Junta de Andalucía

Estrategias de adecuación integrada a la normativa de seguridad de la información (parte I)

Junta de Andalucía

ÍNDICE

Junta de Andalucía

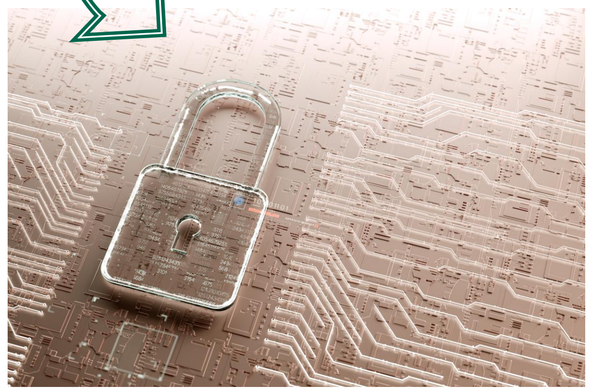
1. Introducción: la necesidad de requisitos regulatorios

Seguro que más vale cumplir que curar

Junta de Andalucía

1.1 Objetivos

- Alcanzar los niveles de confianza a través del cumplimiento legal.
- Patrones para proteger los activos digitales .
- Transformación digital protegida.



- **Disponibilidad**
- **Integridad**
- **Confidencialidad**

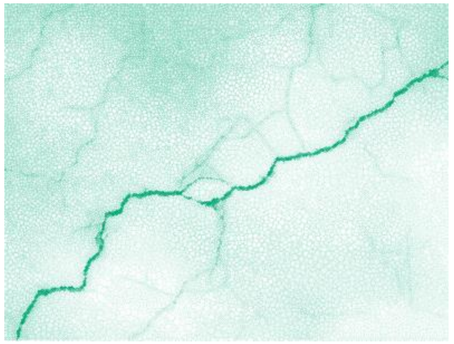
Junta de Andalucía

1.2 Impactos si no nos protegemos

Pérdidas económicas

Infracciones

Daños de imagen



Incluso peligro para las vidas humanas

Junta de Andalucía

1.3 Impactos de una amenaza en una organización

Pérdidas económicas

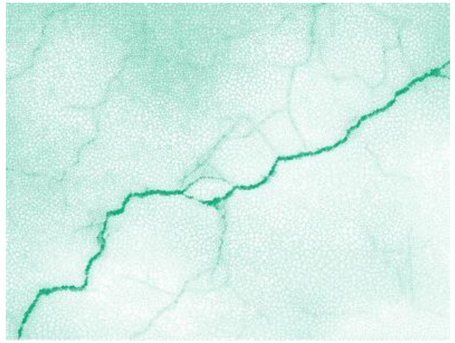
- Por perdida de actividad en caso de indisponibilidad
- Por robo de información (por ejemplo, de tarjetas bancarias)
- Por cese de negocio si se corrompen datos (por ejemplo, si se encriptan)

Infracciones

- No toda la normativa es sancionable directamente (RGPD si lo es, por ejemplo), pero el incumplimiento de una que no lo sea, sí que puede devenir en otro que lo sea.

Daños de imagen

- Perdida reputacional y de confianza ante la sociedad al conocerse que la información está expuesta, sobre todo si es sensible.



Incluso peligro para las vidas humanas

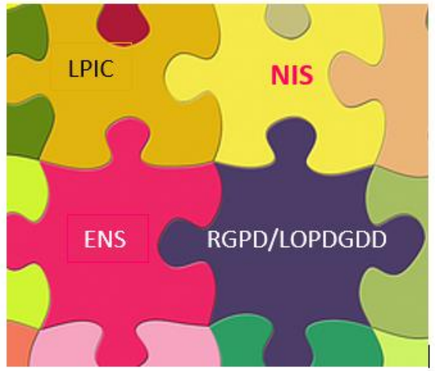
- Algunos ciberincidentes puede causar pérdidas de vidas humanas: accidente en una planta tele controlada, acceso a fórmulas en la industria que puedan causar incluso envenenamiento, indisponibilidad en un hospital.

