it TRENDS

#EncuentrosITTrends

Check Point SOFTWARE TECHNOLOGIES LTD · IaaS365 · elastic · MICRO FOCUS · VEEAM · PENTEO

Generando entornos de datos modernos, inteligentes y seguros

¿Cuál es el rol del CDO y el DPO?
¿Cómo de maduras están las estrategias data-driven?

#ENCUENTROSITTRENDS

Generando entornos de datos modernos, inteligentes y seguros

El mundo de los datos evoluciona constantemente porque cada vez juegan un papel más importante en las empresas. En base a ellos se toman decisiones, se mejora la experiencia de los clientes o se amplía la oferta con productos basados en datos, entre otros.

En ese viaje que hacen los datos desde su captura, procesamiento, visualización, análisis, almacenamiento, protección y recuperación, intervienen numerosas tecnologías que están a su vez evolucionando para reportar a las empresas los mejores resultados: desde la transformación y enriquecimiento de los centros de datos, la nube o el extremo de la red, donde se generan, acceden y almacenan los datos; hasta las técnicas de inteligencia artificial y machine learning que están potenciando su análisis o el business intelligence que soporta la toma de decisiones, pasando por todas las posibilidades que permiten acceder a los datos de una forma segura y recuperarlos para seguir funcionando en caso de pérdida.

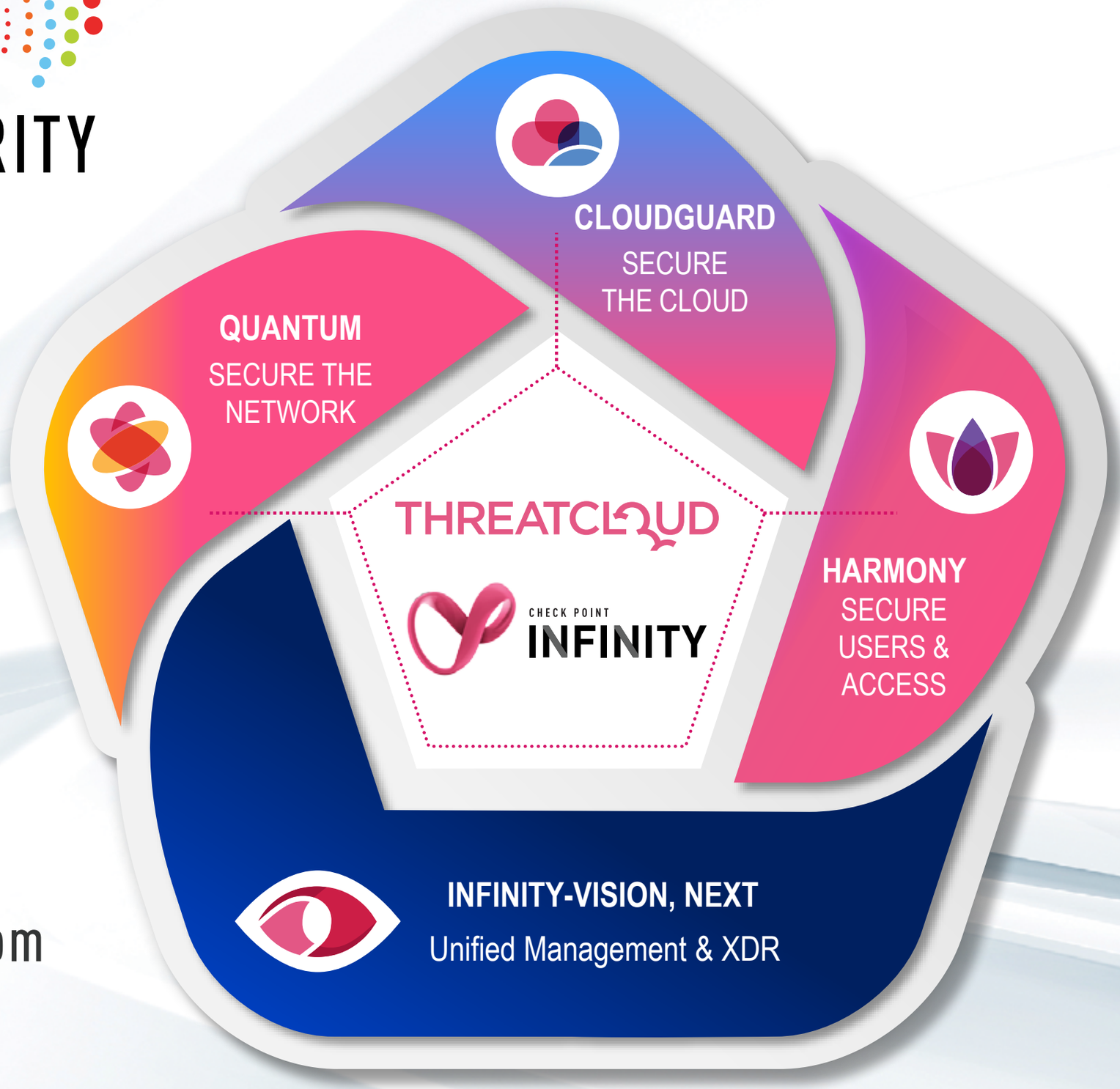
De todo esto hablaremos en este Encuentro IT Trends, donde además responderemos a preguntas como:

- ¿Qué necesita tener/saber una empresa que quiere explotar adecuadamente los datos? ¿por dónde empezar?
- ¿Cuál es el reto de proteger datos dispares y dispersos y a los que se accede desde cualquier parte y con cualquier dispositivo?
- ¿Qué mecanismos clave cree que deben introducir las organizaciones para proteger sus datos en todas las etapas?
- ¿Cómo desarrollar una arquitectura robusta de cumplimiento y pérdida de datos?
- ¿Qué pasos deben darse para convertirse en una empresa Data Driven?
- La visibilidad es un aspecto muy importante cuando se habla de seguridad, ¿lo es también cuando se gestionan o explotar los datos?

Puedes leer las principales conclusiones de este Encuentro IT Trends a continuación. ■

CHECK POINT™

YOU DESERVE THE BEST SECURITY



MÁS INFORMACIÓN:

www.checkpoint.com/es

info_iberia@checkpoint.com

ALEJANDRO MORALES, ANALISTA SENIOR, PENTEO

“Hace falta un Business o Data Translator, un perfil que sirva de puente entre negocio y ciencia de datos”

¿Cuál es la madurez de la empresa española en lo que se refiere a su estrategia de datos? Para responder a esta pregunta hablamos con Alejandro Morales, analista senior de Penteo, consultora independiente de TI.

