ENCUENTROS IT RESELLER

PRIVACIDAD Y COMPLIANCE

COMO OPORTUNIDAD DE NEGOCIO PARA EL CANAL

ORGANIZA

PATROCINADOR

EUROPA ELEVA EL LISTÓN REGULATORIO Y OBLIGA A LOS MSP A REFORZAR SU MADUREZ EN CIBERSEGURIDAD

La región EMEA se ha convertido en el epicentro mundial de la regulación tecnológica. GDPR, DORA y NIS2 redefinen el nivel mínimo de seguridad, resiliencia y gobernanza exigido a proveedores y clientes, un escenario que obliga a los MSP a reforzar controles, automatizar procesos y elevar su madurez operativa.

Europa vive un momento de transformación regulatoria sin precedentes. La combinación de nuevas amenazas, digitalización acelerada y dependencia creciente de proveedores tecnológicos ha impulsado un marco normativo más estricto, amplio y exigente. Para los proveedores de servicios gestionados (MSP), este entorno supone tanto un desafío como una oportunidad, ya que quienes sepan alinearse con los estándares podrán diferenciarse, ganar negocio y convertirse en socios estratégicos de sus clientes.

Los datos son contundentes. El 67% de las pymes considera que la regulación es hoy el principal impulsor de la inversión en ciberseguridad, mientras que el 81% de las brechas de 2024 afectaron a datos protegidos por al menos una normativa. Además, el 58% de los MSP reconoce que las peticiones de soporte en cumplimiento normativo son ya uno de sus mayores desafíos de negocio.

Los informes actuales señalan que los MSP proporcionan controles críticos que los marcos regulatorios exigen, desde monitorización continua hasta gestión de incidentes o retención de logs.

UN MARCO REGULATORIO CADA VEZ MÁS EXIGENTE

En EMEA, tres normas concentran la mayor presión regulatoria: GDPR, DORA y NIS2, cada una de las cuales aborda respectivamente la privacidad, la resiliencia financiera y la seguridad de infraestructuras críticas, pero todas comparten el mensaje común de que la seguridad ya no es negociable.

El Reglamento General de Protección de Datos (GDPR) sigue siendo la piedra angular de la privacidad en Europa. Su alcance afecta a cualquier organización que maneje datos personales de ciudadanos de la UE, independientemente de su sector o tamaño y exige a los MSP apoyar a sus clientes en controles como cifrado en tránsito y en reposo, gestión de políticas de acceso y autenticación, mantenimiento de registros de actividad y auditoría, automatización de flujos de notificación de brechas, e integración de herramientas de filtrado, email security y prevención de fuga de datos. GDPR no solo exige controles técnicos, sino demostrar que existen, y ahí los MSP se convierten en pieza clave.

LOS MSP PROPORCIONAN CONTROLES CRÍTICOS QUE LOS MARCOS REGULATORIOS EXIGEN, DESDE MONITORIZACIÓN CONTINUA HASTA GESTIÓN DE INCIDENTES O RETENCIÓN DE LOGS

El Reglamento de Resiliencia Operativa Digital (DORA) es probablemente la norma más transformadora para el sector financiero europeo. Su objetivo es garantizar que bancos, aseguradoras, fintech y proveedores críticos puedan resistir, responder y recuperarse de incidentes tecnológico, y exige gestión integral del riesgo TIC, planes de continuidad y respuesta a incidentes, pruebas periódicas de resiliencia digital, supervisión estricta de proveedores externos e iInformes obligatorios de incidentes.

Los MSP que operan en el sector financiero deben crear playbooks personalizados para incidentes, integrar monitorización 24/7 y MDR, gestionar parches, configuraciones y hardening, y alinear sus servicios con los requisitos de auditoría y reporting. DORA no solo regula a las entidades financieras, regula también a sus proveedores tecnológicos, lo que convierte a los MSP en actores supervisados de facto.

