ESPECIAL **NIS2**

NIS2. La cuenta atrás ha comenzado. ¿Está tu empresa preparada?

IR A PÁGINA SIGUIENTE

NIS2. La cuenta atrás ha comenzado. ¿Está tu empresa preparada?

Ciberataques que paralizan hospitales, fugas de datos masivas que ponen en riesgo nuestra privacidad... Las amenazas cibernéticas son cada vez más sofisticadas y frecuentes. Ante este panorama, la Unión Europea ha dado un paso adelante con la Directiva NIS2, una normativa que pretende blindar los sectores más sensibles de nuestro continente. ¿Logrará la NIS2 hacer frente a los desafíos del cibercrimen? ¿Qué medidas deben tomar las empresas para cumplir con sus requisitos? Analizaremos estas y otras preguntas en profundidad.

Rosalía Arroyo

En julio de 2016, la Unión Europea aprobó la Directiva sobre Seguridad de las Redes y Sistemas de Información (NIS) buscando fortalecer la ciberseguridad en toda la Unión. Esta normativa se centró en dos grupos clave: operadores de servicios esenciales (como energía y transporte) y proveedores de servicios digitales. El objetivo era mejorar las capacidades nacionales de ciberseguridad, fomentar la colaboración entre países y hacer de la ciberseguridad una prioridad para las organizaciones incluidas.

La Directiva NIS, aunque pionera en su momento, ha demostrado ser insuficiente para hacer frente a la evolución constante del panorama de amenazas cibernéticas. La fragmentación en su aplicación entre los Estados miembros y la incapacidad para abordar de manera efectiva los desafíos planteados por la pandemia y los conflictos geopolíticos han subrayado la necesidad de una normativa más armonizada y resiliente.

Con el objetivo de hacer frente a la creciente sofisticación de los ciberataques, la UE presentó, en enero de 2023, la directiva NIS2, que

busca garantizar un mayor nivel de ciberseguridad y resiliencia en todas las organizaciones europeas. Los Estados miembros tendrán que transponer la NIS2 a su legislación nacional antes del 17 de octubre de 2024, por lo que las organizaciones ya deberían empezar a preparar su camino hacia el cumplimiento.

La NIS2 establece una clasificación detallada de los sectores a los que se aplica, dividiéndolos en 'Alta Criticidad' y 'Otros Críticos'. Esta categorización, que incluye subsectores específicos como electricidad e hidrógeno dentro del sector energético, facilita la identificación de las entidades obligadas a cumplir la normativa. Si bien amplía el número total de sectores, la NIS2 mantiene el enfoque en aquellos considerados críticos para el funcionamiento de la sociedad, como energía, banca y transporte.

Ambos grupos de entidades deben cumplir con las mismas medidas de seguridad. "Sin embargo,

> A la hora de determinar la cuantía de la sanción, las autoridades competentes tendrán en cuenta diversos factores

las que se encuentran en la categoría esencial están bajo supervisión proactiva, mientras que las consideradas como entidades importantes solo serán monitorizadas después de que se notifique un incidente de incumplimiento", explican desde KPMG, añadiendo que las organizaciones deben tomar medidas inmediatas para evaluar si se encuentran dentro del alcance y si se consideran una entidad esencial o importante.

Empresas afectadas

Para determinar si una empresa está sujeta a la NIS2, se consideran varios factores. Por un lado el sector de actividad; es decir, la empresa debe operar en uno de los sectores considerados críticos, que mencionaremos más adelante.

Tamaño de la empresa: La directiva se aplica generalmente a empresas medianas y grandes, aunque también puede afectar a pequeñas empresas en ciertos casos. Naturaleza de los servicios: La empresa debe prestar servicios esenciales o procesar grandes cantidades de datos personales.

De manera concreta los sectores de Alta Criticidad que se ven afectados por NIS2 debido a que presentan un riesgo particularmente alto en caso de ciberataque, ya que su disrupción podría tener consecuencias graves para la sociedad en su conjunto, son:

- Energía
- Transporte
- Banca
- Infraestructuras de los mercados financieros
- Sector sanitario
- Agua potable y aguas residuales
- Infraestructura digital
- Gestión de servicios TIC
- Administración pública
- Espacio

En el Anexo II “Otros sectores críticos” se recogen un total de 7 sectores: Servicios postales y de mensajería; Gestión de residuos; Fabricación, producción y distribución de sustancias y mezclas químicas; Producción, transformación y distribución de alimentos; Fabricación; Proveedores digitales; Investigación.

La Directiva NIS2 se aplicará a: Entidades de más 250 personas, con un volumen de negocios anual de 50 millones o un balance general anual superior a 43 millones de euros; y entidades pertenecientes a los Sectores de Alta Criticidad u Otros Sectores Críticos no consideradas esenciales.

Requerimientos críticos

NIS2 incorpora novedades no sólo en cuanto a los sectores afectados, notificación de incidentes, la seguridad de la cadena de suministro o que ahora los gerentes de las empresas son responsables de asegurar las operaciones. Hay varios artículos dentro de la normativa que son críticos. El Artículo 20 es uno de ellos. NIS2 responsabiliza a los órganos de dirección de las organizaciones esenciales e importantes de garantizar la implementación efectiva de las medidas de ciberseguridad. Para ello, deben aprobar los

planes de seguridad, supervisar su cumplimiento y asegurar que los empleados cuenten con la formación necesaria para identificar y gestionar los riesgos.

Por otra parte, NIS2 otorga a las entidades cierta flexibilidad para adaptar las medidas de seguridad a sus características específicas. Sin embargo, el artículo 21 establece requisitos mínimos que deben cumplirse, como:

- Análisis de riesgos y políticas de seguridad de la información
- Gestión de incidentes
- Continuidad empresarial
- Seguridad de la cadena de suministro
- Gestión y divulgación de vulnerabilidades
- Procedimientos para evaluar la eficacia de la gestión de riesgos cibernéticos
- Prácticas de higiene informática y formación en ciberseguridad;
- Políticas y procedimientos de criptografía y cifrado
- Seguridad de los recursos humanos, políticas de control de acceso y gestión de activos
- Uso de autenticación multifactor y sistemas de comunicación seguros

NIS2 responsabiliza a los órganos de dirección de las organizaciones esenciales e importantes de garantizar la implementación efectiva de las medidas de ciberseguridad

Con el objetivo de proteger a los usuarios, el artículo 23 obliga a las organizaciones a notificar a las autoridades competentes sobre los incidentes cibernéticos y a informar a sus clientes sobre las ciberamenazas que puedan afectarles. Esta medida busca empoderar a los usuarios para que puedan tomar las precauciones necesarias.

Las principales novedades de NIS2

NIS 2 contiene aspectos que abordan deficiencias de la Directiva NIS original y que han dado lugar a las siguientes novedades:

- **Mayor escala que la NIS, más sectores considerados servicios esenciales**
- **Los gerentes son responsables de asegurar las operaciones**
- **La notificación inicial deberá realizarse sin demora y, en cualquier caso, en el plazo de 24 horas desde que se haya tenido constancia del incidente**
- **Requisitos de seguridad y notificación más elevados, donde se debe cumplir una lista de requisitos mínimos**
- **Seguridad para las cadenas de suministro y los proveedores**
- **Medidas de supervisión más estrictas para las autoridades nacionales**
- **Se ha eliminado la distinción entre "operadores de servicios esenciales" y "proveedores de servicios digitales"**
- **Medidas regulatorias más estrictas para las autoridades nacionales, requisitos de cumplimiento más estrictos**
- **Armonizar los sistemas de sanciones entre los Estados miembros y permitir multas administrativas. La multa será de hasta 10 millones de euros o el 2 % de la facturación total de la empresa en todo el mundo**
- **El Grupo de Cooperación adquiere un papel más importante, así como un mayor intercambio de información y cooperación entre las autoridades de los Estados miembros**

Un incidente con impacto significativo "es aquel que ha causado o puede causar graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada y ha afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o inmateriales considerables", aseguran desde Deloitte.