2. Ecosistema de normativas de seguridad.

Una panoplia normativa con aspectos comunes y relaciones de interdependencia

Junta de Andalucía

2.1 Ecosistema de normativas de seguridad



Esquema Nacional de Seguridad: RD 311/2022 del 3 de mayo

Ley de Protección de Infraestructuras Críticas (LPIC): Ley 8/2011 de 28 de abril

Reglamento de protección de Infraestructuras Críticas (LPIC): Real Decreto 704/2011 de 20 de mayo

Reglamento de protección de datos personales (RGPD): (UE) 679/2106 de 27 de abril

Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD): LO 3/2018 de 5 de diciembre

Directiva NIS: Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016. Relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las **redes y sistemas de información** en la Unión Europea,

Transposición de la Directiva NIS (Ley NIS): Real Decreto-ley 12/2018 de 9 de septiembre

Desarrollo de la Ley NIS (Reglamento NIS): Real Decreto 43/2021 de 26 de enero

Por la Estrategia de Ciberseguridad de la UE para la Década Digital, la Comisión Europea publicó en diciembre de 2020 una **propuesta para reemplazar la actual Directiva NIS**, será más exigente y con régimen sancionador. ¡Por tanto cumplir con la actual es crucial para los futuros más exigentes requisitos!

2.1 Ecosistema de normativas de seguridad (II)

ISO 27001
Sistema de gestión de seguridad de la información

ISO 22301
Continuidad de Negocio.

ISO/IEC 27001: estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005 por la International Organization for Standardization y por la International Electrotechnical Commission y la última versión fue publicada en octubre de 2022.

ISO/IEC 27701: extensión de privacidad a ISO / IEC 27001. El objetivo del diseño es mejorar el Sistema de Gestión de Seguridad de la Información existente con requisitos adicionales para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Información de Privacidad y la última versión es de 2019.

ISO/IEC 22301: define los requisitos que deben cumplir los sistemas de gestión de la continuidad del negocio (SGCN) para asegurar que una organización pueda continuar operando durante y después de situaciones de crisis, como desastres naturales, ciberataques, pandemias, conflictos armados o cualquier otra situación que pueda interrumpir sus actividades y la última versión es de 2019,

3. Requisitos de cumplimiento ¿parecidos, iguales o paralelos?

Junta de Andalucía

3.1 ¿Qué requisitos exigen estas normas en general?

Junta de Andalucía

3.2 ¿Qué medidas técnicas y organizativas se exigen en general?

- Medidas para proteger las diferentes piezas que componen los sistemas de información y operación.
- Medidas de la operación y explotación.
- Otras medidas para mitigar riesgos.

Junta de Andalucía

3.3 Requisitos normativos ¿parecidos, iguales o paralelos a los de otra normativa?

ENS, RGPD/LOPDGDD, LPIC Y NIS
Análisis de riesgos
Activos (identificación, inventario)
Planes de acción
Roles y responsabilidades
Documentación (política, procedimientos, normativas, planes de recuperación)
Gestión de Incidentes/ Violaciones
Seguridad desde el diseño y por defecto
Formación y concienciación
Gestion de terceros
Indicadores
Auditoría
Autoridades competentes

3.4 Resumen de Requisitos

Aplicación de una serie de **medidas de seguridad** para gestionar los **riesgos**. En el caso de los operadores de servicios esenciales tomarán como base el **ENS (¡pero no necesariamente con el mismo alcance!)**

Roles y responsabilidades: entidad responsable de seguridad

Gestion de incidentes: procedimientos y mecanismos de gestion y comunicación al CERT de Referencia (CCN-CERT para públicos que nos sean infraestructura crítica, INCIBE-CERT para privados que no sean infraestructura crítica)

Auditorias: colaboración con las autoridades competentes en caso de una auditoría externa

