Junta de Andalucía

REQUISITOS DE SEGURIDAD EXIGIBLES A PROVEEDORES. ENS Y RGPD

Junta de Andalucía

ÍNDICE

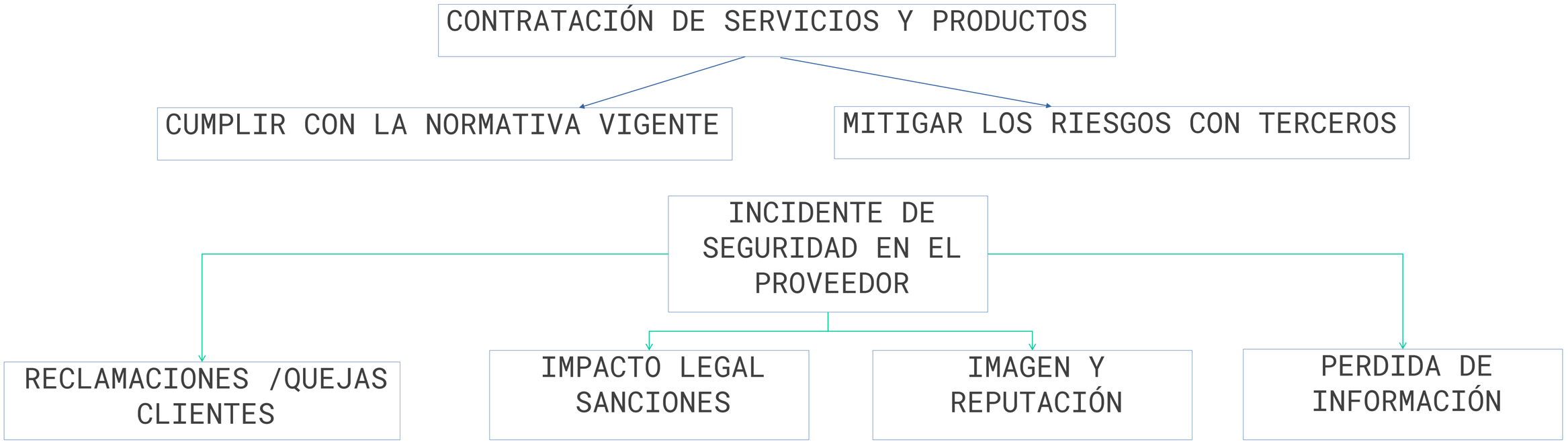
1. Introducción
2. Requisitos RGPD
3. Requisitos ENS
4. Requisitos futuros IA
5. Evidenciar.
6. Conclusiones
7. Referencias
8. Ruegos y Preguntas.

Junta de Andalucía

1. INTRODUCCIÓN

Junta de Andalucía

1. Introducción



Junta de Andalucía

1. Introducción

NORMATIVAS OBLIGATORIAS

- RGPD (Reglamento Protección Datos)
- ENS (Esquema Nacional de Seguridad)
- NIS 2 Directiva (UE) 2022/2555 sobre medidas de ciberseguridad
- DORA (Reglamento de Resiliencia Operativa Digital)
- Reglamento de Inteligencia Artificial
- Decreto 443/2024, por el que se establece el Esquema Nacional de **Seguridad** de **redes** y servicios **5G**

OBLIGACIONES CON TERCEROS:
- realizar comprobaciones sobre su sistema de seguridad y/o protección de datos …etc.
- favorecer una toma de decisiones
- establecer garantías

PRVEEDORES (servicios o productos)
AGENTES, PARTNERS, COLABORADORES, ETC.

Junta de Andalucía

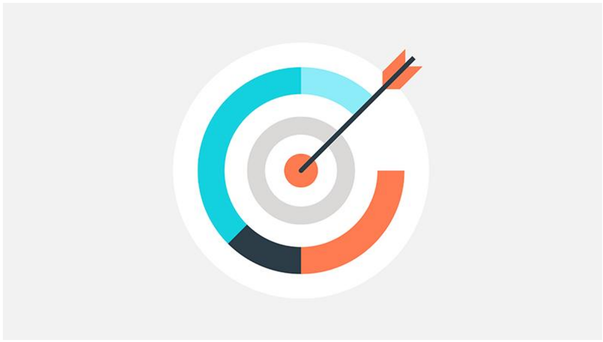
2. REQUISITOS RGPD

Junta de Andalucía

2.1 Regulación

Artículo 28 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 (RGPD)

Artículo 33 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)



MEDIDAS DE SEGURIDAD:
Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

2.2 Requisitos

CONTRATO DE ENCARGADO DE TRATAMIENTO:
Debe existir un contrato escrito entre el responsable del tratamiento (la empresa que decide sobre el tratamiento de datos) y el encargado del tratamiento (el proveedor).
Este contrato debe detallar la naturaleza, la duración, el propósito del tratamiento, los tipos de datos personales y las categorías de interesados.

SEGURIDAD:
El proveedor debe implementar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Esto incluye la pseudonimización y el cifrado de datos personales, la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios, y la capacidad de restaurar la disponibilidad y el acceso a los datos de manera oportuna en caso de un incidente físico o técnico.

SUBCONTRATACIÓN:
El proveedor no puede recurrir a otro subcontratista sin la autorización previa específica o general por escrito del responsable del tratamiento.
Si se subcontrata alguna parte del tratamiento, el proveedor debe asegurarse de que el subcontratista cumpla con los mismos requisitos de protección de datos.

aepd agencia española protección datos

Junta de Andalucía

2.2 Requisitos

NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD:
El proveedor debe notificar sin demora indebida al responsable del tratamiento sobre cualquier violación de seguridad de los datos personales.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO:
Los proveedores deben mantener un registro de todas las categorías de actividades de tratamiento realizadas por cuenta del responsable del tratamiento.