> Los Estados miembro tendrán hasta el 17 de enero de 2025 para comunicar el régimen de sanciones aplicables por incumplimiento de NIS2

Las organizaciones deben informar al CSIRT, o a la autoridad competente, en el plazo de 24 horas desde que tengan conocimiento del incidente significativo, una alerta temprana que indique si se sospecha que el incidente significativo está causado por actos ilícitos o maliciosos o podría tener un impacto transfronterizo. Además, en el plazo de 72 horas desde que se tenga conocimiento del incidente significativo, debe realizar una notificación del incidente que, en su caso, actualizará la información anterior aportando los indicadores de compromiso. A petición de la autoridad competente, la organización afectada por un incidente deberá aportar un informe intermedio sobre las actualizaciones de estado perti-

nentes. Finalmente, deberá enviarse un informe final, a más tardar un mes después de la presentación de la notificación del incidente.

Sanciones

Como recoge Deloitte, los artículos 34 y 36 de la normativa son los que establecen que los Estados miembros tendrán la posibilidad de imponer sanciones administrativas a las entidades que incumplan con los requisitos de la Directiva NIS 2, en especial los requisitos establecidos en los artículos 21 y 23, relativos a las medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación respectivamente.

Las sanciones “deberán ser efectivas, proporcionales y disuasorias teniendo en cuenta las circunstancias en cada caso particular”, asegura la consultora.

A la hora de determinar la cuantía de la sanción, las autoridades competentes tendrán en cuenta diversos factores, como la gravedad de la infracción, la duración del incumplimiento, los beneficios obtenidos de forma ilícita, la capacidad económica de la empresa y la cooperación de la empresa con las autoridades

Las sanciones son de hasta diez millones de euros o un máximo de un 2 % del volumen de negocio anual en el caso de las entidades esenciales; o de hasta 7 millones de euros o un máximo de un 1,4 % de la facturación en el caso de las entidades importantes. En casos graves de incumplimiento, las autoridades pueden suspender temporalmente la prestación de servicios.

Los Estados miembro tendrán como fecha límite el 17 de enero de 2025 para comunicar el régimen de sanciones aplicables por incumplimiento a la Comisión Europea.

La ampliación del ámbito de aplicación de las nuevas normas, al obligar efectivamente a más empresas y sectores a adoptar medidas para gestionar el riesgo de ciberseguridad, contribuirá a aumentar el nivel de ciberseguridad en Europa a medio y largo plazo.

La realidad de NIS 2 en el mercado español

El plazo para cumplir con los requisitos de NIS2 se acerca rápidamente. Las empresas de toda Europa se encuentran en una carrera contra el tiempo para adaptar sus sistemas de seguridad y evitar costosas sanciones. En este artículo recogemos los retos que los directores de TI y/o ciberseguridad de algunas empresas relevantes tienen que afrontar, cuáles creen que son las medidas más importantes que introduce la normativa para reforzar la seguridad o cómo impactará NIS2 en el panorama de ciberseguridad de la Unión Europea.

Rosalía Arroyo

Francisco Sánchez Nauffal, IT Security Director de **EcoVadis**; Pedro Navas Galán, Manager Sourcing & IT Advisory de **Eraneos Iberia**; Enrique Ferrer, Gerente de Sistemas de **Ford Motor Company**; Natalia Galán, responsable de gobierno de la seguridad en **Iberdrola España**; Jesús Abascal Santamaría, CISO en **Plenitude**; y Alejandro Expósito, CIO de **Ullastres**, han sido los directivos que han respondido a un cuestionario.

Fase de implementación

Con el objetivo de conocer cuál es la situación en la que las empresas están a la hora de hacer frente a normativa, la primera pregunta que lanzamos es: ¿En qué fase de implementación de la normativa NIS2 se encuentra su empresa?

Las respuestas, algunas resumidas, son variopintas. Responde Francisco Sánchez Nauffal que, aunque **EcoVadis** no está en el alcance de NIS2, "estamos monitorizando de cerca el desarrollo de la regulación, así como la orientación

> "La implementación de NIS2 es un avance general positivo, pero requerirá ajustes significativos para muchas organizaciones"
>
> **Francisco Sánchez Nauffal,**
> IT Security Director de **EcoVadis**

local sobre estos asuntos, y trabajaremos para alinearnos progresivamente con sus requisitos, aunque puede que no sea oficialmente aplicable a nuestra organización".

Tiene claro Pedro Navas que, dedicándose a la consultoría estratégica, "no prestamos servicios esenciales, luego no nos aplica. Pero como trabajamos con clientes a los que sí les aplica, seguro que trabajaremos en alguna adaptación puntual".

Nos cuenta Enrique Ferrer que en **Ford Motor**, "estamos en fase de implementación de los pocos requisitos que nuestros equipos centrales ven como necesarios. Por nuestra propia visión, cumplimos con la gran mayoría de requerimientos generales, a la espera de la transposición final de la ley en España y de revisar si hay más parámetros que considerar para el cumplimento completo de la normativa".

Asegurando que el nivel de madurez de la compañía es muy elevado, dice Natalia Galán, de Iberdrola, "que a pesar de que el nivel de madurez de la compañía es muy elevado, se han detectado unas líneas de acción prioritarias que se están abordando para anticiparnos ante la futura transposición de la Directiva NIS2 a la legislación española"

En junio de este año, que es cuando se respondió el cuestionario, nos contaba Jesús Abascal que **Plenitude** se encontraba "en la fase inicial de Assessment para determinar qué controles de seguridad se cumplen y cuáles no. Esta evaluación exhaustiva nos permitirá identificar las áreas en las que ya estamos en conformidad con los requisitos de la Directiva NIS2 y aquellas en las que necesitamos mejorar. Además, estamos a la espera de la publicación de la transposición de la normativa NIS2 en España, lo que proporcionará directrices específicas adaptadas a nuestro contexto regulatorio nacional".

Explicando que, con la ampliación de la aplicación de la normativa no solo a las empresas catalogadas como servicios esenciales, "sino también a sus proveedores, nos hemos visto afectados por la normativa, así que estamos en la fase de estudio de la implantación, analizando diferentes colaboradores con los que implantarla", decía Alejandro Expósito.

Desafíos de NIS2

La implementación de NIS2 es un avance general positivo, pero requerirá ajustes significativos para muchas organizaciones, comentaba el IT Security Director de **EcoVadis**, destacando algunos desafíos: el aumento del alcance del cumplimiento, ya que se aplica a grandes grupos de organizaciones, incluidas pequeñas

y medianas empresas que podrían no tener los recursos para implementar prácticas sólidas de ciberseguridad; el enfoque en la gestión de la cadena de suministro, ya que requerirá que las organizaciones tengan una mayor visibilidad de las prácticas de seguridad de sus proveedores (y esto puede ser muy complejo); y los requisitos alrededor del reporte, que son más estrictos que nunca y sin duda aumentarán la carga de trabajo de los equipos de seguridad, lo que hará que algunas organizaciones tengan dificultades para cumplir con los plazos.

Para Pedro Navas, "como suele ocurrir con estas directivas europeas, muchas organizaciones no son conscientes de los requisitos, o no comprenden plenamente su alcance", lo que puede dificultar la elaboración de planes de cumplimiento efectivos. Asegura que los cambios necesarios para la adaptación a NIS2 "pueden ser complejos y costosos porque suponen una inversión en tecnología, cambio de procesos de negocio, formación del personal... la carga financiera puede ser importante, especialmente para las PYMEs".

"Como toda norma europea, presenta los problemas habituales en una compañía americana con una dirección de seguridad muy centralizada en USA: Distintas transposiciones, según los gobiernos locales de cada país, normativas o procedimientos distintos de reporting, auditoria, etc.", comenta Enrique Ferrer, Gerente de Sistemas de **Ford Motor Company**. Asegura que realmente NIS 2 "no trae nada demasiado novedoso para una empresa ya concienciada por la ciberseguridad, salvo la responsabilidad en la Cadena de Suministro"; recuerda que la normativa no sólo exige que se cumpla con lo establecido, "sino además poder demostrar, con evidencias que se toman y mantienen las medidas adecuadas en cada entorno".

"Los cambios para la adaptación a NIS2 pueden ser complejos y costosos porque suponen una inversión en tecnología, cambio de procesos de negocio, formación del personal..."

