HOJA DE RUTA _ FORMACIÓN EN ENTIDADES LOCALES

Prontuario de Ciberseguridad para Entidades Locales

Dr. Carlos Galán

30 de junio de 2021

En colaboración con:

Dr. Carlos Galán

- **Licenciado y Doctor en Informática, Licenciado en Derecho y Abogado especialista en Derecho de las TIC.**
- **Profesor de *Derecho de las TIC* en la Universidad Carlos III de Madrid (Área de Derecho Administrativo) y de *Aspectos Legales de la Ingeniería Informática* (Área de Ingeniería Informática).**
- **Asesor del CCN-CERT.**
- **Miembro de la European Artificial Intelligence Alliance.**
- **Miembro del Grupo de Trabajo de Ciberpolítica del Real Instituto Elcano.**
- **Miembro del Grupo de Trabajo de Formación, Capacitación y Talento del Foro Nacional de Ciberseguridad.**
- **Miembro del Grupo de Expertos para el desarrollo de la Estrategia de Ciberseguridad Nacional, en 2013 y 2019.**

Índice

- Amenazas y riesgos para las EELL y el ENS.
- Las responsabilidades del ENS… y de la legislación local.
- Responsabilidades institucionales y administrativas: cargos electos y cargos directivos.
- Las exigencias del ENS.
- Tabla de responsabilidades en materia de ciberseguridad.

- Tecnológicos.
- Operativos.
- **Jurídicos**
- **Organizativos.**

Objetivo:

Ayudar a las EE.LL. a adecuarse al ENS.

(Especialmente, a aquellas de tamaño o recursos limitados).

La *digitalización local*

ELEMENTOS TECNOLÓGICOS DIVERSOS

APLICACIONES MÓVILES

SERVICIOS EN LA NUBE

El problema: amenazas y riesgos para las EELL

- Código dañino (malware).
- Ransomware.
- Phishing.
- Ingeniería social.
- Explotación de vulnerabilidades.
- Denegación de Servicios (administrativos).
- Acceso no autorizado a la información.
- Suplantación.
- Hacktivismo.
- Terrorismo.
- Espionaje.
- …

El problema: amenazas y riesgos para las EELL

No se trata de saber SI SE PRODUCIRÁ UN ATAQUE O NO...

Se trata de saber QUÉ HACER ANTES, DURANTE Y DESPUÉS DE QUE SE PRODUZCA.

La respuesta: el **E**squema **N**acional de **S**eguridad

Esquema Nacional de Seguridad

EFICACIA y CONFIANZA

Las responsabilidades definidas en el ENS (RD 3/2010)

Personales / Colegiadas

Comité de Seguridad de la Información

- Responsable de la **Información**.
- Responsable del **Servicio**.
- Responsable del **Sistema**.
- Responsable de la **(Ciber)Seguridad**.

Las responsabilidades definidas en el ENS (RD 3/2010)

Personales / Colegiadas

Comité de Seguridad de la Información

- …
- Responsable de la **Información.**

Determina los requisitos (de seguridad) de la información tratada.

Las responsabilidades definidas en el ENS (RD 3/2010)

Personales / Colegiadas

Comité de Seguridad de la Información

- …
- Responsable del **Servicio.**

Determina los requisitos (de seguridad) de los servicios prestados

Las responsabilidades definidas en el ENS (RD 3/2010)

Personales / Colegiadas

Comité de Seguridad de la Información

- …
- Responsable del **Sistema.**

  Explota los sistemas de información.

Las responsabilidades definidas en el ENS (RD 3/2010)

Personales / Colegiadas

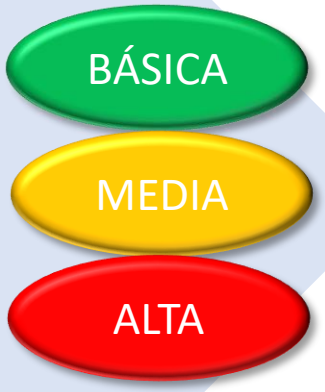
Comité de Seguridad de la Información

- …
- Responsable de la **Seguridad.**

Adopta las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

La determinación de la **categoría de seguridad de un sistema** se basa en la **valoración del impacto** que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa para:

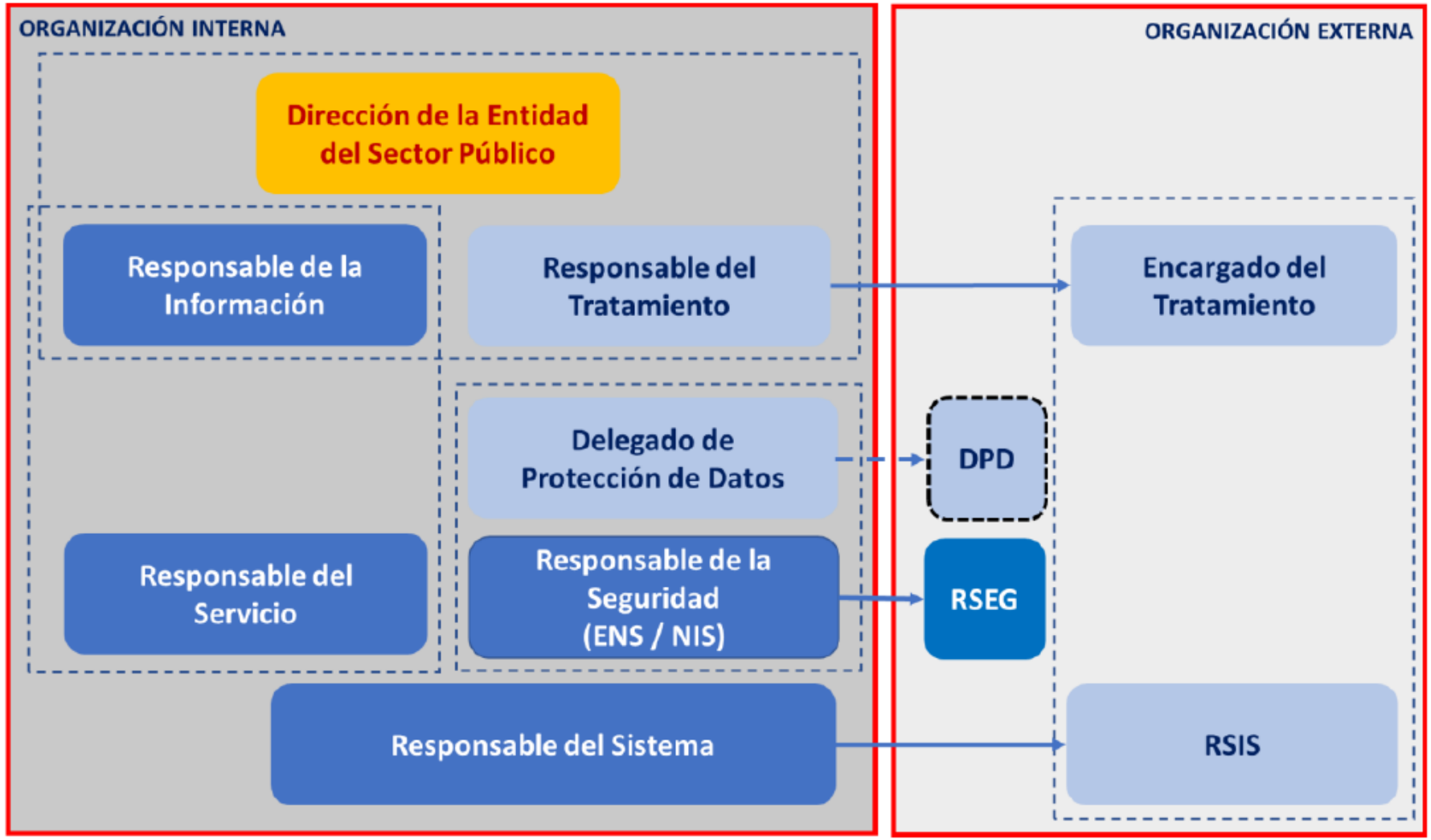
a) Alcanzar sus objetivos.
b) Proteger los activos a su cargo.
c) Cumplir sus obligaciones diarias de servicio.
d) Respetar la legalidad vigente.
e) Respetar los derechos de las personas.



- **DISPONIBILIDAD**
- **CONFIDENCIALIDAD**
- **INTEGRIDAD**
- **TRAZABILIDAD**
- **AUTENTICIDAD**

Las responsabilidades definidas en el ENS (RD 3/2010)

Guía CCN-STIC 801
Responsabilidades y
Funciones



Las responsabilidades definidas en el ENS (RD 3/2010)

Tarea	Dirección	RINFO	RSERV	RSEG	RSIS	AS
niveles de seguridad requeridos por la información		A	I	R	C	
niveles de seguridad requeridos por el servicio		I	A	R	C	
determinación de la categoría del sistema		I	I	R	I	
análisis de riesgos	A	I	I	R	C	
declaración de aplicabilidad		I	I	A/R	C	
medidas de seguridad adicionales		I	I	A/R	C	
configuración de seguridad		I	I	A	C	R
aceptación del riesgo residual	A	C	C	R	I	
documentación de seguridad				A	C	I
política de seguridad	A	C	C	R	C	
normativa de seguridad		C	C	A	C	I
procedimientos de seguridad		I	I	C	A	I
implantación de las medidas de seguridad		I	I	C	A	R
supervisión de las medidas de seguridad				A	I	R
estado de seguridad del sistema	I	I	I	A	I	R
planes de mejora de la seguridad		I	I	A/R	C	
planes de concienciación y formación		I	I	A	C	
planes de continuidad		I	I	C	A	
suspensión cautelar del servicio	I	I	I	A	R	
seguridad en el ciclo de vida				C	A	

Guía CCN-STIC 801
Responsabilidades y
Funciones

Las responsabilidades definidas en el ENS…
… **y en la normativa de las EELL**

Responsabilidad
en materia de
CIBERSEGURIDAD

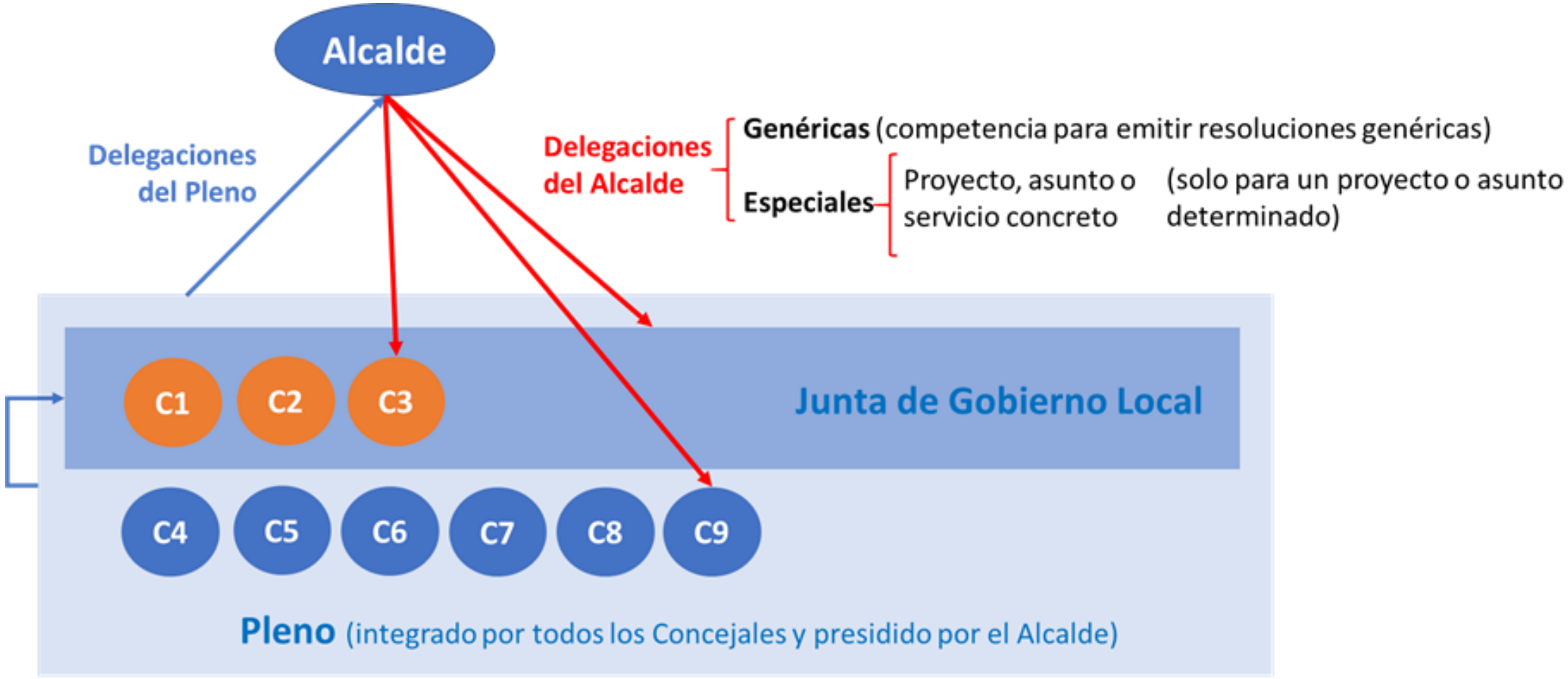
Las responsabilidades **POLÍTICAS/INSTITUCIONALES**:

CARGOS
ELECTOS o DESIGNADOS

- El Alcalde (art. 21, LBRL)
- Los Tenientes de Alcalde.
- El Pleno (art. 22, LBRL)
- La Junta de Gobierno Local (art. 23, LBRL)

Ley 7/1985, de 2 de abril, **Reguladora de las Bases del Régimen Local** (LBRL) y Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el **Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales** (ROF).

Las responsabilidades delegadas:



Las responsabilidades **ADMINISTRATIVAS**:

EL GOBIERNO DE LA ACTIVIDAD ADMINISTRATIVA

- La Secretaría.
- La Intervención-Tesorería.
- La Secretaría-Intervención.

Real Decreto 128/2018, de 16 de marzo, por el que se regula el **régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional**.

Los **municipios de gran población**:

ÓRGANOS SUPERIORES:

a) El Alcalde.
b) Los miembros de la Junta de Gobierno Local.

ÓRGANOS DIRECTIVOS:

a) Los coordinadores generales de cada área o concejalía.
b) Los directores generales u órganos similares que culminen la organización administrativa dentro de cada una de las grandes áreas o concejalías.
c) El titular del órgano de apoyo a la Junta de Gobierno Local y al concejal-secretario de la misma.
d) El titular de la asesoría jurídica.
e) El Secretario general del Pleno.
f) El interventor general municipal.
g) En su caso, el titular del órgano de gestión tributaria.

Los **municipios de gran población**:

- En los Municipios de gran población, el Pleno es el órgano de debate de las grandes políticas locales que afectan al Municipio y de adopción de las decisiones estratégicas.
- El Alcalde de los Municipios de gran población ostenta menos atribuciones gestoras o ejecutivas que el Alcalde de los Municipios de régimen común.
- La Junta de Gobierno Local se constituye como un órgano colegiado esencial de colaboración en la dirección política del Ayuntamiento y está dotada de amplias funciones de naturaleza ejecutiva.
- La Ley regula un régimen económico financiero diferente, previendo un órgano específico de gestión tributaria y otro de resolución de reclamaciones.

Prestación de **SERVICIOS EXTERNOS**:

Cuando los **operadores del sector privado** presten servicios o provean soluciones a las entidades locales, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente **Declaración de Conformidad** con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categoría BÁSICA, o la **Certificación de Conformidad** con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

El ENS dice…

Art. 5. La seguridad como un proceso integral

1. La seguridad se entenderá como un proceso integral constituido por todos los **elementos técnicos, humanos, materiales y organizativos**, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

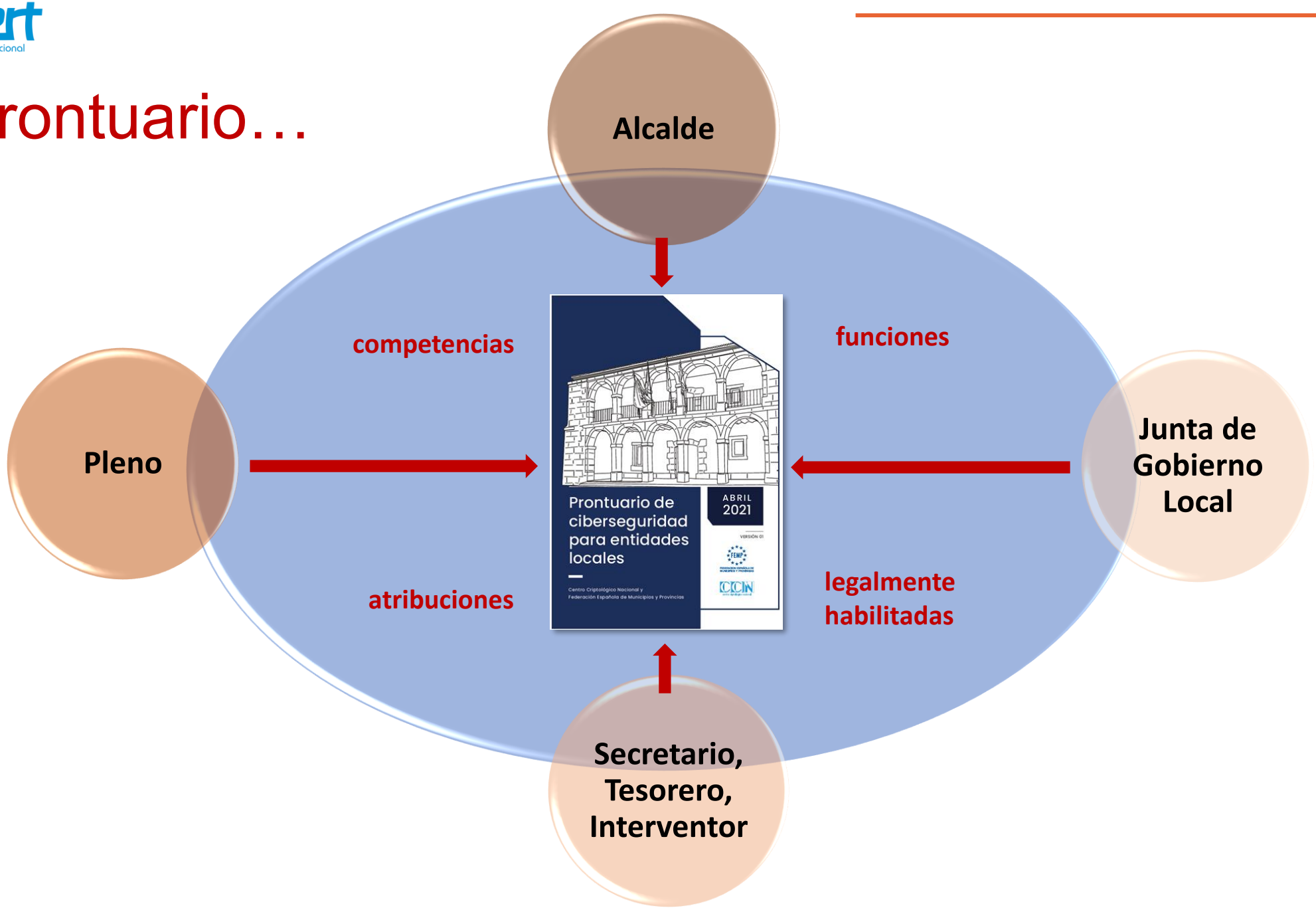
2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a **sus responsables jerárquicos**, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

El ENS dice…

Art. 12. Organización e implantación del proceso de seguridad

La seguridad deberá **comprometer a todos los miembros de la organización**. La política de seguridad según se detalla en el anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.

El Prontuario…



Anexo: Tabla de Funciones y Responsabilidades

Leyenda:

A – Aprobación y responsabilidad de las acciones emprendidas por la entidad local para satisfacer el requisito.
ADP – Aprobación por Delegación del Pleno.
R – Responsable de acometer (total o parcialmente) el requisito, dentro de las competencias o atribuciones del cargo.
RDA – Responsable de acometer y aprobar la función, por Delegación del Alcalde.

Notas:

1. Cuando la responsabilidad R o RDA se repita en un mismo requisito, se entenderá que tal responsabilidad podría ejercerse, alternativamente, por cada uno de los responsables mencionados.

2. No se han incluido las funciones asignadas al Comité de Seguridad de la Información, y a los Responsables de la Información, del Servicio, de la Seguridad y del Sistema, cuyas responsabilidades se encuentran recogidas en la Guía CCN-STIC 801.

Norma, artículo y/o medida del ENS	Descripción del requisito / responsabilidad	Cargos electos				Funcionarios	
		Alcalde	Pleno	Junta de Gobierno Local	Concejal	Secretario	Interventor / Tesorero
1, 3, 4, 9, 35, 38, 41	Velar por la conformidad general con el ENS de los sistemas de información de la entidad local.	A		RDA	RDA	R	R
Con carácter general	La superior dirección de los archivos y registros de la entidad local, incluyendo velar por la garantía de disponibilidad de los archivos electrónicos y la confidencialidad, integridad, trazabilidad y autenticidad de la información contenida en ellos.					R	
ITS de Conformidad	Velar porque los sistemas de información de la entidad local posean las Declaraciones y/o Certificaciones de Conformidad con el ENS y que los Distintivos correspondientes se muestran en la sede electrónica de la entidad.	A		RDA	RDA	R	