3.5 Medidas de seguridad

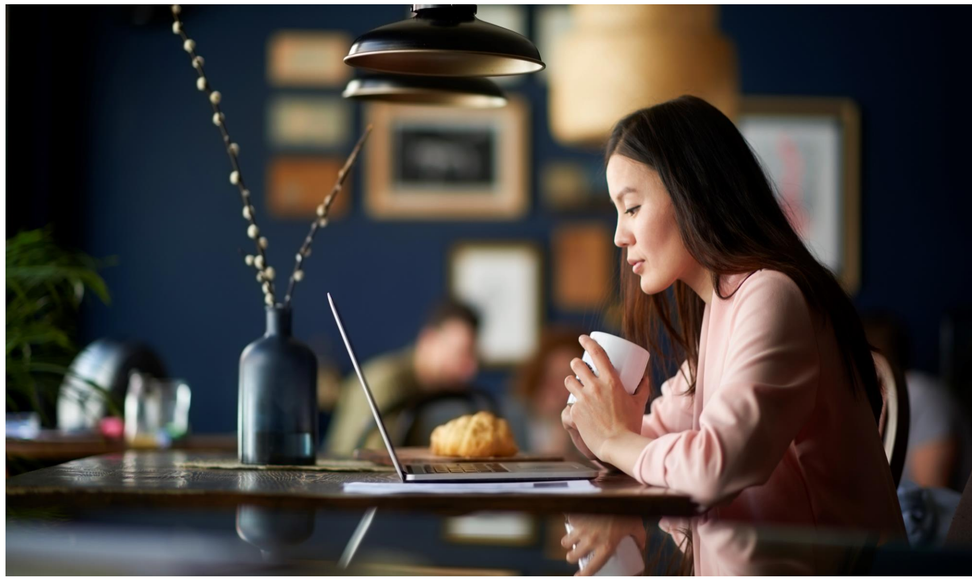
Aplicación de una serie de **medidas de seguridad** para gestionar los **riesgos**.

- Tomarán como base el Anexo II del **ENS** y tener en cuenta **otros estándares internacionalmente reconocidos** (ej.: ISO 27001) y ser complementadas con otras (ej: las que establezca específicamente la autoridad competente de la entidad).
- No olvidar la **dependencia de terceros,** que también deben cumplir con las medidas.
- **Documentar las medidas en la Declaración de Aplicabilidad** (incluida en la política de seguridad).
- Incluir las medidas de protección de los **tratamientos de datos personales** (conforme al análisis de riesgos).

3.6 Roles y responsabilidades

Entidad responsable de seguridad de la Información (persona, unidad u órgano colegiado)

- **Punto de contacto** y coordinación técnica con la autoridad competente y CSIRT de referencia.
- Funciones propias de un **CISO** (proponer las medidas, supervisar, comunicar, capacitar, entre otras). Se podrá apoyar en servicios prestados por terceros.
- Debe tener la debida **independencia** respecto de los responsables de las redes y los sistemas de información, fundamental en los OSEs.
- **Funciones compatibles** con las del Responsable de Seguridad y Enlace (LPIC) y el Responsable de Seguridad del ENS.



Junta de Andalucía

3.7 CSIRT de Referencia

CERT o CSIRT: Son equipos de respuesta a incidentes de seguridad informática.
Los de referencia en materia de seguridad de las redes y sistemas de información son los siguientes:

Incluidos en el ámbito subjetivo de aplicación de la ley 40/2015

NO incluidos en el ámbito subjetivo de aplicación de la ley 40/2015

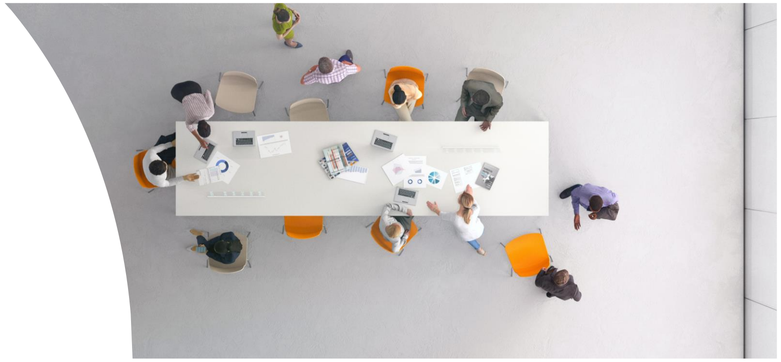
Operado conjuntamente por el **INCIBE y el CNPIC** en la gestión de incidentes que afecten a los operadores críticos