Pedro Navas Galán,
Manager Sourcing & IT Advisory de, **Eraneos Iberia**

Para Natalia Galán, responsable de gobierno de la seguridad en **Iberdrola España,** los desafíos de NIS2 giran en torno al alcance, la gobernanza y la cadena de suministro, que llevan no sólo a la implicación y responsabilidad de la Dirección en relación con el cumplimiento de las normas de gestión de riesgos de ciberseguridad y adquisición de conocimientos en esta materia, sino a la "revisión de los requisitos de ciberseguridad de proveedores y terceras partes, e implementación de procesos de supervisión".

Tiene claro Jesús Abascal Santamaría, CISO en **Plenitude**, que lo más difícil para implantar la NIS2 "será la gestión de la cadena de suministro

y la evaluación de proveedores, dado que asegurar la ciberseguridad de todos los eslabones involucrados requiere una coordinación y vigilancia constante". Añade que la creación de un equipo interno de respuesta a incidentes de seguridad informática (CSIRT) "implica no solo una inversión significativa en recursos humanos y tecnológicos, sino también el desarrollo de procedimientos eficientes y efectivos para la detección y respuesta a incidentes". Además, "promover una cultura de ciberseguridad en toda la empresa es un desafío considerable, ya que requiere un cambio de mentalidad y comportamiento a todos los niveles de la organización, desde la alta dirección hasta los empleados operativos, asegurando que todos comprendan la importancia de la ciberseguridad y actúen en consecuencia". Dice Alejandro Expósito, CIO de **Ullastres**, que, teniendo en cuenta que realmente la NIS2 no es solo tecnología sino también prácticas y operativas, "para nosotros el principal desafío, a parte del lógico de adecuar toda nuestra infraestructura de sistemas para cumplir la norma, es el cambio cultural hacia la inteligencia compartida y colaborativa".

Recomendaciones

Tras proponerle qué recomendaciones haría a otras empresas que están en proceso de implementar NIS2, comenta el directivo de **EcoVadis** que la más importante es "comenzar temprano", así como "estar familiarizado con los requisitos de la normativa y evaluar la postura actual de la compañía con respecto a la misma". Añade Francisco Sánchez Nauffal que hay otras cosas que las empresas deben tener en cuenta: cómo asegurarse de adoptar un enfoque de ciberseguridad basado en el riesgo, invertir en los recursos necesarios (humanos y financieros) y mejorar la colaboración con sus proveedores, "ya que son una pieza fundamental para garantizar que han hecho su diligencia en lo que respecta al cumplimiento de NIS2".

Para Pedro Navas, "el primer paso es realizar una evaluación exhaustiva de los riesgos de ciberseguridad que enfrenta la organización. Esto ayudará a identificar los activos críticos que deben protegerse y las amenazas más probables". Una vez cumplimentado este primer paso, "la organización debe desarrollar un plan de cumplimiento que describa cómo se implementarán las medidas de seguridad necesarias para cumplir con los requisitos de NIS2, en ese plan se han de detallar tareas tales como: elaborar la

"La responsabilidad de las empresas sobre la cadena de suministro es el mayor cambio, y el que mayores dificultades de implementación y control va a tener"

Enrique Ferrer,
Gerente de Sistemas de, **Ford Motor Company**

lista de medidas de seguridad a implantar, planificar esas implantaciones, identificar responsables, revisión y actualización periódica del plan de cumplimiento".

"Es imprescindible disponer de un nivel de concienciación y formación elevados en materia de buenas prácticas de seguridad y ciberseguridad"

Natalia Galán, responsable de gobierno de la seguridad en, **Iberdrola España**

Propone Enrique Ferrer "analizar bien la empresa y asegurarse de que se dispone de un inventario completo de todos los repositorios de datos críticos, no solo de carácter personal, sino operativos", a lo que añade el directivo de **Ford** la necesidad de "auditar los procesos críticos tales como copias de seguridad limpias, realizar una prueba real de capacidad de restauración en caso de un ataque con éxito, y verificar que toda la plantilla propia y de terceros que manejen infraestructuras críticas están convenientemente formados en ciberseguridad". Como ha comentado anteriormente, "además es importante poder probarlo".

La principal recomendación de Natalia Galán es "conocer, objetivamente, el nivel de madurez de ciberseguridad en el que se encuentra la empresa". Explica que "los riesgos a los que nos enfrentamos las organizaciones evolucionan a medida que evoluciona la tecnología y, por tanto, es necesario tratar el riesgo de ciberseguridad como un riesgo de negocio. Disponer de políticas y procedimientos que hayan sido probados, actualizados y que recojan las posibles lecciones aprendidas". Añade que es "imprescindible disponer de un nivel de concienciación y formación elevados en materia de buenas prácticas de seguridad y ciberseguridad".

"Yo siempre recomiendo empezar por una evaluación inicial para determinar el estado actual y el estado objetivo", comenta el CISO de **Plenitude**. Para Jesús Abascal, "también es importante ser transparente con la dirección y buscar su compromiso. "En mi opinión, es mejor fijar un plan de mejora continua que permita iterar periódicamente para incrementar el número de controles y su madurez, en lugar de establecer un programa muy ambicioso con un gran número de controles con gran robustez".

Reconociendo que es obvia, propone el CIO de **Ullastres** que la implementación de NIS2 se haga "lo antes posible. Si ya están certificadas en la ISO27001 es relativamente sencillo de implantar, y si no la tienen, les recomendaría empezar a implantar la ISO27001, y una vez que lo tengan el camino a la NIS2 está bastante allanado".

Medida a destacar

De las medidas introducidas por NIS2 para reforzar la ciberseguridad, ¿cuál considera más

importante? Responde Francisco Sánchez Nauffal que NIS2 introduce varias medidas importantes para abordar y aumentar la postura de seguridad de las organizaciones, “pero el enfoque en gestión de riesgos es el que yo destacaría”. Explica que, al exigir que las organizaciones identifiquen y prioricen sus riesgos de ciberseguridad más críticos, “NIS2 fomenta un enfoque de seguridad más específico y eficaz, que es esencial para empresas de todos los tamaños, y aún más para las empresas más pequeñas que pueden no tener los recursos para proteger todo por igual”.

Además, opina que no deben menospreciarse los requisitos en torno a responsabilidad corporativa en lo referido a la estrategia de ciberseguridad porque “esto hace que la ciberseguridad sea una aspecto muy relevante a nivel de las juntas directivas, lo cual está bastante alineado con la dirección que se está tomando globalmente, pero esto también requiere que la dirección de la empresa tenga que recibir formación para comprender los riesgos de ciberseguridad a su nivel, o incluso la implicación de ser personalmente responsable en caso de graves incumplimientos por negligencia”, dice el IT Security Director de **EcoVadis**.

> “Lo más difícil para implantar la NIS2 será la gestión de la cadena de suministro y la evaluación de proveedores”
>
> **Jesús Abascal Santamaría,**
> CISO en **Plenitude**

“Determinar qué medida es la más importante no es fácil”, asegura Pedro Navas. Explica el Manager Sourcing & IT Advisory de **Eraneos** que todas van orientadas a reforzar la ciberseguridad, y que “cada una aborda aspectos críticos de la protección contra ciberataques”. En todo caso, “la gestión de riesgos de ciberseguridad me parece la más relevante porque es la base. La gestión de riesgos de ciberseguridad establece un marco para identificar, evaluar y mitigar los riesgos a los que se enfrenta una organización. Permite a las organizaciones anticiparse a las amenazas y tomar medidas preventivas para minimizar su impacto”. Añade que es importante que NIS2 exija “que la alta dirección sea responsable de la gestión de riesgos de ciberseguridad. Me parece un gran acierto”.

“Los CIRT ya existen y hay una cierta colaboración, pero la norma va a obligar a que la cooperación sea mucho mayor y efectiva”, comenta Enrique Ferrer, añadiendo que “la compartición de conocimientos entre todos los países, (si realmente se lleva a cabo), ayudaría enormemente en detecciones tempranas, disponibilidad de soluciones ante los distintos tipos de ciberataques, etc.”. Añade que “la responsabilidad de las empresas sobre la cadena de suministro es el mayor cambio, y el que mayores dificultades de implementación y control va a tener”.

Para la responsable de gobierno de la seguridad en **Iberdrola España**, “la optimización de los procesos de gestión de riesgos de ciberseguridad y la oportunidad que brinda para hacer que la empresa y su cadena de suministro sea más resiliente”, son algunas de las medidas importantes que introduce NIS2. Añade Natalia Galán que la obligación de notificación de incidentes requiere que las entidades informen de cualquier incidente con un impacto significativo en sus servicios, facilitando una respuesta más rápida, y que “esta transparencia contribuye a fortalecer la ciberseguridad entre las entidades y/o estados miembros”.

Recordando que la cadena de suministro se ha convertido en uno de los vectores de ataque más explotados, tiene claro Jesús Abascal que la medida más importante que integra NIS2 “es la gestión de la cadena de suministro. Esta medida también se ha establecido como obligatoria en DORA y resulta crucial porque las vulnerabilidades en la cadena de suministro pueden comprometer la seguridad de toda la organización”. Añade que, sin embargo, “no se puede responsabilizar a una empresa de los ataques sufridos dentro de la cadena de suministro”.

Dice Alejandro Expósito que NIS2 exige la aplicación de una serie de medidas de ciberseguridad y actividades de gestión de riesgos, y explica que “entre las medidas se incluyen el control de acceso y la aplicación de privilegios mínimos, una autenticación multifactorial sólida y medidas para disuadir, detectar o prevenir el código malicioso, como el ransomware”. Recuerda el directivo de **Ullastres** que NIS2 tiene estrictas normas de notificación de infracciones cibernéticas “incluso si no hay ninguna indicación de datos personales expuestos. Esto nos permitirá estar mucho más atentos a lo que pueda acontecer y por tanto más prevenidos y saber realmente el alcance de los peligros”.

Impacto de NIS2

La última pregunta que planteamos en nuestro cuestionario es cómo impactará NIS2 en el panorama de ciberseguridad de la Unión Europea. En opinión de Francisco Sánchez Nauffal, “se espera que NIS2 tenga un impacto positivo significativo en el panorama de la ciberseguridad en la UE”. De manera más concreta, menciona mejoras de la postura y la resiliencia en materia de ciberseguridad, mejora en el reporte de incidentes, así como una mayor armonización y estandarización, “garantizando que exista un en-

> “NIS2 nos hará estar más preparados ante posibles ataques, tener más información para poder prevenirlos y una guía de actuación en caso de que se produzcan”
>
> **Alejandro Expósito,**
> CIO de **Ullastres**

NIS2 es una versión más exigente y amplia de la Directiva NIS original

foque coherente de la ciberseguridad en todos los estados miembros, facilitando no sólo una mayor colaboración sino también apoyando la expansión del mercado para varias empresas de forma segura".

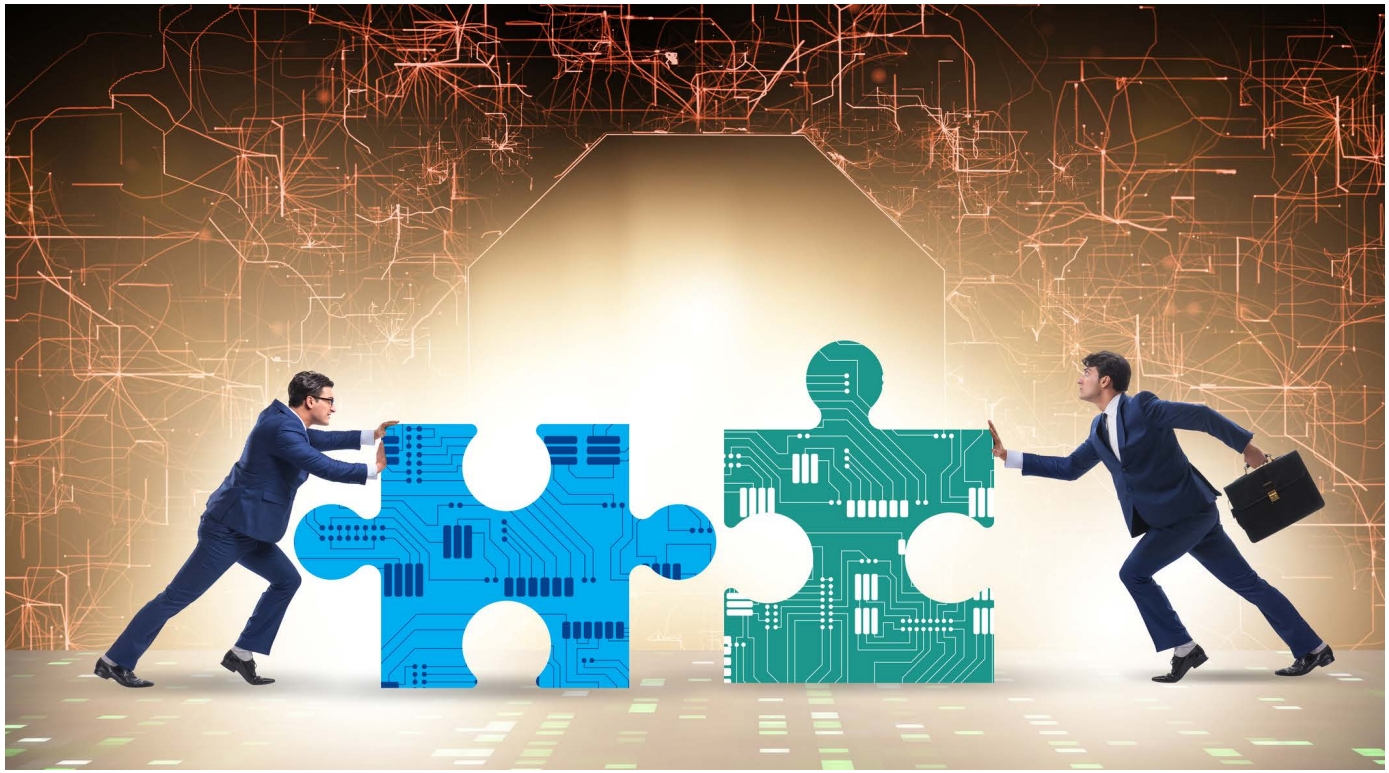
Para el directivo de **Eraneos**, "NIS2 obligará a las organizaciones a adoptar medidas de seguridad más sólidas, lo que a su vez debería reducir la probabilidad y el impacto de los ciberataques". Además, la normativa "debería ver reforzada la capacidad de los países de la Unión Europea para responder a los ciberataques y recuperarse de ellos", así como "producirse una mayor colaboración entre estados de la Unión Europea, un aumento en la concienciación sobre ciberseguridad entre empresas y organizaciones del sector público y, por tanto, una mejor comprensión de los riesgos a los que nos vemos sometidos".

Enrique Ferrer espera un impacto positivo de la normativa, "aunque todo va a depender de las distintas transposiciones que se realicen en cada uno de los estados miembros. Si son similares, las ventajas se conseguirán rápidamente. Si como en el caso de la RGPD, hay diferencias significativas en la legislación que se trasponga en cada estado, las medidas adicionales a implementar en las empresas por supuesto serán beneficiosas, pero si no se alcanza la plena colaboración internacional, la gran ventaja de trabajar en grupo compartiendo conocimientos se verá significativamente reducida, con el consiguiente impacto en conseguir un entorno de trabajo más seguro en toda Europa".

Tiene claro Natalia Galán que la nueva directiva "tiene como objetivo fundamental reforzar el nivel de resiliencia en toda la UE, para responder de manera más efectiva a las crecientes amenazas que plantea la digitalización y el aumento de los ciberataques. Las divergencias de aplicaciones entre estados miembros, la no cooperación o compartición de información, pueden hacer más vulnerable el ciberespacio común".

Desde el punto de vista de Jesús Abascal, "el nuevo alcance establecido por la NIS2 impactará significativamente el panorama de ciberseguridad en la Unión Europea, mejorando también la ciberresiliencia de las empresas que cumplan con la directiva. En este sentido, se promoverá la concienciación en materia de ciberseguridad entre todas las empresas involucradas en la cadena de suministro. Sin embargo, otro objetivo de la directiva, que considero difícil de implementar, es la cooperación efectiva entre los Estados miembros y a nivel europeo".

