Riesgos tecnológicos y *ciberseguridad*

Análisis sobre NIS 2 (Directiva UE 2022/2555)

ManagementSolutions
Making things happen

01 Nuestra comprensión de la NIS 2

Cronología normativa, contexto y objetivos principales

La Directiva NIS 2 entró en vigor en enero de 2023 y el plazo para su transposición al Derecho nacional por parte de los Estados miembros era octubre de 2024. Es aplicable en todos los países de la UE a partir de enero de 2025 y los sujetos NIS deberán cumplirla íntegramente en octubre de 2026.

Contexto normativo

El objetivo principal de la Directiva NIS 2 de la Unión Europea es garantizar un alto nivel de seguridad de las redes y los sistemas de información de las empresas consideradas esenciales o importantes.

Aspectos diferenciales

- La *norma* NIS 2 adopta un **enfoque** de gestión de la seguridad de la información **basado en el riesgo**, según el cual las organizaciones deben identificar, evaluar y abordar los riesgos para la seguridad de la información a los que están expuestas.
- El ámbito de aplicación del reglamento se ha ampliado con:
  - **Nuevas modalidades de notificación de incidentes significativos**
  - **Nuevos requisitos para la seguridad de la información** en un **entorno digital**
- Se establece **una diferenciación** entre las **obligaciones** de las empresas consideradas **esenciales** y las clasificadas como **importantes**. En el caso de **las empresas esenciales**, el nivel de obligaciones es **más exhaustivo**, mientras que en el caso de **las empresas importantes,** el nivel de obligaciones es más **limitado.**
- El reglamento se centra en *la gobernanza* de la organización, donde la **responsabilidad, la dirección y el liderazgo** en el ámbito de **la ciberseguridad** recaen ahora en los órganos de gestión.

Sectores esenciales

Sector bancario	Energía	Transporte	Gestión de servicios TIC	Sanidad	Infraestructura digital

01 Nuestra comprensión de la NIS 2

¿Qué hay de nuevo en la NIS 2?

El Reglamento NIS 2 presenta novedades importantes con respecto al NIS 1, que pueden clasificarse en cuatro bloques principales: 1) ámbito de aplicación, 2) notificación de incidentes, 3) requisitos de ciberseguridad y 4) supervisión y aplicación.

Ámbito de aplicación más amplio

18 +10 con respecto a NIS 1 **sectores críticos** + subsectores

11 +3 con respecto a NIS 1 **sectores altamente críticos**

7 De nueva introducción **sectores críticos**

+20 000 sujetos NIS*

De los cuales +5000 entidades esenciales

Notificación de incidentes

Inclusión de un protocolo de acción y notificación detallado y ampliación de las funciones del CSIRT

Alerta temprana en un plazo de **24 horas** *(desde el conocimiento de la amenaza)*

Notificación en un plazo de **72 horas** *(desde el descubrimiento del incidente)*

***Informe* final** en un mes *(una vez resuelto el incidente)*

Comunicación a los destinatarios de los servicios *(incluidas medidas para reducir el riesgo)*

Otros

Requisitos de seguridad informática

Adopción de nuevos requisitos en el contexto de un *Marco* Nacional para la *Ciberseguridad* y la *Protección de Datos*

Sujetos esenciales: **43** medidas y **117** requisitos

Sujetos importantes: **37** medidas y **87** requisitos

⚠ *Participación y formación en el Consejo de Administración*

⚠ *Inclusión de la cadena de suministro*

⚠ *Evaluación de riesgos*

Supervisión y aplicación

Mecanismo de sanciones en caso de incumplimiento

Sujetos esenciales: **10** millones de euros / **2 %** de la facturación — *Según el valor más alto*

Sujetos importantes – **7** millones de euros / **1,4 %** de la facturación — *Según el valor más alto*

** Entidades NIS identificadas el 10 de abril en la Mesa para la aplicación de la normativa NIS. A partir del 12 de abril, ACN comenzó a comunicar a las entidades interesadas su inclusión o no en la lista de entidades NIS, a través de la plataforma NIS*

01 Nuestra comprensión de la NIS 2

Ámbito de aplicación

Sectores altamente críticos

Sector	Detalle	Organizaciones: Grandes	Organizaciones: Medianas	Organizaciones: Pequeñas
Energía	19 tipos	Esenciales	Import.*	Fuera**
Transporte	10 tipos	Esencial.	Import.*	Fuera**
Sector bancario	DORA Lex Specialis	Esencial.	Importación.*	Fuera**
Infraestructuras de los mercados financieros		Esencial.	Importación.*	Fuera**
Sector sanitario	5 tipos	Esencial.	Importación.*	Fuera**
Agua potable	1 tipo	Esencial.	Importación.*	Fuera**
Aguas residuales	1 tipo	Esencia.	Importación.*	Fuera**
Infraestructuras digitales	9 tipos	Esencial.	Según la autoridad	
Gestión Servicios TIC	2 tipos	Esencial.	Importación.*	Fuera**
Espacio	1 tipo	Esencial.	Importación.*	Fuera**
Administración pública – Central	4 tipos	Esencial.		
Administración pública – Regional/local	11 tipos	Importación.*		

