Ciberseguridad industrial

GUÍA SOBRE NIS2

¿Sabes que quedan pocos meses para que entre en vigor la transposición de la directiva NIS2 en España?

No esperemos al final, porque una vez traspuesta, empezará a aplicar al día siguiente. Te vamos avanzando las claves para ayudarte.

01

La nueva directiva NIS2 de ciberseguridad: Infracciones e impacto para los directivos de las empresas

La nueva directiva NIS2 refuerza la ciberseguridad

Una nueva directiva de ciberseguridad con acciones ante infracciones e impacto para los cargos directivos.

En **enero de 2023** se promulga una **nueva directiva NIS** (siglas de seguridad de sistemas de redes y de información: Network and Information Systems) a través del Reglamento ((UE) 2022/2555), la llamada NIS2, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión y que deroga a la anterior directiva NIS ((UE) 2016/1148). La fecha máxima para que sea traspuesta al ordenamiento jurídico español es el 17 de octubre de 2024.

Esta nueva directiva viene a reforzar los anteriores requisitos de la NIS1, para poder dar una mejor respuesta al creciente panorama de amenazas en los sistemas de redes y de información, de los que cada vez la sociedad es más dependiente. Además de que va a incluir **acciones contra las infracciones**, para endurecer el carácter disuasorio de estas acciones, las autoridades competentes estarán facultadas para llevar a cabo acciones de **suspensión de certificaciones o incluso servicios y prohibir temporalmente que una persona física ejerza funciones de dirección** a nivel de director general o representante legal. Es decir, el mensaje es que hay que anticiparse y empezar a trabajar ya, porque las consecuencias van un paso más allá que la anterior directiva.

NIS2 amplía su alcance

El ámbito de aplicación puede afectar a los entornos industriales OT y a dispositivos IoT.

Uno de los aspectos en los que se diferencia de la NIS1 es su **ámbito de aplicación**. Si bien la NIS1 estaba básicamente reservada para entidades formalmente designadas como proveedores de servicios esenciales dentro de diferentes sectores críticos, **la NIS2 abre el abanico**. En este sentido la NIS2 va a aplicar a medianas y grandes empresas de sectores críticos y a otras entidades que, con independencia de su tamaño, cumplan con ciertas características como, por ejemplo:

- Que presten servicios específicos (tales como los prestadores de servicios de confianza o de DNS),
- Que sean el único proveedor que preste un servicio esencial en un estado miembro
- Que sean una entidad crítica formalmente designada

Dentro de los sectores de aplicación, podemos encontrarnos con algunos que incluyen **tecnologías de operación** (lo que denominamos comúnmente con las siglas **OT**, del inglés “Operation Technologies”, frente a los sistemas de información o corporativos, denominados IT, del inglés “Information Technologies”). Además, estarían los **dispositivos IoT**, no menos importantes, y que también estarían en el ámbito al que se dirige los requisitos de protección de esta directiva.

02

NIS2 amplía su alcance

Sectores afectados

Sectores de alta criticidad		Otros sectores críticos	
	Energía		Servicios postales y de mensajería
	Transporte		Gestión de residuo
	Banca		Fabricación, producción y distribución de sustancias y mezclas químicas
	Infraestructuras de los mercados financieros		Producción, transformación y distribución de alimentos
	Sector sanitario		Fabricación
	Agua potable		Proveedores de servicios digitales
	Aguas residuales		Investigación
	Infraestructura digital		
	Gestión de servicios de TIC (de empresa a empresa)		
	Entidades de la Administración pública, con exclusión del poder judicial, los parlamentos y los bancos centrales		
	Espacio		