Para Alejandro Expósito, NIS2 "nos hará estar más preparados ante posibles ataques, tener más información para poder prevenirlos y una guía de actuación clara en el caso de que se produzcan. Tenemos que tener en cuenta que las nuevas tecnologías como es la IA o en un futuro cercano la Computación Cuántica están permitiendo la 'profesionalización de la ciberdelincuencia' con lo que todos tenemos que estar preparados para contrarrestarla, en este caso una norma como es la NIS2 seguro que ayudará, pero no basta, porque como sucede en muchos campos el marco legislativo va por detrás de la tecnología, si de verdad queremos impactar en el panorama de ciberseguridad deberíamos ser mucho más agiles".



> NIS2 busca crear un entorno más seguro y fiable para el desarrollo de negocios

“Tenemos que ser los más rápidos recuperando el entorno”

Santiago Campuzano es el responsable para la región de Iberia de Veeam Software, una empresa especializada en la gestión del backup, recuperación ante desastres, gestión inteligente de los datos en infraestructuras virtuales, físicas y multi-cloud. Con él hablamos sobre NIS2, una directiva de seguridad que se ha convertido en paso importante hacia un futuro digital más seguro.

Rosalía Arroyo

Santiago Campuzano, country manager para Iberia de **Veeam Software**

Recordando que NIS2 afecta, prácticamente, a todas las empresas u organismos que tengan actividades esenciales, menciona Santiago Campuzano que el plazo que se ha dado para el cumplimiento de NIS2 ha sido “razonablemente corto”, lo que se ha convertido en uno de los desafíos que están afrontando las empresas. Añade el directivo que, en muchos casos, las compañías tienen que pensar “cómo van a cumplir los requerimientos de seguridad con la obligación de poder mantener el negocio en el día a día, que es uno de los puntos clave”.

> “Para cumplir todo lo que nos pide NIS2 y estar preparados tenemos que ser conscientes de que lo importante es recuperar los entornos lo antes posible”

Preguntado por las soluciones y herramientas que tiene Veeam para ayudar a los clientes a cumplir con la normativa, responde Campuzano que “Veeam es una compañía diseñada prácticamente para cumplir con este tipo de regulaciones” que no sólo exige cumplir ciertos requisitos de seguridad, sino ciertos requisitos asociados a la resiliencia, el poder mantener las operaciones dentro de las organizaciones.

Apostando por la Radical Resiliency, dice Campuzado que “las soluciones de Veeam están pensadas para que los clientes puedan mantener sus organizaciones activas en todo momento o que, en caso de incidente, la parada sea la menor posible”.

Menciona el directivo los tres ciberriesgos a los que se enfrentan las empresas: la caída del negocio, el daño reputacional, y las implicaciones legales que tiene esa caída del negocio. “Para cumplir todo lo que nos piden NIS2 y estar preparados ante los tres ciberriesgos tenemos que ser conscientes de que lo importante es recuperar los entornos lo antes posible”, asegura el directivo, añadiendo que es en esa recuperación “donde somos líderes del mercado. Somos la compañía que más eficientemente recupera por cómo se han diseñado siempre los productos”.

La propuesta de la compañía, repartida entre Veeam Data Platform, que son soluciones más orientadas hacia la parte on-prem, y Veeam Data Cloud, que son servicios gestionados en modo nube, ofrecen una proposición de valor muy clara: “tenemos que ser los más rápidos recuperando el entorno, tenemos que tener los informes con la mayor personalización posible de cara a cubrir las necesidades que exige, no solo NIS2, sino cualquier tipo de requerimiento legal y, además, podemos dar un sistema de orquestación que nos permite, tanto durante el periodo de recuperación como la de gestión del entorno, permitir que los recursos estén correctamente gestionados”.

Preguntado por las tendencias de ciberseguridad que más impactan menciona “el ransomware y el secuestro del dato como último punto de todo”. Añade que todos los tipos de amenazas intentan, además, atacar a los sistemas de backup para que las compañías no se puedan recuperar por sí mismas. Menciona también el impacto de la inteligencia recordando que los fabricantes “estamos apostando por la inteligencia artificial, porque si no lo hacemos, es imposible llegar a competir”.

Por otra parte, añade Santiago Campuzano que hay que empezar a pensar que “no solo es importante protegerse de la manera proactiva tradicional; la clave es la resiliencia y la gran pre-

Santiago Campuzano, country manager para Iberia de **Veeam Software**

gunta es: ¿cómo puedo recuperar el entorno lo antes posible?, "y ahí es donde las tecnologías tienen que aportar un diferencial".

¿Cómo está ayudando Veeam a mejorar la postura de seguridad de sus clientes? Responde Santiago Campuzano que lo primero que ha hecho Veeam desde que se fundó es "entender que la resiliencia era un valor crítico y las caídas se tienen que poder levantar lo antes posible con tecnologías específicas". La compañía ha ido ampliando su oferta a través del i+d y de adquisiciones estratégicas que le permiten ofrecer resiliencia y movilidad en entornos de contenedores, por ejemplo. Asegura que Veeam no quiere ser una compañía puramente de ciberseguridad, y que es una compañía de "data resiliency, de radical resiliency, que permite que cualquier entorno pueda mantenerse operativo en cualquier momento".

Como expertos en proteger los datos y la información, ¿cómo cree que evolucionará la regulación en torno a la seguridad de los datos? Asegurando que el dato es fundamental dentro de las organizaciones, incluso a nivel sociedad, opina Santiago Campuzano que las regulaciones "van a tener actualizaciones prácticamente anuales". Actualizaciones que estarán basadas en las nuevas tecnologías, como la inteligencia artificial, "que da un vuelco brutal a la gestión del dato, a la de la información".

"Lo primero que tienen que ser conscientes es de que la normativa hay que cumplirla" y que "si tú tienes un plan de contingencia tecnológico, vas a estar preparado para cumplir casi todo", dice Santiago Campuzano cuando le pedimos que lance un mensaje o consejo a esas empresas que están ahora mismo luchando por querer cumplir con NIS2. Comenta también que es más fácil adaptar la normativa "si tienes las tecnologías adecuadas" y que hay que entender que "esto no se puede hacer solo. Tienes que buscar partners, tanto partners tecnológicos como partners de servicios". CST

“El principal recurso que provee Econocom a sus clientes es el talento”

Econocom es una empresa multinacional de servicios y soluciones tecnológicas. Su principal objetivo es acompañar a las empresas en su transformación digital, ofreciendo un amplio abanico de servicios que abarcan desde la consultoría y el diseño de soluciones tecnológicas, hasta la implementación, la financiación y la gestión del ciclo de vida de los equipos informáticos.

Rosalía Arroyo

Isaac Rosado,
Director Preventa Actividad Servicios de **Econocom**

Isaac Rosado, Director Preventa Actividad Servicios de Econocom, responde a unas preguntas que dejan claro que dentro del portfolio de Econocom hay un amplio número de servicios que pueden preparar a las compañías para el debido cumplimiento de la normativa.

> “La principal amenaza que es ya una realidad es el uso de la inteligencia artificial en manos de los ciberdelincuentes”

¿Qué preocupa y cuáles cree que son los principales desafíos que enfrentan sus clientes al cumplir con NIS?

El principal desafío de las empresas es adecuar sus procesos y organizaciones a la nueva normativa. Encontrar nuevas herramientas y tecnologías es relativamente sencillo ya que el mercado está lleno de ellas con un amplio abanico de funcionalidades. Sin embargo, cambiar organización y procesos para sacar el mejor partido a las mismas requiere de una gestión del cambio madura y profunda lo que en general es considerablemente más lento. Además, ese proceso de cambio debe incorporar una mayor concienciación al respecto de estas necesida-

des lo que se debe traducir en un verdadero cambio cultural para la compañía al respecto del uso de sus datos.

¿Cómo puede Econocom ayudar a los clientes a mejorar su postura de seguridad en general?

Econocom provee a sus clientes de servicios recurrentes y proyectos de transformación que pueden ayudar a las compañías a transitar ese cambio descrito con mayor eficacia. Somos capaces de desplegar servicios que incorporan la seguridad por diseño y que contienen esas herramientas como parte de dicho servicio para aislar a nuestros clientes de parte de la complejidad que conlleva su correcta explotación. Esto permite una vez más a nuestros clientes centrarse en su negocio dejando los procesos IT en manos de un socio de confianza.

¿Qué servicios de Econocom pueden ayudar a los clientes a cumplir con NIS?

