Cumplimiento de la Directiva NIS2 con la Protección Total de la Información de SealPath.

Una guía completa con toda la información que necesitas para comprender la importancia de NIS2, sus requisitos y prepararte para el cumplimiento en tu organización con la ayuda de SealPath.

sealpath
Smart Protection for Sensitive Data

CYBERSECURITY™
MADE IN EUROPE

www.sealpath.com

sales@sealpath.com

INTRO: LA IMPORTANCIA DE ENTENDER LA DIRECTIVA NIS2

La Directiva NIS2 es una normativa crucial de la UE centrada en mejorar la seguridad de las redes y los sistemas de información, en línea con la rápida transformación digital y el panorama de amenazas. Es imprescindible que las entidades conozcan, comprendan y cumplan los requisitos de la NIS2. Aporta un nuevo conjunto de normas y requisitos de cumplimiento que todas las entidades aplicables deben cubrir.

Los riesgos de incumplimiento suponen pérdidas financieras importantes, ya que los incidentes de ciberseguridad tienen un coste medio de 4,45 millones de dólares (IBM Cost of a Data Breach Report 2023). Combinando terminología específica del sector y experiencia en seguridad de datos e identificación de riesgos, nuestra guía te ayudará a mantenerte informado y preparado, reforzando en última instancia tu defensa frente a las crecientes ciberamenazas y garantizando el cumplimiento de la normativa.

¿QUÉ ES LA DIRECTIVA NIS2?

La Directiva NIS2 se inspira en las bases sentadas por la NIS1, su precursora, y marca el camino hacia una normativa sólida en materia de ciberseguridad en toda la Unión Europea. Con los avances tecnológicos y las operaciones orientadas a los datos, se observa un aumento significativo de la complejidad de las operaciones cibernéticas.

Este cambio de paradigma ha dado lugar a una mayor interconectividad de los sistemas digitales, superando con creces los perímetros establecidos durante la creación de la NIS1.

La NIS2 se instigó como respuesta normativa para abordar este ámbito evolucionado de la ciberseguridad. Consciente de la expansión de la infraestructura digital en todos los sectores críticos, la UE puso en marcha esta normativa para hacer frente a los retos contemporáneos y proteger el panorama digital, salvaguardando así los intereses económicos y sociales.

OBJETIVO Y PROPÓSITO

El objetivo de la NIS2 es proporcionar un mayor nivel común de ciberseguridad en toda la UE, teniendo en cuenta la importancia vital de las redes y los sistemas de información para nuestras economías y sociedades. La Directiva engloba procedimientos que abarcan la gestión de riesgos, el tratamiento de incidentes y la seguridad de la cadena de suministro. Al reforzar la resiliencia frente a las amenazas a la ciberseguridad, pretende proteger el buen funcionamiento del mercado interior y la autonomía digital de la UE.

FECHA DE ENTRADA EN VIGOR

La fecha límite de la Directiva NIS2 para los Estados miembros es el 17 de octubre de 2024, lo que subraya la urgencia de cumplir los nuevos requisitos. Para ir por delante y evitar posibles sanciones, las empresas deben familiarizarse con la Directiva NIS2, realizar un análisis de brechas y trabajar continuamente en el desarrollo de una base de ciberseguridad sólida, que cumpla los estrictos criterios de la NIS2. Dado que la preparación es vital, las organizaciones deben actuar con urgencia y diligencia para mitigar los riesgos, proteger los datos y protegerse contra las ciberamenazas.

Figura 1.

¿A QUIÉN SE APLICA LA DIRECTIVA NIS2?

La Directiva NIS2 abarca un amplio abanico de proveedores de servicios y empresas de la UE, mucho más que su predecesora, la Directiva NIS. Es fundamental que todos los posibles afectados comprendan las implicaciones y ajusten sus medidas de ciberseguridad en consecuencia. Un engranaje esencial en la estructurada maquinaria de la infraestructura de la UE son los Operadores de Servicios Esenciales (OES).

