DEBATES ciberseguridad TIC

El DLP entra en una nueva etapa: menos control, más contexto

Symantec by Broadcom

IR A PÁGINA SIGUIENTE

Symantec by Broadcom

El DLP entra en una nueva etapa: menos control, más contexto

Durante años, el Data Loss Prevention (DLP) ha sido una tecnología presente en muchas organizaciones, pero no siempre bien entendida ni correctamente aplicada. Nació para evitar que la información sensible saliera por canales previsibles en un momento en el que el dato todavía tenía un perímetro claro. Pero ese escenario ha cambiado. El cloud, el SaaS, la colaboración y, más recientemente, la inteligencia artificial, han multiplicado los puntos de fuga y han hecho que el dato ya no sólo se mueva, sino que se transforme y se reutilice constantemente. A esto se suma una mayor presión regulatoria y el impacto reputacional de cualquier incidente.

Rosalía Arroyo

En este contexto, el DLP deja de ser una herramienta puntual para convertirse en una pieza clave dentro de la estrategia de seguridad del dato. Ya no hablamos de evitar salidas, sino de entender cómo se usa la información y en qué contexto.

Con este punto de partida, el almuerzo ejecutivo organizado por Ciberseguridad TIC con el patrocinio de Symantec reunió a responsables de tecnología y ciberseguridad para analizar cómo están evolucionando estas estrategias en las organizaciones.

El punto de partida del debate dejó claro que el problema de la fuga de datos ha cambiado de naturaleza: no hablamos únicamente de identificar un canal concreto —SaaS, cloud o correo—, sino de asumir que el dato llevaba tiempo circulando fuera del control tradicional de la organización.

Jesús Alonso, Head of EMEA Cybersecurity de Bridgestone, fue uno de los primeros en poner palabras a esa sensación. A su juicio, uno de los principales riesgos es asumir que parte del dato ya puede estar circulando fuera del control tradicional de la organización. Las empresas están protegiendo el entorno corporativo, sin embargo, sobre todo en el ámbito de la IA generativa existe una brecha complicada de gestionar, y es que "proteges el entorno corporativo, pero no el entorno personal".

Manuel Asenjo, CIO & CISO de Écija Abogados, llevó esa reflexión al terreno de la operativa diaria asegurando que el reto no está únicamente en evitar grandes fugas, sino en gestionar pequeños movimientos aparentemente legítimos que no generan alertas y que, sin embargo, pueden implicar la salida del activo más crítico.

"Si intentas proteger todo con el mismo nivel de control, acabas haciendo la vida imposible al usuario; la clave está en identificar qué es realmente crítico y proteger eso de verdad"

Jesús Alonso,
Head of EMEA Cybersecurity, **Bridgestone**

Ahí afloró uno de los grandes puntos de fricción del DLP actual: la clasificación del dato. Más allá de patrones evidentes —como los datos financieros—, el valor de la información depende del contexto. El problema, resumió, es que en la operativa diaria no siempre se dedica el tiempo necesario a enriquecer la información con metadatos o a clasificarla correctamente. Incluso en entornos avanzados, el etiquetado y la gestión del dato siguen siendo procesos poco escalables.

A partir de ahí, apuntó a una posible evolución: que fuera la propia IA la que entendiera el contenido y la relevancia de los documentos en su contexto, distinguiendo lo crítico de lo accesorio sin depender del usuario.

Durante su intervención, Jacinto Muñoz, CISO para Iberia de Mapfre, añadió una lectura más estructural al vincular el problema no solo con la tecnología, sino con su adopción. A su juicio, el riesgo nace de la combinación de dos factores: tecnologías inmaduras y usuarios inmaduros. Es

> “El problema no es solo proteger lo que sale, sino entender cómo se comparte la información con terceros en un entorno donde no siempre puedes imponer tus reglas”

Manuel Asenjo,
CIO & CISO, **Écija Abogados**

decir, capacidades que llegan al mercado sin mecanismos de protección plenamente desarrollados y organizaciones que las adoptan con rapidez sin entender del todo sus implicaciones. “Las funcionalidades van por delante de las capacidades para protegerlas”, resumió.

El riesgo también está en lo legítimo

Avanzaba el debate para poner sobre la mesa un matiz importante. El riesgo no sólo reside en la salida del dato, sino en la forma en que se gestiona su uso en entornos cada vez más abiertos y colaborativos.