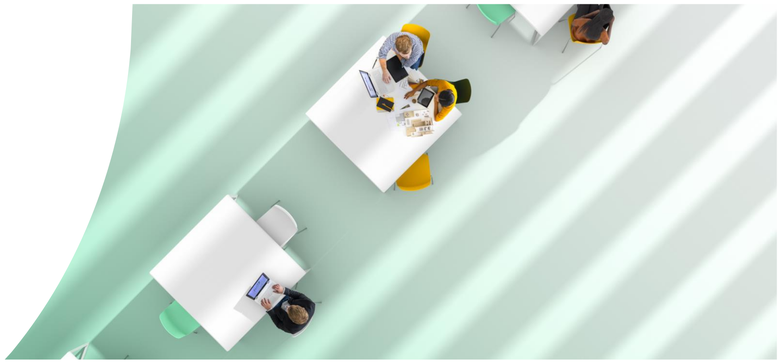
ESPDEF-CERT (CSIRT del Ministerio de Defensa): Coopera con CCN-CERT e INCIBE-CERT si requieren apoyo y en operadores con incidencia en la Defensa Nacional

3.8 Gestión de incidentes

La gestión de incidentes es en sí una medida de seguridad. Se podrá utilizar al CSIRT de referencia ayuda especializada.

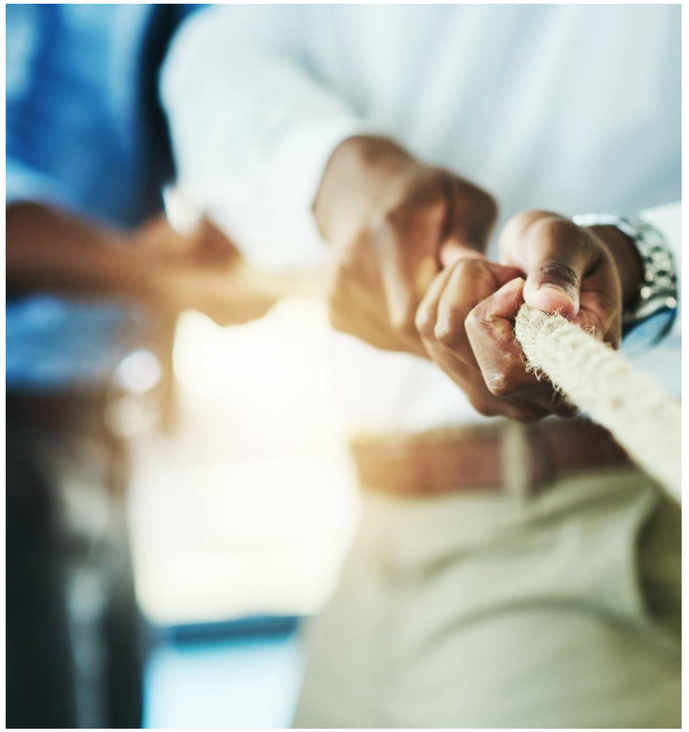
- **Notificación de incidentes**. A su autoridad competentes a través de su CSIRT de referencia y conforme a la **Instrucción nacional de notificación y gestión de ciberincidentes.** Además, puede ser preciso realizar otras notificaciones, por ejemplo a la **AEPD** si hay tratamientos implicados en el ciberincidente.
  - Prevista una plataforma común de notificación de incidentes.
- **Procedimientos de notificación de incidentes.** El responsable de seguridad notifica al CSIRT de referencia.
- **Plataforma Única de notificación**. Se pondrá a disposición (CCN-CERT, INCIBE-CERT y ESPDEF-CERT) como punto único. LUCÍA puede servir como plataforma de notificación centralizada.