Norma, artículo y/o medida del ENS	Descripción del requisito / responsabilidad	Cargos electos				Funcionarios	
		Alcalde	Pleno	Junta de Gobierno Local	Concejal	Secretario	Interventor / Tesorero
ITS de Conformidad	Disponer que se publiquen, cuando sea preceptivo, los actos y acuerdos de la entidad local en los medios oficiales de publicidad, en el tablón de anuncios de la misma y en la sede electrónica, certificándose o emitiéndose diligencia acreditativa de su resultado si así fuera preciso, incluyendo todos los actos o Acuerdos relativos a la seguridad de la información de la entidad, como sería el caso de la publicación de los Distintivos de Conformidad con el ENS de los que la entidad local fuera titular.					R	
10, [op.acc.2]	Determinación de la composición del Comité de Seguridad de la Información y nombramiento del Responsable de la Información, de los Servicios, de la Seguridad, del Sistema y su adecuada segregación.	A		RDA	RDA	R	
11	Velar por la existencia y adecuación de la Política de Seguridad de la Información y la Normativa Interna de la entidad.	R		RDA	RDA	R	
11, [org.1], [org.2]	Aprobación de la Política de Seguridad de la Información y de la Normativa Interna del Uso de los Medios Electrónicos de la entidad local.	ADP	A				
12	Velar por la organización e implantación del proceso de seguridad.	A		RDA	RDA	R	R
13, [op.pl.1]	Velar por la utilización de los principios de análisis y gestión de los riesgos en el proceso de seguridad de la información de la entidad y aprobar el Análisis de Riesgos para los sistemas de información de la entidad.	A		RDA	RDA	R	
14, 15	Aprobación de la plantilla de personal y de la relación de puestos de trabajo, la fijación de la cuantía de las retribuciones complementarias fijas y periódicas de los funcionarios y el número y régimen del personal eventual	ADP	A	ADP			R
14, 15	Velar por la adecuada gestión del personal y su profesionalidad	A		RDA	RDA	R	R
[op.exp.7]	Velar por el cumplimiento de la adecuada notificación de incidentes al Centro Criptológico Nacional.	A		RDA	RDA	R	

Norma, artículo y/o medida del ENS	Descripción del requisito / responsabilidad	Cargos electos				Funcionarios	
		Alcalde	Pleno	Junta de Gobierno Local	Concejal	Secretario	Interventor / Tesorero
ITS de Notificación							
[op.ext]	Velar porque los sistemas de información de los proveedores externos que presten servicios a la entidad sean conformes con el ENS, posean los Acuerdos de Nivel de Servicio idóneos y se gestione adecuadamente su cumplimiento.	A		RDA	RDA	R	R
[op.ext]	Aprobación de los proyectos de obras y servicios, incluidos los relativos a la seguridad de la información, cuando sea competente para su contratación o concesión, y cuando aún no estén previstos en los presupuestos.	ADP	A	ADP		R	R
[op.ext]	Actuar como fedatario en la formalización de todos los contratos, convenios y documentos análogos en que intervenga la entidad local, como aquellos suscritos con terceros proveedores -públicos o privados- de servicios dirigidos a garantizar la seguridad de la información de la entidad local.					R	
[op.cont]	Velar por la adecuada continuidad de los servicios en caso de impacto, incluyendo la aprobación del correspondiente Análisis de Impacto.	A		RDA	RDA	R	
[mp.if]	Velar por la protección de las infraestructuras físicas y lógicas de la entidad, incluyendo su acondicionamiento y abastecimientos y, en su caso, la disponibilidad de instalaciones alternativas, así como la identificación de las personas, especialmente cuando puedan tener acceso a los sistemas de información de la entidad.	A		RDA	RDA	R	R
[mp.per]	Velar porque el personal que trabaja en la entidad local esté debidamente concienciado y/o formado, en materia de seguridad de la información.	A		RDA	RDA	R	R
[mp.info]	Velar porque la información tratada por la entidad, especialmente cuando se trate de datos personales, se custodie adecuadamente, de	A		RDA	RDA	R	