Sectores críticos

Sector	Detalle	Organizaciones: Grandes	Organizaciones: Medianas	Organizaciones: Pequeñas
Servicios postales y de mensajería	1 tipo	Importantes*		Fuera**
Gestión de residuos	1 tipo	Importantes*		Fuera**
Fabricación, producción y distribución de sustancias químicas	1 tipo	Importantes*		Fuera**
Producción, transformación y distribución de alimentos	1 tipo	Importantes*		Fuera**
Fabricación	6 tipos	Importantes*		Fuera**
Proveedores de servicios digitales	4 tipos	Según la autoridad		
Investigación	2 tipos	Importantes*		Fuera**
••• Otros tipos	4 tipos	Identificación de la autoridad		

La revisión del mecanismo de identificación de los sujetos importantes o esenciales prevé un criterio homogéneo basado en el tamaño (*la* denominada *«regla del límite de* tamaño») que amplía la aplicación de la normativa a todas las empresas medianas y grandes que operan en los sectores identificados (en algunos casos, también a las pequeñas y microempresas), así como a numerosas administraciones públicas

** Posible identificación de la Autoridad como esencial*
*** Posible identificación de la Autoridad como importante o esencial*

01 Nuestra comprensión de la NIS 2

Notificación de incidentes

La Directiva NIS 2 exige a las organizaciones que realicen una serie de notificaciones una vez detectado un incidente con un impacto significativo, por lo que debe seguirse el siguiente flujo de comunicación

Detección de un incidente significativo

Un incidente se considera relevante si:

Sujetos esenciales / Sujetos importantes

- El sujeto NIS tiene constancia **de la pérdida de confidencialidad**, hacia el exterior, de datos digitales de su propiedad o sobre los que ejerce control, incluso parcial.
- El sujeto NIS tiene constancia **de la pérdida de integridad**, con impacto hacia el exterior, de datos de su propiedad o sobre los que ejerce control, incluso parcial.
- El sujeto NIS tiene constancia de **la violación de los niveles de servicio esperados** de sus servicios y/o actividades, sobre la base de los niveles de servicio esperados (SL) **definidos de conformidad con la medida** DE.CM-01.
- El sujeto NIS tiene pruebas, también **sobre la base de los parámetros cualitativos y cuantitativos** definidos de conformidad con la medida **DE.CM-01**, del acceso no autorizado o con abuso de los privilegios concedidos a datos digitales de su propiedad o sobre los que ejerce control, incluso parcial.

Notificación de alerta temprana en un plazo de 24 horas

El CSIRT o la autoridad competente proporcionan indicaciones operativas o consejos sobre la aplicación de posibles medidas de mitigación.

Esta alerta debe indicar, si procede, si el incidente es atribuible a una acción maliciosa o si puede tener implicaciones transfronterizas.

Notificación en un plazo de 72 horas sobre el estado del accidente

Esta notificación debe tener en cuenta la gravedad del incidente, el impacto y los indicadores de compromiso

Informe final en el plazo de un mes desde el incidente

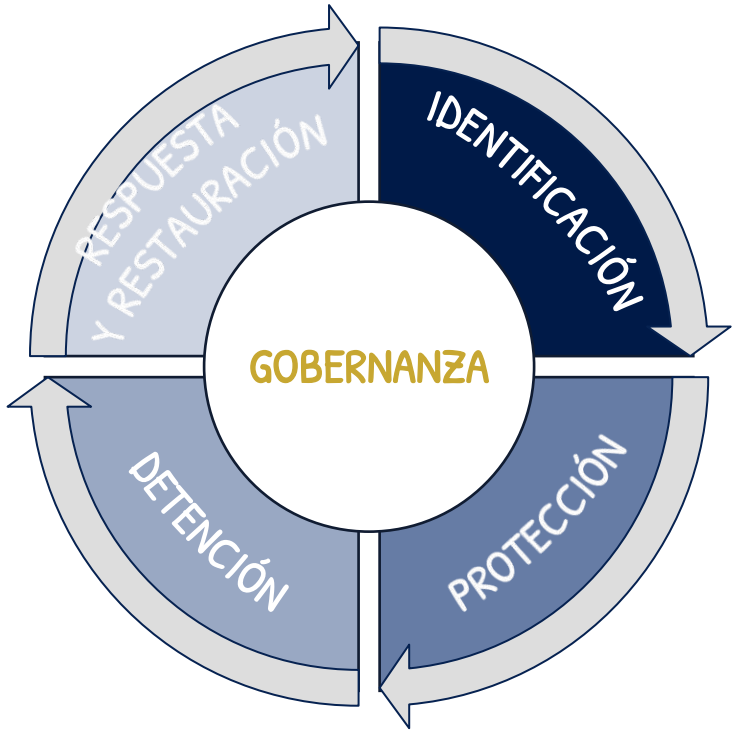
El informe final debe tener en cuenta: la gravedad del incidente, el impacto y los indicadores de compromiso; la causa; las medidas de mitigación; y, en su caso, el impacto transfronterizo del incidente.
*En caso de que **el incidente siga en curso** en el momento de **la presentación del informe final**, se deberá generar un informe sobre el estado en ese momento y el **informe final** deberá entregarse en el plazo de un mes a partir de **la resolución del incidente***