3.9 Auditorías

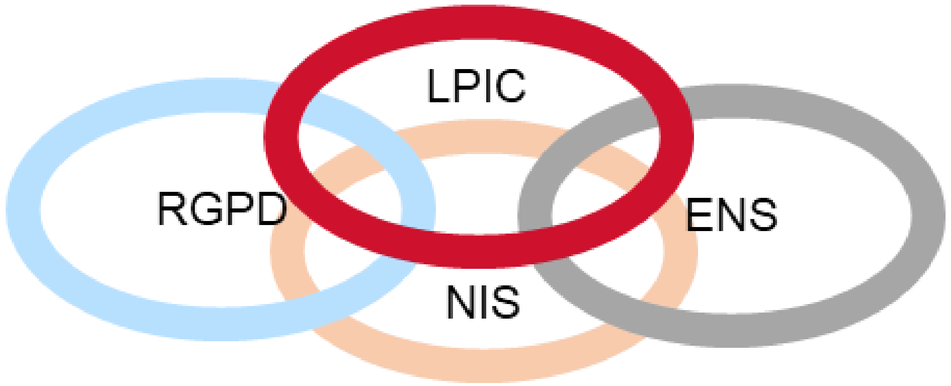
- **Colaboración** con las autoridades competentes en caso de una auditoría externa, ya que las autoridades competentes supervisarán en su ámbito de actuación el cumplimiento de las obligaciones de seguridad y de notificación de incidentes.
- El cumplimiento de las obligaciones de seguridad podrá acreditarse mediante la **certificación** en un esquema de seguridad.
- Las autoridades competentes podrán requerir al operador de servicios esenciales la remisión de un **informe de auditoría**, elaborado por una entidad externa, solvente e independiente, sobre la seguridad de sus redes y sistemas de información.



4 . Los requisitos cruzados – una muestra más de simbiosis normativa.

Junta de Andalucía

4.1 Los requisitos cruzados – una muestra más de simbiosis normativa



Junta de Andalucía

4.2 Requisitos cruzados: una alianza conveniente en la normativa de seguridad

Normativa que exige	Normativa exigida			
	ENS	**RGPD/ LOPDGDD**	**LPIC**	**NIS**
ENS		Mp.info.1		
RGPD/ LOPDGDD	Para administración pública (disposición adicional primera LOPDGDD)			
LPIC	Guías de Buenas Prácticas de contenidos Mínimos PSO y PPEs			
NIS	Artículo 6	Artículo 6.7. Disposición adicional quinta.	Si es IC	

Junta de Andalucía

5. Abordando los requisitos – un enfoque integral.

Junta de Andalucía

5.1 Análisis de Riesgos y gestión de activos

Normativa	Análisis de Riesgos	Gestión de Activos
ENS	Artículo 6. Gestión de la seguridad basada en riesgos Artículo 13. Análisis y gestión de los riesgos Medida - Anexo II.op.pl.1. Análisis de riesgos	Elementos que constituyen el sistema de información utilizado para prestar servicios a los ciudadanos, empleados u tras organizaciones (software, hardware, comunicaciones, etc.)
RGPD/ LOPDGDD	Artículo 32. Seguridad del tratamiento	Tratamientos de datos personales
LPIC	Guías de Buenas Prácticas de contenidos Mínimos PSO y PPEs /(2.2.3. Modelo de gestión aplicado)	Elementos que constituyen el sistema de información de la infraestructura crítica
NIS	Artículo 6. Medidas para el cumplimiento de las obligaciones de seguridad	Elementos que constituyen el sistema de información del servicio esencial o digital

5.2 Planes de acción

Normativa	Planes de Acción
ENS	Plan de Tratamiento de riesgos + plan de cumplimiento = Plan de Mejora de la Seguridad. Plan de Recuperación ante desastres
RGPD/ LOPDGDD	Plan de Tratamiento de riesgos de privacidad+ plan de cumplimiento jurídico = Plan de Cumplimiento RGPD. Necesario por la responsabilidad proactiva. Plan de Recuperación (datos personales) necesario por la responsabilidad proactiva
LPIC	Plan de Seguridad del Operador (PSO) y Planes de Protección Especifica (basados en riesgo). Incluirán Planes de Recuperación,
NIS	Plan de Seguridad basado en riesgos (articulo 6) incluyendo planes de recuperación y aseguramiento de la continuidad de las operaciones.