NIS2 es la actualización más ambiciosa de la directiva europea de seguridad de redes y sistemas, y está destinada a mejorar la ciberseguridad en proveedores de servicios esenciales y digitales. Su alcance es enorme, llegando a energía, transporte, salud, agua, digital services, administración pública y más, convirtiendo la ciberseguridad en un requisito legal, no en una recomendación.

La directiva exige gestión del riesgo y gobernanza, seguridad en la cadena de suministro, monitorización continua, retención de logs y auditorías, planes de continuidad y respuesta y notificación de incidentes en plazos estrictos. Los MSP que trabajan con sectores críticos deben implementar MDR 24/7, automatizar la retención de logs, realizar ejercicios trimestrales de simulación, gestionar parches y vulnerabilidades, y evaluar riesgos de terceros y proveedores.

UN NUEVO ESCENARIO CON MÁS OBLIGACIONES, MÁS OPORTUNIDADES

A este escenario se suma un elemento decisivo: la convergencia regulatoria. Aunque cada normativa responde a objetivos distintos, todas comparten una misma dirección estratégica, que es elevar el nivel de protección digital en toda la región EMEA y reducir la dependencia de prácticas reactivas.

Para los MSP, esto implica adoptar un enfoque mucho más holístico, donde la seguridad, la gobernanza y la continuidad operativa se integran en cada servicio que ofrecen. Ya no basta con desplegar herramientas; ahora deben demostrar capacidad de anticipación, trazabilidad completa y una gestión madura del riesgo tecnológico.

LOS MSP QUE LOGREN ALINEARSE CON LAS NORMATIVAS NO SOLO REDUCIRÁN RIESGOS, SINO QUE SE POSICIONARÁN COMO SOCIOS ESTRATÉGICOS CAPACES DE SOSTENER LA TRANSFORMACIÓN DIGITAL EN UN ENTORNO CADA VEZ MÁS REGULADO Y EXIGENTE

Además, la presión regulatoria está impulsando una profesionalización acelerada del sector. Los clientes exigen evidencias, auditorías, métricas y reportes continuos que acrediten el cumplimiento. Esto obliga a los MSP a invertir en automatización, documentación, estandarización de procesos y plataformas que permitan responder de forma coherente a los requisitos de GDPR, DORA y NIS2.

En paralelo, la supervisión de terceros se ha convertido en un eje crítico: las organizaciones reguladas deben evaluar a sus proveedores con el mismo rigor que aplican a sus propios sistemas, lo que convierte a los MSP en actores clave dentro de la cadena de cumplimiento.

En conjunto, este nuevo marco no solo redefine las obligaciones, sino también las expectativas, y los MSP que logren alinearse con estas normativas no solo reducirán riesgos, sino que se posicionarán como socios estratégicos capaces de sostener la transformación digital en un entorno cada vez más regulado y exigente. ■

MÁS INFO +

- VÍDEO: Privacidad y compliance como oportunidad de negocio para el canal
- WP: Privacidad y compliance como oportunidad de negocio para el canal

COMPARTIR EN REDES SOCIALES

PRIVACIDAD Y COMPLIANCE COMO OPORTUNIDAD DE NEGOCIO PARA EL CANAL

A3Sec, Digitel TS by MADISON, ADM Cloud & Services, MR Informática, Nunsys, DataGuard, Serval Networks y TUYÚ Technology participaron en un Encuentro IT Reseller con la Comunidad IT, con el apoyo de ADM Cloud & Services y DataGuard, para analizar cómo la regulación, la privacidad y el compliance están transformando el modelo MSP. Los expertos coincidieron en que el cliente ya no busca auditorías puntuales, sino modelos continuos de cumplimiento. La madurez desigual del mercado, la presión normativa y la irrupción de la IA marcan un escenario lleno de retos y también de oportunidades.