CONFIDENCIALIDAD:
El proveedor debe asegurarse de que las personas autorizadas para tratar los datos personales se hayan comprometido a la confidencialidad o estén bajo una obligación legal adecuada de confidencialidad.

EVALUACIÓN DE IMPACTO:
El proveedor debe asistir al responsable del tratamiento en la realización de evaluaciones de impacto sobre la protección de datos y en la consulta previa con la autoridad de control, cuando sea necesario.

DERECHOS DE LOS INTERESADOS:
El proveedor debe ayudar al responsable del tratamiento a cumplir con las obligaciones de responder a las solicitudes para ejercer los derechos de los interesados, como el acceso, rectificación, supresión y portabilidad de los datos.

2.3 En la práctica

NO EXISTE UN CERTIFICADO PARA VERIFICAR LA ADECUACIÓN AL RGPD y LOPDGDD

CUMPLIMIENTO NORMATIVO

MEDIDAS A COMPROBAR

Junta de Andalucía

2.3 En la práctica. Checklist

	Pregunta	Sí	No
1	¿Garantiza que cumple con las directrices del RGPD, y, en consecuencia, adopta las medidas de seguridad que establece?		
2	¿Tiene política de seguridad de la información y privacidad?		
3	¿Se ha sometido a auditoria de privacidad o protección de datos en los últimos dos años?		
4	¿Realiza los pertinentes análisis de riesgo y evaluaciones de impacto?		
5	¿Tiene un procedimiento para tratar y comunicar las posibles brechas de seguridad?		
6	¿Dispone de DPO? (Caso de que sea necesario)		
7	Dispone de protocolo para tratar todo tipo de incidencias de seguridad		
8	Si es necesario, ¿cuenta con un registro de actividades de tratamiento?		

	Pregunta	Sí	No
9	¿Asume, mediante su firma, las cláusulas de confidencialidad e instruye a sus empleados sobre las mismas y a la debida confidencialidad que tienen que observar con los datos personales que tratan?		
10	Indique las principales certificaciones o estándares que posee la Compañía en materia de seguridad de la información (ISO 27001, ISO-25999,...) (Indique certificación, entidad certificadora, y fecha de certificación)		
11	¿Aplica medios para detectar vulnerabilidades tecnológicas y procesos para corregirlas?		
12	¿Subcontrata a terceros para llevar a cabo la prestación de sus servicios?		
13	Si subcontrata con terceros, ¿les comunica las cláusulas/exige las medidas de seguridad requeridas?		
14	¿Disponen de un Plan de Continuidad de Negocio?		

2.3 En la práctica. Checklist medidas seguridad

MEDIDAS DE SEGURIDAD EN BASE A RLOPD Real Decreto 1720/2007, de 21 de diciembre de protección de datos de carácter personal.	
Derechos Acceso, Rectificación, Cancelación y Oposición	Debe existir un procedimiento para dar respuesta a los interesados. Las indicaciones para que los interesados ejerciten sus derechos, deben estar informadas (cláusulas LOPD)
Acceso a datos a través de redes de comunicaciones	Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local
Registro de incidencias	Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.
Copias de respaldo y recuperación	1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. 2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. 3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos. 4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales.
Responsable de seguridad	En el documento de seguridad deberán designarse uno o varios responsables de seguridad.
Registro de accesos	1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. 3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos. 4. El período mínimo de conservación de los datos registrados será de dos años. 5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
Telecomunicaciones	La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.
Dispositivos de almacenamiento	Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

3.REQUISITOS ENS

Junta de Andalucía

3.1. Regulación

REAL DECRETO 311/2022 sobre Esquema Nacional de Seguridad

“El artículo 2 del vigente Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, dispone que los pliegos de prescripciones administrativas o técnicas de **los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación del real decreto del ENS contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el mismo de los sistemas de información en los que se sustenten los servicios prestados por los contratistas**, tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS. Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

Así pues, en base a lo anterior, y al análisis de los riesgos a los que están expuestos los suministros y servicios objeto de la licitación, la ENTIDAD CONTRATANTE establece como necesario **que la ENTIDAD LICITADORA deberá estar en condiciones de exhibir la correspondiente Declaración o Certificación de Conformidad con el Esquema Nacional de Seguridad, para la categoría de seguridad [indicar la CATEGORÍA], o superior, de los sistemas que intervengan en la prestación de los servicios indicados, así como mantener la conformidad en vigor durante la vigencia del contrato**. Dicha declaración, o certificado, de conformidad con el ENS se entiende que debe abarcar en su alcance, como mínimo, el ámbito objeto de la contratación.

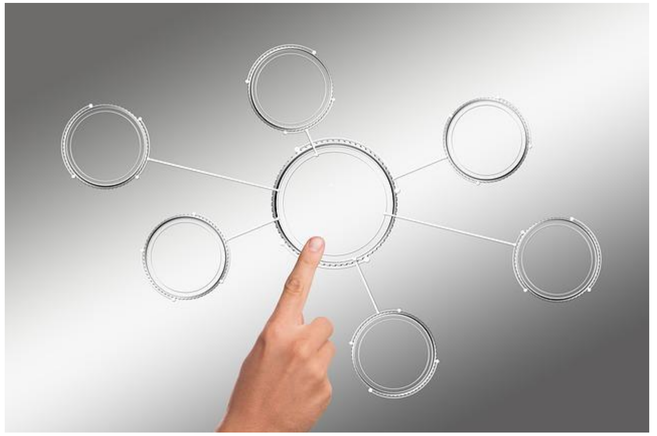
En el supuesto de **que el adjudicatario no pudiera mantener la conformidad con el ENS** durante la vigencia del contrato -por pérdida, retirada o suspensión de la Certificación de Conformidad o imposibilidad de mantener la Declaración de Conformidad-, deberá comunicar esta circunstancia, de forma inmediata y sin dilación indebida, a la **ENTIDAD CONTRATANTE, quien considerará el impacto de dicha circunstancia en la prestación objeto del contrato”**.