5.3 Documentación

Normativa	Documentación
ENS	Análisis de riesgo e impacto. Planes de Seguridad/Recuperación, Política, Normativas, Procedimientos. Registros de cumplimiento (evidencias)
RGPD/ LOPDGDD	Análisis de riesgo e impacto y Planes de Seguridad y privacidad, Manual de procedimientos jurídicos, política de privacidad, políticas del encargado o responsable. Registros de cumplimiento (evidencias)
LPIC	Análisis de riesgo e impacto. Plan de Seguridad del Operador (PSO) y Planes de Protección Especifica (basados en riesgo). Política, Normativas, Procedimientos. Registros de cumplimiento (evidencias)
NIS	Análisis de riesgo e impacto. Planes de Seguridad/Recuperación, Política, Normativas, Procedimientos. Registros de cumplimiento (evidencias)

5.4 Roles y responsabilidades

Normativa	Roles y responsabilidades
ENS	Responsable de seguridad Responsable de la información y servicio
RGPD/ LOPDGDD	DPO Encargados y responsable de tratamiento
LPIC	Responsable de Seguridad y Enlace Delegados de Seguridad (funciones concretas)
NIS	Responsable de la seguridad de la información. **Artículo 7. Punto 5.** Siempre que concurran los requisitos de conocimiento, experiencia, independencia y, en su caso, titulación, las funciones y responsabilidades encomendadas al **responsable de la seguridad de la información podrán compatibilizarse con las señaladas para el Responsable de Seguridad y Enlace y el Responsable de Seguridad del Esquema Nacional de Seguridad,** de conformidad con lo dispuesto en la normativa aplicable a estas figuras.

5.5 Gestión de incidencias

Normativa	Gestión de incidentes
ENS	Artículo 24. Incidentes de seguridad. Medida - Anexo II. op.exp.7. Gestión de incidentes. Medida - Anexo II. op.exp.9. Registro de la gestión de incidentes.
RGPD/ LOPDGDD	Violación de la seguridad de los datos personales. Artículo 33 Notificación de una violación de la seguridad de los datos personales a la autoridad de control. Artículo 34 Comunicación de una violación de la seguridad de los datos personales al interesado.
LPIC	Guías de Buenas Prácticas de contenidos Mínimos PSO y PPEs (5. CRITERIOS DE APLICACIÓN DE MEDIDAS DE SEGURIDAD INTEGRAL)
NIS	CAPÍTULO IV Gestión de incidentes de seguridad (gestión, notificación) Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

5.6 Seguridad desde el diseño y por defecto

Normativa	Seguridad desde el diseño
ENS	Artículo 19. Seguridad por defecto. Medida - Anexo II. op.pl.3. Adquisición de nuevos componentes Medida - Anexo II. mp.sw.1. Desarrollo de aplicaciones.
RGPD/ LOPDGDD	Artículo 25 Protección de datos desde el diseño y por defecto.
LPIC	Guías de Buenas Prácticas de contenidos Mínimos PSO y PPEs (5. CRITERIOS DE APLICACIÓN DE MEDIDAS DE SEGURIDAD INTEGRAL Desarrollo seguro de aplicaciones)
NIS	Indirectamente (por el cumplimiento del ENS)

5.7 Formación y concienciación

Normativa	Formación y concienciación
ENS	Artículo 15. Profesionalidad. Medida - Anexo II. mp.per.3. Concienciación Medida - Anexo II. mp.per.4. Formación
RGPD/ LOPDGDD	Necesario por la responsabilidad proactiva. Artículo 39. Funciones del DPO 1.b) supervisar las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la concienciación y formación del personal que participa en las operaciones de tratamiento.
LPIC	Guías de Buenas Prácticas de contenidos Mínimos PSO y PPEs (2.2. Marco de gobierno, Formación y concienciación)
NIS	Indirectamente (por el cumplimiento del ENS)