Elena Ruiz, Head of GRC de Moeve, situó ahí uno de los grandes puntos de tensión: el equilibrio entre seguridad y operativa. En su caso, explicó, el trabajo había comenzado revisando cómo interactuaban los empleados con la información y hasta qué punto las medidas de protección estaban integradas desde el propio origen del dato. Reconoció que las políticas demasiado restrictivas acababan generando fricción, lo que lleva a la necesidad de encontrar un punto intermedio, combinando herramientas, monitorización y casos de uso más acotados.

Dentro de ese escenario, identificó un frente especialmente complejo: la colaboración con terceros, porque las políticas propias convivían —y a veces chocaban— con las del partner.

A partir de ahí, la conversación derivó hacia una reflexión más de fondo sobre cómo se estaba abordando el problema. Javier Santos, CISO de Santalucía, sostuvo que la industria seguía repitiendo patrones históricos. “Seguimos desplegando tecnología sin tener en cuenta la seguridad”, afirmó, trazando un paralelismo con los inicios de internet. En su opinión, el fallo es más conceptual que tecnológico: se sigue intentando proteger el dato como si fuera un activo físico, cuando en realidad su naturaleza es dinámica y distribuida.

Esa visión le llevó a cuestionar incluso el enfoque tradicional del DLP. El dato, dijo, “sale, es inevitable”, por lo que el foco debería desplazarse desde la protección del dato en sí hacia el control de su uso. Sólo cuando se identificaba con claridad la “joya de la corona” —los datos realmente críticos— resulta posible aplicar medidas eficaces.

Mario Encinas, Cybersecurity Manager de Parques Reunidos, reforzó la idea de que la seguridad suele ir por detrás de la adopción tecno-

lógica y recordó cómo los canales de fuga han ido cambiando —del correo a las plataformas colaborativas y, ahora, a la IA— mientras las organizaciones intentaban adaptarse.

El reto, por tanto, ya no consiste únicamente en proteger el dato en determinados puntos, sino en asumir que se mueve constantemente entre organizaciones, usuarios y tecnologías, y que el verdadero desafío se encuentra en entender su contexto y gobernar su uso en tiempo real.

Del control puntual a la estrategia

La intervención de Jorge Chamizo, New Models Pre Sales de Symantec, supuso un punto de inflexión, porque introdujo una visión más estructurada sobre un problema que hasta ese momento se había descrito.

Chamizo partió de una sensación compartida en la mesa: muchas organizaciones están intentando contener el problema "poniendo vallas al campo". A partir de ahí, planteó dos caminos posibles. Por un lado, el enfoque reactivo —limitar, bloquear, controlar—. Por otro, un planteamiento más estratégico orientado a reducir la superficie de exposición desde el diseño, especialmente en un momento en que las integraciones con IA y APIs se han multiplicado. Ahí introdujo un matiz relevante: el problema es que muchas de esas integraciones se estaban planteando desde una lógica puramente tecnológica, sin conexión real con los procesos de negocio.

> "No puedes aplicar la misma estrategia a todo; necesitas entender cada caso de uso y avanzar de forma gradual para que la protección sea realmente efectiva"
>
> **Elena Ruiz,**
> Head of GRC, **Moeve**

De ahí enlazó con Zero Trust, no como una tecnología concreta, sino como un enfoque arquitectónico orientado a evitar que determinadas fugas vuelvan a producirse. En ese marco, describió un modelo en el que el control se sitúa en el propio flujo del dato: interceptar y analizar en tiempo real comunicaciones —desde APIs que alimentan modelos de IA hasta correo, tráfico web o transferencia de ficheros— para tomar decisiones en función del contenido y del contexto.

Eso sí, dejó claro que ese tipo de estrategias no son inmediatas. Exigían descubrimiento previo de la información, alineación con los procesos de negocio y despliegues progresivos para no generar fricción. En otras palabras, el DLP deja de ser una herramienta que se activa y pasa a convertirse en un proceso que se construye.

En esa misma línea, defendió recuperar el sentido original de esta tecnología: "no orientada a la tecnología, sino a los procesos de negocio".

Bajo ese enfoque, el valor no sólo reside en bloquear o alertar, sino en ofrecer capacidades adaptativas —como el autoetiquetado o la correlación con comportamientos— que permitan gestionar también aquellas fugas que hoy pasan desapercibidas.