3.1. Regulación

REAL DECRETO 311/2022 sobre Esquema Nacional de Seguridad

Artículo 22. Los Puntos o Personas de Contacto (POC)

De conformidad con lo previsto en el apartado 5, del artículo 13 del ENS, en el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos directivos, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio. Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma.



3.2 Requisitos exigibles ENS

SOLICITAR LA DECLARACIÓN DE CONFORMIDAD Y/O CERTIFICACIÓN EN EL ENS

Es importante determinar la categoría exigible a terceros

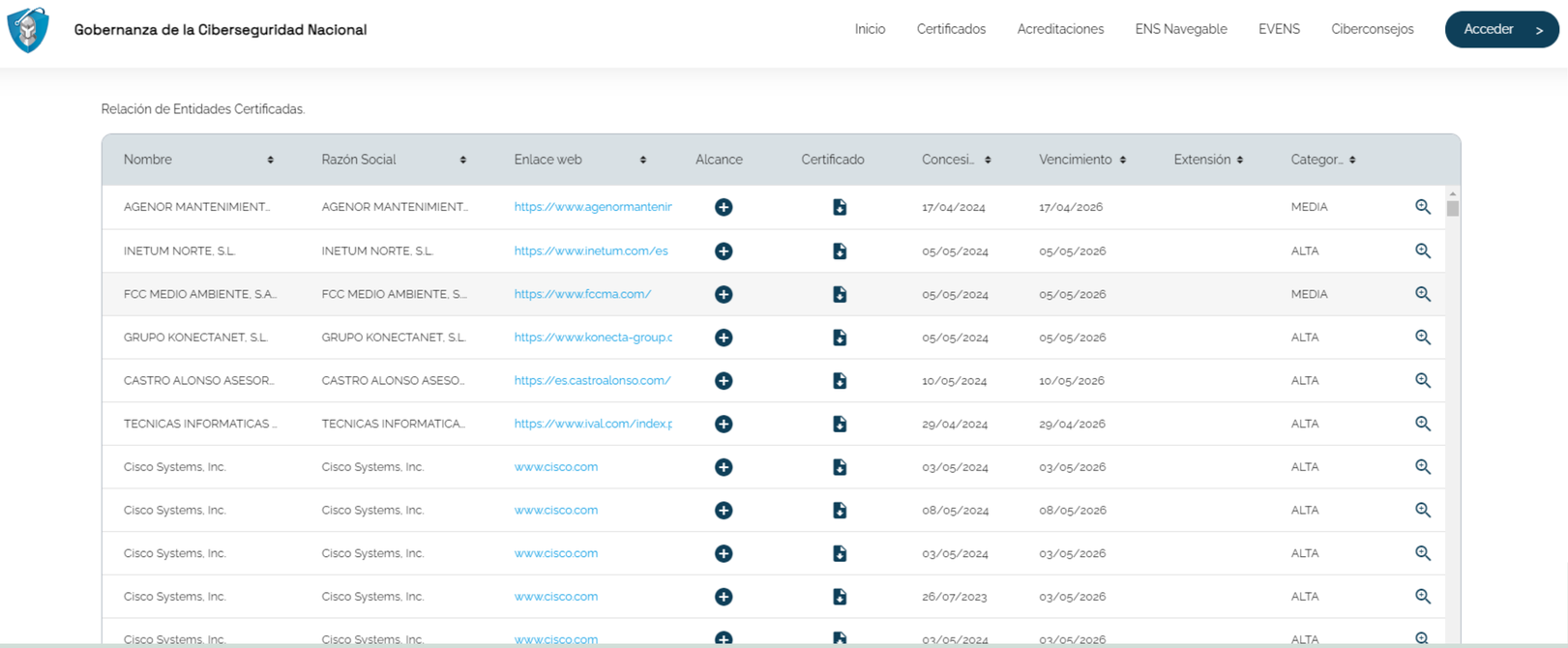
- CATEGORÍA BÁSICA
- CATEGORÍA MEDIA
- CATEGORÍA ALTA

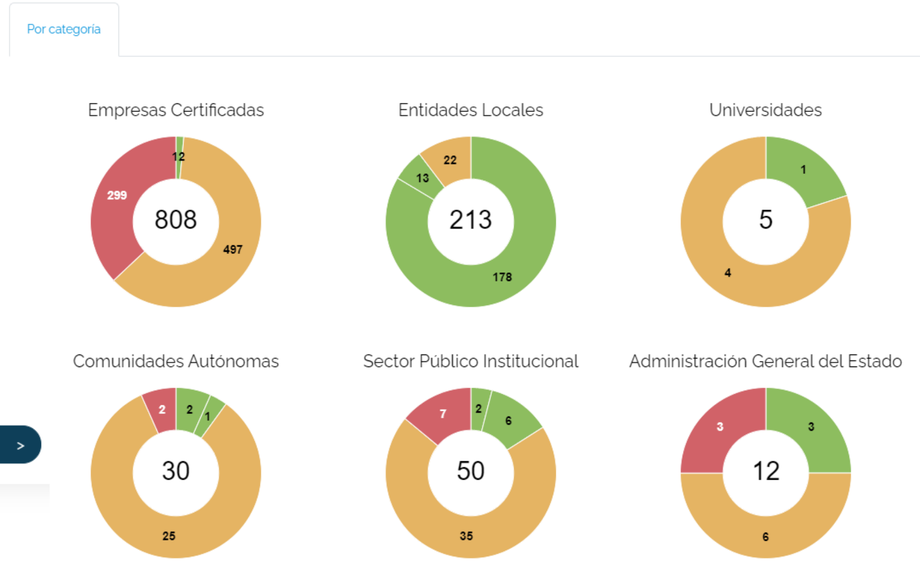
Junta de Andalucía

3.2 Requisitos exigibles ENS

ENTIDADES CERTIFICADAS

https://ens.ccn.cni.es/es/certificacion





Junta de Andalucía

3.2 Requisitos exigibles ENS proveedores

COMPONENTES CERTIFICADOS

Dimensiones: Todas		
B	M	A
n.a.	aplica	aplica

Componentes certificados [op.pl.5]

Sobre su contenido

REQUISITOS:

- ☐ NI [op.pl.5.1] ***Se utilizará el Catálogo*** *de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación* ***(CPSTIC) del CCN****, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas del RD 311/2022.*
- ☐ [op.pl.5.2] ***Si el sistema suministra un servicio de seguridad a un tercero*** *bajo el alcance del ENS,* ***el producto*** *o productos que suministren dicho servicio* ***deben superar un proceso de cualificación*** *y ser incluido en el CPSTIC, o aportar una certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento.*

☐ NI	¿Caso de no existir en el catálogo CPSTIC, o ante cualquier causa de fuerza mayor, se emplean otros productos certificados según se indica en el art. 19 del RD 311/2022, de 3 de mayo? *NOTA: En dicho supuesto podrían ser aceptables productos al corriente de otras certificaciones de seguridad de producto, como es Common Criteria (norma ISO/IEC 15408).*

Junta de Andalucía

3.2 Requisitos exigibles ENS

Cuáles son los productos y servicios certificados aceptados por CCN

CCN-STIC 105
Catálogo de Productos y Servicios STIC (CPSTIC)

Productos y Servicios Cualificados

CCN-STIC 106
Procedimiento de inclusión de productos y servicios STIC cualificados en el CPSTIC

CCN-STIC 140
Taxonomías de referencia para productos y servicios STIC

Productos Conformidad y Gobernanza de la Seguridad

CCN-STIC 140
Taxonomías de referencia para productos y servicios STIC

Productos Aprobados

CCN- STIC 102
Procedimiento para la Aprobación de Productos de seguridad TIC para manejar Información Nacional Clasificada