5.8 Gestión de terceros

Normativa	Gestión de terceros
ENS	op.ext. Servicios externos
RGPD/ LOPDGDD	Artículo 28 Encargado del tratamiento
LPIC	Guías de Buenas Prácticas PPE (Relaciones con terceros)
NIS	Indirectamente (por el cumplimiento del ENS). Articulo 6. b) Gestión de riesgos de terceros o proveedores.

5.9 Auditorías e indicadores

Normativa	Auditoria e indicadores
ENS	Artículo 34. Auditoría de la seguridad. Anexo III. Auditoría de la Seguridad Artículo 35. Informe de Estado de la Seguridad (INES) Medida - Anexo II.op.mon.2. Sistema de Métricas
RGPD/ LOPDGDD	Necesario auditar periódicamente por la responsabilidad proactiva. Artículo 39. Funciones del DPO 1.b)supervisar el cumplimiento de lo dispuesto en el presente Reglamento – Los resultados de esta supervisión deberían ser evaluados (cuantificados).
LPIC	Guías de Buenas Prácticas de contenidos Mínimos PSO y PPEs (2.2. Marco de gobierno, Modelo de gestión aplicado basado en PDCA)
NIS	Indirectamente (por el cumplimiento del ENS) Capitulo V. supervisión (por parte de las autoridades competentes).

5.9 Autoridades competentes

Autoridades competentes	ENS	RGPD/ LOPDGDD	LPIC	NIS
CCN centro criptológico nacional	X			Públicos
aepd agencia española protección datos · Consejo de Transparencia y Protección de Datos de Andalucía		X		
CNPIC			X	Si es IC
Ministerios (y consejos)				Si no es IC ni público
Banco de España · CNMV Comisión Nacional del Mercado de Valores				Sector Financiero

Junta de Andalucía

5.10 Las políticas de la Junta de Andalucía y su normativa asociada: otra pieza que encaja en el puzle de la integración

- ✓ ***Decreto 1/2011***, *de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.*

- ✓ ***Decreto 70/2017,*** *de 6 de junio, por el que se modifica el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.*

- ✓ ***Decreto 171/2020***, *de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía.*

ENS, RGPD/LOPDGDD, LPIC/ NIS Y NORMATIVA JDA	
Análisis de riesgos, activos y planes de acción	Principio de Gestión de riesgos. Evaluación de riesgos y Planes de Seguridad Interior.
Roles y responsabilidades	Comités de Seguridad Interior y Seguridad TIC de Consejerías o entidades dependientes.
Gestión de Incidentes/ Violaciones	· Principio de prevención. Grupo de Respuesta a incidentes en el comité. · Normas sobre gestión de incidentes de seguridad TIC. · Coordinación para la gestión de incidentes de seguridad interior.
Formación y concienciación	Principio de concienciación y formación. Formación en seguridad interior.

Junta de Andalucía

6. CONCLUSIONES

Junta de Andalucía

5.1 Cumplir para protegerse

Cuatro normativas, un ecosistema de coincidencias y sinergias que permiten abordar la seguridad como proceso integral

Seguridad técnica

Nombramientos de Responsables

Marco de gestión

Formación y concienciación

Análisis de riesgos

Planes de acción

Auditoría

Indicadores

Activos (inventario)

