TEMA 127. CIBERSEGURIDAD. LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Actualizado a 11/01/2022

1. ESTRATEGIA DE CIBERSEGURIDAD 2019

El documento se estructura en cinco capítulos:

1. "El ciberespacio, más allá de un espacio común global": visión de conjunto del ámbito de la ciberseguridad, los avances realizados en materia la materia desde la aprobación de la Estrategia de 2013.

2. "Las amenazas y desafíos en el ciberespacio" determina las principales amenazas del ciberespacio. Clasifica estas amenazas y desafíos en dos categorías:
    1. Ciberamenazas: las que amenazan a activos que forman parte del ciberespacio
    2. Acciones con fines maliciosos: usan el ciberespacio como medio para realizar actividades maliciosas e ilícitas de todo tipo.

3. "Propósito, principios y objetivos para la ciberseguridad"
    1. **OBJETIVO GENERAL**
        - *"En línea con la Estrategia de Seguridad Nacional de 2017 y ampliando el objetivo para la ciberseguridad previsto en la misma, España garantizará el **uso seguro y fiable del ciberespacio**, protegiendo los **derechos y las libertades de los ciudadanos** y promoviendo el **progreso socio económico"***
    2. **Objetivos específicos (resumidos)**
        - **Ob1: Seguridad y resiliencia**
        - **Ob2: Uso seguro y fiable** del ciberespacio.
        - **Ob3: Protección del ecosistema**.
        - **Ob4: Cultura y compromiso**.
        - **Ob5: Seguridad** del ciberespacio **internacional**
    3. **Principios rectores**
        - Unidad de acción
        - Anticipación
        - Eficiencia
        - Resiliencia
4. "Líneas de acción y medidas" se dirigen a:
    1. **LA1**: reforzar las capacidades ante las amenazas provenientes del ciberespacio (dentro de Ob1);
    2. **LA2**: garantizar la seguridad y resiliencia de los activos estratégicos para España (Ob1);
    3. **LA3**: reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio (Ob2);
    4. **LA4**: impulsar la ciberseguridad de ciudadanos y empresas (Ob3);
    5. **LA5**: potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital (Ob4);
    6. **LA6**: contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable en apoyo de los intereses nacionales (Ob5);
    7. **LA7**: desarrollar una cultura de ciberseguridad (Ob5);

5. "La ciberseguridad en el Sistema de Seguridad Nacional" define la arquitectura orgánica de la Ciberseguridad:
    1. **El Consejo de Seguridad Nacional**. Asiste al gobierno en política de seguridad nacional. Cooperación transfronteriza con la UE.
    2. **El Comité de Situación**. Gestión de crisis.
    3. **El Consejo Nacional de Ciberseguridad**. Apoya al Consejo de Seguridad Nacional. Coordinación, cooperación, colaboración público-privada. Valoración de riesgos y amenazas. Planes de respuesta. Ejercicios de crisis.
    4. **La Comisión Permanente de Ciberseguridad**. Coordinación ministerial a nivel operacional.
    5. **El Foro Nacional de Ciberseguridad**. Sinergias público-privadas.
    6. **Las Autoridades públicas competentes y los CSIRT de referencia nacionales**. La red de CSIRT incluye:
        - CSIRT privados

- CSIRT de las Comunidades Autónomas
- CSIRT de Ayuntamientos
  Aparte hay que destacar los CSIRT mencionados en el RD-Ley 12/2018 y la red de CSIRTs a la que se hace referencia en el RD 43/2021:
    - CCN-CERT
    - ESPDEF-CERT
    - INCIBE-CERT
- También existen CSIRT internacionales: CERT-UE.