CCN-STIC 130
Requisitos de Aprobación de Productos de Cifra para Manejar Información Nacional Clasificada

CCN-STIC 151
Evaluación y Clasificación TEMPEST de equipos

Junta de Andalucía

3.2 Requisitos exigibles ENS

Exigencias del ENS en categoría MEDIA Y ALTA

Dimensiones: Todas		
B	M	A
n.a.	aplica	aplica

Componentes certificados [op.pl.5]

SI NO ESTÁN CERTIFICADOS

Posible medida complementaria de vigilancia:

- Reunión del comité de seguridad adoptando la decisión de adquirir componentes certificados a la renovación de los existentes.
- Aumentar la monitorización sobre los activos en cuestión.
- Atención prioritaria a los avisos de CVE, y de otras vulnerabilidades o situaciones que afecten a dichos activos, en especial del CERT de referencia.

Junta de Andalucía

3.2 Requisitos exigibles ENS

Exigencias del ENS en categoría MEDIA Y ALTA

Dimensiones: Todas		
B	M	A
n.a.	aplica	aplica

Componentes certificados [op.pl.5]

EVIDENCIAS →

Posibles evidencias

- ❑ Evidencia de inclusión en el catálogo CPSTIC como producto cualificado (o aprobado).
- ❑ Evidencia de otras certificaciones de producto o servicio.
- ❑ Evidencia de producto aprobado libre de emanaciones TEMPEST.

Junta de Andalucía

3.2 Requisitos exigibles ENS

Dimensiones: Todas		
B	M	A
aplica	+R1	+R1+R2

Protección de servicios en la Nube [op.nub.1]

SERVICIOS EN NUBE

Sobre su contenido y gestión

REQUISITOS:

- op.nub.1.1]*Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el* ***conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten****: Software como Servicio (Software as a Service SaaS), Plataforma como Servicio (Platform as a Service PaaS) e Infraestructura como Servicio (Infrastructure as a Service IaaS) definidas en las guías CCN-STIC que sean de aplicación.*
- [op.nub.1.2]*Cuando se utilicen* ***servicios en la nube suministrados por terceros****, los sistemas de información que los soportan deberán ser* ***conformes con el ENS*** *o* ***cumplir con las medidas desarrolladas en una guía CCN-STIC*** *que incluirá, entre otros, requisitos relativos a:*
  - *Auditoría de pruebas de penetración (pentesting).*
  - *Transparencia.*
  - *Cifrado y gestión de claves.*
  - *Jurisdicción de los datos.*

NUEVO!

Esquema Nacional de Seguridad

CCN centro criptológico nacional

Junta de Andalucía

3.2 Requisitos exigibles ENS

Dimensiones: Todas		
B	M	A
aplica	+R1	+R1+R2

Protección de servicios en la Nube [op.nub.1]

Sobre su contenido y gestión

NUEVO!

Refuerzo R1 (Servicios certificados):

- [op.nub.1.r1.1]*Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar* ***certificados bajo una metodología de certificación reconocida*** *por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.*
- [op.nub.1.r1.2]***Si el servicio en la nube es un servicio de seguridad*** *deberá cumplir con los requisitos establecidos en [op.pl.5].*

Refuerzo R2 (Guías de configuración de seguridad específicas):

- [op.nub.1.r2.1]*La* ***configuración de seguridad*** *de los sistemas que proporcionan estos servicios deberá realizarse* ***según la correspondiente Guía CCN-STIC de Configuración de Seguridad*** *Específica, orientadas tanto al usuario como al proveedor.*

ens Esquema Nacional de Seguridad

CCN centro criptológico nacional

Junta de Andalucía

3.2 Requisitos exigibles ENS

Dimensiones: Todas		
B	M	A
aplica	+R1	+R1+R2

Protección de servicios en la Nube [op.nub.1]

EVIDENCIAS →

Posibles evidencias
❑ Informe o checklist de verificación de requisitos de seguridad de la solución en la nube. ❑ Evidencia de conformidad con el ENS de la solución en la nube. ❑ Evidencia de pruebas de penetración.
❑ Certificado de conformidad con el ENS del sistema de información que soporta la solución en la nube. ❑ Referencia a inclusión en el catálogo CPSTIC si es una solución de seguridad en la nube.
❑ Evidencia del empleo de las guías CCN-STIC para la configuración de seguridad del sistema en la nube.

Junta de Andalucía

3.2 Requisitos exigibles ENS. Continuidad

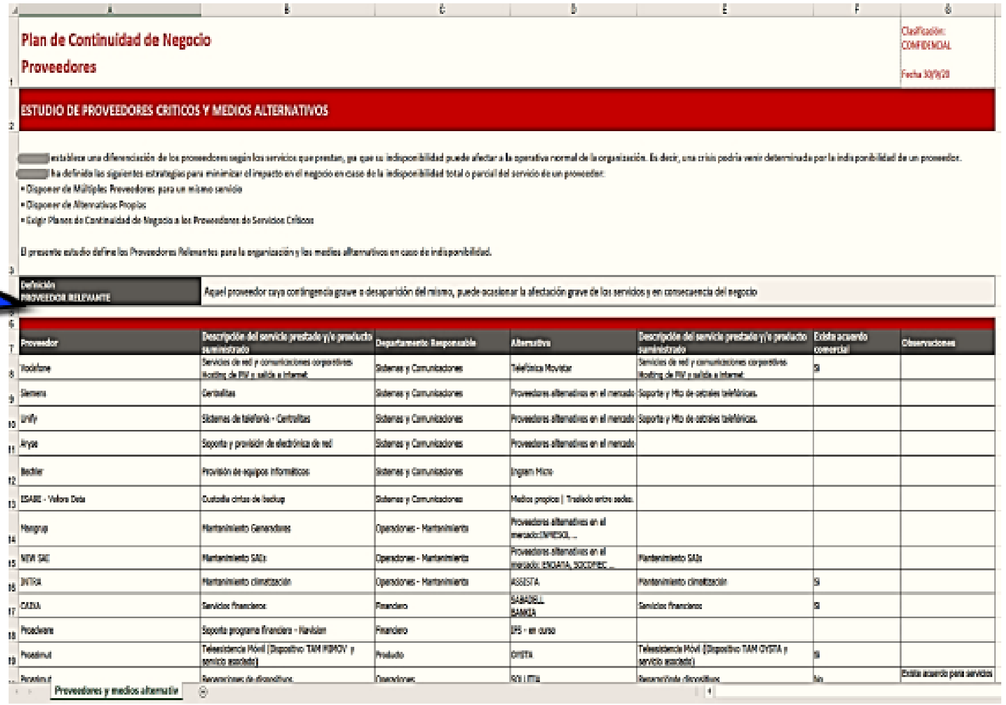
Dimensiones: D		
B	M	A
n.a.	n.a.	aplica

Medios alternativos [op.cont.4]

Sobre su contenido y gestión

REQUISITOS:

- [op.cont.4.1]*Estará prevista la **disponibilidad de medios alternativos** para poder seguir prestando servicio cuando los medios habituales no estén disponibles. En concreto se cubrirán los siguientes elementos del sistema:*
  - *Servicios contratados a terceros*
  - *Instalaciones alternativas*
  - *Personal alternativo*
  - *Equipamiento informático alternativo*
  - *Medios de comunicación alternativos*
- [op.cont.4.2]*Se establecerá un **tiempo máximo para que los medios alternativos entren en funcionamiento**.*
- [op.cont.4.3]*Los medios alternativos estarán **sometidos a las mismas garantías de seguridad** que los originales.*



Plan de Continuidad de Negocio

Proveedores

Clasificación: CONFIDENCIAL

Fecha 30/9/20

ESTUDIO DE PROVEEDORES CRITICOS Y MEDIOS ALTERNATIVOS

establece una diferenciación de los proveedores según los servicios que prestan, ya que su indisponibilidad puede afectar a la operativa normal de la organización. Es decir, una crisis podría venir determinada por la indisponibilidad de un proveedor.

ha definido las siguientes estrategias para minimizar el impacto en el negocio en caso de la indisponibilidad total o parcial del servicio de un proveedor:

- Disponer de Múltiples Proveedores para un mismo servicio
- Disponer de Alternativas Propias
- Exigir Planes de Continuidad de Negocio a los Proveedores de Servicios Críticos

El presente estudio define los Proveedores Relevantes para la organización y los medios alternativos en caso de indisponibilidad.

Definición PROVEEDOR RELEVANTE	Aquel proveedor cuya contingencia grave o desaparición del mismo, puede ocasionar la afectación grave de los servicios y en consecuencia del negocio

Proveedor	Descripción del servicio prestado y/o producto suministrado	Departamento Responsable	Alternativa	Descripción del servicio prestado y/o producto suministrado	Existe acuerdo comercial	Observaciones
Vodafone	Servicios de red y comunicaciones corporativos Hosting de RSV a salida a Internet	Sistemas y Comunicaciones	Telefónica Movistar	Servicios de red y comunicaciones corporativos Hosting de RSV a salida a Internet	SI	
Siemens	Centralitas	Sistemas y Comunicaciones	Proveedores alternativos en el mercado	Soporte y Mto de centrales telefónicas.		
Unify	Sistemas de telefonía - Centralitas	Sistemas y Comunicaciones	Proveedores alternativos en el mercado	Soporte y Mto de centrales telefónicas.		
Aryse	Soporte y provisión de electrónica de red	Sistemas y Comunicaciones	Proveedores alternativos en el mercado			
Bechtler	Provisión de equipos informáticos	Sistemas y Comunicaciones	Ingram Micro			
ESABE - Veloce Data	Custodia cintas de backup	Sistemas y Comunicaciones	Medios propios | Traslado entre sedes.			
Hengrup	Mantenimiento Generadores	Operadores - Mantenimiento	Proveedores alternativos en el mercado:ENPRESOL ...			
NEW SAE	Mantenimiento SAIs	Operadores - Mantenimiento	Proveedores alternativos en el mercado: ENDATA, SOCOMEC ...	Mantenimiento SAIs		
INTRA	Mantenimiento climatización	Operadores - Mantenimiento	ASSISTA	Mantenimiento climatización	SI	
CAIXA	Servicios Financieros	Financiero	SABADELL BANKIA	Servicios financieros	SI	
Procalvare	Soporte programa financiero - Navision	Financiero	EPS - en curso			
Procalmut	Televisencia Movil (Dispositivo TAM MIMOV y servicio asociado)	Producto	CYSTA	Televisencia Movil (Dispositivo TAM CYSTA y servicio asociado)	SI	
Procalmut	Reparaciones de dispositivos	Operadores	SOS ITTA	Reparaciones dispositivos	No	Existe acuerdo para servicios

Proveedores y medios alternativ

NUEVO!

Servicios contratados a terceros (**sector privado**)

Junta de Andalucía

3.2 Requisitos exigibles ENS

Dimensiones: D		
B	M	A
n.a.	n.a.	aplica

Medios alternativos [op.cont.4]

El Sector Público, en base a la "**Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014**" (LCSP), debe someter a la misma todos los procesos de contratación. En consecuencia, no puede disponer de proveedores alternativos a no ser que diversifique una misma necesidad de contratación en dos de ellos mediante concurso público. Tener pensado de antemano un proveedor concreto de reserva, contradice el espíritu de concurso abierto y libre concurrencia por el que debe regirse la contratación pública.

No obstante, como sea que en el sector público se suele presentar más de un proveedor por concurso, podría conservarse toda la documentación aportada por éstos que, en determinados casos de emergencia, tal vez permitiría realizar un contrato de urgencia que, aunque parcial, permitiría disponer de contingencia hasta que se publique el nuevo concurso abierto para sustituir al contratista anterior.

En su lugar, se considera quizá efectivo redactar cláusulas en los pliegos que aporten garantías de aseguramiento del servicio ofrecido por parte del proveedor.

Servicios contratados a terceros (**sector público**)

Junta de Andalucía

Esquema Nacional de Seguridad

CCN centro criptológico nacional

3.2 Requisitos exigibles ENS

Dimensiones: D		
B	M	A
n.a.	n.a.	aplica

Medios alternativos [op.cont.4]

Posibles evidencias

- ❑ Inventario constando los medios alternativos involucrados en la recuperación.
- ❑ Contratos y acuerdos de nivel de servicio de los medios alternativos contratados a terceros.

- ❑ Evidencia de transferencia automática a los medios alternativos.

3.2 Requisitos exigibles ENS. Aplicaciones

Dimensiones: Todas		
B	M	A
aplica	+R1	+R1

Aceptación y puesta en servicio [mp.sw.2]

Posibles evidencias

- ❑ Evidencia de pruebas y verificación de los criterios de aceptación en materia de seguridad.
- ❑ Evidencia de verificaciones de integridad respecto a la seguridad de otras aplicaciones y/o elementos.
- ❑ Informes de pentesting.
- ❑ Si procede, guías de instalación y configuración segura del sistema, facilitadas por los proveedores.
- ❑ Si procede, guías de uso seguro del sistema, facilitadas por los proveedores.
- ❑ Si procede, guías de relación entre cliente y proveedor, facilitadas por los proveedores.

- ❑ Evidencia del entorno de preproducción o test para pruebas.

Junta de Andalucía

3.2 Requisitos exigibles ENS

Dimensiones: Todas		
B	M	A
aplica	+R1	+R1

Deberes y obligaciones [mp.per.2]

Cláusulas de **confidencialidad** // protección de datos

EMPLEADOS PÚBLICOS:

Respecto al empleado público, ya sea éste funcionario o personal laboral, la confidencialidad es inherente a su condición, según el "**Real Decreto Legislativo 5/2015**", de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público que, en su artículo 53.12 sobre Principios Éticos, señala: "*Guardarán secreto de las materias clasificadas u otras cuya difusión esté prohibida legalmente, y mantendrán la debida discreción sobre aquellos asuntos que conozcan por razón de su cargo, sin que puedan hacer uso de la información obtenida para beneficio propio o de terceros, o en perjuicio del interés público*".