Sectores de alta criticidad

Sector	Subsector	Tipo de entidad
1. Energía	a) Electricidad	Empresas eléctricas, tal como se definen en el artículo 2, punto 57, de la Directiva (UE) 2019/944 del Parlamento Europeo y del Consejo, que efectúan la función de «suministro», tal como se define en el artículo 2, punto 12, de dicha Directiva
		Gestores de la red de distribución, tal como se definen en el artículo 2, punto 29, de la Directiva (UE) 2019/944
		Gestores de la red de transporte, tal como se definen en el artículo 2, punto 35, de la Directiva (UE) 2019/944
		Productores, tal como se definen en el artículo 2, punto 38, de la Directiva (UE) 2019/944
		Operadores designados para el mercado eléctrico, tal como se definen en el artículo 2, punto 8, del Reglamento (UE) 2019/943 del Parlamento Europeo y del Consejo Participantes en el mercado de la electricidad, tal como se definen en el artículo 2, punto 25, del Reglamento (UE) 2019/943 que pres ten servicios de agregación, respuesta de demanda o almacenamiento de energía, tal como se define en el artículo 2, puntos 18, 20 y 59, de la Directiva (UE) 2019/944 Operadores de un punto de recarga que sean responsable de la gestión y explotación de un punto de recarga, que presta un servicio de recarga al usuario final también en nombre y por cuenta de un proveedor de servicios de movilidad
	b) Sistemas urbanos de calefacción y de refrigeración	Operadores de sistemas urbanos de calefacción o de refrigeración, tal como se definen en el artículo 2, punto 19, de la Directiva (UE) 2018/2001 del Parlamento Europeo y del Consejo
	c) Crudo	Operadores de oleoductos de transporte de crudo
		Operadores de producción de crudo, instalaciones de refinado y tratamiento, almacenamiento y transporte
		Entidades centrales de almacenamiento, tal como se definen en el artículo 2, letra f), de la Directiva 2009/119/CE del Consejo
	d) Gas	Empresas suministradoras de gas, tal como se definen en el artículo 2, punto 8, de la Directiva 2009/73/CE del Parlamento Europeo y del Consejo
		Gestores de la red de distribución, tal como se definen en el artículo 2, punto 6, de la Directiva 2009/73/CE
		Gestores de la red de transporte, tal como se definen en el artículo 2, punto 4, de la Directiva (UE) 2009/73/CE
		Gestores de almacenamientos, tal como se definen en el artículo 2, punto 10, de la Directiva 2009/73/CE
		Gestores de la red de GNL, tal como se definen en el artículo 2, punto 12, de la Directiva 2009/73/CE
		Compañías de gas natural, tal como se definen en el artículo 2, punto 1, de la Directiva 2009/73/CE
		Operadores de instalaciones de refinado y tratamiento de gas natural
	e) Hidrógeno	Operadores de producción, almacenamiento y transporte de hidrógeno

Sector	Subsector	Tipo de entidad
2. Transporte	a) Transporte aéreo	Compañías aéreas, tal como se definen en el artículo 3, punto 4, del Reglamento (CE) n.o 300/2008 utilizadas con fines comerciales
		Entidades gestoras de aeropuertos, tal como se definen en el artículo 2, punto 2, de la Directiva 2009/12/CE del Parlamento Europeo y del Consejo; aeropuertos, tal como se definen en el artículo 2, punto 1, de dicha Directiva, en particular los aeropuertos de la red básica enumerados en el anexo II, sección 2, del Reglamento (UE) n.o 1315/2013 del Parlamento Europeo y del Consejo; y entidades que explotan instalaciones anexas dentro de los recintos de los aeropuertos
		Operadores de control de la gestión del tráfico que prestan servicios de control del tránsito aéreo, tal como se definen en el artículo 2, punto 1, del Reglamento (CE) n.o 549/2004 del Parlamento Europeo y del Consejo
	b) Transporte por ferrocarril	Administradores de infraestructuras, tal como se definen en el artículo 3, punto 2, de la Directiva 2012/34/UE del Parlamento Europeo y del Consejo
		Empresas ferroviarias, tal como se definen en el artículo 3, punto 1, de la Directiva 2012/34/UE, incluidos los explotadores de instalaciones de servicio, tal como se definen en el artículo 3, punto 12 de dicha Directiva
	c) Transporte marítimo y fluvial	Empresas de transporte marítimo, fluvial y de cabotaje, tanto de pasajeros como de mercancías, tal como se definen para el transporte marítimo en el anexo I del Reglamento (CE) n.o 725/2004 del Parlamento Europeo y del Consejo, sin incluir los buques particulares explotados por esas empresas
		Organismos gestores de los puertos, tal como se definen en el artículo 3, punto 1, de la Directiva 2005/65/CE del Parlamento Europeo y del Consejo, incluidas sus instalaciones portuarias, tal como se definen en el artículo 2, punto 11, del Reglamento (CE) n.o 725/2004, y entidades que operan obras y equipos que se encuentran en los puertos
		Operadores de servicios de tráfico de buques (STB), tal como se definen en el artículo 3, letra o), de la Directiva 2002/59/CE del Parlamento Europeo y del Consejo
	d) Transporte por carretera	Autoridades viarias, tal como se definen en el artículo 2, punto 12, del Reglamento Delegado (UE) 2015/962 de la Comisión responsables del control de la gestión del tráfico, excluidas las entidades públicas para las cuales la gestión del tráfico o la explotación de sistemas de transporte inteligentes sea una parte no esencial de su actividad general
		Operadores de sistemas de transporte inteligentes, tal como se definen en el artículo 4, punto 1, de la Directiva 2010/40/UE del Parla mento Europeo y del Consejo
3. Banca		Entidades de crédito, tal como se definen en el artículo 4, punto 1, del Reglamento (UE) n.o 575/2013 del Parlamento Europeo y del Consejo
4. Infraestructuras de los mercados financieros		Gestores de centros de negociación, tal como se definen en el artículo 4, punto 24, de la Directiva 2014/65/UE del Parlamento Europeo y del Consejo
		Entidades de contrapartida central (ECC), tal como se definen en el artículo 2, punto 1, del Reglamento (UE) n.o 648/2012 del Parlamento Europeo y del Consejo
5. Sector sanitario		Prestadores de asistencia sanitaria, tal como se definen en el artículo 3, letra g), de la Directiva 2011/24/UE del Parlamento Europeo y del Consejo
		Laboratorios de referencia de la UE, tal como se definen en el artículo 15, del Reglamento (UE) .../...del Parlamento Europeo y del Consejo
		Entidades que realizan actividades de investigación y desarrollo de medicamentos, tal como se definen en el artículo 1, punto 2, de la Directiva 2001/83/CE del Parlamento Europeo y del Consejo Entidades que fabrican productos farmacéuticos de base y especialidades farmacéuticas a que se refiere la sección C, división 21, de la NACE Rev. 2 Entidades que fabrican productos sanitarios que se consideran esenciales en situaciones de emergencia de salud pública («lista de productos sanitarios esenciales durante la emergencia de salud pública») en el sentido del artículo 22 del Reglamento (UE) 2022/123 del Parlamento Europeo y del Consejo
6. Agua potable		Suministradores y distribuidores de aguas destinadas al consumo humano, tal como se definen en el artículo 2, punto 1, letra a), de la Directiva (UE) 2020/2184 del Parlamento Europeo y del Consejo, excluidos los distribuidores para los que la distribución de aguas destinadas al consumo humano sea una parte no esencial de su actividad general de distribución de otros bienes y productos básicos

Sector	Subsector	Tipo de entidad
7. Aguas residuales		Empresas dedicadas a la recogida, la eliminación o el tratamiento de aguas residuales urbanas, domésticas o industriales, tal como se definen en el artículo 2, puntos 1 a 3, de la Directiva 91/271/CEE del Consejo, excluidas las empresas para las que la recogida, la eliminación o el tratamiento de aguas residuales urbanas, domésticas o industriales sea una parte no esencial de su actividad general
8. Infraestructura digital		Proveedores de puntos de intercambio de internet
		Proveedores de servicios de DNS, excluidos los operadores de servidores raíz
		Registros de nombres de dominio de primer nivel
		Proveedores de servicios de computación en nube
		Proveedores de servicios de centro de datos
		Proveedores de redes de distribución de contenidos
		Prestadores de servicios de confianza
		Proveedores de redes públicas de comunicaciones electrónicas
		Proveedores de servicios de comunicaciones electrónicas disponibles para el público
9. Gestión de servicios de TIC (de empresa a empresa)		Proveedores de servicios gestionados Proveedores de servicios de seguridad gestionados
10. Entidades de la Administración pública, con exclusión del poder judicial, los parlamentos y los bancos centrales		Entidades de la Administración pública central, tal como se definen en el Estado miembro con arreglo a las disposiciones del Derecho nacional
		Entidades de la Administración pública a escala regional, según su definición en el Estado miembro con arreglo a las disposiciones del Derecho nacional
11. Espacio		Operadores de infraestructuras terrestres, cuya propiedad, gestión y explotación descansa en los Estados miembros o en entidades privadas, que apoyan la prestación de servicios espaciales, excepto los proveedores de redes públicas de comunicaciones electrónicas

Otros sectores críticos

Sector	Subsector	Tipo de entidad
1. Servicios postales y de mensajería		Proveedores de servicios postales, tal como se definen en el artículo 2, punto 1 bis, de la Directiva 97/67/CE, incluidos los proveedores de servicios de mensajería
2. Gestión de residuos		Empresas que realizan la gestión de residuos, tal como se definen en el artículo 3, punto 9, de la Directiva 2008/98/CE del Parlamento Europeo y del Consejo, excepto aquellas para las que la gestión de residuos no es su principal actividad económica
3. Fabricación, producción y distribución de sustancias y mezclas químicas		Empresas que realizan la fabricación de sustancias y la distribución de sustancias o mezclas, tal como se definen en el artículo 3, puntos 9 y 14, del Reglamento (CE) n.o 1907/2006 del Parlamento Europeo y del Consejo y empresas que realizan la producción de artículos, tal como se definen en el artículo 3, punto 3, de dicho Reglamento, a partir de sustancias y mezclas
4. Producción, transformación y distribución de alimentos		Empresas alimentarias, tal como se definen en el artículo 3, punto 2, del Reglamento (CE) n.o 178/2002 del Parlamento Europeo y del Consejo, que se dediquen a la distribución al por mayor y a la producción y transformación industriales
5. Fabricación	a) Fabricación de productos sanitarios y productos sanitarios para diagnóstico in vitro	Entidades que fabrican los productos sanitarios, tal como se definen en el artículo 2, punto 1, del Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, y entidades que fabrican los productos sanitarios para diagnóstico in vitro, tal como se definen en el artículo 2, punto 2, del Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, excepto las entidades que fabrican productos sanitarios a que se refiere el anexo I, punto 5, quinto guion, de la presente Directiva
	b) Fabricación de productos informáticos, electrónicos y ópticos	Empresas que realizan cualquiera de las actividades económicas a que se refiere la sección C, división 26, de la NACE Rev. 2
	c) Fabricación de material eléctrico	Empresas que realizan cualquiera de las actividades económicas a que se refiere la sección C, división 27, de la NACE Rev. 2
	d) Fabricación de maquinaria y equipo n.c.o.p.	Empresas que realizan cualquiera de las actividades económicas a que se refiere la sección C, división 28, de la NACE Rev. 2
	e) Fabricación de vehículos de motor, remolques y semirremolques	Empresas que realizan cualquiera de las actividades económicas a que se refiere la sección C, división 29, de la NACE Rev. 2
	f) Fabricación de otro material de trans porte	Empresas que realizan cualquiera de las actividades económicas a que se refiere la sección C, división 30, de la NACE Rev. 2
6. Proveedores de servicios digitales		Proveedores de mercados en línea
		Proveedores de motores de búsqueda en línea
		Proveedores de plataformas de servicios de redes sociales
7. Investigación		Organismos de investigación

03

Requisitos de seguridad: más allá de las medidas puramente técnicas

Requisitos de seguridad: más allá de las medidas puramente técnicas.

Los requisitos de carácter técnico-organizativo son los recogidos en el artículo 21 de la directiva, a saber:

- Las políticas de seguridad de los sistemas de información y análisis de riesgos;
- La gestión de incidentes;
- La continuidad de las actividades, como la gestión de copias de seguridad y la recuperación en caso de catástrofe, y la gestión de crisis;
- La seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores o prestadores de servicios directos;
- La seguridad en la adquisición, el desarrollo y el mantenimiento de sistemas de redes y de información, incluida la gestión y divulgación de las vulnerabilidades;
- Las políticas y los procedimientos para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad;
- Las prácticas básicas de ciberhigiene y formación en ciberseguridad;
- Las políticas y procedimientos relativos a la utilización de criptografía y, en su caso, de cifrado;
- La seguridad de los recursos humanos, las políticas de control de acceso y la gestión de activos;
- El uso de soluciones de autenticación multifactorial o de autenticación continua, comunicaciones de voz, vídeo y texto seguras y sistemas seguros de comunicaciones de emergencia en la entidad, cuando proceda.

04

Adoptando un enfoque eficaz

Ciberseguridad industrial y NIS2.

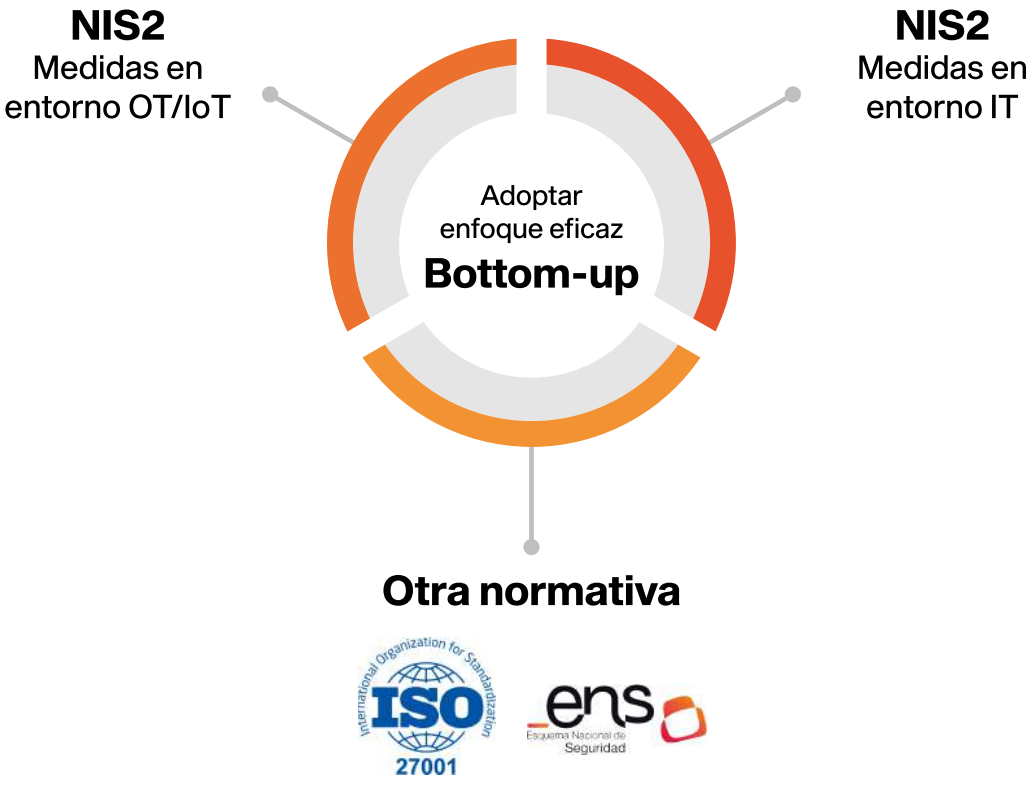
Adoptando un enfoque eficaz.

En 2023, la Unión Europea lanzó una nueva normativa conocida como NIS 2, la cual tiene como objetivo **fortalecer la ciberseguridad en sectores críticos y servicios digitales esenciales**. Esta directiva, que viene a suceder a la anterior NIS, introduce una serie de requisitos técnico-organizativos destinados a proteger los entornos de tecnología operativa (OT) e Internet de las cosas (IoT).

Una de las principales **dificultades que enfrentan las organizaciones** con la implementación de la NIS 2 es la necesidad de adaptar los requisitos técnico-organizativos a la **heterogeneidad de elementos presentes en los entornos IT/OT/IoT**. Esto implica comprender las particularidades de cada uno de estos entornos e integrarlos de manera coherente y eficaz en el marco regulatorio establecido por la directiva.

Por otro lado, es crucial considerar otras **normas o estándares de ciberseguridad que puedan ser aplicables a la organización**, con el fin de evitar la duplicación de esfuerzos en la implementación y mantenimiento de medidas de seguridad.

Evitar la duplicación de esfuerzos en la implementación es la clave de un enfoque eficaz.



Ante este escenario complejo, surge la necesidad de adoptar **un enfoque bottom-up y de mejora continua en la implementación de la NIS 2**. Este enfoque implica comenzar desde el análisis detallado de los riesgos y vulnerabilidades específicos de cada entorno, para luego desarrollar e implementar medidas de seguridad adecuadas. Además, promueve la revisión y actualización periódica de estas medidas en respuesta a los cambios en el panorama de amenazas cibernéticas y a la evolución de los entornos tecnológicos.

Bottom-up | Desarrollo e implementación.

Al adoptar este enfoque, las organizaciones pueden garantizar una mayor eficacia y sostenibilidad en su estrategia de ciberseguridad, así como una mejor preparación para hacer frente a los desafíos del futuro digital.

05

Diseñando la hoja de ruta

Identificar los activos y analizar su estado

En esta sección, nos centraremos en la fase de planificación, es decir, por qué es fundamental diseñar un plan adecuado y cuáles son los requisitos que deberían contemplarse. La fase de planificación de la ciberseguridad en entornos OT/IoT para cumplir con NIS2 es la base de la implementación: un buen plan con orientación a gestión de riesgos es la clave del éxito de las siguientes fases.

Para planificar, primero hay que identificar. Lo que no está identificado no se protegerá.

Para realizar un buen plan de adecuación la primera acción es identificar los elementos IT/OT/IoT afectados por la directiva (activos). Esta identificación será más o menos compleja dependiendo de la dimensión del parque de activos y del grado de madurez que la organización tenga en materia de gestión de activos IT/OT/IoT. En este sentido nos podemos encontrar una casuística variada: organizaciones en las que los inventarios están en “las cabezas” de unos cuantos técnicos, organizaciones en la que hay ciertos inventarios realizados manualmente, pero no necesariamente completos ni actualizados; y otras organizaciones, las más maduras, en la que sí hay inventarios formales, es decir, completos y actualizados.

El riesgo de que los activos no estén identificados es que no se tengan en cuenta en el plan, es decir, lo que no se identifique ahora no se protegerá después (y lo que no se proteja después podrá derivar en incumplimientos, por no decir en ciberincidentes).

¿Y cómo inventariamos?

Identificar = Inventariar

Algunas buenas prácticas son:

- **Inventariar las diferentes clases de activos**, no solo el hardware o software, es decir, los datos, redes, soportes de información y, por supuesto los elementos OT/IoT como como PLCs, cámaras y elementos de climatización inteligente, entre otros. Incluso los locales físicos y las personas, pues ambos son susceptibles de ser atacados. Es decir, hay que inventariar todo lo que sea susceptible de ataque.
- Inventariar los activos intangibles, es decir, los procesos de negocio o servicios y sus dependencias con los activos tangibles, ya que los riesgos de los tangibles repercutirán a los intangibles.
- Por cada activo **definir y completarla información relevante**. Al menos, el responsable de cada activo debe quedar recogido en el inventario, entre otros datos.
- Utilizar técnicas de inventariado manuales (sobre todo para los activos intangibles) y automáticas (con herramientas).
- Definir e implementar un procedimiento de **actualización del inventario**.

Con respecto a las técnicas automáticas de inventariado, hay que tener en cuenta las diferencias entre entornos IT y OT/IoT. En IT se pueden utilizar herramientas basadas en agentes (como SNMP u otros), pero en entornos OT/IoT en general no tiene por qué ser factible esta opción. En este sentido existen herramientas de gestión de activos OT/IoT en el mercado que identifican los dispositivos en una red a través del análisis del tráfico, logrando realizar un inventariado no intrusivo.

Una vez identificados los elementos a proteger hay que analizar madurez y riesgos (AS-IS)

Una vez identificados los activos, el siguiente paso será analizar la madurez de las medidas indicadas en NIS2. Como decíamos capítulos anteriores, las medidas de NIS2 (artículo 21, especialmente) abarcan una serie de áreas que ya existen en otras normativas y estándares, tales como ISO 27001, el Esquema Nacional de Seguridad (ENS), el framework de ciberseguridad CSF NIST o la ISO 62443 (específica de entornos industriales).

Por lo tanto, se realizará un análisis que aglutine los requisitos de la NIS2 integrando los aspectos comunes con la normativa que aplique. Se prestará especial atención al análisis de arquitectura de red como parte de este análisis.

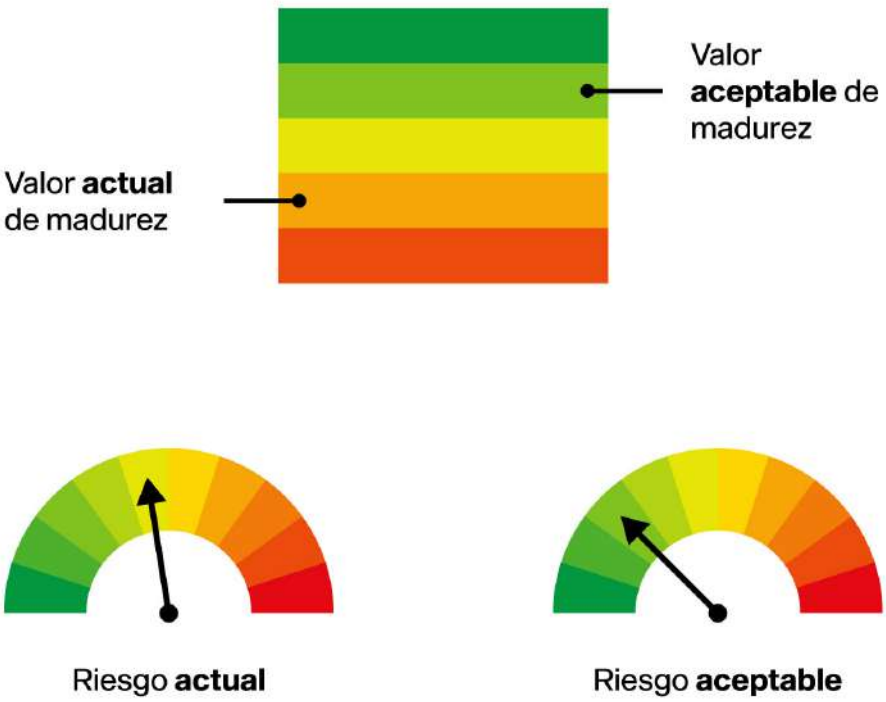
Adicionalmente, además de medirse la madurez de las medidas implantadas, se deben analizar los riesgos, es decir, el grado de exposición a que las diferentes amenazas de seguridad se materialicen sobre los activos causando un impacto. Hoy día existen metodologías/herramientas de análisis de riesgos que contemplan específicamente los entornos OT/IoT como, por ejemplo, MAGERIT/PILAR.

Finalmente, y como un complemento al análisis de la situación, se pueden realizar escaneo de vulnerabilidades con herramientas. En el caso de los activos OT/IoT las propias herramientas de inventariado anteriormente mencionadas pueden tener funcionalidades de detección de vulnerabilidades, aportando un elemento adicional de información de riesgo de los activos.

Del estado de situación actual (AS-IS) al objetivo (TO-BE)

Una vez identificados los activos y analizada su situación de ciberseguridad (**madurez, riesgo, vulnerabilidades**), es decir, la situación actual (AS-IS), el siguiente paso será **evaluar estos niveles**. Para realizar esta evaluación, será preciso **compararlos con unos niveles aceptables (TO-BE) dentro de cada escala de valoración**.

Escala de valoración del AS-IS. Evaluación niveles de madurez y riesgo.

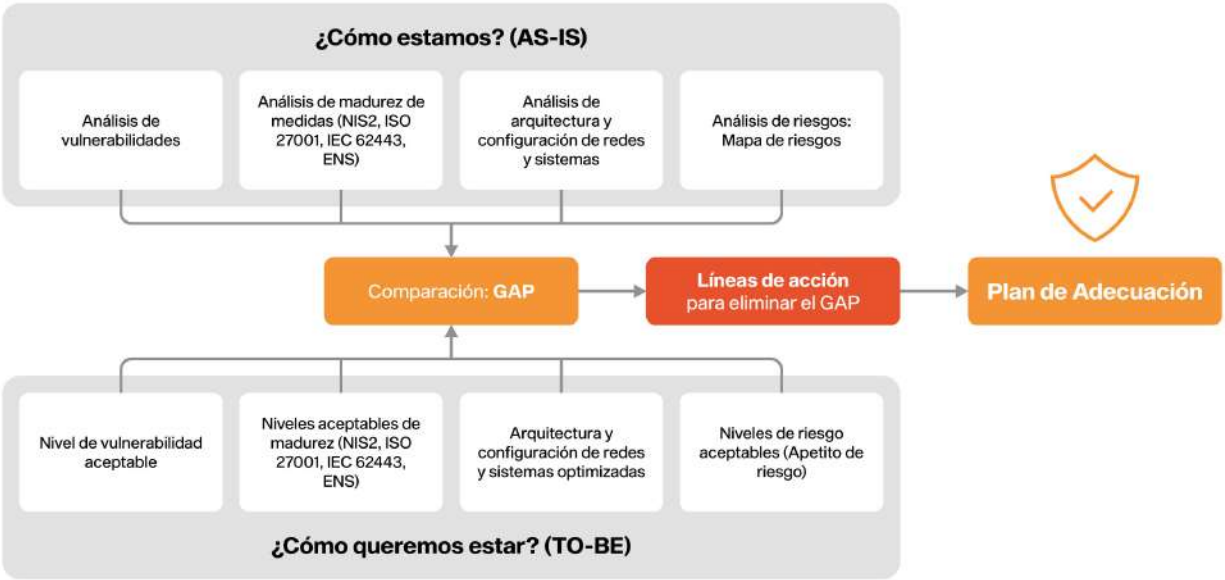


La decisión final sobre los niveles aceptables dependerá del negocio, aunque el personal técnico y de ciberseguridad puedan participar como asesores, sobre todo informando de las implicaciones que suponen los niveles objetivos en términos de equilibrio entre el esfuerzo y el beneficio.

Una vez comparado el estado actual (AS-IS) con el objetivo (TO-BE) en la evaluación, el siguiente paso será **identificar las acciones para cubrir este GAP**, que podrán tener diferentes propósitos:

- Implementar medidas que no estén aún.
- Mejorar la madurez de las medidas existentes.
- Tratar riesgos no aceptables.
- Corregir vulnerabilidades identificadas con las herramientas de escaneo.

Del AS-IS al TO-BE: Identificando las acciones para cubrir el GAP.



Este plan será nuestra hoja de ruta para las siguientes fases, que contaremos en los siguientes capítulos y cubrirá diferentes aspectos, tales como:

- Controles de acceso y autenticación.
- Gestión de actualizaciones y parches.
- Respaldo y restauración de datos.
- Monitorización y registro de eventos.
- Protección contra malware.
- Respuesta ante incidentes.
- Seguridad física.
- Gestión de proveedores.

06

Del Plan a la Acción: Implementando las acciones del plan de adecuación a la NIS2

La ejecución gestionada del plan como factor de éxito

Una vez definido el Plan de adecuación, el siguiente paso será llevar a cabo su ejecución. Para que esta **ejecución sea llevada a cabo en tiempo y forma** con éxito es precisa una **gestión y coordinación** en los siguientes términos:

1. Desglose pormenorizado de tareas.
Las acciones del plan se desglosarán a un nivel pormenorizado en tareas y subtareas que tendrán un carácter implantador, no necesitando más estudios o investigaciones para poder ejecutarse. Estas tareas incluirán calendarios precisos de ejecución.

