Microsoft Security

Prepararse para NIS2

Más que un ejercicio de cumplimiento: una oportunidad de preparar tu organización para el futuro

¿Qué es NIS2?

La Directiva sobre Redes y Sistemas de Información 2, comúnmente denominada NIS2, representa la legislación de la UE sobre ciberseguridad más completa que se haya visto nunca en la región. Prevista para entrar en vigor el 17 de octubre de 2024, **NIS 2 abarca 15 sectores y más de 160 000 empresas,** incluidas las de más de 250 empleados.

El objetivo de NIS2 es **establecer una base de medidas de ciberseguridad para las organizaciones que prestan servicios esenciales.** Esto incluye organizaciones de los sectores público y privado, en industrias que van desde las finanzas al transporte o la sanidad.

Prepararse para NIS2 exigirá que las empresas se replanteen las herramientas, los procesos y las aptitudes que refuerzan su ciberseguridad.

¿Por qué se ha incorporado NIS2?

NIS2, una importante actualización de la directiva NIS original, llega en un momento en que el **panorama europeo de las amenazas a la ciberseguridad sigue evolucionando con rapidez.**

Desde el comienzo de la guerra en Ucrania, han aumentado los ataques de estados-nación, según el informe de defensa digital de Microsoft. Estos agentes malintencionados se han vuelto más sofisticados y emplean tecnologías de automatización y acceso remoto para atacar a un conjunto más amplio de objetivos, a menudo a la búsqueda de un punto de entrada vulnerable en las cadenas de suministro de TI. Y, con frecuencia, dirigidos contra infraestructuras críticas.

De hecho, **el tiempo medio que tarda un atacante en empezar** a moverse en una red corporativa **es inferior a dos horas.**

¿Por qué debe NIS2 ser una prioridad?

NIS2 representa una oportunidad para que las organizaciones se aseguren de que cuentan con las personas, los procesos y los socios necesarios para **proteger las operaciones, garantizar la continuidad empresarial y facilitar la transformación digital.** Además, trabajar para garantizar el cumplimiento de NIS2 **contribuirá a generar confianza entre clientes, socios y accionistas.**

¿Qué puedo hacer como líder empresarial para asegurarme de que abordamos NIS2 de la manera más eficaz?

Aunque trabajar para lograr el cumplimiento con NIS2 requerirá una preparación y una colaboración minuciosas en toda la organización, los líderes pueden plantearse su enfoque a través de tres grandes principios: **Personas, Planificación y Socios.**

Microsoft Security

Personas

Transforma a tus empleados en defensores de la ciberseguridad

Cualquier esfuerzo de transformación que triunfe tiene que ver con las personas y la cultura empresarial tanto como con la tecnología. Optimizar tu ciberseguridad, y prepararte para NIS2, no es una excepción.. No se trata únicamente de una cuestión relegada al departamento de TI o a tu equipo de ciberseguridad. **Una seguridad eficaz requiere trabajo en equipo**, desde los trabajadores de la fábrica hasta los altos cargos.

La aptitud y la educación son componentes importantes para capacitar a tu personal. **La mayoría (62 %) de los ataques a la cadena de suministro es malware.** Y como la mayor parte de los ataques de malware se basa en ingeniería social, verás rápidamente por qué son tan importantes las personas.

Además, como el personal trabaja de forma más flexible, **las herramientas adecuadas pueden contribuir a protegerse contra las amenazas**, tanto si alguien está en la oficina como en casa o de viaje.

También es esencial pensar en la mejor forma de mejorar las aptitudes y la experiencia de tus equipos de ciberseguridad. En estos momentos, Europa se enfrenta a una escasez de unos 500 000 profesionales cualificados en ciberseguridad. Esto significa que a menudo los equipos no dan abasto.

Las **herramientas basadas en IA** ofrecen la oportunidad de **ayudar a los equipos de ciberseguridad a avanzar más deprisa** al mismo tiempo que minimizan la tensión.

1

Formación en ciberseguridad

Forma a los empleados en las prácticas recomendadas de ciberseguridad mediante rutas de aprendizaje de Microsoft 365 y Microsoft Defender para Office 365.

2

Procedimientos de seguridad para empleados

Controla el acceso a los datos confidenciales y vigila las amenazas internas con Azure Active Directory, Privileged Identity Management, Microsoft Information Protection y Microsoft Insider Risk Management.

3

Uso de la criptografía

Administración segura de claves y cifrado con Azure Key Vault y Microsoft Defender for Cloud.

4

Autenticación multifactor

Mejora la seguridad del inicio de sesión de los usuarios con la autenticación multifactor de Azure Active Directory.

5

Aumentar el talento en ciberseguridad

Security Copilot se basa en la inteligencia global sobre amenazas de Microsoft y en más de 65 billones de señales diarias. La herramienta proporciona información que mejora la calidad de la detección de amenazas y reduce los tiempos de respuesta.

Microsoft Security

Planificación

Elabora un plan para prevenir y responder a los incidentes

Las organizaciones inteligentes planifican adelantarse a los ataques. Pero también planifican el caso de que se produzcan filtraciones. Es importante tener en cuenta que **NIS2 exigirá que las empresas dispongan de planes** tanto para mitigar el riesgo como para gestionar los incidentes cuando se produzcan.

Adelantarse a los ataques requiere **conocer dónde hay vulnerabilidades** e **implementar protecciones en consecuencia.**

Evaluaciones de riesgos

Evalúa los riesgos y cumple la normativa mediante el Administrador de cumplimiento de Microsoft 365 y Microsoft Defender for Cloud.

Seguridad de la cadena de suministro

Protege los dispositivos y las redes contra los ataques a la cadena de suministro mediante Microsoft Defender para punto de conexión.

La planificación de contingencias implica implementar herramientas y procesos para proteger la continuidad empresarial. Significa **garantizar que la organización pueda informar de los incidentes con precisión** y a la máxima velocidad.

Gestión de incidentes de seguridad

Gestiona las alertas de seguridad con Microsoft Sentinel y los incidentes de seguridad de los datos con Microsoft Purview Information Protection e Insider Risk Management.

Continuidad empresarial

Garantiza las operaciones durante y después de incidentes de seguridad con Microsoft Azure Site Recovery and Backup.

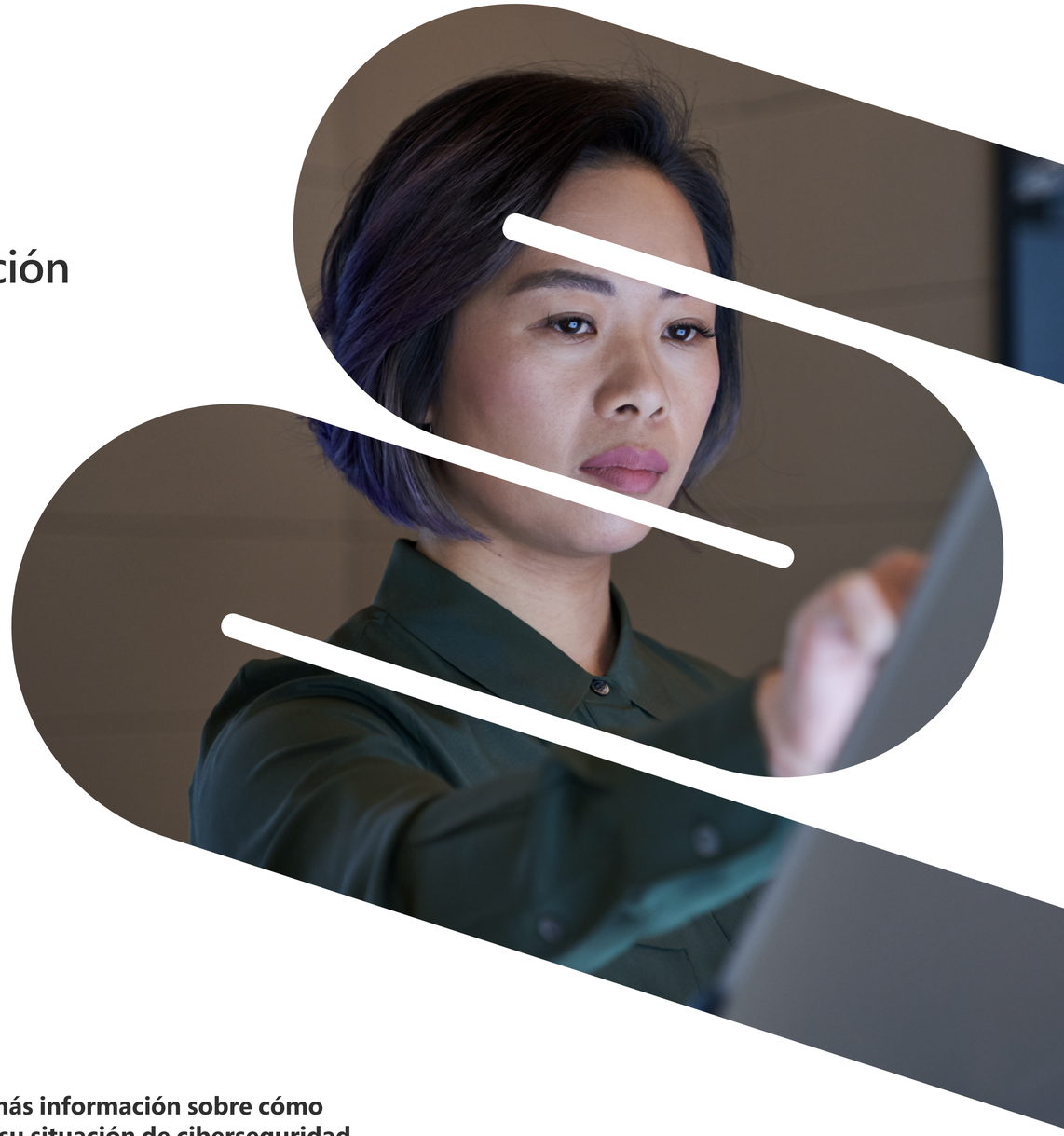
Microsoft Security

Socios

Forma equipo con un socio de confianza para mejorar tu situación de ciberseguridad

En el caso de las organizaciones que desean modernizar su enfoque de la ciberseguridad, **las alianzas son fundamentales**. A medida que evoluciona el panorama de las amenazas, ninguna organización puede mitigarlas eficazmente, ni garantizar la notificación precisa y oportuna de los incidentes, mientras funcione en un silo.

Trabajar con un proveedor de servicios de cloud de confianza representa un paso esencial para maximizar los controles de seguridad. **Microsoft adopta un enfoque «seguro por diseño»** con centros de datos reforzados, servicios administrados y mitigación predictiva de amenazas.



Conclusión: NIS2 no es únicamente un requisito normativo, **es una oportunidad para salvaguardar tu empresa, contribuir a proteger la soberanía de Europa y generar confianza con tus partes interesadas.**

Más de
$20
mil millones
invertidos

Microsoft tiene el compromiso de ayudar a aumentar la resistencia cibernética de nuestros clientes, con más de 20 000 millones de dólares invertidos **en investigación y desarrollo de tecnología de seguridad** y un equipo de profesionales de la ciberseguridad de primer nivel. Si trabajamos juntos, podemos ayudar a nuestros clientes a planificar NIS2, preparar a su personal y, en última instancia, mejorar su situación de ciberseguridad.

Ponte en contacto con tu equipo de la cuenta hoy mismo para obtener más información sobre cómo Microsoft puede ayudar a tu organización a cumplir con NIS2 y mejorar su situación de ciberseguridad.