Empleado público


AJUNTAMENT DE VALENCIA

Acuerdo de Confidencialidad

En València, a ___ de _____ de ____

REUNIDOS

De una parte, ***, con DNI ***, actuando en nombre y representación del Ay
de València, con CIF ***, y con domicilio a efectos del presente
adelante, ORGANISMO)

Y de otra, ***, actuando en nombre propio o en nombre y representación
sea física o jurídica), con CIF ***, y con domicilio a efectos del presente acu
(en adelante, PROVEEDOR)

Ambas partes se reconocen recíprocamente la capacidad legal necesaria p
del presente Acuerdo de Confidencialidad, y a tal efecto:

Personal contratista

Esquema Nacional de Seguridad

CCN centro criptológico nacional

Junta de Andalucía

4.INTELIGENCIA ARTIFICIAL

Junta de Andalucía

4.1 Regulación

El **Proveedor de IA** es “toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que desarrolle un Sistema de IA o para el que se ha desarrollado un sistema de IA con vistas a introducirlo en el mercado o ponerlo al servicio con su propio nombre o marca comercial, ya sea de manera remunerada o gratuita”.

Los proveedores de IA debe cumplir los siguientes requisitos:

1. Cumplir y superar pruebas de conformidad
2. Tener un sistema de gestión de calidad documentado
3. Custodiar los registros del sistema para que estén bajo su control
4. Colaborar con autoridades registrando el sistema, demostrando el cumplimiento, notificando incumplimientos y riesgos que detecten y acciones correctivas

4.2 Objetivos

El Real Decreto tiene por objeto establecer un entorno controlado de pruebas para ensayar el cumplimiento de ciertos requisitos por parte de algunos sistemas de inteligencia artificial que puedan suponer riesgos para la seguridad, la salud y los derechos fundamentales delas personas

1) estudiar la operatividad de los requisitos establecidos en la propuesta de Reglamento europeo sobre inteligencia artificial (cuya versión definitiva debería llegar a finales de año); y

2) obtener unas guías técnicas de ejecución y supervisión basadas en la evidencia y la experimentación que faciliten la alineación con el mencionado reglamento, en especial para pequeñas y medianas empresas.

Junta de Andalucía

4.3 Finalidad

¿PARA QUÉ SISTEMAS ESTÁ DIRIGIDO?

1.- Sistemas de IA de alto riesgo: son aquellos que requerirán la conformidad de un tercero y que pueden poner en peligro la salud y seguridad de las personas o bienes, los derechos de los trabajadores o derechos fundamentales, en general.
2.- Sistemas de IA de propósito general: son los que pueden utilizarse en una pluralidad de contextos e integrarse en múltiples sistemas de IA, desde el reconocimiento de texto, imágenes y del habla; a la generación de textos, audios, imágenes y/o vídeos; la detección de patrones; respuesta a preguntas; traducción y otras.
3.- Modelos fundacionales: son normalmente los llamados “Large Language Model”, ya que han sido entrenados en una gran cantidad de datos no etiquetados a escala, lo que da como resultado un modelo que se puede adaptar a una amplia gama de tareas posteriores.
Además, **esos sistemas deberán tener algunas particularidades** para poder formar parte del entorno de pruebas de inteligencia artificial:
- Deben tener un nivel de desarrollo avanzado para poder comercializarse
- Cumplir en materia de protección de datos
- Cumplir la normativa sobre propiedad intelectual

5.EVIDENCIAR LOS REQUISITOS

Junta de Andalucía

5. Evidencias de los requisitos

Requisitos de seguridad en productos y servicios.

Requisitos de seguridad para los productos y servicios coherentes con **la Política de Seguridad**

Proveedores
Suministradores
Colaboradores
Partners
Canales de Venta

Junta de Andalucía

5. Evidencias de los requisitos

Definir cláusulas contractuales en materia de seguridad de la información

Contratos y acuerdos de confidencialidad

- Información a la que se accede, cómo se accede y su clasificación y protección
- Indicar requisitos de cumplimiento: RGPD, ENS, propiedad intelectual, LSSI, ISO27001
-Derecho de auditoría y control
-Incluir situaciones de finalización contrato
-Otras garantías: penalizaciones, certificaciones

Junta de Andalucía

5. Evidencias de los requisitos

Definir las responsabilidades concretas por ambas partes.

Establecer responsabilidades de cada parte

- Quien accede y transforma la información
- Realizar copias de seguridad y cuando
-Controlar logs
-Activar, mantener y controlar sistemas de seguridad: antimalware, firewall, cifrado de comunicaciones