La Directiva NIS 2 establece formalmente que los Estados miembros deben garantizar que las organizaciones críticas e importantes notifiquen al CSIRT, o a la autoridad competente, cualquier impacto significativo. Se considera que un impacto es significativo cuando tiene el potencial de causar una interrupción sustancial de las operaciones del servicio o de suponer una pérdida económica importante para la organización afectada. Además, puede afectar a personas físicas o jurídicas, causándoles daños materiales o inmateriales importantes.

01 Nuestra comprensión de la NIS 2

Requisitos de seguridad informática

Los sujetos esenciales e importantes deben gestionar los riesgos de las TIC y de seguridad con el objetivo de prevenir y mitigar el impacto de los incidentes adoptando medidas basadas en *el Marco* Nacional para la *Ciberseguridad* y la *Protección de Datos* que se defina en cada páis. (Las medidas indicadas a continuación se corresponden con el marco italiano, ya publicado)



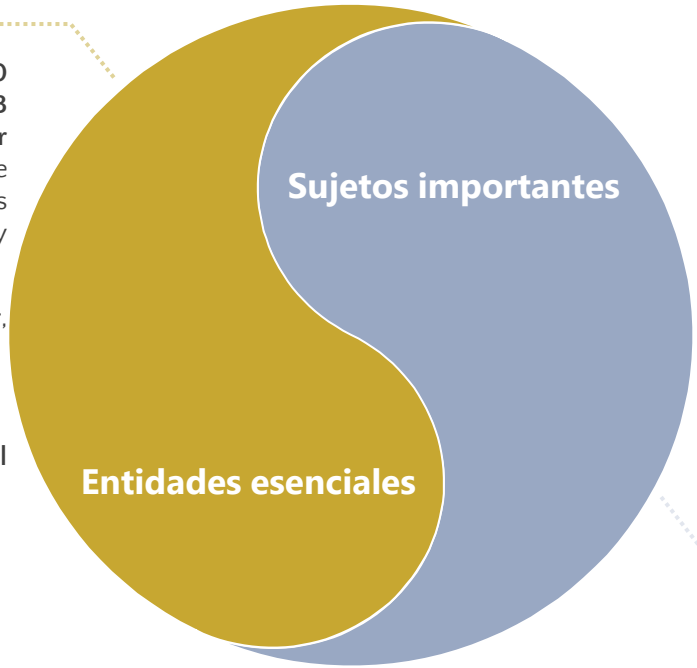
Ámbito	Descripción Ámbito	Sujetos esenciales		Temas importantes	
		# Aspectos	# Req.	# Aspectos	# Req.
GOBIERNO	Definición de los objetivos y requisitos necesarios para gestionar los riesgos, las funciones y responsabilidades, el marco normativo y la cadena de suministro (terceros)	11	25	11	21
IDENTIFICACIÓN	Identificación y registro de *activos*, evaluación del riesgo expuesto y mejora continua	10	28	9	21
PROTECCIÓN	Definición de controles y prácticas de seguridad para prevenir, limitar y contener posibles incidentes (IAM, formación, seguridad de los datos, de las plataformas y resiliencia de la infraestructura)	16	48	12	34
DETECCIÓN	Definición de herramientas para la supervisión continua de *los activos* y la detección de vulnerabilidades y amenazas	2	9	2	5
RESPUESTA Y RECUPERACIÓN	Gestión de incidentes, definición de planes de respuesta y recuperación para proteger y restablecer la integridad y disponibilidad de las operaciones	4	7	3	6
		43	**117**	**37**	**87**

01 Nuestra comprensión de la NIS 2

Supervisión y aplicación

Los Estados miembros tienen la posibilidad de imponer sanciones administrativas a las diferentes organizaciones que entran en el ámbito de aplicación del Reglamento NIS 2. Dichas sanciones deben ser eficaces, proporcionadas y disuasorias y, en función del tipo de organización, se tomarán como referencia los siguientes importes