Al apostar por la información, el gobierno y el rendimiento, la empresa española está buscando obtener un mayor reconocimiento, así como mejorar la calidad con la información que tiene. Explica Alejandro Morales, analista senior de Penteo durante su entrevista en el Encuentro IT Trends “Generando entornos de datos modernos, inteligentes y seguros”, que las empresas se han dado cuenta de que, con los grandes volúmenes de datos que se manejan, se requiere de un gobierno del dato, y que “donde están poniendo foco las empresas es en democratizar la información, romper los silos y tener un mayor autoservicio”.

El 95% de los CEOs considera que el dato es un activo estratégico, lo que lleva a pensar que ese mismo porcentaje tiene planes estratégicos en torno al dato, “pero en torno al 66% aún no lo ha hecho, o lo ha hecho y ha fracasado”, dice el analista de Penteo. ¿Por qué fracasan

“UNO DE LOS FOCOS DEL CDO ES HACER UNA ESTRATEGIA DATA DRIVEN”

DIAGNÓSTICO DE LAS ORGANIZACIONES ORIENTADAS AL DATO

¿Qué iniciativas alrededor de los datos están llevando a cabo las empresas en España? ¿Dónde se está invirtiéndo? ¿En qué proveedores y tecnologías? ¿Qué perfiles son los más demandados? Y el CDO, ¿qué hace en su día a día? Este informe resume las conclusiones de Penteo tras una encuesta realizada entre empresas españolas acerca de sus estrategias data-driven.

estos proyectos de estrategias de datos? Diferencia Alejandro Morales entre proyectos y expectativas. Habla el analista de una estrategia mal definida o escoger un caso de uso irrelevante como uno de los motivos que llevan al fracaso de una expectativa, al tiempo que asegura que "no se invierte como se debería de invertir y falta una figura que para mí es clave: el CDO". Sobre esto último asegura que no sólo se trata de nombrar un CDO, sino de nombrar una oficina del CDO "y dotarla de recursos".

En relación al tiempo que debería esperarse para tener resultados en una estrategia de datos, asegura Alejandro Morales que se empiezan a obtener resultados tangibles entre el primer y el tercer año, por lo que "hay que tener paciencia". En todo caso "la experiencia nos dice que, pasados esos tres años, si no has obtenido éxito, tus probabilidades de obtenerlos se reducen a un 18%, con lo cual es muy importante ir midiendo el avance cada seis meses".

¿Qué tipo de personal están buscando las empresas para acometer estos proyectos de datos? Responde el analista de Penteo que actualmente el 62% de las empresas están buscando perfiles en torno al dato, y que el 47% de las empresas que buscaban estos perfiles el año pasado no los encontraron. Explica además este directivo que donde se está poniendo foco ahora en el perfiles de Data Science (54%), Data Engineer (47%) y Business o Data Translator, un perfil que sirve de puente entre negocio y ciencia de datos.

Una figura que está cogiendo más fuerza es la del CDO, que tiene como objetivo "liderar y coordinar la estrategia y el gobierno del dato", explica Alejandro Morales, añadiendo que tiene que entender muy bien cuáles son las necesidades del negocio, así como las bases de datos, la arquitectura del dato, etc. "Uno de los focos del CDO es hacer una estrategia Data Driven", asegura también.

Respecto a las tecnologías que están dando soporte a estas estrategias de datos, menciona el analista de Penteo que cerca de un 26% utiliza Spark; respecto al almacenamiento prima el on premise, un 72% es SQL Server y se está viendo una migración hacia AzureMySQL. En cuanto al modelaje triunfa Python, en el consumo se utiliza más Power BI y en el Gobierno, Informatica.

A la hora de saber qué departamentos están haciendo mayor uso de los datos y, por lo tanto, aprovechando las estrategias Data Driven, comparte el analista de Penteo los datos de un estudio según el cual el 71% de las empresas recogen datos internos de la compañía, "lo que significa que hay bastante madurez". Por áreas de negocio, Gestión Comercial suele ser bastante madura con una recolección de datos interna y externa por encima del 60%. Y acostumbrado a tratar con datos desde hace muchísimo tiempo, el departamento de Operaciones fue de los primeros en tratar con estrategias Data Driven, mientras que Recursos Humanos "está a la cola y le falta mucho por mejorar". ■

elastic

PRESENTAMOS

Elastic Security for Cloud

Una nueva forma de gestionar el riesgo en la nube, y la protección necesaria de la carga de trabajo en la nube.

¿Quieres saber más?

TONI NAVAS PACHECO, CIO & CDXO, DORNA SPORTS

“El reto para ser una empresa Data Driven es más cultural que tecnológico”

El mundo de los datos evoluciona constantemente porque cada vez juegan un papel más importante en las empresas. En base a ellos se toman decisiones, se mejora la experiencia de los clientes o se amplía la oferta con productos basados en datos, entre otros.

Las habilidades humanas, que nos van a permitir una correcta comunicación, son algunas de las que debe tener un DPO. Lo dice durante su entrevista en el Encuentro IT Trends “Generando entornos de datos modernos, inteligentes y seguros”, Toni Navas Pacheco, CIO & CDxO de Dorna Sports. Añade otras, como las capacidades de gestión, “tan imprescindibles en el día a día y en el liderazgo actual”, así como conocimiento del negocio y, finalmente “experiencia en toda la cadena de modelos de captación de los de los datos, para convertirlos primero en información y posteriormente en conocimiento para la compañía, usando las tecnologías que cada uno crea convenientes para habilitar este modelo”.

Además de CIO y responsable de transformación digital, Toni Navas ejecuta el rol de

“EL RETO PARA SER UNA EMPRESA DATA DRIVEN ES MÁS CULTURAL QUE TECNOLÓGICO”

El desarrollo de innovación a través de asociaciones entre industrias debe basarse en una colaboración de datos coordinada, y muchas organizaciones no tienen esto en cuenta

CDO, que en muchas otras empresas está presente de manera directa. Comenta que, dentro del trabajo de un CISO, el 20% está relacionado con las tareas de CDO, al igual que el 80% de las tareas de transformación digital; en esos tiempos “tenemos embebida la responsabilidad del CDO como máximo responsable de los datos de la compañía, con lo cual yo creo que antes incluso de que existiera esta cultura Data Driven ya había realizado una apuesta por inculcar esta cultura del dato, la cultura de la toma de decisiones basada en datos, en información”. Nos cuenta también este directivo que, en el caso de Dorna Sports, la compañía lleva tres años trabajando la cultura Data Driven, instaurándola en todos los procesos de negocio.

