IMPLANTACIÓN DEL ENS Y GOBERNANZA DE LA CIBERSEGURIDAD EN LOS GOBIERNOS LOCALES

Segovia, 11 de abril de 2024

Dra. Dolors CANALS AMETLLER

Profesora Titular de Derecho Administrativo-Universidad de Girona (UdG)

Investigadora de la Cátedra INCIBE: “DIGITALIZACIÓN y CIBERSEGURIDAD HÍDRICA” (sede UdG)

dolors.canals@udg.edu

Universitat de Girona
Departament de Dret Públic

CONCEPTO DE CIBERSEGURIDAD Y DERECHO A LA CIBERSEGURDAD

- **CIBERSEGURIDAD:**

Sentencia del Tribunal Constitucional 142/218, de 20 de diciembre: Fjco 4 y 5:

- Seguridad en la RED (Internet): SEGURIDAD DIGITAL
- Se integra en la SEGURIDAD PÚBLICA y de las telecomunicaciones (ENS 2022: "SEGURIDAD NACIONAL")
- Conjunto de MECANISMOS dirigidos a LA PROTECCIÓN DE LAS INFRAESTRUCTURAS INFORMÁTICAS Y DE LA INFORMACIÓN DIGITAL que albergan.

Luego:

a) protección de las redes y sistemas de información: infraestructuras tecnológicas que soportan la RED (uso por AAPP, ciudadanía y empresas)

b) protección de la integridad y confidencialidad de la información (DATOS, INTIMIDAD) ante ciberincidentes que se generan en la Red

c) protección de la seguridad de la ADMINISTRACIÓN ELECTRÓNICA: ciberseguridad: "la organización de medios y previsión de medidas de protección de la Administración y, por extensión, la protección de los derechos de los ciudadanos cuando se relacionan con la Administración por medios electrónicos" (FJ 5): **CONFIANZA**

DERECHO A LA CIBERSEGURIDAD (Carta de derechos digitales, julio 2021)

CONCEPTO DE CIBERSEGURIDAD Y DERECHO A LA CIBERSEGURIDAD

DERECHO A LA CIBERSEGURIDAD (Carta de derechos digitales, julio 2021)

Como "*derecho de libertad*" (SOFT LAW)

"1. Conforme al ordenamiento jurídico, toda persona tiene derecho a que los sistemes digitales de información que utilice para su actividad personal, profesional o social, o que traten sus datos o **le presten servicios**, posean las medidas de seguridad adecuadas que permitan garantizar la **integridad, confidencialidad, resiliencia y autenticidad de la información tratada y disponibilidad de los servicios prestados.**

2. Los **poderes públicos, de conformidad con la regulación europea y nacional**, velarán para que las garantías expresadas en el número anterior sean satisfechas por **todos los sistemas de información**, ya sean de titularidad pública o privada, **proporcionalmente a los riesgos** a los que. extén expuestos. A tal efecto podrán contar con la **colaboración de la sociedad civil.**

3. Los **poderes públicos promoverán la sensibilización y formación en materia de ciberseguridad de toda la sociedad e impulsaran mecanismes de certificación**".

RASGOS GENERALES DE LA CIBERSEGURIDAD Y SU GESTIÓN ("GOBERNANZA")

- **CIBERSEGURIDAD:**
  - **GESTIÓN O "GOBERNANZA" HÍBRIDA: pública y privada: CORRESPONSABILIDAD** público-privada y **AUTORRESPONSABILIDAD individual (**autoseguridad**): la importancia de la ÉTICA ****
    - **DEBER de conductas digitales responsables de toda la ciudadanía, del personal al servicio de los gobiernos locales y los operadores económicos: CONTRATISTAS PUBLICOS**
    - **Gestión de riesgos globales (de TODO TIPO: hibridación de la seguridad) y acciones locales: idea "GLOCAL"** (ciberseguridad, medio ambiente: cambio climático)
      - RIESGOS DIGITALES: **riesgos de seguridad jurídica** (protección de datos y otros derechos constitucionales, incluida la igualdad: remisión IA) y **riesgos de prestigio para las instituciones públicas**
    - **COOPERACIÓN, COLABORACIÓN e idea COLABORATIVA en la "gobernanza" (al margen del beneficio individual).**

- **SEGURIDAD y FIABILIDAD (CONFIANZA)** son derechos digitales y atributos esenciales de **una Red confiable**, aunque el **ECOSISTEMA DIGITAL** (infraestructura principalmente **PRIVADA** es, por naturaleza, **INESTABLE** (fácilmente modificable, manipulable e incluso eliminable).