- Se trata de sectores altamente críticos **con más de 250 empleados** y un **presupuesto anual total superior a 43 millones de euros** o un **volumen de negocios anual superior a 50 millones de euros,** proveedores de servicios de comunicaciones electrónicas, proveedores de servicios DNS y proveedores cualificados de servicios de confianza y registros de dominios de primer nivel.
- Para los sujetos **esenciales**, las sanciones pueden ascender, según el valor más alto, hasta:
  - **10 000 000 €**
  - Un máximo del **2 % del volumen de negocios mundial total anual** del ejercicio anterior



- Se trata de todas las organizaciones que forman parte de **sectores altamente críticos** u **otros sectores críticos no considerados como organizaciones esenciales.**
- Para los sujetos **importantes**, las sanciones pueden ascender, según el valor más alto, hasta:
  - **7 000 000 €**
  - Un máximo **del 1,4 % del volumen de negocios mundial total anual** del ejercicio anterior.

Si una organización esencial o significativa no cumple con la NIS 2, los Estados miembros pueden imponer multas repetidas hasta que la empresa decida cumplirla.

02 Propuesta de valor

Trending topics

La normativa NIS2 amplía las obligaciones en materia de seguridad e impone requisitos más exhaustivos para la gestión de riesgos y la resiliencia

Ámbito	Descripción	Actividades principales (No exhaustivo)
Participación del consejo de administración	**Participación directa del Consejo de Administración** en *la gobernanza* de *la ciberseguridad*, con funciones y responsabilidades claras e integración de la gestión de las TIC como parte de la estrategia empresarial	• Formación específica del consejo de administración • Definición de responsabilidades • Estrategia de TIC en línea con la estrategia empresarial
Gestión de incidentes	**Proceso estructurado para la gestión de incidentes**, con capacidad de respuesta en línea con el **proceso de notificación definido** (notificaciones iniciales, notificaciones intermedias y notificaciones finales)	• Simulaciones de incidentes y crisis • *Manual* de continuidad • Actualización de los procesos
Gestión de terceros	Garantizar la **gestión estructurada del riesgo TIC a lo largo de la cadena de suministro**, definiendo funciones, responsabilidades y requisitos TIC para proveedores y terceros críticos, garantizando un control continuo y una evaluación de los riesgos asociados durante todo el ciclo de vida (*diligencia debida*, negociación, supervisión, renovación o *salida*)	• Criticidad de los proveedores • Modelo de gestión y análisis de riesgos de los proveedores • Revisión de las condiciones generales del contrato
Evaluación del riesgo de las TIC	Establecer un **enfoque estructurado y continuo para la evaluación de riesgos**, incluyendo vulnerabilidades, amenazas e impactos. Además, se debe considerar un sistema de clasificación, registro y actualización, con acciones claras de mitigación y seguimiento	• *Marco* de gestión de riesgos • Taxonomía del riesgo • Modelo de control • RAF y cuadro de mando de indicadores (KRI/KPI)
Refuerzo de la seguridad	**Refuerzo completo de todas las medidas de seguridad** existentes en función de las necesidades identificadas (*inventario de activos*, IAM, formación del personal, resiliencia de las infraestructuras, etc.).	• Formación del personal • Análisis GAP y definición del modelo *TO BE*

A Anexos

A1 Ámbitos de aplicación

A2 *Marco* nacional para la *ciberseguridad* y la *protección de datos*

A.1 Sectores de aplicación

Sectores altamente críticos (1/3)

SECTOR	TIPOLOGÍA DE SUJETOS
Energía	**Electricidad** • Empresas eléctricas • Operadores de la red de distribución • Gestores del sistema de transmisión • Productores • Operadores designados del mercado de la electricidad • Participantes en el mercado eléctrico • Operadores de puntos de recarga responsables de la gestión y el funcionamiento de un punto de recarga, que prestan un servicio de recarga al usuario final también en nombre y por cuenta de un proveedor de servicios de movilidad
	Sistemas de calefacción y refrigeración • Gestores de sistemas de calefacción o refrigeración urbanas
	Crudo • Operadores de oleoductos para el transporte de petróleo crudo • Operadores de instalaciones de producción, refinación y tratamiento de petróleo crudo, almacenamiento y transporte • Organizaciones de almacenamiento central
	Gas • Empresas de suministro de gas • Operadores de la red de distribución • Gestores del sistema de transporte • Gestores de almacenamiento • Operadores del sistema GNL • Empresas de gas natural • Gestores de instalaciones de refinación y tratamiento de gas natural
	Hidrógeno • Operadores de producción, almacenamiento y transporte de hidrógeno

A.1 Ámbitos de aplicación

Sectores altamente críticos (2/3)