¿Cuáles son los retos a la hora de conseguir una empresa Data Driven? “Es un reto absolutamente cultural, un reto organizativo”, responde Toni Navas, añadiendo que poco tiene que ver la tecnología y mucho la adopción Big Data o Inteligencia Artificial, que ya tienen que ser parte de los procesos de negocio. Menciona también el directivo de una necesaria colaboración entre negocio y tecnología “para trabajar y perseguir los objetivos de una manera conjunta”

La importancia, el valor de los datos, no sólo está generando figuras como el CDO. Nos cuenta Toni Navas que en Dorna Sports, donde se trabaja con metodologías Agile, se ha creado un grupo de trabajo al que se denomina Data and Analytics que da soporte a todas las unidades de la compañía, lo que pone de manifiesto que “el dato y la analítica tienen que estar presentes en todos los procesos de la compañía, ya sean procesos internos, procesos de negocio, ya sean procesos corporativos o procesos que tengan que ver con nuestros clientes”. El objetivo, añade Toni Navas, es que el dato esté implicado desde el principio hasta el final en toda la cadena de valor de la compañía.

Respecto a los elementos específicos que necesita utilizar un CDO, Tony Navas menciona el Data Lake, “ese repositorio común donde ingestamos diferentes tipos de datos en formato raw”, que Dorna Sports tiene en AWS. Se añade como necesario una herramienta de BI, o Business Intelligence, que en el caso de su compañía ha sido Power BI y está migrando a Google Data Studio “porque pensamos que, especialmente a nivel de performance, es una herramienta que tiene mucha más potencia”. ■

IaaS365

Uniendo Personas & Tecnología

La innovación TI aporta valor en cualquier aspecto de la sociedad.

Afrontamos los retos, inspiramos y creamos soluciones tecnológicas con el objetivo de ayudarte a afrontar tus desafíos digitales.

- #Cloud
- #Ciberseguridad
- #Proyectos de Infraestructura TI
- #Servicios Gestionados
- #Consultoría Tecnológica

www.iaas365.com

Síguenos

#ENCUENTROSITTRENDS

Generando entornos de datos modernos, inteligentes y seguros

En plena digitalización, el acceso y análisis de los datos ofrece a las empresas un enorme valor para entender mejor a sus clientes y tomar decisiones más adecuadas. Sin embargo, en este viaje hacia un enfoque impulsado por datos surgen algunos retos, que requieren de una aproximación experta.

Los datos son poder y esta máxima no pasa desapercibida para las empresas que, cada vez más, se afanan por recogerlos, entenderlos y utilizarlos en su propio beneficio. Sin embargo, explotarlos y protegerlos adecuadamente puede no ser tan sencillo, sobre todo ahora, cuando la información está repartida en distintos entornos a los que se accede desde diferentes dispositivos.

Fernando Calvo (IaaS365), Víctor Pérez de Mingo (Veeam Software), Eusebio Nieva (Check Point), Miguel Estévez (CyberRes, una unidad de negocio de Micro Focus) y María Campos (Elastic), abordan en este debate las mejores estrategias para diseñar entornos de datos seguros y modernos, acordes a las necesidades de las empresas. Clica en la imagen para ver el vídeo.

“Para que los datos sean realmente utilizables, deben cumplir tres parámetros: integridad, disponibilidad y confidencialidad”

MIGUEL ESTÉVEZ, INGENIERO DE VENTAS DE SEGURIDAD, CYBERRES

Entonces, ¿qué pasos debe dar una empresa para convertirse en Data Driven?

Para hablar sobre esta realidad y analizar otras cuestiones ligadas a la seguridad y al análisis de los datos, además de otros retos y tendencias que esta filosofía integra, nos acompañan en esta #Mesa Redonda, Fernando Calvo, Business Development Manager de IaaS365; Víctor Pérez de Mingo, Senior System Engineer de Veeam; María Campos, Regional Vice President Iberia & Italy de Elastic; Eusebio Nieva, Technical Director para España y Portugal de Check Point; y Miguel Estévez, Ingeniero de Ventas de Seguridad de CyberRes, a Micro Focus line of business. Especialistas en la materia, aportarán su visión y conocimiento sobre esta corriente que explotan cada vez más empresas.

ENTENDER EL DATO, PRIMER PASO

Una empresa Data Driven maneja un conocimiento y una información que le aseguran un gran valor a la hora de tomar decisiones. Sin embargo, el cambio hacia esta filosofía es parte de un proceso en el que elementos como la seguridad u otras tecnologías que faciliten su reutilización, juegan un papel clave. ¿Qué pasos debe dar una empresa para convertirse en Data Driven?

Para Eusebio Nieva, de Check Point, lo primero que tiene que hacer una organización que pretende adoptar un enfoque impulsado por datos es tener claro qué información quiere proteger, qué accesos va a permitir -y con qué condiciones- y cuál es la naturaleza y criticidad de dichos datos a fin de establecer los parámetros y las tecnologías necesarias para su seguridad “Este es el primer paso. Una vez ya se ha decidido qué usuarios pueden acceder a qué datos y que clasificación tienen cada uno de ellos, es el momento de implantar barreras para su protección”.

Desde la perspectiva de que las empresas tienden cada vez más hacia una arquitectura data driven, Fernando Calvo, de IaaS365, resalta la trascendencia de analizar los datos lo más cerca posible de dónde se producen -no centralizándolos como en el pasado- para tomar

“Unos datos completamente aislados, probablemente no sirvan para nada. Es crucial securizar el acceso de los usuarios a esos datos. Si los usuarios están protegidos, tendremos asegurada la seguridad de los datos”

EUSEBIO NIEVA, TECHNICAL DIRECTOR, CHECK POINT

decisiones más estratégicas gracias a su estudio inmediato. “Por la gran cantidad de datos que se obtienen de diferentes fuentes es importante analizarlos en tiempo real. Las empresas deben adaptar los servicios, recursos y datos y acercarlos al lugar donde se generan”.

Para ser una compañía impulsada por datos es fundamental distinguir que, estos, se sitúan en el centro de todo. “Estamos en un mundo híbrido -data first, data drive- en el que el dato debe estar siempre disponible”, asegura Víctor Pérez de Mingo, de Veeam. A partir de aquí se puede aplicar tecnología para asegurar esa disponibilidad e incluso reutilizar información para hacer data mining, análisis de riesgos, testing... sin riesgos para los datos y sin impactar en los sistemas de producción.

Llegados a este punto, no hay duda de que para convertirse en data driving es necesario hacer un uso eficiente de los datos, para lo que Miguel Estévez, de CyberRes, recomienda entender primero lo que significa este concepto, aplicable, según él, a cualquier negocio. “En la práctica, significa tomar decisiones basadas en el análisis y en la interpretación de los datos. Sin embargo, para que los datos sean utilizables, deben cumplir tres parámetros: integridad, disponibilidad y confidencialidad. Esa es la triada de la seguridad de los datos”.

La utilización de datos adquiere una singular magnitud por el valor añadido que aporta.

