DEBATES ciberseguridad TIC

Seguridad del dato más IA: hacia una protección real, automatizada y transversal

VARONIS

IR A PÁGINA SIGUIENTE

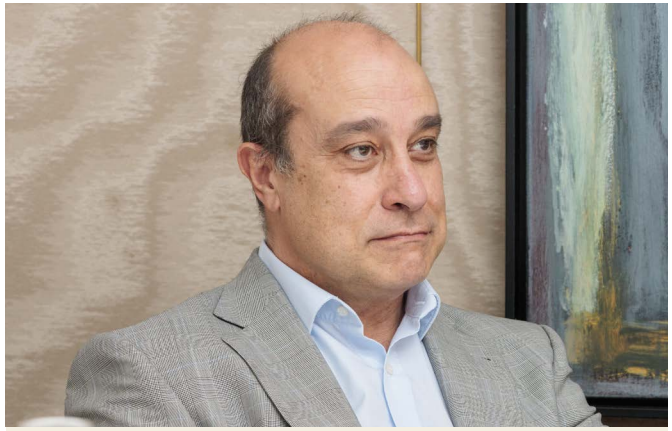
VARONIS

Seguridad del dato más IA: hacia una protección real, automatizada y transversal

En un momento de transformación acelerada, donde los datos se mueven a través de nubes híbridas, entornos colaborativos y modelos de trabajo distribuidos, la protección de la información crítica se ha convertido en una de las prioridades estratégicas de cualquier organización. Frente a un escenario de riesgos crecientes, ataques sofisticados y entornos desbordados de información, herramientas tradicionales como los DLP o los cortafuegos resultan insuficientes si no se cuenta con una estrategia centrada en el dato.

Rosalía Arroyo

Varonis, compañía especializada en seguridad del dato y protección de identidades, lleva cerca de 20 años desarrollando una plataforma que proporciona visibilidad, control y automatización sobre los datos sensibles, independientemente de dónde se encuentren o quién los use. Su enfoque, que ha cobrado aún



“El dato sensible no es sólo el personal; es aquel que realmente impacta en la organización”

Francisco Javier Santos, CISO Corporativo, **Santalucía**

más relevancia con el auge del trabajo remoto, la nube y la inteligencia artificial generativa, responde a una necesidad creciente: proteger el activo más valioso y vulnerable de las empresas: la información.

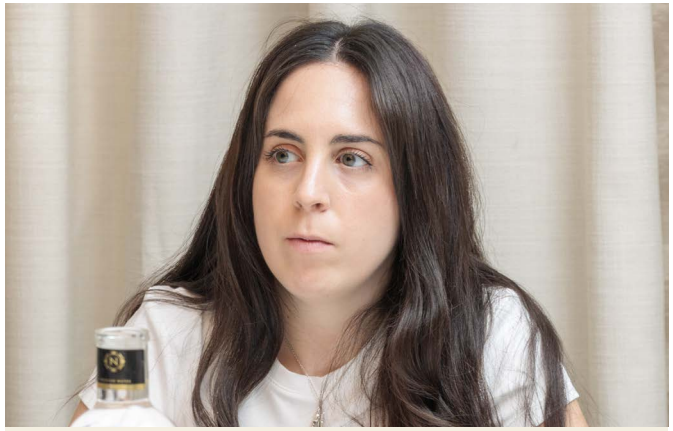
Con esta premisa como punto de partida, se celebró el almuerzo-debate “Seguridad del dato más IA: El escudo que tu empresa necesita”, organizado por Ciberseguridad TIC con el patrocinio de Varonis. El encuentro reunió a responsables de ciberseguridad de distintas organizaciones, que compartieron de forma abierta sus preocupaciones, estrategias y experiencias prácticas.

Muchas organizaciones aún no saben con certeza qué datos sensibles tienen ni quién accede a ellos

Saber dónde están los datos... ¿de verdad?