SECTOR	TIPOLOGÍA DE SUJETOS
Transporte	**Transporte aéreo** • Compañías aéreas • Organizaciones de gestión aeroportuaria • Operadores de control de tráfico que prestan servicios de control del tráfico aéreo
	Transporte ferroviario • Gestores de infraestructuras • Compañías ferroviarias
	Transporte marítimo y fluvial • Compañías de navegación marítima, fluvial y costera, tanto para pasajeros como para mercancías • Entidades de gestión portuaria • Operadores del servicio de tráfico marítimo (VTS)
	Transporte por carretera • Autoridades viarias responsables del control de la gestión del tráfico, excluidas las organizaciones públicas para las que la gestión del tráfico o la gestión de sistemas de transporte inteligentes no es una parte esencial de su actividad general. • Operadores de sistemas de transporte inteligentes
Sector financiero	**Sector bancario** • Organizaciones de crédito
	Infraestructuras del mercado financiero • Gestores de centros de negociación • Organizaciones de contrapartida central (CCP)
Público Adm.	**Administración pública, excluidos el poder judicial, el parlamento y los bancos centrales** • Organizaciones de la administración pública central, tal y como se definen en el Estado miembro de conformidad con las disposiciones del Derecho nacional. • Organizaciones de la administración pública a nivel regional, tal y como se definen en el Estado miembro de conformidad con las disposiciones del Derecho nacional.

A.1 Sectores de aplicación

Sectores altamente críticos (3/3)

SECTOR	TIPO DE SUJETOS
Sector Sanitario	• Proveedores de asistencia sanitaria • Laboratorios de referencia de la UE • Organizaciones dedicadas a la investigación y el desarrollo de medicamentos • Organizaciones que producen productos farmacéuticos básicos y especialidades medicinales contempladas en la sección C • Organizaciones que producen productos sanitarios considerados esenciales en emergencias de salud pública
Agua	**Agua potable** • Proveedores y distribuidores de agua destinada al consumo humano, excluidos los distribuidores para los que la distribución de agua destinada al consumo humano es una parte no esencial de su actividad general de distribución de otras mercancías y productos. **Aguas residuales** • Empresas que se dedican a la recogida, eliminación o tratamiento de aguas residuales urbanas, domésticas o industriales
Infraestructura digital	• Proveedores de puntos de intercambio de Internet • Proveedores de servicios DNS, excluidos los operadores de *servidores raíz* • Registros de nombres de dominio de primer nivel • Proveedores de servicios de *computación en la nube* • Proveedores de servicios para centros de datos • Proveedores de redes de distribución de contenidos • Proveedores de servicios fiables • Proveedores de redes públicas de comunicaciones electrónicas • Proveedores de servicios de comunicaciones electrónicas accesibles al público
Gestión de servicios TIC	• Proveedores de servicios gestionados • Proveedores de servicios de seguridad gestionados
Espacio	• Operadores de infraestructuras terrestres, propiedad de los Estados miembros o de organizaciones privadas, gestionadas y explotadas por ellos, que prestan apoyo a la prestación de servicios espaciales, con excepción de los proveedores de redes públicas de comunicaciones electrónicas.

A.1 Sectores de aplicación

Sectores críticos (1/2)

SECTOR	TIPOLOGÍA DE SUJETOS
Servicios postales y de mensajería	• Proveedores de servicios postales, incluidos los proveedores de servicios de mensajería
Gestión de residuos	• Empresas dedicadas a la gestión de residuos, excluidas aquellas para las que la gestión de residuos no es la actividad económica principal
Fabricación, producción y distribución de sustancias químicas	• Empresas dedicadas a la fabricación de sustancias y a la distribución de sustancias o mezclas, y empresas dedicadas a la producción de artículos
Producción, transformación y distribución de alimentos	• Empresas alimentarias dedicadas a la distribución al por mayor y a la producción industrial y transformación
Fabricación	• Fabricación de productos sanitarios y productos sanitarios para diagnóstico in vitro • Fabricación de ordenadores y productos electrónicos y ópticos • Fabricación de equipos eléctricos • Fabricación de maquinaria y equipos no clasificados en otra parte (n.c.o.p.) • Fabricación de vehículos de motor, remolques y semirremolques • Fabricación de otros medios de transporte

A.1 Sectores de aplicación

Sectores críticos (2/2)

SECTOR	TIPOLOGÍA DE SUJETOS
Proveedores de servicios digitales	• Proveedores de mercados en línea • Proveedores de motores de búsqueda en línea • Proveedores de plataformas de *redes sociales* • Proveedores de servicios de registro de nombres de dominio
Investigación	• Organizaciones de investigación
Otros tipos de sujetos	• Entidades que prestan servicios de transporte público local • Centros educativos que realizan actividades de investigación • Entidades que realizan actividades de interés cultural • Empresas *internas*, empresas participadas y empresas de control público

