Políticas de Ciberseguridad en la UE Ciberseguridad y Democracia

Reconocimientos

Cátedra Gobernanza y Regulación en la Era Digital. Proyecto 101127331 *GovReDig.*
Financiado por la UE. Las opiniones no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea, ni la EACEA pueden ser considerados responsables de ellos

Fernando Val Garijo

UNED

GovReDig

Financiado por la Unión Europea

Introducción

- **La Unión Europea promueve la ciberseguridad y la ciber-resiliencia a través de diversas políticas y agencias**.
- Los grandes **objetivos** son mantener la **seguridad en la sociedad y en la economía y proteger la comunicación y los datos**.
- Para ello, la UE despliega una serie de acciones en diversas **áreas:**

1. **Ciberseguridad**
2. **Legislación y certificación**
3. **Gestión de ciber-crisis**
4. **Diplomacia (ciber-diálogos)**
5. **Ciberdefensa**

Estrategia UE de Ciberseguridad (I)

- Presentada por la Comisión y el Alto Representante para la PESC a finales de **2020**
- **Objetivo: utilizar y reforzar recursos y herramientas para que la UE y los EM tengan autonomía/soberanía tecnológica**
- **Fundamento. Resiliencia de servicios y productos interconectados**. Las **4 ciber-comunidades** (Mercado Interior, FCS, Diplomacia y Defensa)deben desarrollar una conciencia común de las ciber-amenazas, y poder responder conjuntamente
- **Garantizar la seguridad de servicios esenciales** como hospitales, redes energéticas, ferrocarriles, y los objetos interconectados en fábricas, oficinas y hogares

Estrategia UE de Ciberseguridad (II)

- **Cooperación con terceros países**, especialmente con los que compartan valores con la UE en materia de democracia, Estado de Derecho y derechos humanos. **Cooperación para garantizar un ciberespacio global y abierto**
- **Creación de capacidades colectivas para responder a los principales ciberataques**
- **Ciber-Unidad Conjunta** (Joint Cyber Unit), plataforma para reforzar la cooperación entre Instituciones UE, Agencias, y autoridades EM
- **Idea central: Poderes públicos, empresas y ciudadanos tienen una responsabilidad compartida** de asegurar una transformación digital con altos estándares de ciberseguridad

Legislación y Certificación

- **Directivas para garantizar un elevado nivel común de ciberseguridad (SRI 2016/1148 y SRI2 2022/2555).**
- **Requiere que los EM aumenten sus capacidades en materia de ciberseguridad**. Han de adoptar una **Estrategia de Ciberseguridad Nacional** que asegure la implementación de medidas de ciberseguridad. Claves de cada estrategia deben ser la seguridad de las cadenas de suministro, la gestión de vulnerabilidades y la educación y formación en ciberseguridad
- **Sectores críticos**: energía, transporte, salud, sector financiero, gestión del agua e infraestructura digital (**SRI)**. También plataformas sociales, gestión de residuos, servicios postales y mensajería, administración pública, entre otros **(SRI2)**

Legislación y Certificación ENISA

- **ENISA es la Agencia de Ciberseguridad de la UE. Creada en 2005, mandato revisado en 2019**. Sede en Atenas, con oficinas en Bruselas y Heraklion
- Centro de expertise (conocimiento + competencias técnicas) en materia de ciberseguridad
- Proporciona **asesoramiento y asistencia técnica a EM, Instituciones y órganos UE y empresas en áreas sensibles**
- **ENISA interviene en el proceso de certificación de ciberseguridad** de productos, servicios y procesos TIC
- **Reglamento (EU) 2019/881** de Ciberseguridad. Refuerza el mandato de ENISA y crea el **Marco Europeo de Certificación de Ciberseguridad**. Requisitos y criterios de evaluación de productos. Enmienda 15 enero 2025

Legislación y Certificación Ciber-solidaridad

- **Reglamento (UE) 2025/38 de Ciber-solidaridad. En vigor desde el 4 de febrero de 2025**
- **Objetivo: Mejorar la preparación, la detección y la respuesta a los incidentes de ciberseguridad en toda la UE**
- **Escudo Europeo de Ciberseguridad**. Propuesta de **sistema UE de alerta integrado por centros de operaciones de seguridad nacionales y transfronterizos** que usen tecnología avanzada e IA para detectar amenazas y compartir la respuesta
- **Mecanismo de Ciber-emergencia**: 1) **Someter sectores clave a pruebas de ciberseguridad** (finanzas, energía, atención médica); 2) creación de una **Reserva de Ciberseguridad, con proveedores privados de confianza**; 3) **Apoyo a la ayuda mutua entre EM**

Diplomacia
Diálogos cibernéticos

- **Colaboración con terceros países para promover intereses comunes en materia de ciberseguridad**
- **Diálogo cibernético UE-Estados Unidos (9).** Cooperación entre ENISA y CISA. Notificación de incidentes
- **Diálogo cibernético UE-Ucrania (3).** Desarrollo de capacidades, intercambio de buenas prácticas
- **Diálogo cibernético UE-Reino Unido (2).**
- **Diálogo cibernético UE-Japón (6).** Intercambio de información y buenas prácticas
- **Diálogos UE-OTAN** sobre a) Resiliencia de Infraestructuras Críticas y b) Ciberseguridad y Defensa

Ciberdefensa

- **Comunicación conjunta sobre política de ciberdefensa UE (Comisión y ARPESC, noviembre 2022). Se basa en cuatro pilares:**

1. **Actuar conjuntamente**. Ello refuerza la ciberdefensa. Intercambio de información, coordinación entre actores militares y civiles, mayor apoyo a misiones PESD
2. **Asegurar el ecosistema de defensa**. Estandarización y certificación de la ciberseguridad. Hasta los componentes no críticos del software pueden abrir la puerta a un ciberataque
3. **Invertir en capacidades.** PESCO, Fondo Europeo de Defensa, Programa Europa Digital
4. **Asociarse con terceros para afrontar retos comunes**

Ciberseguridad, Democracia y Procesos Electorales (I)

- **Injerencia extranjera: Uso de desinformación y ciberataques para intentar influir en la opinión pública de la UE**
- **Tácticas de desinformación**:

1. **Difundir información falsa o engañosa**. Confundir para que la Verdad no se distinga de la mentira
2. **Polarización de opiniones** para reforzar las más extremas y debilitar las moderadas. Hacer imposible el debate democrático
3. **Narrativas que socavan la legitimidad de las instituciones**

- **Normativa** sobre servicios digitales, Transparencia publicidad política; defensa de los periodistas de demandas abusivas, Libertad medios de comunicación

Ciberseguridad, Democracia y Procesos Electorales (II)

- **Garantizar que las elecciones europeas sean libres y justas.** Responsabilidad primordial: autoridades electorales nacionales, conforme al Derecho UE y nacional. Apoyo Instituciones UE
- **EM, distintos sistemas de voto**: papeletas, voto electrónico, online. Doble control recuento de votos. Elecciones, de jueves a domingo
- **Red Europea de Cooperación Electoral**. Autoridades electorales EM
- **ENISA, Equipo de Respuesta ante Emergencias Informáticas**. Protección de redes, sistemas de información . También análisis de riesgos y ejercicios de ciberseguridad previos a la cita electoral
- **Grupo NIS.** EM, Comisión y ENISA