Sergio Martos, Regional Sales Manager de Symantec, sumó entonces una idea más directa: la necesidad de priorizar. Frente a la tesis, repetida durante el debate, de que cierta exposición del dato es inevitable, puso el acento en que no toda la información tiene el mismo impacto. “Hay documentación crítica que no puedes permitir que se filtre”, advirtió, subrayando el riesgo reputacional y operativo asociado a determinados datos.

Su intervención reforzó uno de los consensos que ya empezaban a aflorar: en un entorno donde el dato está en constante movimiento, el objetivo no puede ser controlarlo todo, sino identificar qué es realmente crítico y aplicar ahí un nivel de protección mucho más preciso y eficaz. En esa capacidad de discriminar, contextualizar y actuar en consecuencia es donde, según defendieron desde Symantec, el DLP encontraba hoy su verdadero valor.

Lo difícil no es ver el dato, sino entender la información

A partir de ahí, el debate profundizó en una idea que ya había aparecido varias veces, pero que aquí se formuló de manera más explícita: el reto ya no consiste tanto en identificar datos sensibles como en entender la información en contexto —quién la usa para qué y cómo se mueve—, algo que desborda las capacidades tradicionales de las herramientas.

Javier Santos lo expresó con rotundidad: “el dato no es el problema, el problema es la información”. La distinción no es menor. El dato, por sí solo, carece de valor o riesgo; lo adquiere según cómo se combina, quién lo utiliza y en qué momento. De ahí su crítica a estrategias centradas en proteger “ladrillos” aislados sin comprender el flujo completo.

Desde su experiencia, el verdadero desafío está en mapear esos flujos: saber dónde reside la información crítica, cómo circula y qué contexto le da valor. Es un ejercicio complejo y, en muchos casos, difícil de abarcar a gran escala. Por eso advirtió que, cuando no se entiende ese contexto, las organizaciones tienden a sobrerregular: “intento proteger todo… y al final protejo menos de lo que pienso”. Solo cuando se identifican claramente las “joyas de

> “El dato en sí no es el problema; el problema es la información, el contexto en el que se usa y cómo se combina, y eso es mucho más difícil de controlar”

Javier Santos, CISO, **Santalucía**

la corona" tiene sentido aplicar controles más estrictos.

Mario Encinas coincidió en ese diagnóstico, pero lo llevó al terreno operativo. La clave, en su opinión, esté en clasificar la información y hacer partícipe al usuario. Recordó que el valor del dato no siempre es evidente de forma aislada, porque puede emerger al combinarse con otros. De ahí su insistencia en la concienciación: "la seguridad de la información afecta a toda la compañía". Al mismo tiempo, reconoció una realidad práctica: confiar en que el usuario etiquetara correctamente no es suficiente.

Ese equilibrio entre estrategia, tecnología y usuario quedó bien reflejado en la intervención de Elena Ruiz. En el caso de Moeve, la protección del dato se aborda como un marco global, más allá del DLP, integrando controles de acceso, colaboración, infraestructura y gobierno del dato. "La protección del dato va mucho más allá", explicó al describir cómo han definido distintos escenarios —usuarios, herramientas— y construido una estrategia progresiva.

Uno de los aspectos clave es evitar despliegues masivos sin contexto. Han optado por avanzar

> "La seguridad tiene que estar desde el minuto uno en cualquier iniciativa, porque si no, el problema crece más rápido de lo que puedes controlarlo"
>
> **Jacinto Muñoz,** CISO Iberia, **Mapfre**

de forma gradual con un objetivo claro: reducir fricción y evitar ruido. "Si aplicamos todo a todos no funciona", admitió, en referencia a los falsos positivos de enfoques indiscriminados.

Desde una perspectiva más clásica, Jacinto Muñoz introdujo un punto de realismo operativo. Aunque mapear todos los flujos resulta extremadamente complejo, las organizaciones sí suelen tener identificadas sus "Puntos sensibles", es decir, los datos más críticos. Ahí es donde se concentra el esfuerzo: control de accesos, trazabilidad, monitorización y aplicación de principios básicos como el mínimo privilegio y la "necesidad de conocer".

Cuando el problema no es un ataque

Muchas fugas no tienen nada de sofisticado, sino que nacen de decisiones cotidianas que, en un entorno cada vez más complejo, terminan generando riesgos difíciles de prever.

Jesús Alonso ponía sobre la mesa de los grandes problemas del DLP: su complejidad operativa. "Al final pones un montón de etiquetas... y se hace inmanejable", resumió. "Si empiezas a poner controles de verdad, haces la vida imposible al usuario", comentó, defendiendo una simplificación del enfoque: "tender a ser binario... qué información es sensible de verdad y cuál no". A partir de ahí, proteger de verdad lo crítico.

Javier Santos introdujo entonces una reflexión más incómoda sobre el papel de la seguridad. Frente al discurso habitual, sostuvo que, cuando se trata de proteger lo importante, “la seguridad tiene que ser intrusiva”. Es decir, hay que restringir, limitar y asumir que no todo podía ser transparente para el usuario.

La realidad operativa seguía introduciendo fricciones. Manuel Asenjo puso sobre la mesa un escenario muy común: la relación con terceros. “Yo hablo con todo el mundo y todo el mundo me manda información”, explicó, dejando claro que no siempre es viable imponer un único modelo de intercambio de información.

La conversación se desplazó después hacia cómo aterrizar todo lo anterior en una propuesta concreta, y ahí Jorge Chamizo introdujo una de las ideas más estructuradas del debate: el DLP no debe abordarse como una pieza aislada, sino como parte de una estrategia global de seguridad.

Partió de una premisa clara: “no creo que haya que afrontarlo como una única cosa”. En su opinión, el punto de partida no es la herramienta, sino el entendimiento del negocio. Propuso

> “El éxito del DLP no es solo bloquear, sino definir con precisión los patrones de uso legítimo del negocio; solo así protegemos los activos críticos en tiempo real sin generar ruido ni fricción operativa”
>
> **Mario Encinas,**
> Cybersecurity Manager, **Parques Reunidos**

construir el modelo desde los orígenes del dato y su relación con la organización, incorporando elementos como terceros, cadena de suministro y estructura interna. A partir de ahí, lo relevante no es tanto identificar datos como definir “flujos de información”.

Ese enfoque permite avanzar hacia un modelo mucho más granular. No se trata de aplicar políticas genéricas, sino de adaptar los controles al contexto real de uso. Introdujo una de las claves de madurez del DLP: cuando está bien implementado, “no hace ruido”. Pero llegar a ese punto exige un trabajo previo considerable: descubrimiento, clasificación, definición de flujos y uso de automatización —incluida la IA— para correlacionar información y reducir la carga operativa.

Sergio Martos aportó un ángulo distinto, más ligado a la evolución del mercado. Lo hizo, además, con una afirmación deliberadamente provocadora: “el DLP va a ser una condición *sine qua non* para operar”. En su visión, la presión no vendrá sólo de la necesidad técnica, sino del propio ecosistema: proveedores, partners y cadenas de valor en las que la protección del dato terminará siendo un requisito para participar.

Eso dibujaba un escenario en el que el DLP

dejará de ser opcional para convertirse en una capa más dentro de un modelo de seguridad cada vez más complejo, impulsado además por la expansión de la IA generativa.

Qué diferencia a Symantec

La última parte permitió, por fin, aterrizar una cuestión que hasta entonces había quedado más difusa: qué diferenciaba realmente la propuesta de Symantec frente a otras soluciones de DLP.

Jorge Chamizo respondió conectando con una idea ya muy presente en la mesa: no todos los DLP son iguales porque no todos cubren el mismo alcance. Según explicó, en comparativas reales de uso —no solo teóricas— "se cubren más casos de uso con Symantec que con cualquier otro". La razón principal está en su capacidad de operar de forma homogénea en entornos híbridos: "cubrimos toda la parte on-premise también", algo que no todos los fabricantes mantienen con el mismo nivel de profundidad en un contexto cada vez más volcado al cloud.

El segundo punto clave se sitúa en la tecnología de clasificación y detección. Chamizo recordó el legado de Vontu —uno de los orígenes del DLP moderno— y una capacidad que, a su juicio, sigue marcando diferencias: "no detecta palabras clave... detecta patrones". El matiz es importante, porque permite ir más allá de los enfoques basados en diccionarios o reglas estáticas, especialmente en entornos con información no estructurada. Bajo esa lógica, el sistema puede interpretar documentos complejos —financieros, propiedad intelectual o incluso archivos multimedia— desde su contexto, no sólo desde su contenido literal.