Documentación

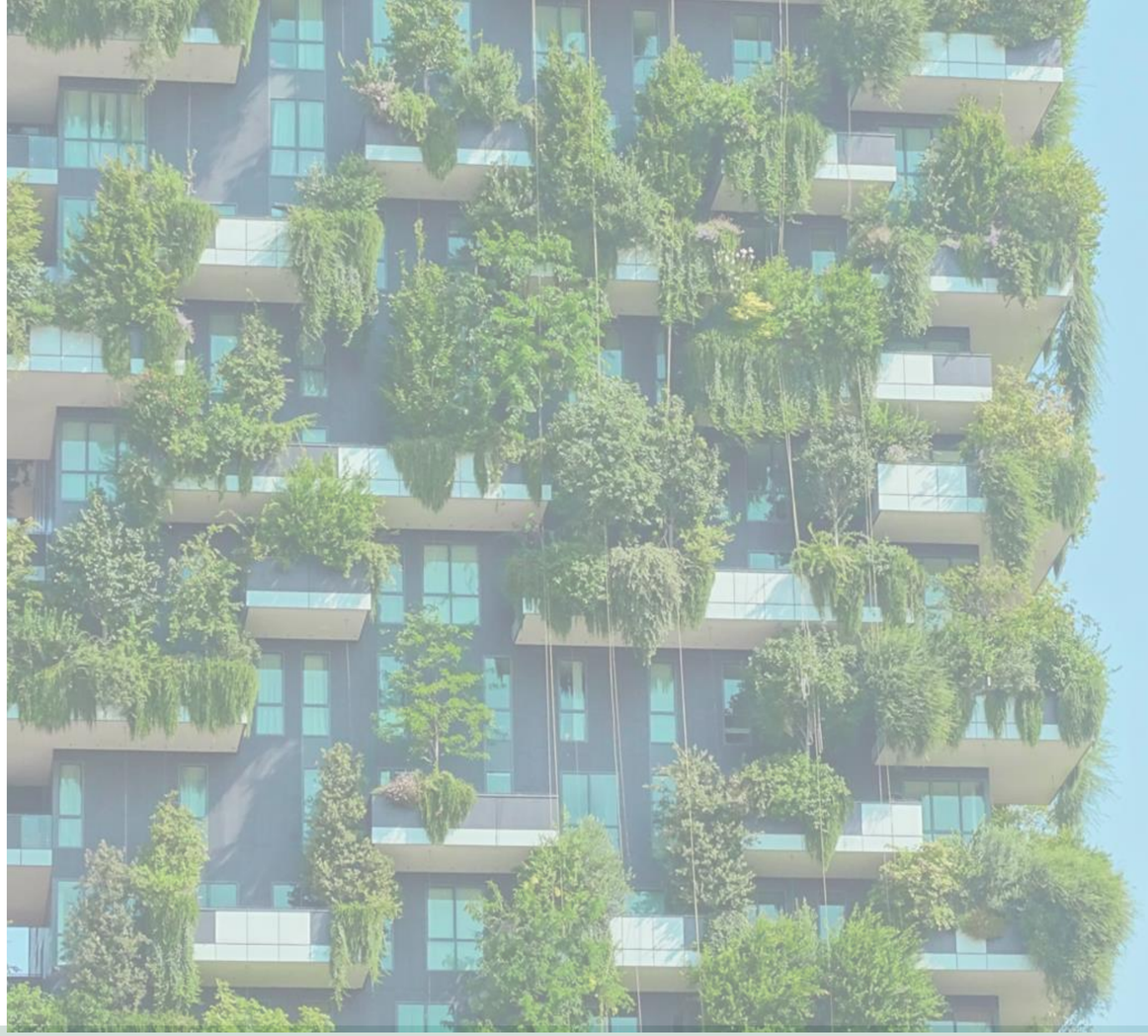
Gestión de Incidentes

Junta de Andalucía

5.2 Integración

La integración multinorma como mecanismo para atajar las dificultades de cumplimiento

Con la integración, hemos atajado parte de los escollos



Junta de Andalucía

5.2 Conclusión

La seguridad como proceso integral tiene sus beneficios

Requisitos de seguridad y de cumplimiento

Información y los sistemas de la manejan

Seguridad implantada, gestionada eficazmente y con garantías de cumplimiento

✓Seguridad de la información como un importante proceso corporativo gestionado de forma eficaz.

Junta de Andalucía

7. Ruegos y Preguntas

Junta de Andalucía

Junta de Andalucía