Dentro del portfolio de Econocom hay un amplio número de servicios que pueden preparar a las compañías para el debido cumplimiento de la normativa. Desde nuestros servicios en nube que incorporan de forma intrínseca servicios de DDoS, microsegmentación o detección preventiva de vulnerabilidades, en lo que llamamos una protección activa, hasta servicios de recuperación ante desastres y backup inmutable, en lo que denominamos protección pasiva. Todas estas soluciones son entregadas en modalidad de servicio con modelos de relación y gobierno claros incorporando una transformación continua que adapta estos servicios a las necesidades actuales y a las que estén por venir.

¿Qué recursos ofrece Econocom para ayudar a los clientes a aprender más sobre NIS y cómo cumplir con él?

El principal recurso de provee Econocom a sus clientes es el talento de las personas que hacen realidad sus servicios en el día a día. Es el recurso más escaso y de valor que una empresa de servicios puede ofrecer. Sólo de esta forma podemos desarrollar y mantener en el tiempo la confianza que depositan en nosotros.

¿Qué tendencias en torno a las ciberamenazas cree que podrían afectar el cumplimiento de NIS?

La principal amenaza que es ya una realidad es el uso de la inteligencia artificial en manos de los ciberdelincuentes, las herramientas que incorporan IA Generativa van a potenciar sus capacidades de forma nunca antes vistas. Asimismo, el propio uso inadecuado de la IA por parte de las empresas las hará más vulnerables que antes y les puede dificultar el control sobre sus propios datos. Por tanto, el aumento exponencial de los casos de uso de la IA hará que los mecanismos para su cumplimiento deban actualizarse constantemente.

Isaac Rosado, Director Preventa Actividad Servicios de **Econocom**

¿Cómo cree que el panorama regulatorio en torno a la seguridad de datos evolucionará en los próximos años?

Las propias normativas deberán también evolucionar ahondando en la gestión de riesgos y de su mitigación. Asimismo, evolucionarán haciendo más responsables a las empresas sobre la gobernanza de los datos, probablemente con más restricciones sobre esos datos a almacenar y su protección.

> "El principal desafío de las empresas es adecuar sus procesos y organizaciones a la nueva normativa"

¿Qué consejo daría a las empresas que están luchando por cumplir con NIS?

Aconsejaría empezar por acondicionar procesos a los nuevos requerimientos e invertir en talento para su correcta gestión. A partir de ello y entendiendo las verdaderas necesidades entorno a ellos definir entonces los servicios, soluciones y tecnologías que verdaderamente se requieren. Por otro lado, les aconsejaría acompañarse de los mejores socios que les faciliten la transformación continua que sus servicios van a requerir en un entorno en constante cambio.

“NIS2 va a poner ventanas muy exigentes para notificar brechas”

Hablamos con Agustín Valencia, responsable del negocio OT de Fortinet, sobre NIS2, la directiva de la Unión Europea que actualiza y refuerza las normas de ciberseguridad para un amplio espectro de sectores considerados esenciales para el funcionamiento de la sociedad y la economía. Entre las novedades de la normativa, destaca la responsabilidad de la dirección, que “está transformando radicalmente el ámbito competencial”, asegura el directivo, explicando que, lo que persigue NIS2 es que la ciberseguridad se lleve al negocio y que sea transversal. Que no sea algo del departamento de sistemas, del departamento de ciberseguridad”.

Rosalía Arroyo

Agustín Valencia, responsable del negocio OT de **Fortinet**

Esta nueva matriz de roles y responsabilidad es uno de los grandes retos que trae la normativa, asegura Agustín Valencia. Menciona un segundo desafío: “NIS2 abre un abanico muy interesante de lo que llaman las entidades importantes”, que son todas aquellas pertenecientes a sectores como la manufactura, alimentación o logística. Y el reto no sólo es entender que si tienes más de 50 empleados y facturas más de 10 millones eres entidad importante, sino que “plantea dificultades operativas para las entidades públicas porque ¿quién hace ese registro?”. Planteado cómo puede ayudar Fortinet a todas estas empresas a hacer frente a la normativa, destaca Agustín Valencia el valor de Fortinet Security Fabric, la plataforma de una compañía que ofrece desde la protección del endpoint

> “Orquestar adecuadamente todas esas herramientas es muy difícil si no hay una tecnología que permita coordinarlas”

a la de las redes, la protección del dato, de la nube, el control de usuario, el acceso remoto... "Orquestar adecuadamente todas esas herramientas es muy difícil si no hay una tecnología que permita coordinarlas", dice el directivo.

Comenta también Agustín Valencia que la compañía trabaja en plataformas de monitorización de seguridad, de detección avanzada contra el malware o de orquestación, "no solo para la respuesta ante incidentes, sino también para ayudar en la gobernanza y tomar información de todas esas otras herramientas que tú tienes para darte reportes adecuados de cómo estás", que es algo que también pedirá la normativa, dice el responsable del negocio de OT en Fortinet Iberia.

En general, Fortinet puede ayudar a las empresas "a tener información de tus proveedores y de tí mismo, de tu perímetro, de si has tenido una brecha de datos y que podamos decirte que tus datos se están poniendo en la dark web, en el mercado negro, y eso es el precursor de un ataque. Que podamos reaccionar antes de eso en nuestro entorno o con tu red de terceras partes, que es crítico".

Un tema que Agustín Valencia considera importantísimo de NIS2 es que "va a poner ventanas muy exigentes para notificar brechas". Por lo tanto, "si no tenemos herramientas bien desplegadas, si no tenemos equipos formados entre las distintas partes de la empresa, una coordinación adecuada, va a ser muy difícil, por no decir imposible, que podamos notificar en tiempo". Además de toda una batería de herramientas que no sólo protegen, sino ayudan a automatizar tareas, Fortinet pone a disposición de las empresas un blog en el que hay publicados varios artículos de NIS2, y de DORA también. Además, "estamos haciendo también eventos donde poder explicar de primera mano dónde podemos ayudar más aplicando una escala de madurez". Destaca como punto fuerte de la compañía el gran equipo humano que tiene así como "la cantidad de ingenieros para ayudar a solventar problemas, y ese ecosistema de part-

ners con los que poder dar una atención personalizada en cada proyecto a los clientes".

¿Estáis viendo alguna tendencia en el mercado de ciberseguridad, de ciberamenazas, que puede impactar directamente contra NIS2? Destaca como novedoso "cómo los atacantes están consiguiendo cada vez más disrupciones operativas, que se paren los negocios, porque eso es lo que duele y lo que obliga a pagar". No dice que no sea importante una brecha de datos, "pero que el ataque te pare la fábrica un día es muchísimo. Y ya no solo mi fábrica, es que si mi fábrica es proveedora de otra fábrica, empieza a haber un impacto en cadena. Y es en esa línea en la que yo creo que hay cierto consenso en que NIS2 lo que persigue es que elevar el nivel de seguridad en cada uno de los sectores".

Planteada durante la entrevista cómo evolucionará en los próximos años el panorama regulatorio, menciona que lo importante no es sólo lo que dice la norma, sino su aplicación. "No se va a conseguir eliminar todos los agentes de amenaza, pero en la medida en que las empresas demuestran esa diligencia en la toma de medidas, en la comunicación de la información de los incidentes, etcétera, eso va a ayudar a que el sector madure".

Agustín Valencia, responsable del negocio OT de **Fortinet**

¿Qué consejo le daría a aquellas personas que están ahora mismo haciendo frente a cómo adoptar NIS2? "Pues a mí me gusta el símil de la bicicleta. Si te paras, te caes. Tenemos que conseguir una velocidad, que es lo que nos va a mantener en ese equilibrio", responde Agustín Valencia. Comenta que aquellos que no han empezado, tiene que arrancar y que hay dejarse aconsejar; "hay partners muy expertos. Hay grandes empresas de ciberseguridad que podemos ayudar a cubrir este camino. No hay balas de plata, no hay una herramienta que lo solucione todo. Es una parte de tecnología, pero hay otra parte importantísima de procesos y personas".

“El principal objetivo de NIS es poner foco en la ciberseguridad en diferentes sectores críticos”

Explica durante esta entrevista Alberto López, vicepresidente de Soluciones de Ciberseguridad e Inteligencia Artificial de Mastercard, que una de las muchas cosas que cambia en NIS2 respecto a la primera versión de la normativa, “cuyo principal objetivo era poner foco en la ciberseguridad en diferentes sectores críticos”, es que el número de sectores críticos se amplía. Ahora hay 18 sectores críticos que deben poner foco en la ciberseguridad.