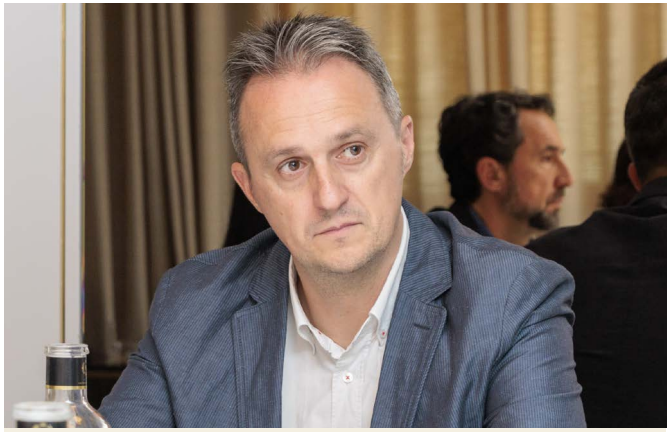
Una de las primeras preguntas planteadas fue directa: ¿Sabemos qué datos sensibles tenemos, dónde están y quién accede a ellos? La mayoría de los asistentes coincidió en que la visibilidad es razonable, pero no absoluta.

Desde Santalucía, Francisco Javier Santos, su CISO Corporativo, apostó por una aproximación centrada en las “joyas de la corona”: “El dato sensible es aquel que realmente impacta en la organización. El personal lo es por regulación, pero también lo es la información crítica de negocio, y esa no siempre está claramente etiquetada”, explicaba.



“Hay que ofrecer una herramienta segura para compartir información hacia fuera, o el usuario buscará su propio atajo”

Sara Soleto, **Women4Cybwer Spain,**



"Aunque tengamos clasificación y etiquetas, cuando el dato empieza a moverse y transformarse, podemos perder la trazabilidad "

Jesús Alonso,
CISO, **Línea Directa Aseguradora**

Juan Miguel Gil, IT Manager Spain Holding, señaló que "cada unidad del grupo es responsable de gestionar sus datos sensibles", dentro de unos principios comunes como la minimización de exposición o el modelo de confianza cero. Sara Soleto, experta en ciberseguridad y socia de Women4Cyber Spain, que asistió al evento como experta en ciberseguridad, remarcó la dificultad de mantener el control en entornos colaborativos como Microsoft 365: "Lo más importante es que lo que se comparta esté previamente etiquetado y controlado, y revisar los accesos de forma periódica".

Etiquetado y clasificación: entre la esperanza y la cautela

Uno de los temas que generó más debate fue el de los proyectos de etiquetado y clasificación de datos. Aunque todos coinciden en su importancia teórica, muchos dudan de su eficacia en la práctica si se basan en la intervención humana.

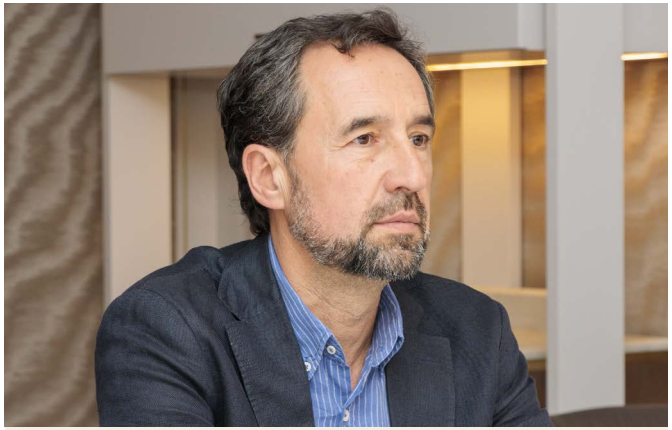
"Personalmente, soy escéptico con los proyectos de etiquetado", reconocía Francisco Javier Santos. "No siempre podemos confiar en que el usuario actúe correctamente. Por eso prefiero asumir que todo lo que entra en un proceso crítico es sensible, y a partir de ahí aplicar controles". Julián Domínguez, Iberia Sales Manager de Varonis, coincidía y aseguraba que si no se puede confiar en las etiquetas ni en la clasificación, "no puedes aplicar políticas eficaces. Y eso sucede más a menudo de lo que parece".

Proteger el dato exige mirar más allá del dato aislado y centrarse en la información que generan sus relaciones

Desde Varonis, Mónica Banegas, enterprise sales engineer de la compañía, destacaba otro reto: "En cuanto cambias de plataforma, las etiquetas pierden validez. Salesforce, Google, Microsoft... cada uno tiene su propio sistema. Por eso es clave unificar la protección del dato, sin depender del etiquetado manual".