Según quedó claro a lo largo de esta mesa redonda, las empresas necesitan ayuda para cumplir con las normativas, y quienes sepan traducir la regulación en soluciones prácticas, escalables y conti-

ENCUENTRO COMUNIDAD IT >> Con la colaboración de ADM Cloud & Services y DataGuard, en este Encuentro IT Reseller de la Comunidad IT, analizamos, de la mano de portavoces de A3Sec, Digitel TS by MADISON, ADM Cloud & Services, MR Informática, Nunsys, DataGuard, Serval Networks y TUYÚ Technology, cómo en el contexto español actual la privacidad y el compliance no solo son obligatorios, sino que representan una oportunidad clara de crecimiento para el canal tecnológico.

nuas estarán mejor posicionados para capturar valor sostenido.

UN SECTOR OBLIGADO A EVOLUCIONAR

El encuentro comenzó con una fotografía clara del momento que vive el ecosistema MSP. La sensación generalizada es que el sector se encuentra en un punto de inflexión, empujado por una avalancha regulatoria que no da tregua. Alejandro Agudelo, Director Global de Operaciones en A3Sec, lo expresó con claridad: “Es un momento súper interesante para todos los MSP”. Para él, la combinación de NIS2, DORA y las crecientes exigencias de soberanía del dato está obligando a los proveedores a replantear su modelo de servicio. El cliente final, explicó, ya no quiere auditorías aisladas, sino “un cumplimiento continuo”, lo que implica integrar evidencias, SOC, controles y procesos en un modelo vivo y permanente.

Esa visión fue compartida por José Antonio Díaz, Director de Digitel TS by MADISON, quien recordó que los prestadores de servicios viven “hiperregulados” y afrontan un ciclo de exigencias crecientes. “Ahora mismo lo que tenemos que hacer de base es cumplimiento, no solo en normativa, sino en DORA, NIS2 y la nueva identidad europea”, afirmó. Para él, la regulación ya no es un elemento externo, sino un componente estructural del negocio, que condiciona desde la oferta hasta la operación diaria.

La perspectiva de Jesús Valverde, CISO de MR Informática, añadió un matiz crítico, y es la falta de conciencia real en muchas empresas. “Todavía hay compañías que no se han enterado de que GDPR lleva diez años”, advirtió. Y alertó de que la Ley de Ciberresiliencia (CRA) “cambiará muchísimo el planteamiento de muchas empresas”, especialmente fabricantes e importadores, obligados a gestionar SBOM y dependencias de software. Para él, la regulación está avanzando más rápido que la capacidad de adaptación de muchas organizaciones, lo que obliga a los MSP a asumir un rol de acompañamiento constante.

Por su parte, Elvira García, Information Security Director en Nunsys, subrayó la enorme disparidad de madurez entre organizaciones. “Tenemos entidades muy maduras y otras que no tienen nada”, señaló. Esa brecha condiciona la capacidad de los MSP para automatizar procesos o implantar servicios gestionados completos. En su opinión, la madurez del cliente determina no solo el alcance del servicio, sino la velocidad a la que puede evolucionar.

En medio de este escenario, Óscar Vierge, Sales Director Strategic Accounts & Marketing Manager en Serval Networks, sintetizó la preocupación del cliente final sentenciando que “el cliente lo que quiere es dormir tranquilo y no salir en las noticias”, una frase que resume la esencia del compliance: evitar riesgos, evitar titulares, evitar daños reputacionales.

LA COMPLEJIDAD DEL CUMPLIMIENTO

La conversación avanzó hacia la complejidad creciente del compliance. Ramón García, Socio Director en TUYÚ Technology, explicó que cada cliente interpreta la normativa de forma distinta, incluso dentro del mismo

> EL CLIENTE FINAL YA NO ESTÁ BUSCANDO UNA AUDITORÍA NADA MÁS, SINO UN CUMPLIMIENTO CONTINUO

ALEJANDRO AGUDELO
Director Global de Operaciones en **A3Sec**

sector. “En algunas compañías manda más la parte legal, en otras la tecnológica, en otras la de negocio”, señaló. Esa diversidad obliga a los MSP a navegar entre prioridades, intereses y niveles de conocimiento muy dispares, lo que complica la estandarización del servicio.