La Directiva NIS2 amplía la definición y los criterios de inclusión de los OES, que ahora trascienden sectores como la energía, el transporte, la banca, las infraestructuras de los mercados financieros, la sanidad, el suministro de agua potable y las infraestructuras digitales.

Estas entidades deben aplicar medidas de gestión de riesgos adecuadas a los riesgos que puedan afectar a la seguridad de sus redes y sistemas de información. La gestión de riesgos incluye el empleo de protocolos eficaces de ciberseguridad, comprobaciones periódicas de la seguridad de los sistemas y mecanismos de notificación de incidentes. Las inspecciones de los operadores se realizarán a intervalos regulares para comprobar el cumplimiento de la normativa.

Figura 2.

PROVEEDORES Y EMPRESAS: EJEMPLOS

Caso 1: Empresa de Transporte

Bajo la directiva NIS2, una empresa transeuropea de transporte tuvo que reevaluar su infraestructura de ciberseguridad. Gracias a una detallada evaluación de riesgos, la empresa descubrió varias vulnerabilidades en sus sistemas heredados. Actualizaron su sistema, implantaron una gestión de accesos más estricta y crearon un sólido plan de respuesta contra posibles amenazas a la ciberseguridad. Con estos cambios, garantizaron el cumplimiento de la Directiva NIS2 y reforzaron su resiliencia operativa.

Caso 2: Operador Energético

Un operador regional de servicios energéticos de la UE fue identificado como OES en virtud de la Directiva NIS2. Emprendieron un análisis de brechas para determinar en qué aspectos sus operaciones no cumplían la normativa. En consecuencia, mejoraron sus sistemas de detección de violaciones de datos, reforzaron su infraestructura informática y formaron periódicamente a su personal en los últimos métodos de prevención de ciberamenazas. Sus acciones proactivas les permitieron no sólo cumplir la Directiva, sino también estar mejor equipados contra posibles ciberamenazas.

Estos casos ponen de relieve cómo los proveedores y las empresas afectadas por la Directiva NIS2 se están adaptando de forma proactiva al cambio en el panorama normativo, garantizando su continuidad empresarial y preservando la confianza de sus partes interesadas en el proceso.

¿CUÁLES SON LOS REQUISITOS PARA EL CUMPLIMIENTO DE NIS2?

Uno de los artículos más importantes a tener en cuenta por las entidades es el número 21, Medidas de gestión de riesgos de ciberseguridad. Las entidades esenciales e importantes deberán asegurarse de que adoptan medidas para gestionar el riesgo y prevenir el impacto de los incidentes mediante:

- Políticas de análisis de riesgos y seguridad de los sistemas de información;
- Gestión de incidentes;
- Continuidad de la actividad, como gestión de copias de seguridad y recuperación en caso de catástrofe, y gestión de crisis;
- Seguridad en la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores directos o proveedores de servicios;
- Seguridad en la adquisición, desarrollo y mantenimiento de redes y sistemas de la información, incluida la gestión y divulgación de vulnerabilidades;
- Políticas y procedimientos para evaluar la eficacia de las medidas de gestión de riesgos de ciberseguridad;
- Prácticas básicas de ciberhigiene y formación en ciberseguridad;
- Políticas y procedimientos relativos al uso de criptografía y, en su caso, cifrado.
- Seguridad de los recursos humanos, políticas de control de acceso y gestión de activos;
- Uso de soluciones de autenticación multifactor o autenticación continua.

Figura 3.

ANÁLISIS DE RIESGOS Y POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las organizaciones sujetas a la NIS2 deben llevar a cabo sesiones periódicas de análisis de riesgos en profundidad para evaluar la naturaleza y el nivel de las amenazas a las que se enfrentan su tecnología y sus datos, como se menciona en el artículo 21 «Medidas de gestión de riesgos de ciberseguridad». Este sólido análisis de riesgos alimenta una política global de seguridad de la información. La política debe articular, en términos claros, cómo se gestionará y mitigará cada riesgo, sirviendo de hoja de ruta para las prácticas de gestión de riesgos de su organización.