Rosalía Arroyo

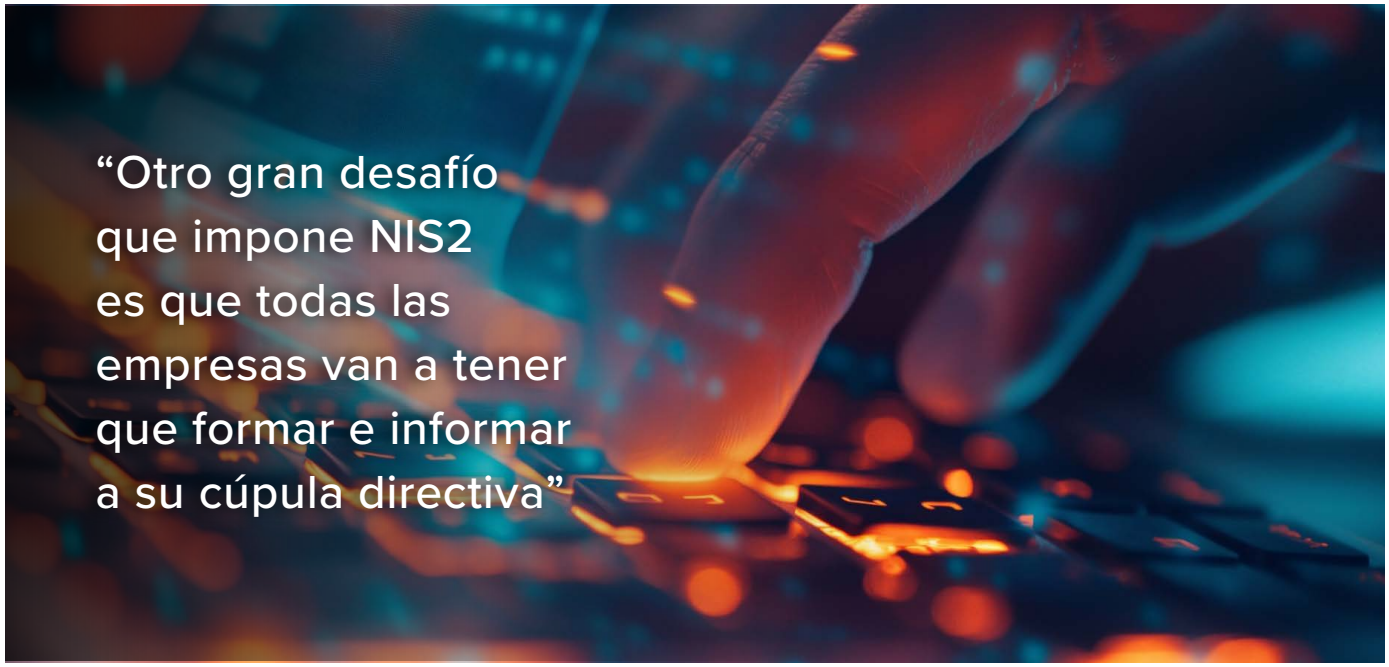
Alberto López, vicepresidente de Soluciones de Ciberseguridad e Inteligencia Artificial de **Mastercard**

Los ataques de ransomware y el malware son algunos de los grandes desafíos a los que se enfrentan las empresas, dice Alberto López, explicando que el 20 % de los ataques busca obtener datos financieros, pero también buscan datos personales (11 %) e incluso datos de propiedad intelectual (7 %). Añade que una de las novedades de NIS2 “tiene que ver con la cadena de suministro o la relación con partners y proveedores”, que es un aspecto que, hasta ahora, “se dejaba un poco olvidado desde el punto de vista ciberseguridad”.

> “La evaluación de riesgos sistémicos permite monitorizar y evaluar de manera proactiva el riesgo comercial complejo y en evolución en múltiples dimensiones”

Otro gran desafío que impone NIS2 es que “todas las empresas van a tener que formar e informar a su cúpula directiva”, porque “no hay que olvidar que la ciberseguridad es esencial y, si no tienes ciberseguridad, no vas a tener negocio”. Recuerda Alberto López que Mastercard no sólo protege y securiza los pagos, que hace tiempo

que la compañía ha ampliado su alcance para tener un enfoque más global; “es evidente que hay que proteger los pagos, pero también hay que proteger cuando un usuario hace un onboarding en un banco digital, o cuando uno hace login en tu página de un comercio, o cuando uno está realizando una transacción con la administración o con una empresa”, dice el directivo, mencionando que Mastercard “lleva trabajando más de diez años en el mundo de la inteligencia artificial para proteger nuestra red”. Habla de una inteligencia artificial que requiere de datos para ser entrenada y recuerda que, por la red de Mastercard pasan al año más de 143.000 millones de transacciones, millones de datos que permiten a la compañía identificar qué conversaciones son legítimas y cuales son un fraude. De manera más concreta: Masteraad monitoriza más de 13 millones de comercios de 40 sectores en más de 200 países para “ayudar en esa interacción con los proveedores o con los terceros”.



Oferta de ciberseguridad

La oferta de ciberseguridad de Mastercard es amplia. De cara a normativas como NIS2 o DORA cuenta la compañía con una suite de servicios que empiezan con una consultoría que ayuda a los clientes a entender cómo le afecta la normativa, o saber si sus sistemas están preparados o no. Teniendo claro el impacto de la normativa, se suman otros servicios, como Cyber Insights, que informa sobre cuáles son las tendencias en cuanto a ciberamenazas, cuáles son las nuevas vulnerabilidades; Cyber Front o CyberQuant.

Menciona también Alberto López la propuesta de RiskRecon, la empresa de gestión de riesgos que Mastercard compró a primeros de 2020 y que ayuda a saber “qué debo tener en cuenta de mis proveedores, cómo me relaciono con ellos, o con cuántos proveedores me relaciono”. Por último habla el directivo de Systemic Risk Assessment, que permite monitorizar y evaluar de manera proactiva el riesgo comercial complejo y en evolución en múltiples dimensiones, incluido el riesgo catastrófico, el riesgo cibernético, el riesgo geopolítico, el riesgo financiero y los riesgos de sanciones/restricciones en toda su red de relaciones comerciales, con el fin de

"tener un plan de acción en caso de que efectivamente algo de esto ocurra".

Evolución ciberamenazas

Tiene claro Alberto López que la Inteligencia Artificial tiene un impacto en la ciberseguridad en dos vertientes. Una que tiene que ver con las ciberamenazas "que pueden verse potenciadas por un mal uso de la inteligencia artificial". Al mismo tiempo, "la inteligencia artificial también nos ayuda a protegernos de esas ciberamenazas, y por eso Mastercard lleva ya diez años trabajando en ello".

Habla de una inteligencia artificial con gran capacidad de análisis, de ejecutarse de forma automática y en tiempo real para entender "quién está entrando y saliendo de tu red, hacer una autenticación en doble factor o multifactor y, sobre todo, analizar a tus proveedores".

Asegurando que la tecnología avanza y la normativa tiene que avanzar con ella, dice Alberto López que "en Europa estamos especialmente bien posicionados desde el punto de vista normativo". No solo menciona NIS2, sino DORA, PSD2 o MiCA, la primera norma a nivel global que regula el mercado de criptoactivos. ¿Qué va a ocurrir en los próximos años? "Pues veremos probablemente un NIS3, un DORA2, un MiCA 2, la PSD4... Es decir, eso va a seguir evolucionando y saldrán nuevas normativas que ayuden a que el ecosistema sea más seguro. Eso sin duda".

Alberto López, vicepresidente de Soluciones de Ciberseguridad e Inteligencia Artificial de **Mastercard**

Para acabar la entrevista pedimos a Alberto López algún consejo o mensaje para todas las empresas que están haciendo frente a la llegada de NIS2. Propone colocar la seguridad en la agenda de los directivos y que tanto el CEO como el responsable de finanzas de la compañía, "también tienen que estar perfectamente informados y formados sobre qué es esta normativa, cómo afecta al negocio y cuánto dinero tengo que invertir para que la normativa se pueda aplicar. Porque además esta nueva normativa viene de la mano de grandes multas".