MARCO NORMATIVO DE LA CIBERSEGURIDAD Y SU ”GOBERNANZA”

- **MARCO COMUN EUROPEO DE CIBERSEGURIDAD: SEGURIDAD HÍBRIDA** principalmente en el sector de los servicios públicos y servicios esenciales DIGITALIZADOS, por su **DEPENDENCIA de las infraestructuras digitales y por ello de los más que posibles ciberincidentes** (afectación de la **accesibilidad y continuidad** de la prestación de servicios esenciales):

- Directiva de ciberseguridad o NIS2: Directiva 2022/2555 de diciembre de 2022
- Directiva de Entidades Críticas: Directiva 2022/2557 de Resiliencia de las Entidades Críticas
- Reglamento EU de Inteligencia Artificial de 2024
- Proyecto de Reglamento UE de Ciberresiliencia o ciberseguridad industrial
- Proyecto de Reglamento UE de Cibersolidaridad (entre EEMM)

MARCO NORMATIVO DE LA CIBERSEGURIDAD Y SU ”GOBERNANZA”

- **Directivas de 2022:**

La Directiva de CIBERSEGURIDAD (NIS2) considera la Administración pública ESTATAL (**AGE)** como **“entidad ESENCIAL” a efectos de las medidas de seguridad digital**: más en concreto, **a las entidades de la AGE y su sector público prestador de servicios por medios digitales y la AGE también es una “entidad CRITICA” a efectos de la Directiva de Resiliencia de las Entidades Críticas**, en la prestación de servicios esenciales en sectores (lo son LOS OPERADORES con determinada capacidad) tales como **energía (electricidad, gas), transporte aéreo, marítimo, fluvial, banca y servicios financieros, sector sanitario, SERVICIO DE AGUA POTABLE y tratamiento de AGUAS RESIDUALES (servicios locales), servicios de distribución de alimentos (grandes ciudades), las propias infraestructuras digitales, etc.**

SMART CITIES y las *URBES DIGITALES* (territorios rurales inteligentes) (redes de entidades locales: plataformas compartidas de las administraciones locales de manera colaborativa).

NADA establecen para las CCAA y los EELL: decisión EEMM previa evaluación de riesgos exponenciales.

MARCO NORMATIVO DE LA CIBERSEGURIDAD Y SU ”GOBERNANZA”

ENTORNO NORMATIVO NACIONAL:

- Normativa de protección de datos personales
- RD 203/2021, de 30 de marzo, reglamento de actuación y funcionamiento del sector público por medios electrónicos
- **RD 311/2022, de 3 de mayo, ENS de 2022** (sistema de “seguridad nacional”) **y desarrollo por instrucciones técnicas (“de obligado cumplimiento”) y guías y soluciones CNI: CCN-CERT, además de INCIBE-CERT (sector privado y ciudadanía: telf. ayuda 017 Incibe)**: ******certificados ENS 2010: la fecha máxima de validez de los certificados no podrá superar el **5.5.2024**
- Futura Ley de Ciberseguridad (ESTADO)
- **Estrategias (la EUROPEA** de diciembre de 2020**) ordenadas en paralelo y en escala**: europea, nacional (2019), autonómicas.

LA ARQUITECTURA INSTITUCIONAL DE LA CIBERSEGURIDAD

- Garantizar y mantener la seguridad digital requiere una específica arquitectura institucional (estatal, autonómico y local)

  - **Agencia Europea para la Ciberseguridad (ENISA)**
  - **Consejo de Seguridad Nacional**
  - **Centro Nacional de Ciberseguridad**
  - **CNI: CCN-CERT** -Equipos de Respuesta ante Incidentes de Ciberseguridad de la Información- **y Centro Criptológico Nacional (CCN):**
  - **INCIBE**
  - **Autoridades autonómicas competentes**
  - **OC: Organismos de Certificación**
  - **SOCv: Centros de Operaciones de Ciberseguridad** de diferente ámbito: ministerios, diputaciones o entidades locales (ahora también existen los **Operadores de Servicios Esenciales**): son plataformas (infra TIC) que proporcionan a las entidades las capacidades de prevención, protección, detección y respuesta ante los ciberincidentes, así como capacidades de gestión de la seguridad.