A Anexos

A1 Ámbitos de aplicación

A2 *Marco* nacional para la *ciberseguridad* y la *protección de datos*

A.2 *Marco* nacional para la *ciberseguridad* y la *protección de datos*

Enfoque en el gobierno

GOBIERNO

ID	Aspecto	Medidas	Descripción	# requisitos esenciales	# requisitos importantes
GV.OC	Contexto organizativo	GV.OC-4	Se comprenden y comunican los objetivos, capacidades y servicios críticos de los que dependen las *partes interesadas* o que esperan de la organización (actualización de la lista de sistemas de información y redes relevantes).	1	1
GV.RM	Estrategia de gestión de riesgos	GV.RM-03	Las actividades y los resultados de la gestión del riesgo de *ciberseguridad* forman parte integrante de los procesos de gestión del riesgo de la organización (definición del plan de gestión de riesgos para la ciberseguridad).	1	1
GV.RR	Funciones, responsabilidades y poderes relacionados	GV.RR-02	Las funciones, responsabilidades y poderes relacionados con la gestión del riesgo de *ciberseguridad* se establecen, comunican, comprenden y aplican (aprobación de la organización para la seguridad informática, actualización de la lista de personal, inclusión del punto de contacto, actualización de funciones y responsabilidades).	4	4
		GV.RR-04	La *ciberseguridad* se incluye en las prácticas de recursos humanos (identificación del personal autorizado para acceder a los sistemas de información, identificación de los administradores de los sistemas de información, documentación de los procedimientos, definición de las obligaciones contractuales, documentación del cumplimiento de las obligaciones).	5	3
GV.PO	Política	GV.PO-01	La política de gestión del riesgo de *ciberseguridad* se establece en función del contexto organizativo, la estrategia de *ciberseguridad* y las prioridades, y se comunica y aplica (definición de los ámbitos de aplicación de las políticas de seguridad, definición de los requisitos necesarios, aprobación de los requisitos).	3	3
		GV.PO-02	La política de gestión del riesgo de *ciberseguridad* se revisa, actualiza, comunica y aplica para reflejar los cambios en los requisitos, las amenazas, la tecnología y la misión de la organización (actualización de la política, verificación del cumplimiento de la política, elaboración de una lista actualizada).	3	2
GV.SC	Gestión del riesgo de *ciberseguridad* de la cadena de suministro	GV.SC-01	El programa, la estrategia, los objetivos, las políticas y los procesos de gestión del riesgo de *ciberseguridad* de la cadena de suministro están establecidos y aceptados por *las partes interesadas* (participación de la organización, definición de los requisitos de seguridad, definición de los ámbitos básicos).	3	1
		GV.SC-02	Las funciones y responsabilidades en materia de *ciberseguridad* para proveedores, clientes y *socios* se establecen, comunican y coordinan interna y externamente (definición de funciones y responsabilidades en materia de terceros, actualización de la lista de personal).	2	2
		GV.SC-04	Los proveedores son conocidos y priorizados en función de su importancia (actualización del inventario de proveedores).	1	1
		GV.SC-05	Los requisitos para hacer frente a los riesgos de *ciberseguridad* en la cadena de suministro se establecen, priorizan e integran en los contratos y tipos de acuerdos con los proveedores y otros terceros relevantes (inclusión de requisitos de seguridad en las licitaciones y convocatorias públicas).	1	1
		GV.SC-07	Los riesgos que plantean un proveedor, sus productos y servicios y otros terceros se comprenden, registran, priorizan, evalúan, tratan y supervisan a lo largo de la relación (evaluación del riesgo asociado a los suministros de terceros, verificación del cumplimiento de los suministros).	2	2