Por eso, María Campos, de Elastic, entiende que las empresas deben encontrar el modo de traducirlos y convertirlos en información procesable en tiempo real. Para ello, deben “localizarlos, centralizarlos -independientemente de su ubicación- y estructurarlos, para que los campos estén indexados y se puedan buscar. Con todo esto ya se pueden utilizar dashboards para visualizar datos críticos y poder analizarlos como parte del proceso de toma de decisiones”.

“Si un backup no es recuperable, no sirve para nada. Es valioso saber que cuando el dato sale del backup está limpio y se puede llevar a producción”

VÍCTOR PÉREZ DE MINGO, SENIOR SYSTEM ENGINEER, VEEAM

PROTEGER AL USUARIO...

El debate avanza con una serie de preguntas más específicas para entender cómo debe modelarse una estrategia data driving. En este punto, el usuario es un factor clave, y, sobre todo, conocer ¿qué papel juegan este y su identidad a la hora de proteger los datos?

La información es el activo principal. Por eso, Eusebio Nieva, juzga que, en cualquier empresa, la protección fundamental debe ser la de los datos, pero esa seguridad pasa obligatoriamente por resguardar a los usuarios: su identidad, dispositivo, localización... para que su acceso a la información sea seguro. “Unos datos completamente aislados que nadie puede ver, a los que nadie se puede aproximar, es probable que no sirvan para nada. Por dicho motivo, es crucial securizar el acceso de los usuarios a esos datos. Si los usuarios están protegidos, tendremos fortalecida la seguridad de los datos”.

Como en todo, el avance hacia un modelo as a service es imparable. Pero ¿qué beneficios suponen este tipo de soluciones en las estrategias de Modern Data Protection?

Según Fernando Calvo, Business Development Manager de IaaS365, estos son múltiples, al permitir a las empresas centrarse en sus negocios. “Los más relevantes son: el ahorro de costes de utilización, solo se paga por lo que se consume; el acceso desde cualquier lugar y momento; y la disponibilidad y la protección de los datos, basado todo en unos niveles de seguridad para cada entorno. Otras ventajas son su adaptabilidad a las necesidades de cada cliente, las actualizaciones automáticas de las plataformas, la fácil integración con otros ecosistemas y la garantía de la continuidad de negocio.

... Y, POR SUPUESTO, EL DATO

Y cuándo se trata de proteger los datos, ¿es posible centralizar esa protección para cualquier tipo de cargas de trabajo, ya sean físicas, cloud, SaaS, virtuales y de Kubernetes?

“El proveedor debe aportar conocimiento, más allá de la tecnología; ayudar en esa curva de aprendizaje y proporcionar el soporte estratégico para identificar el nivel de madurez y sugerir los próximos pasos para evolucionar”

MARÍA CAMPOS, REGIONAL VICE PRESIDENT IBERIA & ITALY, ELASTIC

Ciertamente es posible, y, de hecho, para Víctor Pérez de Mingo, es una necesidad. Vivimos en un mundo híbrido, donde hay que proteger todo tipo de cargas. Por ello, es imprescindible contar con una solución que sepa entender ese entorno; una única plataforma modular adaptable a cualquier entorno, con capacidad de centralización y que pueda mover las cargas de trabajo. “Antes hablábamos de data driven, de encajar el dato en el centro de todo. Ahora se trata de recuperar el backup de los datos en cualquier lugar. Y esto es algo muy sencillo que se puede realizar en cuatro pasos”.

Los datos están dispersos en diferentes ecosistemas, entonces, ¿cómo se pueden migrar los datos a la nube de forma segura?

Aunque la migración a la nube es un tema que a algunas empresas les atemoriza, porque pone en riesgo, cuanto menos, la confidencialidad de los datos, Miguel Estévez incide en lo trascendental que es asegurar el dato, ya que, en sí mismo, no suele estar protegido. “Nos preocupamos mucho de cifrar las comunicaciones, el soporte de los datos o el sistema de ficheros, pero no tanto de salvaguardar el dato que está en cloud. Es esencial protegerlo siempre, cifrarlo en sí mismo”.

Desde hace años se habla de lo valioso que es explotar los datos, pero ¿qué necesita saber una empresa que quiere hacer esto adecuadamente? ¿Por dónde hay que empezar?

Este proceso, María Campos, lo plantea como un viaje en el que se van recorriendo etapas, partiendo de una inicial de conocimiento de los datos, en la que se decide cuáles tendrán valor, para luego definir los casos de uso -que permitirán determinar los valores de acceso y auditoría- y concretar un presupuesto. “El proveedor más allá de la tecnología debe aportar el conocimiento, ayudar en ese aprendizaje, y proporcionar el soporte estratégico para ir

“Para una Modern Data Protection existen soluciones de continuidad de negocio que ofrecen un máximo rendimiento y accesibilidad a los datos siempre activa, además de tecnologías de disaster recovery con alto rendimiento y potencia y análisis predictivo”

FERNANDO CALVO, BUSINESS DEVELOPMENT MANAGER, IAAS365

identificando el nivel de madurez y sugerir los próximos pasos para seguir avanzando”.

SALVAGUARDAR EL DATO EN TODAS SUS ETAPAS

La protección del dato es una prioridad para las organizaciones, pero, para lograrla, es necesario delimitar los mecanismos más adecuados para salvaguardarlo en todas sus etapas.

Sobre estos mecanismos, Fernando Calvo, reconoce que, para preservar los datos, las empresas deben comprender los riesgos y recurrir a un proveedor especializado que les muestre estos peligros, y cómo administrarlos, reducirlos y, por supuesto, a securizar los datos. “Se trata de ayudarles a identificar, proteger, detectar, responder y, en caso de ser necesario, a recuperar los datos y sistemas en el mismo momento en el que estaban”.

