reguladores, necesidad de formalizar metodologías de análisis y escasa cultura de corresponsabilidad en materia de ciberseguridad.

También se puso en valor el potencial de los modelos de *scoring*, no como mecanismos excluyentes, sino como herramientas objetivas para tomar decisiones informadas y establecer mínimos comunes en procesos de contratación o evaluación. Algunos participantes ya están explorando cómo integrarlos en sus flujos internos, incluso como parte de cláusulas contractuales progresivas.

En definitiva, quedó claro que avanzar hacia una gestión del riesgo más ágil, basada en datos y capaz de adaptarse al entorno, requiere no solo tecnología, sino liderazgo, colaboración y una transformación cultural que alcance a toda la organización. CST

Mastercard apuesta por una plataforma de riesgo multidimensional para afrontar NIS2 y DORA

Mastercard ha consolidado su apuesta por la ciberseguridad mediante la creación de una unidad de negocio específica que combina tecnología propia y adquisiciones estratégicas. Entre ellas destacan RiskRecon —inicialmente centrada en *scoring* de ciberseguridad— y, más recientemente, Recorded Future, especializada en inteligencia de amenazas. "La idea de lo que estamos haciendo es construir un portfolio que nos permita tener, no solamente protección de datos, sino protección de los clientes y de toda la parte de los activos", explica Juan Rodríguez, director regional para España y Portugal de Mastercard.

Juan Rodríguez, director regional España y Portugal, **Mastercard**

RiskRecon, inicialmente centrada en *scoring* de ciberseguridad, evoluciona hacia una plataforma de riesgo multidimensional, con módulos de privacidad, ESG y financieros. La demanda de este tipo de soluciones se ha extendido más allá del sector financiero, impulsada por normativas como NIS2 o DORA. "Incluso las empresas medianas están empezando a tomar medidas para proteger su cadena de suministro", apunta Juan Rodríguez.