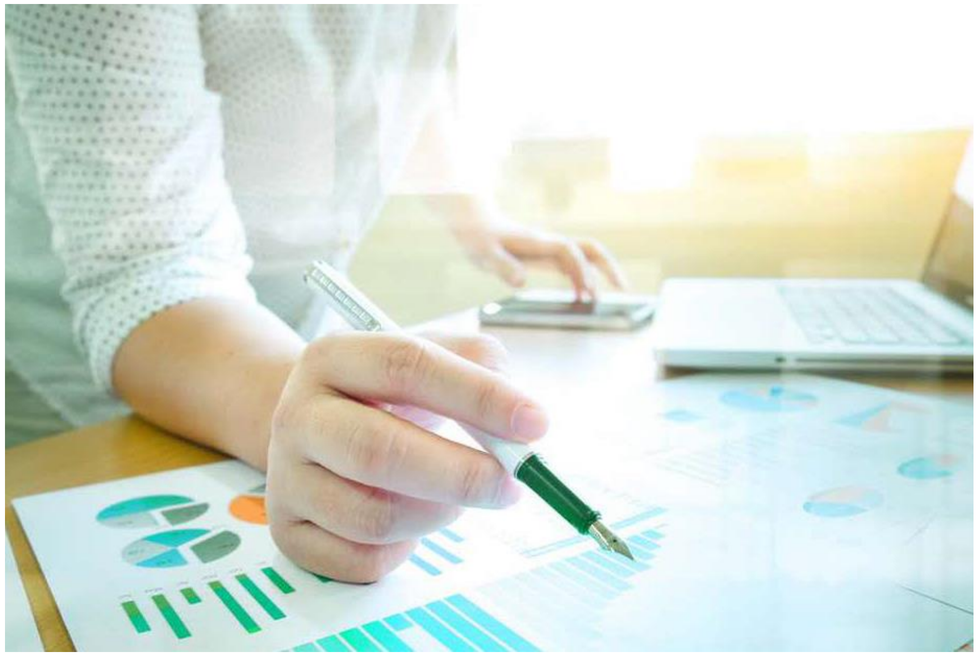
Junta de Andalucía

5. Evidencias de los requisitos

Definir los ANS (Acuerdos de Nivel de Servicio)

Establecer calidad y garantías del servicio

- Responsabilidades de cada parte
- Duración del acuerdo/servicio
-Nivel de servicio: disponibilidad, tiempo de respuesta, canales de contacto, procedimiento de incidencias, personal asignado
-Procedimiento para el seguimiento del servicio
-Sanciones en caso de incumplimiento



Junta de Andalucía

5. Evidencias de los requisitos

Controles de seguridad obligatorios.

Identificar los controles obligatorios

- Servicios e información a la que se permite acceder
- Como se accede a esa información
-Gestionar los incidentes de seguridad

Junta de Andalucía

5. Evidencias de los requisitos

Certificación de los servicios contratados.

En servicios críticos es recomendable exigir certificaciones

- Certificación ENS
- ISO 27001 seguridad de la información
- Certificación ISO 22301 continuidad de negocio

Junta de Andalucía

5. Evidencias de los requisitos

Auditoría y control de los servicios contratados.

Establecer como monitorizar, revisar y auditar los servicios de los proveedores

- Procedimiento de seguimiento de proveedores
- Responsables

Junta de Andalucía

5. Evidencias de los requisitos

Finalización de la relación contractual.

Garantizar la seguridad finalizado el contrato

- Indicar los activos a devolver
- Eliminar permisos de acceso
- Borrado de la información almacenada en los sistemas del proveedor

Junta de Andalucía

5 Check de requisitos

CONTROL	
Requisitos de seguridad en productos y servicios Estableces los requisitos de seguridad mínimos que deben cumplir los productos que adquieres y los servicios que contratas.	☐
Definir cláusulas contractuales en materia de seguridad de la información Eres riguroso en la elaboración y aceptación de las cláusulas contractuales en materia de ciberseguridad.	☐
Definir las responsabilidades concretas por ambas partes Delimitas las responsabilidades en materia de ciberseguridad para cada una de las partes involucradas.	☐
Definir los ANS (Acuerdos de Nivel de Servicio) Defines en detalle los ANS a los que sometes los servicios contratados.	☐
Controles de seguridad obligatorios Determinas que controles de seguridad son de obligado cumplimiento en las relaciones con tus proveedores de servicios tecnológicos.	☐
Formar parte de los foros y organizaciones de usuarios de los productos/servicios software utilizados Participas en las organizaciones de usuarios de los productos y servicios software que adquieres. Controlas la reputación de tus proveedores.	☐
Certificación de los servicios contratados Exiges a tus proveedores certificaciones que garanticen la calidad en materia de seguridad de ciertos servicios contratados de especial criticidad.	☐
Auditoría y control de los servicios contratados Supervisas que los productos y servicios contratados responden a lo acordado en materia de ciberseguridad.	☐
Finalización de la relación contractual Garantizas la seguridad de tu información tras la finalización de un servicio o contrato.	☐

Junta de Andalucía

6. CONCLUSIONES

Junta de Andalucía

6. Conclusiones

OBLIGACIONES PROVEEDORES

- Establecer los **requisitos de seguridad en los pliegos de contratación**
- Exigir a los proveedores el cumplimiento de la normativa mediante **certificaciones**: ENS, ISO…
- Revisar los **procesos implantados**, y contrastarlo con el marco normativo, nuevas exigencias, carencias, técnicas,
- Preparar una campaña de **comunicación y formación a todas las partes implicadas** sobre la necesidad de la diligencia debida y de cómo actualizarse
- Reforzar internamente las áreas relacionadas con Compliance, Protección de Datos, Ciberseguridad, etc.
- **Dedicar tiempo y equipos a mejorar el nivel de acreditación** de procedimientos y políticas para lograr más confianza en clientes.
- Diseñar y mantener un plan de Certificaciones actuales y futuras.
- Implantar a su vez un proceso de seguimiento para sus proveedores. **Checklist**

7. REFERENCIAS

6. Referencias

- BOE del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 https://www.boe.es/doue/2016/119/L00001-00088.pdf

-LOPDGDD https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

- Reglamento IA https://portal.mineco.gob.es/es-es/digitalizacionIA/sandbox-IA/Documents/20220919_Resumen_detallado_Reglamento_IA.pdf

- Infografías sobre el ENS 2022 desarrollado por el Centro Criptológico Nacional. Infografías ENS (CCN)

- Página sobre el ENS del Centro Criptológico Nacional. https://ens.ccn.cni.es/es/

Junta de Andalucía

8. RUEGOS Y PREGUNTAS

Junta de Andalucía


Junta de Andalucía