A.2 *Marco* nacional para la *ciberseguridad* y la *protección de datos*

Enfoque en la identificación

	ID	Nombre Aspecto	Medidas	Descripción	# requisitos esenciales	# requisitos importantes
IDENTIFICACIÓN	ID.AM	Gestión de *activos*	ID.AM-01	Mantener un inventario actualizado *del hardware* gestionado por la organización	1	1
			ID.AM-02	Mantener un inventario actualizado del *software*, los servicios y los sistemas gestionados por la organización	1	1
			ID.AM-03	Mantener un inventario actualizado de los flujos de comunicaciones de red y de los flujos de datos de red internos y externos, autorizados por la organización	1	-
			ID.AM-04	Mantener un inventario actualizado de los servicios informáticos prestados por los proveedores	1	1
	ID.RA	Evaluación de riesgos (*risk assessment*)	ID.RA-01	Las vulnerabilidades de *los activos* se identifican, confirman y registran (identificación de vulnerabilidades de los sistemas de información, realización *de evaluaciones de vulnerabilidad* y/o *pruebas de penetración*, desarrollo de una descripción general de las acciones y vulnerabilidades).	3	1
			ID.RA-05	Las amenazas, vulnerabilidades, probabilidades e impactos se utilizan para comprender el riesgo inherente e informar la priorización de la respuesta al riesgo (evaluación del riesgo de seguridad de los sistemas de información, actualización de los criterios de evaluación, aprobación de las evaluaciones realizadas, definición de ámbitos útiles).	4	3
			ID.RA-06	Las respuestas al riesgo se eligen, priorizan, planifican, supervisan y comunican (definición del plan de tratamiento del riesgo, aplicación de medidas de mitigación compensatorias, aprobación de los riesgos).	3	3
			ID.RA-08	Se establecen procesos para la recepción, el análisis y la respuesta a las divulgaciones de vulnerabilidades (supervisión de los canales de comunicación, actualización de la seguridad y las medidas de mitigación, definición del plan de gestión de vulnerabilidades, aprobación del plan, supervisión de los canales de los proveedores).	5	4
	ID.DM	Mejora	ID.DM-01	Se identifican mejoras como resultado de las evaluaciones (definición del plan de adaptación, comunicación del plan a los órganos pertinentes, definición del plan para evaluar la eficacia de las medidas de gestión del riesgo para la seguridad informática, comunicación del plan a los órganos pertinentes).	4	2
			ID.DM-04	Se establecen, comunican, mantienen y mejoran los planes de respuesta a incidentes y otros planes de *ciberseguridad* que afectan a las operaciones (definición del plan de continuidad operativa, definición del plan de recuperación, definición del plan de gestión de crisis, aprobación de planes, actualizaciones de planes).	5	5

A.2 *Marco* nacional para la *ciberseguridad* y la *protección de datos*

Enfoque en la protección (1/2)

	ID	Nombre Aspecto	Medidas	Descripción	# requisitos esenciales	# requisitos importantes
PROTECCIÓN	PR.AA	Gestión de identidades, autenticación y control de accesos	PR.AA-01	Las identidades y credenciales de los usuarios, servicios y *hardware* autorizados son gestionadas por la organización (aprobación de usuarios con privilegios administrativos y de acceso remoto, actualización de credenciales, verificación de usuarios y autorizaciones relacionadas, documentación de procedimientos).	4	4
			PR.AA-03	Los usuarios, los servicios y *el hardware* están autenticados (evaluación de los riesgos asociados, uso de métodos de autenticación multifactorial, documentación de los procedimientos).	3	3
			PR.AA-05	Los permisos, derechos y autorizaciones de acceso se definen en una política e incorporan los principios del privilegio mínimo y la separación de tareas (asignación de permisos de acuerdo con los principios del privilegio mínimo, distinción entre usuarios con y sin privilegios administrativos, documentación de procedimientos).	3	3
			PR.AA-06	El acceso físico a *los activos* se gestiona, supervisa y aplica de forma adecuada al riesgo (protección del acceso físico, documentación de procedimientos).	2	2
	PR.AT	Concienciación y formación	PR.AT-01	El personal está formado para poseer las competencias necesarias para realizar tareas de carácter general teniendo en cuenta los riesgos de *ciberseguridad* (definición del plan de formación en materia de seguridad informática, aprobación del plan, actualización de la lista de empleados que han recibido la formación).	3	3
			PR.AT-02	Las personas que desempeñan funciones especializadas reciben formación para adquirir las competencias necesarias para realizar las tareas pertinentes teniendo en cuenta los riesgos de *ciberseguridad* (definición de formación específica para el personal con funciones especializadas, actualización de la lista de empleados que han recibido la formación).	2	-
	PR.DS	Seguridad de los datos	PR.DS-01	La confidencialidad, integridad y disponibilidad de los datos en reposo (*data-at-rest*) están protegidas (uso de datos cifrados con protocolos y algoritmos de última generación y considerados seguros, desactivación de la ejecución automática de soportes extraíbles, documentación de procedimientos).	3	3
			PR.DS-02	Se protege la confidencialidad, la integridad y la disponibilidad de los datos en tránsito (*datos en tránsito*) (uso de protocolos y algoritmos de cifrado de última generación y considerados seguros, documentación de procedimientos).	2	2
			PR.DS-11	*Las copias* de *seguridad* de los datos se crean, protegen, mantienen y verifican (realización periódica de *copias* de *seguridad* de los datos y las configuraciones, documentación de los procedimientos, verificación de la confidencialidad e integridad de la información contenida en *las copias de seguridad*, verificación periódica de la utilidad de *las copias de seguridad*, documentación de los procedimientos).	5	2

A.2 *Marco* nacional para la *ciberseguridad* y la *protección de datos*

Enfoque en la protección (2/2)