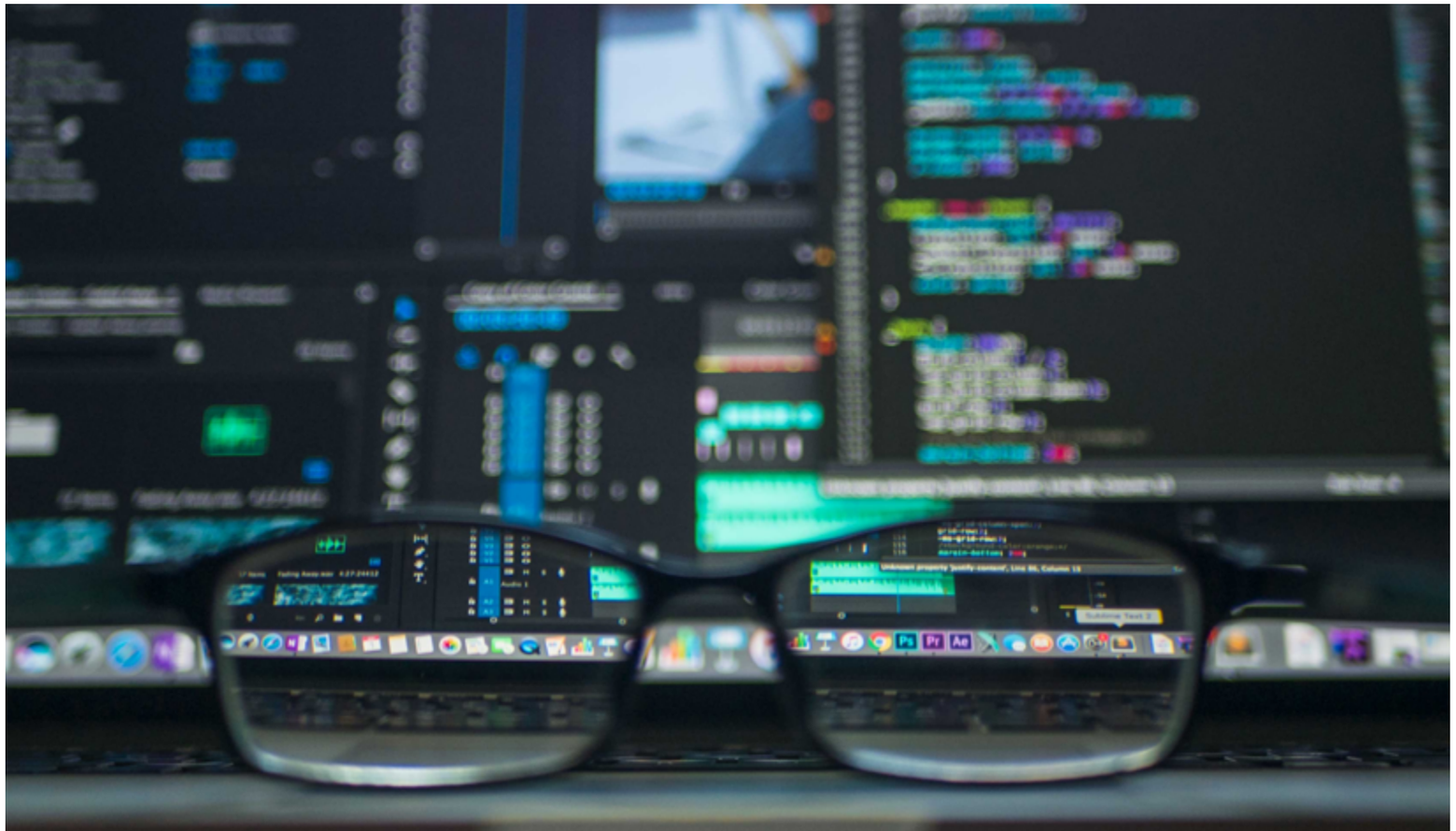
¿Y qué ocurre cuando el dato sale de producción? ¿Cómo es posible certificar su seguridad?

Víctor Pérez de Mingo recurre a la regla del 3-2-1-0 como medida para proteger el backup, tener un respaldo y certificar su recuperación. Basada en la conocida backup 3-2-1, esta pauta suma al hecho de contar con 3 copias de seguridad de los datos, 2 soportes de almacenamiento distintos y 1 copia fuera de las instalaciones, un cuarto elemento: 0 errores al recuperar. “Si un backup no es recuperable, no sirve para nada. Es valioso saber que cuando el dato sale del backup, este está limpio y se puede llevar a producción”.

Proteger el dato en todas sus etapas sí es posible. Y, para conseguirlo, Miguel Estévez incide de nuevo en la importancia del cifrar estos datos, para hacerlos ilegibles e inusables ante quien no esté autorizado. “Hay muchas formas de resguardar los datos, pero la más adecuada durante todas las etapas es cifrándolos en sí mismos. Con esto se va a garantizar su segu-

ridad, tanto cuando se encuentren en tránsito, en reposo, en un acceso no deseado o ante cualquier otra situación".

Como complemento y clave de protección en todas las etapas del dato, y de cara a identificar y abordar vulnerabilidades, María Campos apuesta por introducir plataformas que ofrezcan visibilidad sobre cualquier tipo de datos, permitiendo así descartar puntos ciegos. "Una capa de visibilidad que elimine esos puntos ciegos junto con otra de búsqueda agregará, sin duda, una importante capa de protección y seguridad para preservar el dato en todas las etapas".



Además de los pasos ya citados, que, entre otras, postulan la protección del dato y de sus copias de seguridad, Eusebio Nieva considera imprescindible securizar el acceso, ya que si quien está accediendo de manera maliciosa cuenta con los permisos necesarios, podrá descifrar ese dato. Por ello, la tecnología de seguridad tiene que pasar por la protección del dato, pero también del usuario, de sus dispositivos y de los accesos, estén donde estén. "Tenemos que ser capaces de aplicar una arquitectura de Zero Trust al dato. Una defensa en profundidad que sea capaz de eliminar las amenazas actuales que son muy avanzadas, multifases y que, además, denotan en muchos de los casos una gran profesionalidad de los atacantes".

NUEVAS ESTRATEGIAS

Las empresas se vuelven cada vez más dependientes de los datos, buscando además obtenerlos más rápidamente. Sin embargo, el hecho de que los datos corporativos se encuentren bajo diferentes formas, y cada vez más en la nube, puede complicar su protección. En este contexto, ¿qué funcionalidades de los entornos cloud definen y favorecen una estrategia de Modern Data Protection?

La nube no es un problema, se adapta a los distintos tipos de negocio. Frente al antiguo enfoque de protección de datos consistente en salvaguardar los sistemas en caso de fallo, Fernando Calvo explica que "para una protección de datos moderna y proactiva existen soluciones de continuidad de negocio que ofrecen un máximo rendimiento y accesibilidad siempre activa, además de tecnologías para disaster recovery con alto rendimiento, potencia y análisis predictivo para percibir los problemas antes de que ocurran".

¿Y cómo es posible afrontar una protección proactiva frente amenazas como el ransomware u otros ataques de última generación?

Para Víctor Pérez de Mingo, si esta pregunta se le hace a una empresa como la suya, especializada en proteger el backup, la respuesta

será muy clara: “tenemos la capacidad de detectar ataques, de saber cuándo el sistema ha sido infectado. En backup somos la última línea de defensa por lo que proporcionamos las herramientas para que después de ese ataque podamos garantizar que se van a recuperar todos los datos de forma rápida y sin tener que pagar un rescate o negociar con criminales”.