Seguridad sin frenar el negocio

Uno de los dilemas más recurrentes fue cómo reducir la exposición de datos sensibles sin afectar a la productividad. "Lo ideal sería que un sistema automático analice y clasifique los ficheros según su contenido", señaló Sara Soleto. "Mu-



> “Cada unidad es responsable de sus datos, pero necesitamos principios comunes para minimizar riesgos”
>
> **Juan Miguel Gil,**
> IT Manager Spain Holding **ArcelorMittal**

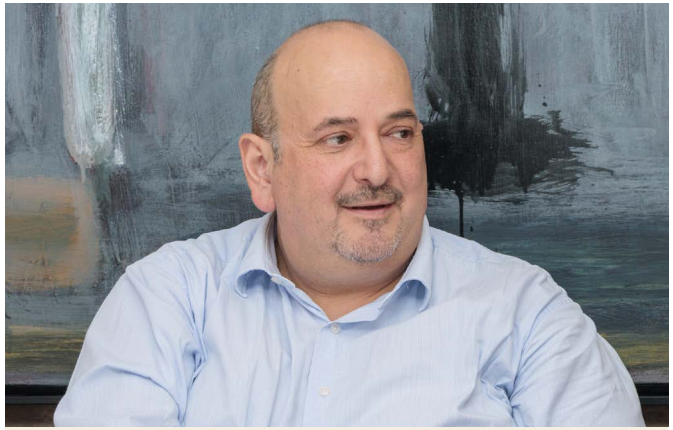
chas veces el usuario lo etiqueta como ‘interno’ sin pensarlo demasiado. Y a la hora de compartir fuera, debemos facilitar herramientas seguras”.

Desde Varonis, Domínguez reforzó esta idea comentando que se trata de ayudar, “no de castigar. Si un usuario intenta compartir algo sensible y se lo bloqueamos con una alerta, probablemente no vuelva a hacerlo. La tecnología debe servir de guía”.

De proteger datos a proteger información

A lo largo de la conversación surgió una idea clave que va más allá del enfoque técnico: el verdadero valor —y riesgo— no siempre reside en un dato aislado, sino en la información que se genera al relacionar varios datos entre sí. Como explicó Francisco Javier Santos, “lo que realmente nos preocupa es la información, no el dato aislado”, ya que “un conjunto de datos aparentemente inocuos puede derivar en información altamente confidencial”. Esta perspectiva obliga a replantear los sistemas de clasificación y protección, que no siempre tienen en cuenta el contexto ni la interpretación de los datos combinados.

Mark Wilcox, vicepresidente de Varonis para el sur de Europa, lo ilustró con claridad: “El dato está creciendo de forma exponencial. Aparece en nuevos repositorios constantemente. Y hoy, muchas veces, son los propios empleados quienes comparten sin ser plenamente conscientes del riesgo”.



> “Si no puedes confiar en las etiquetas ni en la clasificación, no puedes aplicar controles eficaces”
>
> **Julián Domínguez,**
> Iberia Sales Manager, **Varonis**

La carta a los Reyes Magos: automatización, integración real y control sin fricciones

En la parte final del encuentro, los participantes

> “Llevamos más de 20 años centrados en la protección del dato, antes incluso de que existiera una categoría para ello”

Mónica Banegas,
Enterprise Sales Engineer, **Varonis**

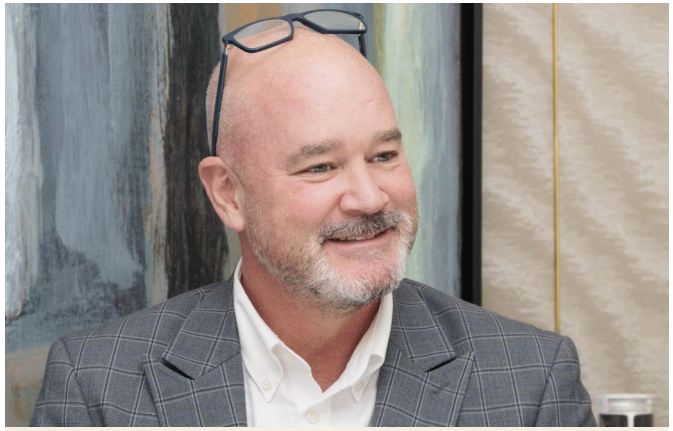
compartieron de forma más personal sus deseos y prioridades en materia de protección del dato, bajo el formato simbólico de una “carta a los Reyes Magos”. Las respuestas evidenciaron una coincidencia clara en las prioridades, aunque con matices según la experiencia de cada organización.

