XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectiva

El marco institucional de la Ciberseguridad en España

CCN-CERT
centro criptológico nacional

- Alejandra Frías López
- Magistrada.
  Ex Vocal del Consejo Nacional de Ciberseguridad
- a.frias@poderjudicial.es

INTRODUCCIÓN

❑**Mundo desconocido en la Historia de la Humanidad**

- Cambio absoluto en la forma de vivir, de trabajar, de relacionarnos… de crecer y aprender

- Dos mundos paralelos

- ❑ **Gran reto sociedad/humanidad del S. XXI**
- ❑ **NECESARIA RECONFIGURACIÓN DEL MARCO LEGAL E INSTITUCIONAL**
- ❑ **Piedra angular de la regulación del mundo digital:**
  Las mismas normas, derechos, principios y valores que rigen fuera de línea son aplicables en el ciberespacio

ACTUACIONES DESARROLLADAS EN ESPAÑA

- ✓ La Estrategia de Seguridad Nacional: **1 de diciembre de 2017**
- ✓ El Consejo de Seguridad Nacional
- ✓ La Estrategia de Ciberseguridad Nacional: **5/12/2013**
- ✓ El Consejo Nacional de Ciberseguridad: **Orden PRA/33/2018**
- ✓ El Plan Nacional de Ciberseguridad: **31 de octubre de 2014**
- ✓ Los Planes Derivados de Ciberseguridad: **CNCS 14 de julio de 2015. Presentados al CSN el 20 de julio de 2015.**
- ✓ La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional
- ✓ El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

PERSPECTIVA DE SEGURIDAD NACIONAL: STC 184/2016, 3 Nov.

EL CONSEJO NACIONAL DE CIBERSEGURIDAD

- **Orden PRA/33/2018, de 22 de enero,** por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad. **BOE 23/01/2018**
- **Órgano de apoyo del Consejo de Seguridad Nacional en el marco del Sistema de Seguridad Nacional**: Ley 36/2015, de Seguridad Nacional
- **Presidencia: Secretario de Estado Director del CNI, miembro CSN**
- Funciones específicas:
  - ✓ Proponer al CSN las directrices relacionadas con la ciberseguridad.
  - ✓ Apoyar al CSN en su función de verificar el grado de cumplimiento de la Estrategia de Seguridad Nacional y proponer, en su caso, su revisión.
  - ✓ Verificar el grado de cumplimiento de la Estrategia.

OBLIGACIONES GUBERNAMENTALES DIRECTIVA 2016/1148, NIS

Contenido mínimo de toda Estrategia: artículo 7

General:

objetivos estratégicos

- ❑ las medidas políticas y *normativas* adecuadas

Específico:

a) los objetivos y prioridades de la estrategia nacional de seguridad de las redes y sistemas de información;

b) un marco de gobernanza para lograr los objetivos y las prioridades de la estrategia nacional de seguridad de las redes y sistemas de información, **incluidas las funciones y responsabilidades de las instituciones públicas y de los demás agentes pertinentes.**

OBLIGACIONES GUBERNAMENTALES DIRECTIVA NIS

Contenido mínimo de toda Estrategia: artículo 7

- c) la identificación de medidas sobre **preparación**, **respuesta** y **recuperación**, incluida la cooperación entre los sectores público y privado;
- d) una indicación de los **programas de educación**, **concienciación** y **formación** relacionados con la estrategia nacional de seguridad de las redes y sistemas de información;
- e) una indicación de los **programas de investigación y desarrollo** relacionados con la estrategia nacional de seguridad de las redes y sistemas de información;
- f) un plan de evaluación de riesgos para identificar riesgos;
- g) una **lista de los diversos agentes que participan en la ejecución de la estrategia** de seguridad de las redes y sistemas de información.

ACTUACIONES DESARROLLADAS EN ESPAÑA

Planes Derivados aprobados el 14 de julio de 2015:

1. Plan de **fortalecimiento y potenciación de Capacidades** y aseguramiento de la Cooperación para la Ciberseguridad y la **Ciberdefensa**.
2. Plan de seguridad de los sistemas de información y telecomunicaciones que soportan las **Administraciones Públicas**.
3. Plan de protección y resiliencia de los sistemas de información y telecomunicaciones que soportan las infraestructuras críticas.
4. Plan contra la **ciberdelincuencia y el ciberterrorismo**.
5. Plan de protección y resiliencia de las **TIC en el sector privado**.
6. Plan de **impulso al desarrollo industrial, capacitación de los profesionales y refuerzo de la I+D+i en materia de ciberseguridad**.
7. Plan de Cultura de ciberseguridad. **Concienciación, sensibilización y Educación**.
8. Plan de **Cooperación internacional y UE.**
9. Plan para el **intercambio de información sobre ciberamenazas**.