Pero para aplicar las medidas de protección para proteger el dato ¿es suficiente con anonimizarlos o hay que cifrarlos?

Entendiendo la anonimización como la eliminación de las posibilidades de identificar a una persona a partir de unos datos, Miguel Estévez afirma que, dentro de ese proceso, hay varias técnicas aceptadas por los principales marcos legales, aunque la dificultad radica en cómo ponerlas en práctica, pues existe un equilibrio muy ajustado entre la protección y la usabilidad, que puede conducir a una pérdida de valor para las operaciones basadas en datos. “En CyberRes utilizamos un algoritmo de cifrado con preservación de formato que permite mantener su longitud, los caracteres de la cadena cifrada, y que asegura su cifrado correcto para su posterior gestión y uso”.

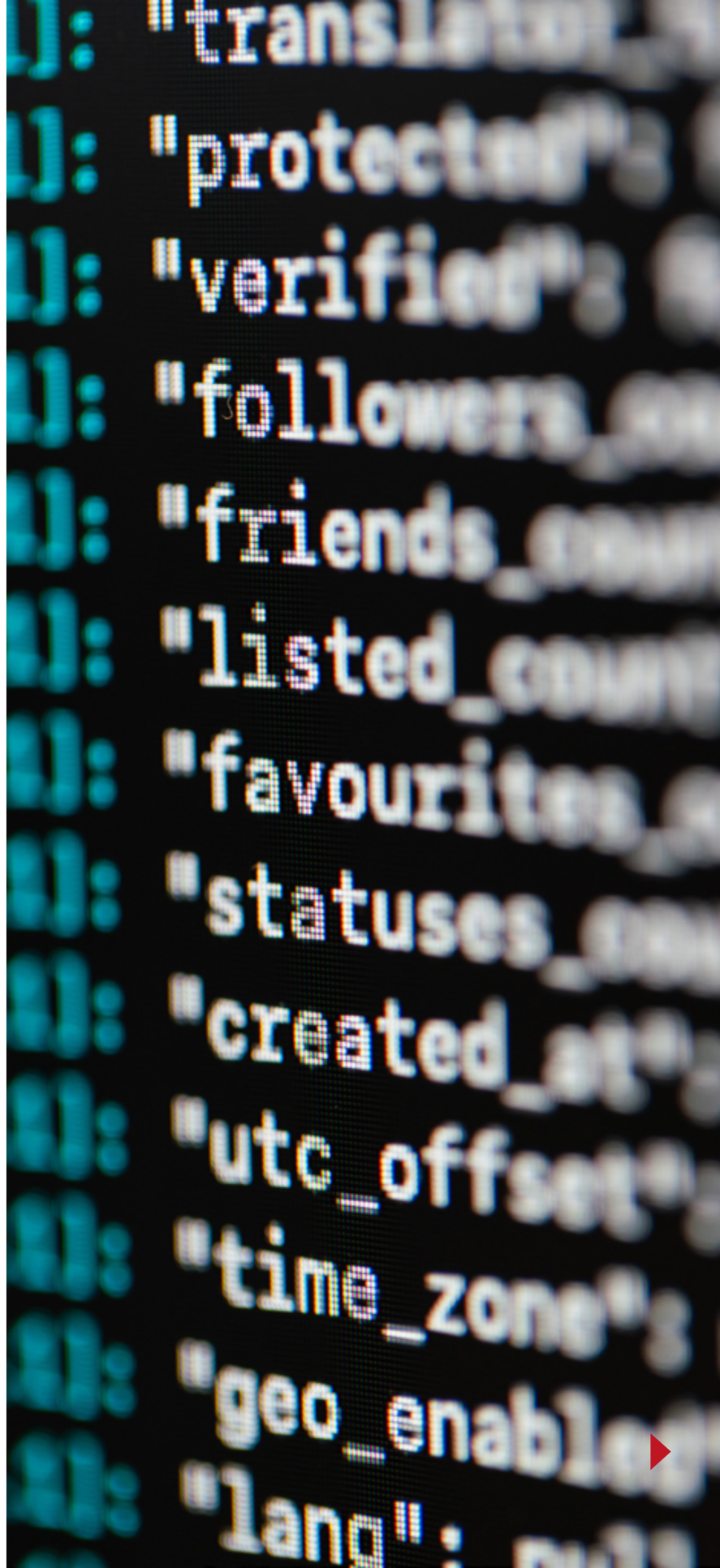
VER PARA PROTEGER

En seguridad se habla acerca de que lo que no se puede ver no se puede proteger. Sin embargo, la visibilidad va más allá de la seguridad, siendo crucial cuando se gestionan o explotan los datos.

A este respecto, María Campos refleja que introducir plataformas que ofrezcan visibilidad es un ‘must’, un elemento clave que trasciende a la seguridad, y que, en armonía con otras tecnologías, permite un mejor funcionamiento, además de ser un pilar de protección. “Dado que todo son flujos de datos, la visibilidad es clave. Por eso, hay cada vez una mayor convergencia entre las tecnologías de seguridad y de observabilidad. Está todo muy unificado; esa visibilidad y esa explotación del dato, y no solo en seguridad sino también en la gestión en sí de las aplicaciones”.

Visibilidad y seguridad ya caminan de la mano. Sin embargo, otras tendencias como Zero Trust o SASE están siendo también relevantes para proteger el dato.

Defensor de esta idea, Eusebio Nieva confirma que, “ambas tendencias están ofreciendo una mejor protección, permitiendo que podamos enfrentarnos con mejores armas a las amenazas de hoy”. En el caso de Zero Trust, el principio de no confiar en nada ni nadie por defecto, aplica perfectamente con la protección del dato y con ser una compañía data driven, mientras que con SASE se ha conseguido democratizar el acceso a las tecnologías y a los servicios de seguridad a los que antes solo podían acceder las grandes.



PROTECCIÓN, RECUPERACIÓN

Además de protegerlos, ¿cómo pueden las empresas asegurar que los datos y las aplicaciones sean seguros y recuperables en poco tiempo?

Para lograrlo, Víctor Pérez de Mingo explica que además de desplegar mecanismos que aseguren que ese dato es de verdad recuperable, hay que certificar que el dato recuperado no esté comprometido. "Con nuestra tecnología garantizamos que el dato sea recuperable y seguro, antes de llevarlo a producción". En cuanto al tema de la velocidad, Pérez de Mingo señala la importancia de conocer dónde se va a recuperar ese dato, on prem o en cloud, ya que no es lo mismo. "Lo bueno es que la flexibilidad de Veeam permite hacerlo en ambos entornos, sacando el máximo rendimiento del utilizado".

Desarrollar una robusta arquitectura de cumplimiento y de pérdida de datos es crucial para las empresas para fortalecer la seguridad y cumplir con la legislación. Para hacerlo, Fernando Calvo aconseja optar por una arquitectura as a service, que asegure los planes de continuidad de negocio, y disaster recovery para cada uno de los servicios, datos y/o aplicaciones. "Dicha solución debe asegurar que tanto RTO como RPO cuente con sus niveles de servicio garantizados; gestión de disponibilidad de BCM, BCP y DRP; orquestación de failover y de failback, y facilidad para la ejecución de tests periódicos. "Y todo en la modalidad de pago por uso, sin necesidad de inversiones adicionales".

Continuando con los mecanismos de protección más adecuados, surge la cuestión de si es conveniente cifrar los datos en origen o es suficiente con anonimizarlos a la hora de explotarlos.

Ante este asunto, Miguel Estévez explica que los datos pueden anonimizarse en origen, cifrándose y mostrándose tal cual en la aplicación al consumirlos o, por el contrario, en la propia aplicación. Así, y según él, aunque muchas veces se opta por el segundo enfoque, por miedo a cifrar los datos en origen o por considerarse más rápido este método, no es así: "hay que añadir un paso de cifrado cada vez que se quieren consumir y si los datos son sustraídos al no haber sido cifrados en origen, pueden ser leídos". Por tanto, y "aunque legalmente es suficiente con anonimizar los datos, es mejor cifrarlos en origen".

Por último, y aunque la analítica de datos se suele relacionar con una mejora del negocio o con una reducción de los tiempos de respuesta, su papel se aplica cada vez más a la seguridad, donde, según María Campos, se busca acortar los tiempos de respuesta, tanto el que el atacante pasa sin ser detectado en una red, como el de remediación al sufrir una brecha o el de respuesta. Por lo que, al final, todo se traduce en una cuestión de datos; en analizar lo más relevantes para proporcionar esa respuesta temprana. "Y aquí es donde la analítica datos, junto con el threat hunting y la detección y respuesta temprana con técnicas de machine learning, pueden mejorar la seguridad". ■

MÁS INFORMACIÓN

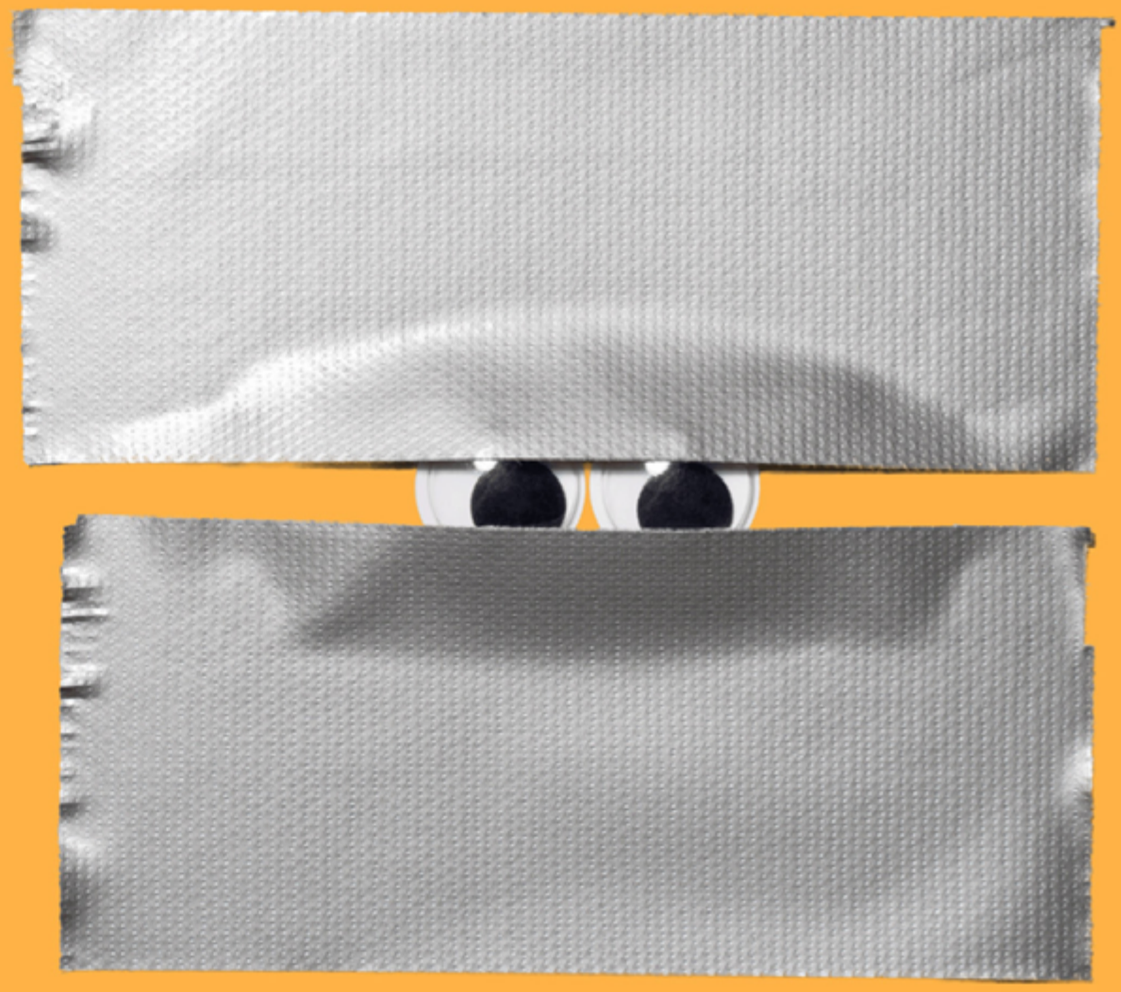
- Tendencias en privacidad de datos
- "Utilizamos el dato para crear salud", Antonio Herrero, Data & Analytics Director en Quirónsalud
- "El Big Data nos ayuda a adelantarnos a las necesidades de nuestros clientes", Alfonso Negrete, CDO de IKEA en España

CyberRes

La confidencialidad no se puede subestimar

La confidencialidad comienza con Data Discovery

Leer más

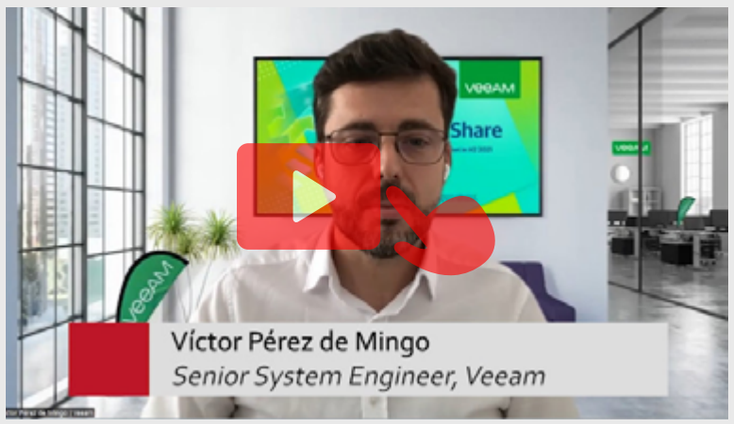


cyberres.com/voltage

Generando entornos de datos modernos, inteligentes y seguros: Propuestas Tecnológicas