En el artículo 32, «Medidas de supervisión y ejecución en relación con las entidades esenciales», se establece que los países velarán por que las autoridades competentes, en el ejercicio de sus funciones de supervisión, estén facultadas para someter a dichas entidades, como mínimo, a:

- Inspecciones in situ y supervisión externa.
- Auditorías de seguridad periódicas y específicas.
- Auditorías ad hoc.
- Escaneos de seguridad.
- Solicitudes de información, incluidas las políticas de ciberseguridad documentadas.

GESTIÓN DE INCIDENTES (RESPUESTA A AMENAZAS, CONTINUIDAD DE LA ACTIVIDAD Y RECUPERACIÓN)

La directiva NIS2 obliga a las organizaciones a disponer de un proceso optimizado para la gestión de incidentes, que abarque desde la respuesta a las amenazas hasta la continuidad de la actividad y la recuperación. Para ello es necesario establecer procedimientos claros de detección y gestión de amenazas, un sólido plan de continuidad de la actividad que oriente las actuaciones durante las interrupciones del servicio y una estrategia de recuperación en caso de catástrofe en la que se esbocen las medidas de restauración tras el incidente.

SEGURIDAD DE LA CADENA DE SUMINISTRO (GESTIÓN DE RIESGOS ENTRE SOCIOS COMERCIALES Y PROVEEDORES, ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO SEGUROS)

La directiva NIS2 reconoce que la ciberseguridad es tan fuerte como el eslabón más débil de la cadena de suministro. Requiere una evaluación y gestión adecuadas de los riesgos que plantean los socios y proveedores.

Además, exige procedimientos seguros en la adquisición, desarrollo y mantenimiento de sistemas informáticos. Por lo tanto, es esencial imponer acuerdos contractuales claros sobre el cumplimiento de la seguridad, realizar auditorías de seguridad periódicas e impulsar prácticas de desarrollo seguras en toda la cadena de suministro.

Para navegar eficazmente por este laberinto de requisitos, las organizaciones deben adoptar diligentemente una postura proactiva, mejorando sus medidas de ciberseguridad, sus prácticas de gestión de riesgos y su garantía de calidad para el cumplimiento de la Directiva NIS2.

Figura 4.

ÁREAS CLAVE PARA EL CUMPLIMIENTO DE LA NIS2

Algunas áreas de interés son clave, pueden orientar el establecimiento de prioridades y la asignación de recursos, facilitando el camino a las organizaciones.

CIBER ESTRATEGIA/GOBERNANZA

En el rompecabezas NIS2, la ciber estrategia y la gobernanza son las piezas angulares. Unir los objetivos empresariales con las prerrogativas de ciberseguridad impulsa la formación de una ciber estrategia sólida. A continuación, una gobernanza cibernética eficaz garantiza que esta estrategia esté arraigada en las operaciones diarias de la organización. En el centro de todo ello se encuentra la gestión de riesgos, que traduce las amenazas cibernéticas en riesgos empresariales, los eleva al nivel de la junta directiva y garantiza que se aborden en consonancia con el apetito de riesgo de la organización. El consejo también debe difundir una cultura de ciberseguridad, fomentando el diálogo abierto sobre riesgos y contra medidas.

El artículo 20, «Gobernanza», establece que cada país «velará

por que los órganos de dirección de las entidades esenciales e importantes aprueben las medidas de ciberseguridad para cumplir el artículo 21, supervisen su aplicación y puedan ser considerados responsables de las infracciones». También dice que los países «velarán por que los miembros de los órganos de dirección de las entidades ofrezcan formación similar a sus empleados de forma periódica». La NIS2 ordena la ejecución de un marco general de gobernanza del ciber riesgo, estableciendo funciones, responsabilidades y vías de escalado específicas. Para las organizaciones, es una señal para mejorar su vigilancia cibernética y proteger sus operaciones y reputación.

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La información es la savia de las empresas modernas, y NIS2 hace hincapié en su gestión segura. Las organizaciones que cumplen la normativa deben mostrar procedimientos eficaces para la seguridad de la información, desde métodos de cifrado y canales seguros para la transmisión de datos hasta formación periódica en ciberseguridad para el personal. Las evaluaciones periódicas de riesgos, reforzadas por sólidos protocolos de autenticación y controles de acceso, mejoran aún más la seguridad de los datos. Los procedimientos de notificación de incidentes y las estrategias de respuesta eficaces constituyen aspectos cruciales de esta ecuación. En esencia, NIS2 aboga por una postura proactiva en la gestión de la seguridad de la información, haciendo hincapié en las medidas de seguridad preventivas frente a las reactivas, y pidiendo un cambio significativo en la forma en que las organizaciones ven la seguridad de la información. Un cambio que pase de ser una función de apoyo a ser una palanca estratégica para la continuidad y el crecimiento de la empresa.

CÓMO PREPARARSE PARA LA DIRECTIVA NIS2

El camino hacia el cumplimiento de NIS2 comienza con una visión estratégica y culmina con acciones tácticas bien planificadas. Sigue estos pasos para recorrer eficazmente este camino:

1. Comprende los requisitos de NIS2: Empiece por interiorizar lo esencial de la directiva. Comprender los requisitos en profundidad le ayudará a planificar mejor su estrategia de cumplimiento.

2. Establezca un equipo de cumplimiento interfuncional: Forme un equipo con las partes interesadas de las áreas clave de su organización. El cumplimiento no es una tarea aislada, sino que requiere un enfoque multidisciplinar.

3. Realice un análisis de brechas: Identifique cuál es la situación actual de su organización y cuál debe ser su situación con respecto a los requisitos de NIS2. El objetivo es poner de relieve las áreas de vulnerabilidad e incumplimiento.

4. Desarrolla una estrategia cibernética global y un marco de gobernanza: Tu estrategia debe centrarse en alinear las medidas de ciberseguridad con los objetivos empresariales, mientras que el marco de gobernanza establece funciones claras y vías de escalado.

5. Implantar prácticas sólidas de gestión de la seguridad de la información: Mejora las medidas de seguridad en la transmisión de datos, el cifrado, el control estricto del accesos, los procedimientos de notificación de incidentes y crea estrategias de respuesta potentes.

6. Mejora las medidas de seguridad de la cadena de suministro: Adopta normas estrictas de cumplimiento de la seguridad para socios o proveedores. También serán cruciales las auditorías periódicas y las estrategias seguras de adquisición y desarrollo de TI.

Figura 5.

7. Probar, revisar y mejorar: Por último, prueba periódicamente tus sistemas, revisa la eficacia de las medidas de seguridad y toma medidas proactivas para mejorar.

SEALPATH PARA EL CUMPLIMIENTO DE NIS2 Y MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

¿Qué es SealPath?

SealPath es líder en soluciones de protección de datos empresariales. Nos dedicamos a ayudar a las empresas para controlar y asegurar su información crítica a lo largo de todo su ciclo de vida de una forma sencilla y fácil de usar.

En palabras sencillas, gestionamos las identidades y el acceso a los documentos, los ciframos, gestionamos los permisos de

los usuarios y monitorizamos las acciones realizadas. Y todo ello independientemente de dónde se encuentre el archivo, para cualquier extensión de archivo.

La solución despliega una capa transparente de seguridad que viaja con los datos, garantizando su protección y controlando los permisos sobre ellos: sólo lectura, edición, impresión, copia y pegado...

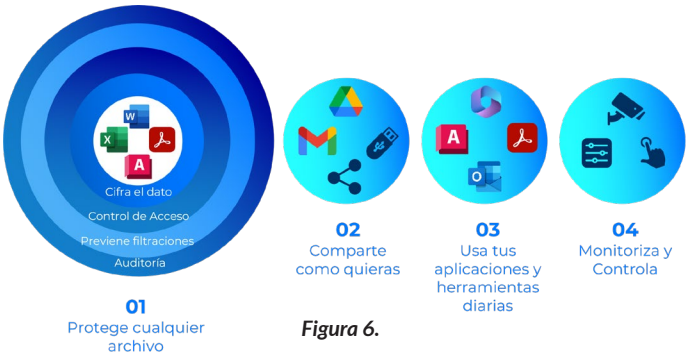

Figura 6.