La irrupción de la inteligencia artificial añadió un nuevo nivel de incertidumbre. Ramón García fue contundente al afirmar que “tenemos demasiada normativa. Ya llegamos a un punto en que no nos dejan trabajar, no nos dejan crear. Ya lo crea la inteligencia artificial”. Para él, la regulación está avanzando más rápido que la capacidad de adaptación de las empresas, y la IA está introduciendo riesgos que muchos clientes no comprenden.

A este respecto, Jesús Valverde introdujo un aviso importante, y es que por mucho que confiemos en la IA, la responsabilidad legal sigue siendo humana. “Si damos por bueno un resultado de una IA que no esté adecuadamente entrenada, la

> ESTAMOS HIPERREGULADOS, Y MÁS EN ESTE MOMENTO

JOSÉ ANTONIO DÍAZ
Director de
Digitel TS by MADISON

responsabilidad es nuestra”, recordó.

Valverde puso un ejemplo claro: el SBOM (lista de materiales de software), que será obligatorio con la Ley de Ciberresiliencia (CRA), que muchos clientes desconocen. Para él, el MSP debe actuar como guía, advirtiendo al cliente cuando se acerca “demasiado al precipicio”.

Elvira García insistió en que la madurez desigual del mercado condiciona cualquier intento de estandarización. “Cuando intentas montar un servicio gestionado tienes que

ver qué procesos pueden asumir y cuáles no”, explicó. Sectores como el financiero, impulsados por DORA, están muy avanzados, mientras que NIS2 abre el abanico a verticales mucho menos preparados, lo que obliga a los MSP a adaptar su oferta a cada caso.

DEL PROYECTO PUNTUAL AL CUMPLIMIENTO CONTINUO

Uno de los puntos centrales del debate fue la transición del cumplimiento puntual al modelo continuo. Alejandro Agudelo destacó que las empresas empiezan a entender

> TODAVÍA HAY COMPAÑÍAS QUE NO SE HAN ENTERADO DE QUE HAY NORMATIVAS COMO GDPR, QUE LLEVA 10 AÑOS

JESÚS VALVERDE,
CISO de **MR Informática**

que el cumplimiento no es un hito, sino un proceso permanente. “Voy a tener un modelo continuo donde siempre tenga evidencias y pueda controlar esto”, afirmó. Y añadió que la automatización será clave, porque “las personas que vienen no van a querer hacer trabajo manual”.

Sobre si las empresas buscan solo la certificación o entienden que esta es la consecuencia de ser compliance, Óscar Vierge fue tajante, apuntando que “hay verticales que están años luz. Algunas grandes cuentas ni siquiera saben si les aplica NIS2”. Y añadió que el verdadero factor disuasorio no son las multas, sino la reputación: “Es mucho más caro el daño reputacional que la multa”, recalcó.

A este respecto, Elvira García introdujo un matiz relevante al señalar que muchas organizaciones buscan primero el sello porque lo necesitan para operar, aunque no tengan aún una cultura de cumplimiento. “Hay entidades que quieren la certificación y contra eso no podemos hacer nada”, reconoció.

> EL CLIENTE LO QUE QUIERE ES DORMIR TRANQUILO Y NO SALIR EN LAS NOTICIAS

ÓSCAR VIERGE
Sales Director Strategic Accounts & Marketing Manager en **Serval Networks**

Pero también señaló que cada vez más empresas buscan adecuarse a la regulación sin necesidad de un sello, lo que abre la puerta a modelos de servicio más estables y recurrentes.

Jesús Valverde defendió que muchas compañías deben empezar externalizando incluso el rol del CISO, pero evolucionar hacia perfiles internos senior que marquen criterio. “No pueden estar absolutamente en manos del proveedor”, advirtió. Para él, el equilibrio entre externalización y capacidad interna es clave para garantizar un cumplimiento sostenible.