EL ESQUEMA NACIONAL DE SEGURIDAD Y SU LA IMPLANTACIÓN EN LOS GOBIERNOS LOCALES

El ENS 2022: carácter obligatorio del ENS (ex art. 156.2 LRJSP) fue reconocido por el Tribunal Constitucional en la Sentencia 142/2018, de 20 de diciembre: su incumplimiento **por parte de las Administraciones y sus entidades dependientes que, en caso de producción de daños, podría generar supuestos de responsabilidad patrimonial.**

CONTENIDO: POLITICA DE SEGURIDAD: personal responsable (organización), infraestructura TIC y productos digitales certificados o seguros

a. **PRINCIPIOS BASICOS siguientes**: **seguridad como proceso integral**; **gestión de la seguridad basada en riesgos**; **prevención, detección, respuesta y conservación**; **existencia de líneas de defensa**; **vigilancia continua**; **reevaluación periódica** y diferenciación de **responsabilidades**. Entre los otros **principios adicionales,** destaca el **principio de proporcionalidad** de las medidas adoptadas para mitigar o suprimir los riesgos que deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos (art. 14.3 ENS 2022).

EL ESQUEMA NACIONAL DE SEGURIDAD Y SU LA IMPLANTACIÓN EN LOS GOBIERNOS LOCALES

b. REQUISITOS MINIMOS (DILIGENCIA): análisis y gestión de riesgos; **gestión de personal**; profesionalidad; autorización y control de los accesos; protección de las instalaciones; adquisición de productos de seguridad y contratación de servicios de seguridad; mínimo privilegio; integridad y actualización del sistema; protección de la información almacenada y en tránsito; prevención ante otros sistemas de información interconectados; registro de la actividad y detección de código dañino; incidentes de seguridad; continuidad de la actividad; **mejora continua del proceso de seguridad**.

AUDITORÍA y CERTIFICACIÓN: para los procedimientos de determinación de la **conformidad con el ENS, los sistemas de información de las Administraciones se clasifican por categorías (BAJA, MEDIA, ALTA)**, atendiendo a la eventual **afectación de las distintas dimensiones de seguridad y niveles de seguridad (BAJO, MEDIO, ALTO)**, **categorías que tendrán asignadas las correspondientes medidas de seguridad adoptadas en función de una evaluación de los riesgos** (Anexo II ENS). **Los sistemas de categoría "MEDIA o ALTA" precisarán de una auditoría para la certificación de su conformidad**, sin perjuicio de la auditoría de la seguridad ordinaria, al menos cada dos años, prevista en el artículo 31 del ENS (art. 38 ENS y Anexo I).

Los sistemas de categoría "BAJA" solo requieren de una autoevaluación para su declaración de conformidad al ENS, lo que no impide que se pueda someter a una auditoría de certificación.

EL ESQUEMA NACIONAL DE SEGURIDAD Y SU LA IMPLANTACIÓN EN LOS GOBIERNOS LOCALES

- **AMBITO SUBJETIVO DE APLICACIÓN**: incluye a los **CONTRATISTAS PÚBLICOS:** de acuerdo con la LOPDCP, el ENS es **aplicable a todos** los contratistas de las Administraciones públicas y no únicamente a los prestadores de servicios de asistencia informática o de provisión de soluciones tecnológicas a las Administraciones públicas.

- **IMPLANTACION: AYUDA DEL CNI: el Centro Criptológico Nacional (CCN-CERT)** elabora y difunde **Guías de seguridad de las tecnologías de la información y comunicación (Guías CCN-STIC)**, en particular de la **serie 800**, que habrán de incorporarse al conjunto documental utilizado para la realización de las **auditorías de seguridad y de verificación del cumplimiento de las medidas del ENS** (disposición adicional segunda ENS).
- Proceso de **comunicación de incidentes de seguridad (art. 25 ENS)** y **de la respuesta a incidentes de seguridad articulada a través de los CCN-CERT** los cuales actuarán sin perjuicio de las capacidades de respuesta que pueda tener cada Administración pública.
- **Sistema de alerta temprana (SAT), por ejemplo, en materia de redes de AGUA y de SMART CITIES**