¿En qué destaca SealPath?

1. Brechas y fugas de datos. Nos enfrentamos a dos tipos de actores, internos y externos, ya sean maliciosos o accidentales. Cualquiera de ellos puede extraer información sensible de muchas maneras, no podemos controlar todos los medios, redes, dispositivos, usuarios... Ya no hay perímetros.

Si se extrae un fichero no se puede acceder a él, o se puede retirar el acceso de forma remota y en tiempo real. SealPath protege la información y ayuda en la respuesta ante una violación de datos en cualquier situación o forma en la que se produzca.

Figura 7.

2. Visibilidad y control. La trazabilidad de los datos es esencial para poder actuar y controlar el uso que se hace de ellos. El control total permite actuar a tiempo y evitar consecuencias graves.

Accede a alertas e informes en tiempo real que identifican todos los eventos que se producen y ajusta los permisos de los ficheros para minimizar el riesgo. SealPath facilita el control por parte del departamento de TI.

3. Necesidades de infraestructura. Hay que tener en cuenta la flexibilidad, cada organización tiene sus propias características y las soluciones deben adaptarse a ellas, no las organizaciones a las soluciones.

Ya sea SaaS, MSSP, On-Premise o Híbrido, Sealpath se adapta a cada organización sin problemas. No te obliga a cambiar la infraestructura ni a afrontar engorrosos ajustes.

4. Complejidad diaria de gestión. Las medidas sólo son rentables y eficaces si se cumplen, y para ello deben ser fáciles de gestionar. Muchas soluciones no tienen en cuenta las responsabilidades y la carga de trabajo del área de IT.

La protección puede recaer en los responsables de cada departamento o en los usuarios, descargando a IT. SealPath es intuitivo, por lo que su gestión requiere muy pocos recursos.

Figura 8.

Uso de SealPath para NIS2

SealPath, con su avanzado conjunto de funcionalidades, se alinea a la perfección con los estrictos requisitos de la Directiva NIS2.

SealPath facilita el cifrado de datos, un aspecto explícitamente mencionado en la NIS2, dentro del artículo 21. SealPath protege tus datos sensibles de accesos no autorizados, asegurando que conservas el control total de tus datos.

Las medidas preventivas son una parte importante de los requisitos de NIS2. La protección dinámica de datos de SealPath, como los derechos de acceso granular, las fechas de caducidad, el bloqueo remoto de documentos y el acceso controlado, ofrecen una capa adicional de seguridad para sus datos y se alinean directamente con estas medidas. La facilidad de uso puede simplificar notablemente la tarea, normalmente compleja, de la protección de datos y la gestión de riesgos.

El mecanismo para facilitar el intercambio seguro de archivos que ofrece SealPath encaja perfectamente con el énfasis que pone NIS2 en los canales seguros para la transmisión de datos. Al mismo tiempo, las funcionalidades de colaboración garantizan la compatibilidad multiplataforma de los documentos protegidos, un activo fundamental en el actual panorama empresarial interconectado.

A continuación encontrarás una descripción detallada de las áreas más importantes en las que SealPath puede ayudar a tu organización.

Secciones	Cumplimiento con SealPath
Preámbulo 78 - La seguridad de las redes y los sistemas de información debe incluir la seguridad de los datos almacenados, transmitidos y procesados.	La protección de SealPath permite mantener a salvo la documentación en sus tres estados: En tránsito, en remoto y en uso. La protección viaja con el documento y lo acompaña allá donde viaje permitiendo al usuario trabajar con los datos, sabiendo que en caso que quiera, no tendrá el control total de los mismos.
Preámbulo 88 - Las entidades esenciales e importantes también deben abordar los riesgos derivados de sus interacciones y relaciones con otras partes interesadas dentro de un ecosistema más amplio, incluso con respecto a la lucha contra el espionaje industrial y la protección de los secretos comerciales.	SealPath te permite proteger tu documentación sensible y tus diseños CAD independientemente de su ubicación. Puedes controlar quién accede, cuándo y con qué permisos. SealPath ofrece una solución única para la protección de secretos comerciales y propiedad intelectual en forma de diseños CAD.
Preámbulo 89 - Adoptar prácticas básicas de ciberhigiene, como los principios de confianza cero, las actualizaciones de software, la configuración de dispositivos, la segmentación de redes, la gestión de identidades y accesos o la concienciación de los usuarios, organizar formaciones para su personal y concienciarlo sobre las ciberamenazas, el phishing o las técnicas de ingeniería social.	Las organizaciones tienen que aplicar los principios de confianza cero en la gestión de accesos, donde el acceso a los datos se limita a lo que se necesita durante el tiempo que se necesita. SealPath está perfectamente alineado con estos principios a través del control de acceso granular, áreas de confianza y segmentación. SealPath también mejora su cultura interna de seguridad de la información al concienciar al personal interno de que el control de la información es una cuestión crítica.
Preámbulo 98 - El uso de tecnologías de cifrado, en particular el cifrado de extremo a extremo, así como los conceptos de seguridad centrada en los datos...	SealPath es una solución centrada en la seguridad de los datos que ofrece una serie de funcionalidades para ayudar a proteger los datos en cualquier momento y lugar, lo que la convierte en una solución que cumple todos los requisitos de seguridad de los datos de la Directiva.
Art. 21.2 b) - Gestión de incidentes	SealPath proporciona capacidades de respuesta remota y en tiempo real para los archivos incluso después de que hayan salido de tu red, incluyendo la revocación del acceso a los usuarios deseados, el bloqueo de acceso por IP, el cambio de permisos e incluso el bloqueo de un archivo para que nadie pueda acceder a él. En caso de incidente, puede tomar medidas inmediatas y evitar consecuencias mayores.
Art. 21.2 d) - Seguridad de la cadena de suministro	Puedes controlar qué usuarios acceden a la información, revocar el acceso de forma inmediata y remota si deja de trabajar con un socio, y decidir quién puede y quién no puede acceder a su información confidencial. No importa con quién compartas archivos, siempre tendrás el control en toda la cadena de suministro.
Art. 21.2 g) - Prácticas básicas de ciberhigiene y formación en ciberseguridad.	Con SealPath, puedes llevar a cabo algunas prácticas básicas de ciberhigiene, como cifrar los datos corporativos allá donde vayan para garantizar su protección en reposo y en movimiento. También permite controlar el acceso a los datos identificando a los usuarios que intentan acceder. Permite el acceso remoto seguro a los archivos desde cualquier lugar. Sigue un enfoque de confianza cero.

Art. 21.2 h) - Políticas y procedimientos relativos al uso de criptografía y, en su caso, cifrado.	El artículo menciona expresamente el uso de criptografía y, en su caso, cifrado». SealPath no sólo gestiona los permisos de los ficheros, sino que además los encripta para que nadie ajeno a tu control pueda acceder a la información que contienen.
Art. 21.2 i) - Seguridad de los recursos humanos, políticas de control de accesos y gestión de activos.	Proporcionamos varias características para restringir el acceso y determinar quién está autorizado, tanto con usuarios internos como externos. SealPath permite la integración con Active Directory y la creación de permisos específicos para grupos de usuarios. Esto permite adaptar la seguridad a las necesidades de cada grupo de usuarios para que sólo tengan los permisos que necesitan para realizar sus tareas habituales, tal y como recomienda el marco de seguridad Zero Trust.
Art. 32 - Medidas de supervisión y cumplimiento en relación con las entidades esenciales	El artículo autoriza a las autoridades a realizar auditorías y revisiones de seguridad periódicas y ad hoc de las entidades esenciales, incluida la verificación de la presencia y aplicación de políticas de seguridad de los datos. Si se ha desplegado SealPath, las autoridades competentes verán que todos los datos sensibles están encriptados y protegidos, confirmando los esfuerzos realizados para asegurar los datos, por ejemplo, en caso de una violación de datos. Esto puede ayudarte a no ser sancionado.