HACIA UN MODELO RECURRENTE Y APOYADO EN EL ECOSISTEMA

El debate dedicó un espacio relevante a analizar si el compliance puede consolidarse como un servicio recurrente dentro del porfolio MSP. La mayoría coincidió en que el mercado se está moviendo en esa dirección, aunque todavía existe una brecha importante entre la

> EL COMPLIANCE NO SOLO ES CUMPLIMIENTO LEGAL, ES PONER ORDEN Y ES GESTIÓN

ELVIRA GARCÍA
Information Security Director en **Nunsys**

> EN ALGUNAS COMPAÑÍAS MANDA MÁS LA PARTE LEGAL, EN OTRAS LA PARTE TECNOLÓGICA Y EN OTRAS LA PARTE DE NEGOCIO

RAMÓN GARCÍA
Socio Director en **TUYÚ Technology**

« Clica en la imagen para ver la galería completa »

necesidad real de las empresas y su nivel de madurez.

Óscar Vierge apuntó que, desde la perspectiva del proveedor, “el compliance es una palanca de negocio siempre que se mida bien el servicio y se garantice la estabilidad de la plataforma del cliente”. Sin embargo, también reconoció que no todos los MSP pueden asumir internamente un servicio de cumplimiento completo, lo que obliga a apoyarse en terceros especializados.

En este contexto, Julia Gil, Channel Account Executive en DataGuard, explicó que el modelo Compliance as a Service ya es una realidad para muchas organizaciones que necesitan apoyo continuo, no solo consultoría puntual. “Nuestra propuesta es traer compliance as a service y explicar los riesgos en el mismo lenguaje que el cliente”, señaló. Su intervención puso de relieve que el fabricante especializado se convierte en un aliado estratégico del MSP, aportando metodología, herramientas y un marco de cumplimiento que el partner puede integrar en su oferta.

A esta visión se sumó Víctor Orive, CEO de ADM Cloud & Services, quien introdujo el papel del mayorista en este nuevo escenario. Desde su posición, explicó que el mayorista ya no puede limitarse a distribuir tecnología, sino que debe convertirse en un agente activo que acompañe al MSP en la implantación de modelos de cumplimiento. “El mayorista tiene que aportar estructura, conocimiento y capacidad de acompañamiento real. No basta con entregar producto; hay que ayudar al partner a aterrizar la tecnología y a garantizar que cumple con lo que exige la normativa”, afirmó.

Clica en la imagen para ver la galería completa

EL GRAN DESAFÍO Y LA GRAN OPORTUNIDAD DE LA PYME

Una parte central del encuentro se centró en la pyme, el segmento más vulnerable y, al mismo tiempo, el que más volumen representa para los MSP. Víctor Orive recalcó

> TODA ESTA NORMATIVA OBLIGA, INDEPENDIENTEMENTE DEL TAMAÑO

VÍCTOR ORIVE,
CEO de **ADM Cloud & Services**

que “la experiencia con la pyme es una lucha continua. Todo se basa en la confianza”.

Para Orive, el coste proporcional del cumplimiento es mucho mayor que en las grandes compañías, lo que obliga a los MSP a diseñar modelos más ajustados y escalables. “Si la pyme está obligada por estar en la cadena, el partner también lo está, y nosotros como mayorista tenemos la responsabilidad de darle las herramientas, la formación y el respaldo que necesita para cumplir”, aseguró.

Óscar Vierge añadió que muchas pymes están paralizando proyectos porque creen que la IA resolverá el cumplimiento “dentro de un año”. Y advirtió que esa expectativa es irreal y peligrosa, porque retrasa decisiones críticas.

Elvira García defendió que, para la pyme, el modelo ideal es que el MSP incluya todo. “A la pyme sí le puedes dar el paquete entero”, aseguró y añadió que la cadena de suministro está obligando a muchas pequeñas empresas a ser compliance porque sus clientes se lo exigen. Para ella, el compliance no es solo cumplimiento legal, sino “poner orden y gestión”.