Jesús Alonso, CISO de Línea Directa Aseguradora, puso el foco en la automatización inteligente: “Aunque hay funcionalidades de automatización, no es sencillo hacerlo bien. Mi petición sería que, al menos, todo lo que de verdad es importante para la organización —las famosas joyas de la corona— pueda localizarse, controlarse y protegerse sin intervención manual constante”.

Francisco Javier Santos, CISO Corporativo de Santalucía, fue más allá, pidiendo una integración real y estándares compartidos entre tecnologías:

“Uno de los grandes problemas es que tenemos multitud de tecnologías para cada cosa. Mi ilusión sería que se estandarizara la forma en que se generan alertas y que esas fuentes se pudieran correlacionar fácilmente, sea con Varonis o con otra herramienta”.

Juan Miguel Gil, IT Manager Spain Holding de ArcelorMittal, complementó esta visión con una petición muy concreta: implicar más y mejor a los usuarios.



> “Llevamos más de 20 años centrados en la protección del dato, antes incluso de que existiera una categoría para ello”

Mark Wilcox,
VP South Europe, **Varonis**

“No se trata solo de tener la integración técnica. También hace falta que los usuarios se involucren y que entiendan que proteger la información es parte de su responsabilidad”.

Sara Soleto, especialista en seguridad, por su

parte, pidió más madurez en dos frentes: el control del dato compartido al exterior y la trazabilidad interna.

"Necesitamos saber qué se está compartiendo, cómo y con quién. Pero también poder trazar internamente qué ha pasado con ciertos datos. Porque siempre puede haber un insider o un fallo que explote una vulnerabilidad".

Desde la visión de fabricante, Julián Domínguez, Iberia Sales Manager de Varonis, recogió todas esas demandas con un enfoque práctico: "Con millones de archivos, miles de usuarios y decenas de repositorios, el control manual es imposible. Hay que empezar protegiendo al menos lo más crítico y crecer desde ahí. También hay que unificar el plano operativo, para que lo que defines en una política pueda aplicarse por igual en Salesforce, en Office 365 o en on-prem".

Mónica Banegas, Enterprise Sales Engineer de Varonis, cerró la ronda reivindicando la trayectoria de Varonis: "Llevamos más de 20 años protegiendo el dato, cuando aún ni siquiera existía una categoría para ello en los analistas. Ahora somos líderes en Gartner, Forrester o GigaOm. Pero no basta con saber dónde está el dato: hay que aplicar automatización, reducir el riesgo en tiempo real y proteger también la identidad, porque es la puerta al dato".

> El etiquetado manual no basta: automatizar la protección del dato es clave en entornos colaborativos

La visión de Varonis: visibilidad, automatización y vigilancia continua

Wilcox cerró el debate recordando los tres pilares que sustentan la protección eficaz del dato:

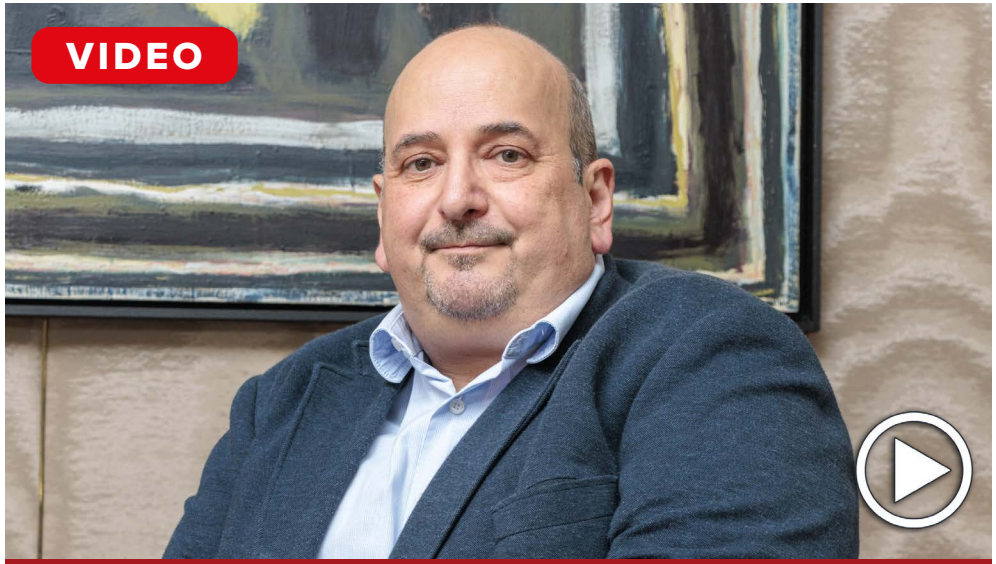
1. **Visibilidad total:** "Dónde está el dato, quién tiene acceso, y quién lo utiliza".
2. **Priorización del riesgo y automatización:** "Detectar riesgos y aplicar medidas automáticamente, por ejemplo, eliminando enlaces públicos tras un periodo definido".
3. **Monitorización continua:** "Establecer patrones normales de uso y detectar comportamientos anómalos, como una cuenta de servicio que de repente empieza a cifrar archivos".

También insistió en que sin confianza en la clasificación ni en las etiquetas, no es posible desplegar medidas de protección fiables: "Todo debe comenzar por la visibilidad real del dato y por clasificaciones que podamos verificar".

Mónica Banegas añadió una perspectiva clave: "Hoy ya no basta con saber dónde está la información. Tenemos que poder protegerla, minimizar el riesgo en tiempo real y vigilar también quién accede, cómo y desde qué identidad. Porque la identidad es ahora la verdadera puerta de entrada".

Y cerró con una invitación práctica: "Llevamos más de 20 años centrados en el dato. Ofrecemos análisis de riesgo gratuitos que os muestran, con datos y contexto, dónde está la información más crítica y cómo se está utilizando. Es nuestra forma de demostrar valor, más allá de las palabras". CST

“La sobreexposición de información es un problema muy difícil de resolver”



Julián Domínguez, Iberia Sales Manager, **Varonis**

Julián Domínguez, Iberia Sales Manager de Varonis, advierte que la sobreexposición de datos es un reto creciente por el aumento masivo de información derivado de la transformación digital y las herramientas de colaboración. “Esto crea una complejidad que además genera mucha sobreexposición de información. Y esto es un problema muy difícil de resolver”, afirma. Varonis lleva 20 años ayudando a las empresas a proteger sus datos allí donde estén, minimizando el riesgo sin afectar la continuidad del negocio. Su propuesta se basa en identificar los datos sensibles, relacionarlos con los permisos de acceso y la actividad de los usuarios para detectar riesgos y amenazas en tiempo real. Además, destaca su capacidad para descubrir información sensible mal ubicada: “Varonis ayuda a identificar esa información fuera de los repositorios, poniéndola otra vez de manera segura automáticamente”.

“Proteger el dato debe abordarse antes, durante y después de implementar inteligencia artificial”

Mónica Banegas, Enterprise Sales Engineer de Varonis, subraya que la madurez en la gestión del dato varía mucho entre organizaciones, según su cultura tecnológica y ritmo de adopción. Lo común es que todas busquen avanzar sin comprometer la seguridad. En este contexto, la inteligencia artificial plantea nuevos retos: “Lo que antes podía ser un posible riesgo, ahora la inteligencia artificial hace que sea un riesgo real”. Por eso, insiste en proteger los datos antes y durante su uso con IA, monitorizando qué hacen las herramientas generativas con la información. Varonis, explica, se adapta a estas exigencias ampliando su cobertura cloud y ofreciendo soluciones en formato SaaS. Destaca el servicio MDD de protección del dato en tiempo real, con un SLA de solo 30 minutos ante ataques de ransomware. “Vamos adaptando las nuevas tecnologías para que nuestro producto ayude a las empresas a proteger los datos”, concluye.

Mónica Banegas, Enterprise Sales Engineer, **Varonis**