2. Asignación de responsabilidades.
Tras el desglose, se asignarán ejecutores y responsables. En este sentido, se recomienda la creación de una matriz RACI (siglas en inglés de "Responsible, Accountable, Consulted, Informed") como mecanismo de asignación de responsabilidades en la ejecución. Así pues, para cada acción o grupo de acciones se identificarán los siguientes roles:

- **Responsable (Responsible).** Es la persona encargada de realizar las tareas en sí y, en caso de que una tarea tenga más de una persona, se designaría a una de ellas como Responsable, para que haya un único interlocutor.
- **Aprobador (Accountable).** Este rol se responsabiliza del seguimiento y supervisión de la ejecución de las tareas, aprobando el resultado del trabajo. Para desarrollar su rol interaccionará con el responsable que esté asignado a la tarea (R).
- **Consultado (Consulted).** Este rol se corresponde con la persona o grupo de personas especialistas a los que se les puede consultar por información relacionada con las tareas realizadas por el responsable (R) y supervisadas por el aprobador (A). Por lo tanto, deberán tener el suficiente conocimiento y experiencia como para poder opinar y asesorar sobre dichas tareas.
- **Informado (Informed).** Será la persona o grupo de personas a las que se les informará sobre la marcha de los trabajos (grado de avance, resultados y cambios, entre otros aspectos).

Tareas de Plan	Roles			
	Responsable de Sistemas	Responsable de Planta	CISO	Colaborador
Elaborar procedimiento	A	C	C / I	R
Implantar sonda	I	A	C / I	R
Acción formativa	C / I	C / I	A	R
Otras	C / I	C / I	A	R

3. Puesta en marcha
Una vez asignados los roles empezará la ejecución del plan, que, además de la propia ejecución llevada a cabo por los responsables (R), tendrá un componente de seguimiento continuo (realizado por los aprobadores A), de asesoría (realizada por los consultados C) y reporting (a los informados I).

En este sentido, se recomienda la implantación de una oficina técnica, que aglutinaría todas las funciones anteriores, velando por que no solo se implementen las acciones del plan sino que también haya una adecuada gestión.

Las acciones del plan podrán ser de diferente tipología

Las acciones del plan podrán ser de diferente tipología, por lo cual **el equipo ejecutor será multidisciplinar**, aglutinando expertos de ciberseguridad, legales, de sistemas y comunicaciones entre otros. Dado que en el alcance podrá haber tanto sistemas de información (IT) como de operación (OT e IoT) dentro del equipo ejecutor se deberá contar con personal especialista en ciberseguridad en ambos entornos, quienes podrán interaccionar para que se tengan en consideración los aspectos que sean comunes y se pueden integrar.

Las acciones podrán ser de **carácter documental**, por ejemplo, desarrollar políticas y procedimientos. También podrán ser de **carácter técnico**, como, por ejemplo, en los entornos OT/IoT, instalar una herramienta de monitorización, de la que ya se habló en la etapa Plan para la identificación continua de elementos OT/IoT y de sus vulnerabilidades. Y, por supuesto, también habrá acciones de **carácter organizativo**, tales como las relacionadas con la gestión de proveedores (cada vez más ciberincidentes en entornos OT/IoT vienen causado por vulnerabilidades en la cadena de suministro), la formación y la gestión de ciberincidentes.

La evaluación periódica de la eficacia de las medidas y toma de acciones de mejora

Por último, y en línea con el ciclo de mejora continua (PDCA: Plan-Do-Check-Act), tras la ejecución, o en puntos intermedios de la misma, es importante que se realicen auditorías de NIS2 objetivas e imparciales y medición de indicadores (Check). Esto servirá para la verificación de la eficacia de las medidas del Plan que están siendo implantadas y la detección de posibles acciones correctivas yo/preventivas, que deberían incorporarse al Plan y acometerse (Act).

Si estás afectado por la NIS2 o no sabes si te puede afectar, cuenta con BABEL

Desde BABEL apostamos por el lema de que cumplir con la legislación de ciberseguridad protege el negocio y, sobre todo, en el caso de la NIS2, donde podrá haber **repercusiones directas para personal directivo** por infracciones. Por ello, con nuestro equipo de expertos podemos ayudar a nuestros clientes con la adecuación a esta nueva normativa, desde la realización del análisis de situación y plan hasta su implementación y posterior mantenimiento.

BABEL

www.babelgroup.com