EL ESQUEMA NACIONAL DE SEGURIDAD Y SU LA IMPLANTACIÓN EN LOS GOBIERNOS LOCALES

CCN-CERT: los servicios de **notificación y aviso de violaciones o brechas de seguridad digital que proporciona CCN-CERT son de gran ayuda para las Administraciones públicas**. Además, el mismo servicio del CNI elabora **recomendaciones de ciberseguridad y ofrece herramientas informáticas de protección directa (*soluciones*) contra la infección de determinados agentes dañinos.**

ALGUNAS SOLUCIONES ("herramientas"), GUIAS ("recomendaciones") y DOCUMENTOS DE INTERES:

AMPARO: Solución para la implantación de seguridad y conformidad del ENS: para la Gobernanza de la ciberseguridad: para ENTIDADES de CERTIFICACION y ORGANOS de AUDITORIA TECNICA (para la auditorías de conformidad)

LORETO: Solución para el almacenamiento en la nube

- Guía CCN-STIC 105 (marzo de 2024): Catálogo de Productos y Servicios de Seguridad de las TICs
- Guía CCN-STIC 890 (marzo de 2023: Guía de Adecuación del ENS conforme al Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad: **metodologia uCeENS para la CERTIFICACION BASICA del ENS (categoria bàsica): Modelo de Politica de Seguridad (diseño)**
- **Guía CCN-STIC 890A: Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad: ENTIDADES LOCALES** (agosto de 2023)
- **I- NFORME (enero 2023) CCN-CERT: "Gestión de crisis para ciberincidentes en entidades locales"**

BIBLIOGRAFÍA

- ALAMILLO DOMINGO, I., "El Esquema Nacional de Seguridad y el cumplimiento del artículo 32 del RGPD en el ámbito local", *El Consultor de los Ayuntamientos y de los Juzgados: Revista técnica especializada en administración local y justicia municipal,* núm. 3, 2019, pp. 163-174.
  - "Esquena Nacional de Seguridad en la Administración electrónica y responsabilidad patrimonial por incidente de seguridad", en ALMONACID LAMELAS, V. (Coord.): *Manual para gestión inteligente del Ayuntamiento,* Madrid: La Ley-El Consultor, 2013.
- CANALS AMETLLER, D., (et altri), "*La digitalización en los servicios públicos"*, Madrid-Barcelona: Marcial Pons, 2024.
  - "La seguridad digital en pequeñas y medianas entidades locales: hacia una gestión municipal colaborativa", en FONDEVILA ANTOLÍN, J. (Dir.): *La transformación digital en las medianas y pequeñas entidades locales. Retos en clave de eficiencia y sostenibilidad*, Madrid: Wolters Kluwer-El Consultor de los Ayuntamientos, 2022, pp. 241-267.
  - "El fenómeno colaborativo en la gestión pública local: algunas experiencias en curso", en CARBONELL PORRAS, E. (dir.), *Gobiernos locales y economía colaborativa,* Madrid: Iustel, 2022, pp. 69-93.
  - "La seguridad en el entorno digital", en CANALS AMETLLER, D. (dir*.), Ciberseguridad. Un nuevo reto para el Estado y los Gobiernos Locales,* Madrid: Wolters Kluwer-El Consultor de los Ayuntamientos, 2021, pp. 61-88.
- FONDEVILA ANTOLÍN, J., "Régimen jurídico de la ciberseguridad en la contratación pública: un gran olvidado, pero con importantes consecuencias por su incumplimiento", *El Consultor Contratación Administrativa, La Ley,* 24 de abril de 2023.
  - "Seguridad en la utilización de medios electrónicos. El Esquena Nacional de Seguridad", en GAMERO CASADO, E. (Dir.): *Tratado de Procedimiento Administrativo Común y Régimen Jurídico Básico del Sector Público,* Valencia: Tirant lo Blanch, 20

FUERTES, M., *Metamorfosis del Estado. Maremoto digital y ciberseguridad,* Madrid-Barcelona: Marcial Pons, 2022.

MUCHAS GRACIAS POR SU ATENCIÓN