“La protección de los usuarios es un medio para conseguir que los datos estén seguros”. Eusebio Nieva (Check Point)

“Ayudamos a nuestros clientes a ser empresas Data Driven”. Fernando Calvo (Iaas365)



“La apuesta de Veeam es proporcionar una protección de datos moderna”. Víctor Pérez de Mingo (Veeam)

“Elastic apuesta por maximizar el valor del dato”. María Campos (Elastic)

“No podemos proteger lo que no sabemos si existe ni dónde está” Miguel Estevez (CybeRes)

COVADONGA PÉREZ, DELEGADA DE PROTECCIÓN DE DATOS (DPD/DPO) Y PERITO JUDICIAL EN COMPLIANCE

“Un DPD no necesita herramientas, necesita formación continua”

A medida que los datos han ido cogiendo una mayor entidad en las organizaciones, se ha hecho necesario el rol de un encargado de proteger esos datos, el DPO.

La figura del DPO nace al amparo del Reglamento Europeo de Protección de Datos, y dentro de sus funciones está la de informar y asesorar para dar cumplimiento a esta normativa, explica Covadonga Pérez, Delegada de Protección de Datos (DPD/DPO) y Perito judicial en Compliance, en su entrevista en el Encuentro IT Trends “Generando entornos de datos modernos, inteligentes y seguros”. Añade que también son los encargados de cooperar con la autoridad de control, que es la Agencia Española de Protección de Datos, “ya que somos los que atendemos los derechos que afectan en esta normativa, como el derecho de acceso o rectificación”.

“Que las empresas entiendan que nosotros, como delegados de protección de datos, lo que hacemos es dar instrucciones, asesorar, para que la empresa cumpla con

“UN DPD NO NECESITA HERRAMIENTAS, NECESITA FORMACIÓN CONTINUA”

protección de datos y no se vulneren los derechos y libertades de los interesados" es uno de los grandes retos a los que se enfrentan los DPO, asegura Covadonga Pérez, añadiendo que existe la idea de que "somos nosotros los de debemos ejecutarlo. Y no es así. Es la empresa quien debe ejecutar esas esas directrices en materia de protección de datos".

Menciona también Covadonga Pérez que aún hay muchas empresas que no entienden que los datos son el activo más valioso que tiene cualquier empresa, que "una empresa sin datos no es nada", y que por eso hay que protegerlos adecuadamente.

"El usuario está más concienciado de que los datos son suyos y te los da para una finalidad, no para lo que tú quieras"

Desde que en 2018 se creara esta figura del DPO, lo que ha cambiado mucho "es la forma de afrontar los diferentes riesgos en la seguridad informática", sobre todo después de una pandemia que ha expandido las fronteras empresariales y ha planteado la necesidad de controlar los sistemas que están fuera.

Planteamos a Covadonga Pérez si, en general, se están tomando las medidas necesarias para proteger adecuadamente los datos de los usuarios. Asegura que cada vez hay más información y que el usuario está más concienciado "de que los datos con míos y te los doy para una finalidad, no para lo que tú quieras"; que los usuarios quieren que sus datos estén protegidos y conocen sus derechos en materia de protección de datos. Esto ha llevado a muchas empresas a que, aunque no estén obligadas por ley a tener designado un Delegado de Protección de Datos, opten por tenerlo voluntariamente "para estar seguros de que cumplen con protección de datos"

Preguntada por las herramientas que necesita en su día a día, responde Covadonga Pérez que un Delegado de Protección de Datos no necesita herramientas, sino formación continua, "estar especializado en el sector para el que se está prestando el servicio, que conozca las normas que indirecta o directamente entroncan con protección de datos". Insiste en que las funciones de un DPD son asesorar y velar porque los datos estén almacenados en un entorno seguro y que sean los necesarios para las finalizadas que se están persiguiendo, que estén anonimizados en el caso que así se requiera, etc.

A un DPD le afecta ciberseguridad, los derechos digitales, los protocolos de desconexión digital... que son temas "que no lleva el DPD como tal, pero debe conocer porque debe asesorar a su a su cliente empresa". ■

Modern Data Protection

Own, control, backup and recover your data anywhere in the hybrid cloud. Ensure business resilience, protect your data from malicious actors and eliminate data loss and downtime. Confidently move to the cloud, avoiding lock-in with cloud mobility.

Ransomware Protection

Cloud Acceleration

Backup Modernization

La documentación TIC, a un solo clic

Impacto económico de la plataforma de comunicaciones unificadas de Zoom

Las comunicaciones unificadas han cambiado radicalmente el funcionamiento del mundo de los negocios. Zoom Phone, como parte de la plataforma de Comunicaciones Unificadas como Servicio (UCaaS) de Zoom, sirve de impulso para el mundo empresarial actual, y lo prepara para el espacio de trabajo del futuro.

Tendencias tecnológicas digitales 2022

El estudio del mercado tecnológico realizado a lo largo de los últimos meses por ADVICE Strategic Consultants para ITDM Group, ha permitido identificar y definir cuáles serán las tendencias tecnológicas que dominarán este 2022.
Jorge Díaz-Cardiel, autor del estudio, lleva más de 32 años trabajando en el mercado TIC-Digital, dirigiendo las filiales de grandes multinacionales en nuestro país.

Cinco características de una plataforma de experiencia digital

Según Garnet, una plataforma de experiencia digital (DXP) es un conjunto de tecnologías bien integradas y cohesionadas diseñadas para permitir la composición, gestión, entrega y optimización de experiencias digitales contextualizadas a través de customer journeys de múltiples experiencias. ¿Qué tecnologías forman parte de este conjunto? ¿Por qué integrar el módulo de comercio electrónico en tu plataforma de gestión de información?

Empresas nativas digitales

Las Empresas Nativas Digitales son aquellas que han nacido y desarrollado sobre una premisa tecnológica ágil y flexible, y con el objetivo de poner la Experiencia de Usuario al frente de todo. Conocen a la perfección el entorno y el cliente, y han sido capaces de adelantar los cambios necesarios en la propia definición de su operativa, aplicando una visión y filosofía B2C a un entorno B2B.