> "El DLP no puede plantearse como una herramienta aislada, sino como parte de una estrategia global donde lo importante es entender los flujos de información"
>
> **Jorge Chamizo,**
> New Models Pre Sales, **Symantec**

También introdujo un elemento especialmente relevante en el contexto regulatorio actual: el análisis basado en metadatos. "Trabajamos con metadatos y eventos de seguridad que no incluyen información confidencial", explicó. Eso permite analizar el comportamiento del dato sin necesidad de exponerlo, algo especialmente sensible en marcos como DORA, donde la gobernanza del dato y su tratamiento seguro son críticos incluso dentro de los propios sistemas de seguridad.

Sergio Martos reforzó la propuesta desde una perspectiva más estratégica. Subrayó el peso de la inversión en innovación —"un 25% del revenue destinado a I+D"— como elemento que explica la evolución del producto en los últimos

años. En su visión, el DLP ya no es una herramienta estática, sino un componente en transformación continua dentro de un ecosistema más amplio de seguridad.

Symantec, en definitiva, situó su DLP no tanto como una herramienta aislada, sino como una pieza central dentro de una arquitectura más amplia de seguridad del dato, alineada con la complejidad real que las organizaciones habían ido describiendo a lo largo de la conversación.

Priorizar sin perder de vista el conjunto

El último bloque funcionó casi como un cierre conceptual, porque obligó a los participantes a priorizar en un escenario en el que todo parecía importante.

Javier Santos volvió a trazar una línea muy clara desde el inicio: antes de hablar de herramientas o automatización, hay que entender qué preocupa realmente a la organización, insistiendo una vez más en la diferencia entre dato e información, y en la necesidad de comprender el contexto.

Mencionó durante su intervención Mario Encinas la importancia de entender los procesos de negocio como punto de partida. “Lo importante es que me describas qué es para ti algo legítimo”, explicó. Solo así se pueden diferenciar comportamientos normales de acciones sospechosas y, sobre todo, reducir el ruido.

Elena Ruiz adoptó una posición más pragmática. Reconoció que resulta difícil priorizar una única línea en un entorno tan complejo y apostó por avanzar de forma acotada: “empezar por pocos servicios y de manera controlada”. Su enfoque volvió a poner el acento en los casos de uso y en la necesidad de construir una estrategia global, donde distintas medidas —no solo el DLP— se combinen para dar una respuesta coherente.

Para Jacinto Muñoz, la clave está en el “entendimiento mutuo” entre negocio y seguridad. Es decir, no sólo en formar a los usuarios, sino también en que los equipos de seguridad entiendan qué se quiere hacer y por qué. Su planteamiento fue claro: la seguridad debe integrarse desde el inicio. “O estás desde el minuto uno… o es probable que ya llegues demasiado tarde”. De ahí que defienda participar en las iniciativas desde su concepción como parte del equipo y no como un control externo.

> “No todos los DLP son iguales, y la diferencia está en la capacidad de evolucionar, adaptarse al negocio y aportar valor real más allá de la tecnología”

Sergio Martos,
Regional Sales Manager, **Symantec**

Manuel Asenjo reforzó esa idea desde una visión integradora: no se trata de elegir entre visibilidad, clasificación o automatización, sino de

combinarlas dentro de un enfoque transversal; “hay que tener un plan que englobe todo”.

Por último, Jesús Alonso recuperó un enfoque más táctico, pero útil en fases iniciales. Propuso priorizar un awareness no restrictivo: “que sepas que te estoy viendo”. Es decir, generar visibilidad sobre el uso del dato sin bloquear de entrada, algo que podía ayudar especialmente en entornos como la IA, donde el comportamiento del usuario sigue siendo todavía incierto. Al mismo tiempo, apuntó a un reto que permance abierto: la protección de la información no estructurada, un ámbito donde muchas estrategias siguen sin cerrarse.

La seguridad no puede ir por verticales

El cierre del debate reforzó una idea que había ido apareciendo de forma recurrente: la protección del dato —y la seguridad en general— ya no puede abordarse por piezas aisladas.