	ID	Nombre Aspecto	Medidas	Descripción	# requisitos esenciales	# requisitos importantes
PROTECCIÓN	PR.PS	Seguridad de las plataformas	PR.PS-01	Se establecen y aplican prácticas de gestión de la configuración (actualización de la lista de configuraciones de referencia seguras, documentación de procedimientos).	2	-
			PR.PS-02	El *software* se mantiene, sustituye y elimina en función del riesgo (instalación exclusiva de *software* específico, instalación de las últimas actualizaciones de seguridad publicadas por el fabricante, documentación de procedimientos, verificación de actualizaciones *de software* consideradas críticas, documentación de procedimientos).	5	3
			PR.PS-03	*El hardware* se mantiene, sustituye y retira en función del riesgo (definición de procedimientos para la transferencia física y el desmantelamiento de dispositivos destinados al almacenamiento seguro de datos, actualización de registros de mantenimiento realizado *en el hardware*).	2	-
			PR.PS-04	Se generan *registros* y se ponen a disposición para su supervisión continua (registro de accesos remotos, conservación *de los registros* necesarios para la supervisión de los eventos de seguridad, definición de los plazos de conservación de *los registros*, documentación de los procedimientos).	4	4
			PR.PS-06	Las prácticas de desarrollo seguro de *software* están integradas y su rendimiento se supervisa durante todo el ciclo de vida del *software*	1	1
	PR.IR	Resiliencia de la infraestructura tecnológica	PR.IR-01	Las redes y los entornos están protegidos contra el acceso lógico y el uso no autorizados (definición de actividades permitidas de forma remota, definición de sistemas informáticos y de red a los que se puede acceder de forma remota, configuración de sistemas perimetrales, documentación de procedimientos).	4	4
			PR.IR-03	Se han implementado mecanismos para cumplir los requisitos de resiliencia en situaciones normales y adversas (uso de sistemas de comunicación de emergencia protegidos, documentación de procedimientos).	2	-

A.2 *Marco* nacional para la *ciberseguridad* y la *protección de datos*

Enfoque en la detección

	ID	Nombre Aspecto	Medidas	Descripción	# requisitos esenciales	# requisitos importantes
DETECCIÓN	DE.CM	Supervisión continua	DE.CM-01	Las redes y los servicios de red se supervisan para detectar eventos potencialmente adversos (actualización de herramientas para detectar incidentes, definición de los niveles de servicio esperados, documentación de procedimientos, uso de herramientas de análisis y filtrado, supervisión de accesos y actividades, supervisión de accesos no autorizados, documentación de procedimientos).	7	3
			DE.CM-09	Se supervisan *el hardware* y el *software* de procesamiento, los entornos de *tiempo de ejecución* y sus datos para detectar eventos potencialmente adversos (actualización de los sistemas de protección de los terminales para la detección de código malicioso, documentación de procedimientos).	2	2

A.2 *Marco* nacional para la *ciberseguridad* y la *protección de datos*

Enfoque en la respuesta y la recuperación

	ID	Nombre Aspecto	Medidas	Descripción	# requisitos esenciales	# requisitos importantes
RESPUESTA	RS.MA	Gestión de incidentes	RS.MA-01	El plan de respuesta a incidentes se ejecuta en coordinación con las terceras partes interesadas una vez declarado un incidente (definición del plan para la gestión de incidentes de seguridad informática y notificación al CSIRT Italia, aprobación del plan, actualización del plan).	3	3
	RS.CO	Notificación y comunicación de la respuesta a incidentes	RS.CO-02	Se informa a *las partes interesadas* internas y externas de los incidentes (adopción de procedimientos para comunicar sin demoras injustificadas, adopción de procedimientos para informar al público sobre los incidentes ocurridos).	2	2
RECUPERACIÓN	RC.RP	Ejecución del plan de recuperación ante incidentes	RC.RP-01	La parte del plan de respuesta a incidentes relativa a la recuperación se ejecuta una vez iniciado el proceso de respuesta a incidentes (adopción de procedimientos para la recuperación, al menos en lo que respecta al restablecimiento del funcionamiento normal de los sistemas informáticos y de red afectados por incidentes de seguridad informática).	1	1
	RC.CO	Comunicación sobre la recuperación tras incidentes	RC.CO-03	Las actividades de recuperación se coordinan con las partes internas y externas (adopción de procedimientos para comunicar a las partes internas interesadas las actividades de recuperación tras un incidente).	1	-

ManagementSolutions
Making things happen

Internacional
Una sola firma

Equipo
Multidisciplinario

Mejores prácticas
Conocimientos técnicos

Experiencia
Demostrada

Máximo
compromiso

CONTACTOS:

Jorge Monge Alonso
Socio - CISO
jorge.monge@managementsolutions.com

Alejandro Iglesias Rodríguez
Socio
alejandro.Iglesias@msspain.com

Para obtener más información sobre la empresa, visite:

www.managementsolutions.com

O en nuestras redes sociales: