WHITE PAPER

Liderando la respuesta ante la NIS2: **ASAC como aliado estratégico en Ciberseguridad**

asac

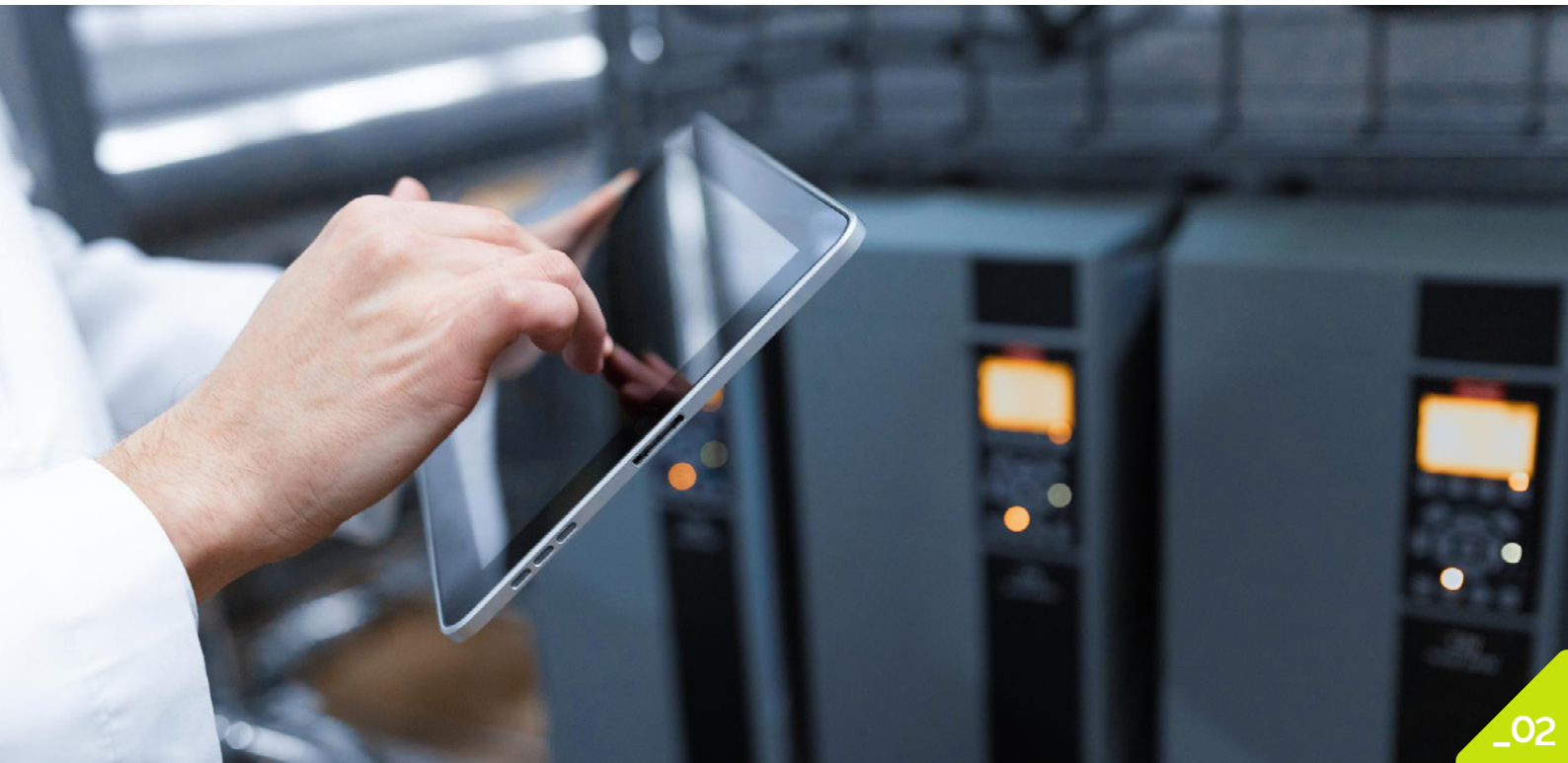
Tecnología para crecer

¿Qué es la normativa NIS2?

Con la evolución de las amenazas cibernéticas, la Unión Europea ha intensificado sus esfuerzos para proteger las infraestructuras críticas a través de la Directiva NIS2 (Network and Information Security). Esta normativa, que reemplaza la NIS original, amplía su alcance y refuerza los requisitos en gestión de ciberseguridad para empresas y organizaciones clave.

ASAC, como líder en ciberseguridad gestionada, se posiciona como un socio clave para la implementación y cumplimiento de la NIS2, pudiendo guiar a su organización en cuatro áreas clave:

1. **Gestión del riesgo.**
2. **Protección contra ciberataques.**
3. **Recuperación tras incidentes.**
4. **Concienciación en ciberseguridad.**
5. **Reporte de incidentes.**



¿A quién aplica?

— **Entidades esenciales de los sectores de:**

- **Energía** (sectores de electricidad, petróleo y gas).
- **Transporte.**
- **Salud** (hospitales, atención primaria y laboratorios de investigación).
- **Gestión de agua potable y aguas residuales.**
- **Banca y mercado financiero** (bolsas de valores y proveedores de servicios de pago).
- **Infraestructura crítica.**

— **Proveedores de servicios digitales:** servicios Cloud, Data Center, etc.

— **Administración Pública.**

Puntos clave

01. Gestión del riesgo

La NIS2 establece que las organizaciones deben implementar un enfoque proactivo en la gestión del riesgo, lo que implica identificar, evaluar y mitigar los riesgos cibernéticos antes de que puedan causar daños.

Es necesario realizar evaluaciones exhaustivas de vulnerabilidades y amenazas que afecten tanto a infraestructuras tecnológicas como a procesos internos. Utilizando metodologías avanzadas para:

- **Identificar puntos débiles en sus sistemas críticos y redes.**
- **Priorizar los riesgos según su impacto y probabilidad.**
- **Desarrollar planes de mitigación** adaptados a la naturaleza y complejidad de cada entorno.

02. Protección contra ciberataques

Uno de los principios fundamentales de la NIS2 es la **obligación de las organizaciones de proteger sus infraestructuras** de los ciberataques cada vez más sofisticados. Es necesario contar con soluciones integrales que fortalezcan las defensas de su empresa ante todo tipo de amenazas.

03. Recuperación tras incidentes

La resiliencia es clave en el contexto de la NIS2.

Las organizaciones deben contar con planes detallados de respuesta y recuperación ante incidentes para minimizar el impacto de un ataque cibernético. Es necesario disponer de un enfoque estructurado para segurar que su organización pueda recuperarse rápidamente de cualquier incidente.

04. Concienciación en ciberseguridad

La NIS2 pone un fuerte énfasis en la formación y concienciación en ciberseguridad, con el objetivo de fortalecer la cultura de seguridad dentro de las organizaciones.

05. Reporte de incidentes

Las entidades esenciales no están obligadas a avisar proactivamente del cumplimiento, a menos que las autoridades lo soliciten. Sin embargo, en caso de incidente de ciberseguridad, sí deben notificar a las autoridades y proporcionar información detallada posteriormente.

La Directiva obliga a detectar la incidencia y notificarla en un plazo de 24 horas al CSIRT y a los destinatarios de servicios que puedan verse afectados por el fallo de seguridad. Pasadas 72 horas, las empresas deben ser capaces de actualizar el estado del incidente y realizar una evaluación inicial del mismo. Transcurridos 30 días, las entidades deberán informar si la incidencia se ha resuelto, elaborando un informe final; o si siguen trabajando en ella, informando del destalle de la evolución.

ASAC, la respuesta eficiente a la NIS2

Herramientas y metodologías

Para una correcta gestión del riesgo, ASAC emplea tecnologías de vanguardia y marcos de referencia reconocidos internacionalmente (como ISO/IEC 27001 e ITIL) para implementar soluciones a medida que cubren:

- **Monitoreo continuo:** A través de soluciones RMM y SIEM, ASAC puede ofrecer una supervisión ininterrumpida de los activos críticos.
- **Evaluaciones periódicas:** Se realizan análisis de riesgos de manera periódica para mantener la seguridad al ritmo de los cambios tecnológicos y las nuevas amenazas.

Enfoque de protección multicapa

ASAC ofrece una estrategia de defensa en profundidad que incluye las siguientes capas de protección:

- **Cortafuegos de última generación y soluciones de seguridad perimetral:** Para proteger las redes frente a accesos no autorizados.
- **Protección de endpoints:** Con herramientas optimizadas para el rendimiento en entornos virtuales.
- **Seguridad de la nube y los sistemas distribuidos:** Asegurando que las arquitecturas cloud, redes híbridas y servicios remotos estén correctamente protegidos.
- **Soluciones de respuesta automática ante incidentes (EDR):** Con tecnología avanzada de detección y respuesta para actuar de manera inmediata ante cualquier intrusión.

Servicios de recuperación

ASAC se especializa en:

- **Planes de recuperación ante desastres:** Diseñados para restaurar servicios críticos en el menor tiempo posible.
- **Recuperación de datos:** Asegurando la disponibilidad de copias de seguridad actualizadas y soluciones de almacenamiento seguro.
- **Evaluación post-incidente:** Análisis exhaustivo de las causas del incidente para evitar recurrencias y mejorar las defensas existentes.

Soluciones de continuidad del negocio

ASAC colabora estrechamente con su equipo para implementar planes de continuidad del negocio, asegurando que los sistemas esenciales puedan seguir operando incluso en caso de interrupciones graves.

Capacitación y simulaciones

ASAC proporciona:

- **Formación personalizada:** Programas adaptados al nivel de conocimiento del personal y las necesidades específicas de cada empresa.
- **Simulacros de phishing y ejercicios de respuesta a incidentes:** Para que el personal esté preparado para identificar y reaccionar ante intentos de ciberataques.

Políticas y procedimientos

ASAC trabaja con su organización para desarrollar políticas de ciberseguridad robustas y procedimientos claros que todos los empleados deben seguir, asegurando que la seguridad no sea una barrera, sino una parte integrada del día a día.

Equipo comprometido y altamente cualificado

En ASAC contamos con un equipo de consultores altamente especializados en ciberseguridad y cumplimiento normativo, que están preparados para guiar a su organización en cada fase de la implementación de la NIS2. Desde la gestión del riesgo hasta la formación en ciberseguridad, nuestro equipo está comprometido a proporcionar soluciones a medida que cumplan con los más altos estándares del mercado.

Para obtener más información sobre cómo ASAC puede ayudarle a fortalecer su estrategia de ciberseguridad y cumplir con la normativa NIS2, no dude en contactar con nosotros. Nuestro equipo estará encantado de atender cualquier consulta y brindarles la mejor solución adaptada a sus necesidades.