“Nosotros ya sabemos que la prevención no es suficiente”

Asegurando que en Europa sabemos que NIS2 es importante para unificar criterios de cara a las ciberamenazas, comenta Adela de Toledo, country manager de Pure Storage para la región de Iberia, que, gracias a nuestro Esquema Nacional de Seguridad, estamos mejor preparados para cumplir con la normativa europea.

Rosalía Arroyo

Dice Adela de Toledo que el mercado de seguridad hace tiempo que está muy fragmentado, donde hay muchísimas soluciones y ha generado mucha complejidad, por lo que contar con una visibilidad que unifique y tenga en cuenta “todos los elementos que realmente son críticos para poder ser efectivos a la hora de poder detectar es tremendamente importante”. Las plataformas de almacenamiento de Pure Storage “están muy preparadas realizar analítica en tiempo real para la prevención”, asegura la directiva.

Pero “como nosotros ya sabemos que la prevención no es suficiente porque realmente todas las compañías están siendo atacadas”, la segunda parte de la propuesta de la compañía ofrece una solución al “qué tengo que hacer realmente cuando tengo un ataque”. Asegura que una estrategia de backup no es suficiente, y propone una arquitectura de tres capas “más preparada” para hacer frente a los ataques.

> “NIS2 es un avance interesante sobre la anterior porque, en un mercado tan dinámico, es bueno que la ciberseguridad esté unificada”

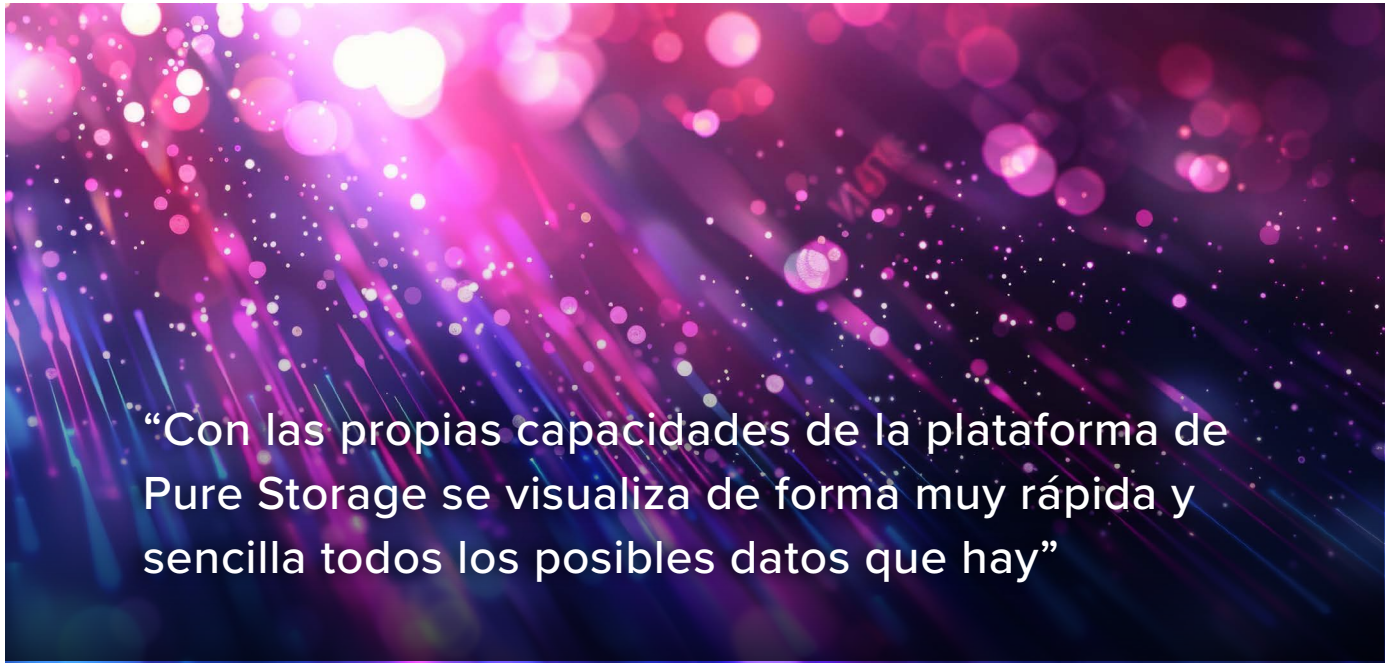
La primera capa de esa arquitectura “es de un almacenamiento primario, donde se tienen los datos de los últimos días, normalmente de tres a siete días”.

Adela de Toledo, country manager de **Pure Storage** para la región de Iberia

A la hora de hablar de la protección, menciona Adela de Toledo que, cuando se creó la compañía hace unos doce años ya se incorporaron de base y de manera muy sencilla, capacidades de protección. “Tenemos la habilidad, solo dando de alta una capacidad que ya existe, de guardar fotos de los datos, snapshots, que son inmutables; que no se pueden ni encriptar ni modificar”. Sobre esta capacidad, hay un proceso que se llama Safe Mode por el que “sólo se pueda acceder a esos datos cuando dos o tres personas del cliente, y dos o tres personas de nuestro soporte cruzan unas claves que previamente se han dado al poner en marcha esta funcionalidad”.

Se trata de una funcionalidad que permite que la recuperación sea ultrarrápida para que no haya riesgo reputacional, que es el objetivo final de la arquitectura en tres capas de la compañía.

La segunda capa que propone Pure Storage es especialmente interesante para realizar “tantos análisis como sea posible para investigar dónde pueden estar los errores”. Y la tercera capa, muy importante, es la capa de backup, “donde hay datos de larga retención, datos de muchos meses”, comenta Adela de Toledo añadiendo que,



“con nuestra estrategia de Safe Mode y con las propias capacidades de la plataforma de Pure Storage se visualiza de forma muy rápida y muy sencilla todos los posibles datos que hay”, lo que permiten realizar una “recuperación ordenada y rápida” gracias a los sistemas de almacenamiento de la compañía, Flash Array y Flash Blade, que no solo están preparados para guardar sino “para que tengan esa recuperación ultrarrápida que minimizar el riesgo reputacional”.

La protección moderna de datos, estrategia, plataformas y alianzas que ayudan y simplifican la aproximación a la hora de hacer frente a NIS2, es parte de la información que Pure Storage pone a disposición de sus clientes. Además, la compañía cuenta con “un equipo muy experto, tanto a nivel local como a nivel internacional, que atacan este problema y que ayudan a los clientes a navegar en esta complejidad alrededor de la seguridad”.

En busca de la simplicidad

Preguntada por lo que Pure Storage está observando en el mercado, asegura Adela de To-

> "Las plataformas de almacenamiento de Pure Storage están muy preparadas realizar analítica en tiempo real para la prevención"

Adela de Toledo, country manager de **Pure Storage** para la región de Iberia

ledo que "hace tiempo que sabemos que las compañías no invertían lo suficiente en seguridad, y desde los últimos tres, cuatro años, sí que estamos viendo que hay una mayor sensibilización, y mucho más presupuesto motivado por todos estos ataques que se están produciendo". Reconoce que los clientes son ahora mucho más conscientes y que "están clamando por soluciones muy sencillas y que sean cuanto más intrínsecas a las plataformas mejor".

Sobre la evolución del panorama regulatorio, tiene claro la directiva que NIS2 es "un avance interesante sobre la anterior" porque, en un mercado tan dinámico, es bueno que la ciberseguridad esté unificada. Menciona que los ataques se van a profesionalizar más, que van a ser mucho más complicados y que "la inteligencia artificial tiene que ser un elemento a nuestro favor, a favor de los que estamos previniendo y aliviando estos ataques".

Pedimos por último a Adela de Toledo un consejo para aquellos que se enfrenta al cumplimiento de NIS2. Apuesta porque se confíe en el mercado, donde hay "un grupo muy importante de profesionales que les pueden ayudar, muy preparados y con una estrategia". También recomienda que busquen "soluciones que sean sencillas de implementar en el menor tiempo posible. Que busquen la simplicidad en sus aproximaciones, porque cuando llega el momento de la recuperación el proceso tiene que ser muy sencillo y tiene que ser muy automático. Simplicidad". CST