Jorge Chamizo lo resumió de manera directa: “no se puede plantear la seguridad como verticales”. En su visión, uno de los principales errores sigue siendo gestionar cada capa —firewall, DLP, correo, endpoint— como un mundo independiente, cuando en la práctica un incidente araviesa todas ellas. Desde la identidad hasta la ejecución de acciones, pasando por red, endpoint o datos, todo formaba parte de una misma cadena. Por eso insistió en la necesidad de una estrategia unificada, donde las políticas no compitan entre sí, sino que respondan a una lógica común.

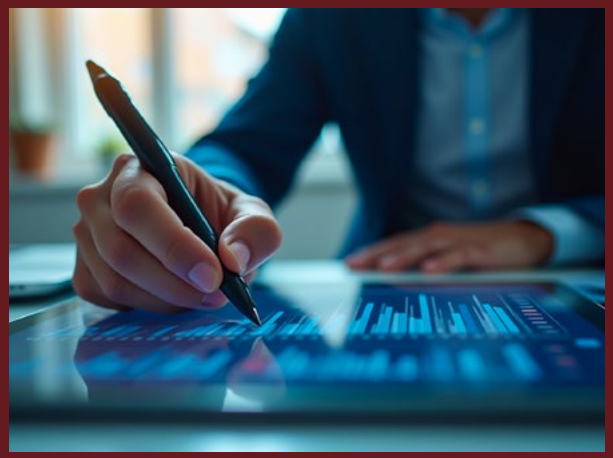
En ese planteamiento volvió a aparecer un elemento clave de todo el debate: el negocio. Chamizo subrayó que ninguna tecnología, por avanzada que fuera, puede sustituir el conocimiento real de cómo funciona la organización. “Hay cosas que no vas a poder entender porque la telemetría no te da ese contexto”.

Sergio Martos cerró con un mensaje más directo, alineado con el posicionamiento de mercado. Reafirmó que el DLP —entendido en sentido amplio— no es una opción, sino una necesidad creciente. En línea con lo que se había apuntado anteriormente, recordó que “no todos los DLP son iguales”, y situó a los grandes fabricantes como actores que no solo responden a necesidades, sino que también contribuyen a definirlas.

Symantec by Broadcom

DLP como estrategia: la propuesta de Symantec

La propuesta de Data Loss Prevention de Symantec se aleja del enfoque tradicional centrado en reglas estáticas y control de canales concretos para situarse dentro de una estrategia más amplia de protección del dato. Tal y como se puso de manifiesto durante el debate, el objetivo ya no es únicamente evitar la salida de información, sino entender cómo se utiliza, en qué contexto y con qué nivel de riesgo.



Uno de los pilares diferenciales de la aproximación de Symanrec es su capacidad para operar de forma homogénea en entornos híbridos, combinando protección en cloud, SaaS y entornos on-premise. Esto permite mantener una visión unificada del dato en escenarios donde la información ya no reside en un único perímetro.

A nivel tecnológico, Symantec incorpora capacidades avanzadas de clasificación y detección que van más allá de los enfoques tradicionales basados en palabras clave. Su tecnología —heredada del desarrollo original de Vontu— permite identificar patrones y contexto en información estructurada y no estructurada, lo que facilita la protección de documentos complejos como informes financieros, propiedad intelectual o contenidos multimedia.

Otro elemento clave es el uso de metadatos para analizar el comportamiento del dato sin necesidad de exponer la información sensible. Este enfoque resulta especialmente relevante en entornos regulados, donde la trazabilidad y la gobernanza del dato son críticas, y permite cumplir con marcos como DORA sin comprometer la confidencialidad.

Además, la propuesta evoluciona hacia modelos más integrados, en los que la protección del dato se incorpora a plataformas de detección y respuesta como XDR, permitiendo correlacionar contexto entre endpoint, red, identidad y uso de la información. Esta integración permite correlacionar eventos y entender el contexto completo en el que se mueve la información, alineándose con marcos como MITRE ATT&CK y facilitando una respuesta más precisa.

Desde el punto de vista operativo, Symantec pone el foco en la madurez del despliegue. Un DLP eficaz no es una herramienta que se activa, sino un proceso que requiere descubrimiento, definición de flujos y adaptación progresiva a los procesos de negocio. El objetivo final, como señalaban sus portavoces, es alcanzar un modelo en el que la protección del dato funcione de forma natural, con el mínimo impacto en la operativa y el máximo alineamiento con el negocio.