Óscar Vierge coincidió en que la oportunidad es enorme si se libera a la pyme de la carga mental del cumplimiento. “En el momento en que le quites el marrón de pensar en auditorías, la oportunidad de negocio es exponencial”, sentenció.

UN FUTURO MARCADO POR EL OPTIMISMO Y LA EXIGENCIA

El cierre del encuentro dejó una mezcla de optimismo, prudencia y una sensación compartida de que el sector MSP está entrando en una nueva etapa donde el cumplimiento será un eje estratégico, no un añadido. Alejandro Agudelo se mostró convencido de que los servicios de compliance y privacidad serán fundamentales en los próximos años, ya que “los riesgos se están incrementando y el ambiente les da ese impulso necesario”.

José Antonio Díaz adoptó un tono más realista al recordar que el cumplimiento no es opcional. “Tenemos que cumplir sí o sí. Otra cosa es que el mercado lo valore”, destacó. Su reflexión apuntó a un reto clave para los MSP, el de convertir una obligación en una propuesta de valor clara, diferenciada y rentable. La regulación seguirá endureciéndose, pero el cliente no siempre está dispuesto a pagar por algo que percibe como un coste y no como una inversión.

Desde una perspectiva más pragmática, Óscar Vierge recordó que el reto no es solo técnico, sino

> NUESTRA PROPUESTA PARA LOS MSP ES PODER TRAER COMPLIANCE AS A SERVICE

JULIA GIL
Channel Account Executive en **DataGuard**

comercial. Según él, “ofrecemos un servicio para que otros cumplan. Monetizarlo es otra cosa”. Su intervención puso sobre la mesa que el compliance es necesario, pero requiere inversión, especialización y un modelo de servicio que permita escalar sin disparar los costes internos. No todos los MSP podrán asumirlo solos, y ahí entra en juego el apoyo de terceros.

Por su parte, Elvira García aseguró que “el cliente te lo empieza a demandar. Y ahí está el negocio”. Para ella, el futuro pasa por integrar el cumplimiento en la oferta de forma natural, como un servicio transversal que acompaña a cualquier proyecto tecnológico. ■

Clica en la imagen para ver la galería completa

MÁS INFO +

» Privacidad y compliance como oportunidad de negocio para el canal

COMPARTIR EN REDES SOCIALES

RESPONDIENDO A LOS RETOS DEL SECTOR

JULIA GIL, DATAGUARD

“Proporcionamos a los MSP un negocio recurrente alrededor de la privacidad”

Julia Gil, Channel Account Executive en DataGuard, destacó que, tal y como quedó claro en esta cita de la Comunidad IT, “uno de los principales retos a los que se enfrentan los MSP es adecuarse a la exigencia y el nivel de cada uno de los clientes, y la complejidad de adaptar estos servicios a las necesidades específicas que tiene cada uno de estos clientes”.

Esta dificultad, lejos de reducirse, “se amplifica con la llegada de la inteligencia artificial, y es fundamental hacer explicar a los clientes que las certificaciones necesarias no son una causa de la complejidad de las soluciones, sino todo lo contrario, es la consecuencia de aplicar los correspondientes niveles de privacidad que existen en las organizaciones”.

Por este motivo, “nuestra propuesta para los MSP pasa por ayudarles ofreciendo Compliance as a Service, poniendo a su disposición las herramientas necesarias para generar un negocio recurrente alrededor de la privacidad y la seguridad. Para ello, contamos con una plataforma que les ayuda a explicar los riesgos en un lenguaje que los clientes puedan entender. Además, les ofrecemos auditorías externas y profesionales especializados para ayudarles a la hora de proporcionar el servicio a sus clientes”.

Tus clientes creen que cumplen.

Ayúdales a demostrarlo.

ADM Cloud & Services

DataGuard

Con DataGuard, los MSP pueden convertir privacidad y cumplimiento en servicios gestionados de alto valor.

De la obligación al servicio gestionado

Privacy-as-a-Service | Compliance-as-a-Service

Descubre cómo incorporar DataGuard