DIRECTIVA NIS: REAL DECRETO-LEY 12/2018, 7 SEPTIEMBRE

Plazo transposición Directiva NIS: 9/05/2018

- ***Esboza*** el marco institucional de la ciberseguridad, [que desarrollará la Estrategia], compuesto por:

1. **Las autoridades públicas competentes** [funciones de vigilancia y régimen sancionador]:

- Secretaría de Estado de Seguridad, Mº Interior, a través del CNPIC
- La autoridad sectorial correspondiente por razón de la materia
- Secretaría de Estado para el Avance Digital
- Ministerio de Defensa, a través del CCN

DIRECTIVA NIS: REAL DECRETO-LEY 12/2018, 7 SEPTIEMBRE

Plazo transposición Directiva NIS: 9/05/2018

1. Las autoridades públicas competentes **y los CSIRT de referencia** [análisis de riesgos y supervisión de incidentes a escala nacional]: art. 11 RDL:

a) **En lo concerniente a las relaciones con los operadores de servicios esenciales:**

1.º El CCN-CERT, del Centro Criptológico Nacional

2.º El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España,

3.º El ESPDEF-CERT, del Ministerio de Defensa.

DIRECTIVA NIS: REAL DECRETO-LEY 12/2018, 7 SEPTIEMBRE

Plazo transposición Directiva NIS: 9/05/2018

CSIRT de referencia:

b) **En lo concerniente a las relaciones con los proveedores de servicios digitales que no estuvieren comprendidos en la comunidad de referencia del CCN-CERT**: el INCIBE-CERT,

- **CONTENIDO ESTRATEGIA**: entre otras cuestiones, las establecidas en el art. 7 de la Directiva NIS. Ley 36/2015: Enfoque de seguridad nacional
- **Punto de contacto único**, art. 13 RDL: Consejo de Seguridad Nacional a través del Departamento de Seguridad Nacional.

ÚLTIMAS ACTUACIONES DESTACABLES

- Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre **normas de Derecho civil sobre robótica.**
- Cumbre Digital de Tallin: 29 de septiembre de 2017
- Conclusiones del Consejo Europeo de 19 octubre 2017
  - Necesidad de crear una **Europa digital más fuerte**
  - Administraciones y servicios públicos digitales
  - Ultimar la Estrategia para el Mercado Único Digital
  - Luchar contra el **terrorismo y la delincuencia en línea**
  - **Mercados laborales y sistemas de educación y formación adaptados a la era digital**
  - Esfuerzo en materia de **investigación y desarrollo e inversión**
  - Concienciarse de la **urgencia de hacer frente a las nuevas tendencias: planteamiento europeo frente a la inteligencia artificial en 2018**
  - **Un sistema tributario eficaz y justo que se adapte a la era digital**

ÚLTIMAS ACTUACIONES DESTACABLES

- Conclusiones del Consejo Europeo sobre la Comunicación conjunta al Parlamento Europeo y al Consejo titulada “Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE”: 20 noviembre 2017
  - **crear un Centro Europeo de Investigación en Ciberseguridad**
  - establecer una **Red de centros de competencia en ciberseguridad**
  - ciberseguridad es responsabilidad de todos, UE y Estados miembros
  - **fomentar las aptitudes digitales y la alfabetización mediática**, ayudando a los usuarios a proteger su información digital en línea y concienciándolos acerca de los riesgos que conlleva poner datos personales en Internet

ÚLTIMAS ACTUACIONES DESTACABLES

- Avances en el ámbito de la ciberseguridad anunciados por el Presidente de la Comisión Europea, Juncker, en el Estado de la Unión 2018:

  septiembre 2018

  - **Un Centro Europeo de Competencia Industrial, Tecnológica y de Investigación**, coordinar los fondos destinados a la ciberseguridad en el próximo presupuesto de la UE a largo plazo (2021-2027), de los programas de Europa Digital y Horizonte Europa: crear nuevas capacidades europeas de ciberseguridad: impulsar la investigación y la innovación en ciberseguridad, y organizará inversiones conjuntas de la UE, los Estados miembros y la industria.
  - **Red de Centros Nacionales de Competencia en ciberseguridad**.

XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectiva

- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

centro criptológico nacional