Norma, artículo y/o medida del ENS	Descripción del requisito / responsabilidad	Cargos electos				Funcionarios	
		Alcalde	Pleno	Junta de Gobierno Local	Concejal	Secretario	Interventor / Tesorero
	conformidad con las regulaciones que resulten de aplicación, calificándola de acuerdo con su naturaleza.						
[mp.info.4]	Velar porque se utilizan los procedimientos de firma electrónica, sello electrónico y sello de tiempo electrónico, atendiendo a los procedimientos administrativos de que se trate, de conformidad con la legislación vigente.	A		RDA	RDA	R	
[Anexo III] ITS de Auditoría	Velar porque se realice periódicamente una auditoría de conformidad con el ENS y, si procede, una Auditoría externa de Certificación, cada dos años o siempre que se hayan producido cambios en los sistemas de información afectados que induzcan a pensar que no son eficaces las medidas de seguridad adoptadas.	A		RDA	RDA	R	R
Con carácter general	Preparar los asuntos que hayan de ser incluidos en el orden del día de las sesiones que celebren el Pleno, la Junta de Gobierno y cualquier otro órgano colegiado de la Corporación en que se adopten acuerdos que vinculen a la misma, incluyendo también todos aquellos asuntos relativos a garantizar la seguridad de la información tratada y los servicios prestados por la entidad local.					R	
Con carácter general	Transcribir en el Libro de Resoluciones, cualquiera que sea su soporte, las dictadas por la Alcaldía o Presidencia, por los miembros de la Corporación que resuelvan por delegación de las mismas, así como las de cualquier otro órgano con competencias resolutivas. Entre tales resoluciones estarán las relativas a la seguridad de la información de la entidad local.					R	
Con carácter general	Certificar todos los actos o resoluciones de la Alcaldía o Presidencia y los acuerdos de los órganos colegiados decisorios, así como los antecedentes, libros y documentos de la entidad, como los que puedan involucrar a actos o resoluciones relativas a la seguridad de la información de la entidad local.					R	

Norma, artículo y/o medida del ENS	Descripción del requisito / responsabilidad	Cargos electos				Funcionarios	
		Alcalde	Pleno	Junta de Gobierno Local	Concejal	Secretario	Interventor / Tesorero
Con carácter general	Anotar en los expedientes, bajo firma, las resoluciones y acuerdos que recaigan, así como notificar dichas resoluciones y acuerdos en la forma establecida en la normativa aplicable, incluyendo entre tales resoluciones y acuerdos aquellos que se refieran a acciones relativas a la seguridad de la información de la entidad.					R	
Con carácter general	Llevar y custodiar el Registro de Intereses de los miembros de la Corporación, el Inventario de Bienes de la Entidad Local y, en su caso, el Registro de Convenios, como todos aquellos Bienes (activos) y Convenios relativos a la seguridad de la información de la entidad.					R	
Con carácter general	La emisión de informes previos en aquellos supuestos en que así lo ordene el Presidente o Alcalde de la Corporación o cuando lo solicite un tercio de miembros de la misma. Tales informes deberán señalar la legislación en cada caso aplicable y la adecuación a la misma de los acuerdos en proyecto. (Este sería el caso, por ejemplo, de aquellos informes relativos a acciones o iniciativas en relación con la seguridad de la información de la entidad).					R	
Con carácter general	La emisión de informes previos siempre que un precepto legal o reglamentario así lo establezca o la emisión de informe previo siempre que se trate de asuntos para cuya aprobación se exija la mayoría absoluta del número legal de miembros de la Corporación o cualquier otra mayoría cualificada, como podría ser el caso, entre otros, de la emisión de informes relativos a la aprobación o modificación de Ordenanzas, Reglamentos o Estatutos rectores de Organismos de derecho público, sociedades mercantiles, fundaciones, etc., cuyos requisitos en materia de seguridad de la información hayan de modificarse.					R	

Norma, artículo y/o medida del ENS	Descripción del requisito / responsabilidad	Cargos electos				Funcionarios	
		Alcalde	Pleno	Junta de Gobierno Local	Concejal	Secretario	Interventor / Tesorero
Con carácter general	Asistir al Presidente o Alcalde de la Corporación, para la formación del presupuesto, a efectos procedimentales y formales, no materiales.					R	R

Etc.

La ciberseguridad es una responsabilidad compartida (ECSN'19)…

… también en las Entidades Locales.

Muchas gracias

En colaboración con:

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

FEMP 40 AÑOS Poder Local