SEGURIDAD DE LOS DATOS EN LA CADENA DE SUMINISTRO: ESTUDIO DE CASOS REALES

Caso 1: Multinacional del sector de las energías renovables

Líder mundial en energías renovables, abordó sus retos de seguridad de datos aprovechando las soluciones de SealPath. Tenían una necesidad acuciante: compartir y controlar de forma segura su documentación con propiedad intelectual con técnicos remotos. Su principal objetivo era compartir de forma eficiente la documentación crítica de la compañía con entidades externas, al tiempo que ejercían un control de acceso completo sobre los documentos compartidos. Utilizando SealPath, la organización garantizaba la seguridad y el control de los datos offline, incluso en ubicaciones remotas con conectividad limitada. SealPath jugó un papel vital en la gestión de las identidades y autenticación de usuarios externos en el sistema. Al adoptar la solución SaaS, la empresa ganó en seguridad y eficiencia operativa sin necesidad de una compleja configuración de infraestructura. Este caso pone de manifiesto cómo las soluciones flexibles y escalables de SealPath pueden ser fundamentales para garantizar el cumplimiento de directivas como NIS2 y subraya el camino hacia una mayor ciberseguridad.

Caso 2: Empresa multinacional del sector de los semiconductores

Una multinacional del sector de los semiconductores confió en las soluciones de protección de datos de SealPath para proteger sus archivos y documentos críticos. Al operar en un sector caracterizado por intrincadas cadenas de suministro y archivos CAD sensibles, la empresa buscaba un medio automático y eficaz para proteger sus activos confidenciales. Al almacenar documentos y archivos CAD sensibles en sitios de SharePoint y M365, la empresa garantizaba la seguridad al compartir interna y externamente. Mediante la implementación de las sofisticadas políticas de protección automáticas de SealPath en las carpetas sensibles, se aseguraron de que cada archivo cargado estuviera protegido al instante. Esta provisión automática protegía no sólo los archivos dentro de su red, sino que también garantizaba que los documentos permanecían seguros cuando eran descargados por terceros. El sistema, equipado con SealPath, permitía revocar el acceso en tiempo real, lo que permitía a la empresa revocar instantáneamente el acceso de forma remota. Con la capacidad de rastrear la actividad en tiempo real, la empresa mantuvo de forma eficaz un nivel superior de control sobre sus activos digitales.

BENEFICIOS

SealPath protege los datos no sólo dentro de tu red o perímetro, sino también cuando salen de tu red, ya sea con tus empleados o externamente. La seguridad se extiende sin importar dónde estén los datos.

Sencillo de implantar, robusto y fácil de usar. SealPath se alinea con tus procesos de negocio globales y asegura el futuro de tu organización, evitando la fuga de datos y ayudándote a cumplir con normativas como NIS2, DORA y GDPR:

1. **Protección avanzada de la información de forma sencilla, SealPath ofrece a tu organización el control sobre tus datos, ya sean de Office, diseños Cad, PDF o cualquier otra extensión de archivo.**
2. **Controles de monitorización y respuesta a incidentes en tiempo real, SealPath te permite revocar remotamente los permisos de un usuario que esté intentando acceder o ver tu información y proporciona informes detallados de quién está accediendo, cuándo y a qué información.**
3. **Despliegue y gestión eficientes, SealPath puede desplegarse de forma sencilla en SaaS u On-Premise y requiere una dedicación mínima de tiempo y recursos, sin impacto operativo.**
4. **Diseño intuitivo y fácil de usar, cada usuario puede proteger su información arrastrándola y soltándola en una carpeta local, en una carpeta de red, en la aplicación SealPath o simplemente asignando permisos por archivo de forma individual.**

Sobre SealPath

SealPath, empresa europea con sede en España y fundada en 2010, ayuda a clientes de más de 25 países en la seguridad de sus datos y desarrolla una fuerte apuesta en I+D para la mejora continua de sus soluciones. Más de 10 años dando servicio a algunas de las organizaciones más reconocidas del Euro Stoxx 50 y Fortune 500. Su galardonada solución cuenta con alrededor de 120 partners en todo el mundo en una extensa y sólida red de canal.