uc3m | Universidad Carlos III de Madrid

OpenCourseWare

DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Coordinadora Curso: **-Profª (PhD) María Nieves de la Serna Bilbao**

Titular de Derecho Administrativo UC3M// Departamento de Derecho Público

Co-directora del Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz

LECCIÓN 10: CIBERSEGURIDAD Y AMENAZAS HÍBRIDAS

I. LA CIBERSEGURIDAD Y SUS DIMENSIONES

Elaborado por Profs. Dr. Carlos Galán Pascual (PhD) y Carlos Galán Cordero

Profesores Área Derecho Administrativo// Departamento de Derecho Público

Profesores Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz

uc3m | Universidad Carlos III de Madrid

Asignatura: Derecho de las Tecnologías de la Información
Lección 10: Ciberseguridad y Amenazas Híbridas

Universidad Carlos III de Madrid

SUMARIO:

I. LA CIBERSEGURIDAD Y SUS DIMENSIONES

1.1 Los sistemas de información y la ciberseguridad

Con el propósito de favorecer la comprensión de esta lección, conviene comenzar recordando algunos conceptos esenciales antes de sumergirnos en unos contenidos tan poliédricos como los que presenta la ciberseguridad. Como toda aproximación científica, lo primero que hemos de hacer es definir el campo de nuestro estudio: los *sistemas de información* y su *ciberseguridad*.

Apoyándonos en la regulación vigente, podemos definir **sistema de información** como[1]:

> *Cualquiera de los elementos siguientes:*
>
> *1º Las redes de comunicaciones electrónicas que utilice la entidad del ámbito de aplicación de este real decreto sobre las que posea capacidad de gestión.*
>
> *2º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales.*
>
> *3º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1º y 2º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.*

Por su parte, podemos definir **ciberseguridad (**o **seguridad de los sistemas de información)** como:

> *La capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos*

[1] Según aparece en el Anexo IV-Glosario del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS)

almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos[2].

Obsérvese que, de estas definiciones, podemos extraer ya algunas conclusiones:

1. El concepto sistema de información comprende cualquier elemento físico (*hardware*) o lógico (*software*) que se vea involucrado en el tratamiento de datos, cualesquiera que sean estos.
2. La ciberseguridad no persigue garantizar siempre y en cualquier situación la absoluta inmunidad de los sistemas de información concernidos frente a las amenazas -cuestión esta imposible de alcanzar, por otro lado-, sino más bien construir un modelo de seguridad sustentado en medidas de *resistencia* -aquellas que razonable y ponderadamente impiden la penetración del ataque y, en general, el progreso del ciberincidente-, y en medidas de *resiliencia* -aquellas dirigidas a recuperar la plena funcionalidad de un sistema de información, una vez concluido el ciberincidente.

1.2 La ciberseguridad como manifestación de la seguridad.

Definidos los conceptos esenciales de nuestro trabajo, debemos proseguir analizando hasta qué punto *seguridad* y *ciberseguridad* son conceptos jurídicamente diferenciados; análisis que no resulta baladí, pues, de estar ubicados dentro de un bien jurídico protegido común, cabría deducir que podrían ser igualmente aplicables las precisiones que en torno a cualquiera de ellos pudieran realizarse.

[2] Idem. Definición asimismo coincidente con la recogida en el artículo 3 b) del Real Decreto-ley 12/2018, dictado al amparo de las competencias exclusivas del Estado en materia de telecomunicaciones y régimen general de comunicaciones (art. 149.1.21 CE) y seguridad pública (art. 149.1.29 CE), que define la *seguridad de las redes y sistemas de información* del mismo modo.

Debemos mencionar, en primer lugar, lo señalado por la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, que identifica en su artículo 10 la ciberseguridad como uno de los "*ámbitos de especial interés de la seguridad nacional... que requieren una atención específica, por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales*".

Asimismo, la Ley 8/2011, de 28 abril, de medidas para la Protección de las Infraestructuras Críticas -a las que define como aquellas infraestructuras estratégicas "*cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales*", dictada al amparo de la competencia atribuida al Estado en virtud del artículo 149.1.29 de la Constitución Española (CE), hace referencia a la ciberseguridad. El artículo 2 de esta Ley define las infraestructuras estratégicas como "*las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales*", entendiendo que tales servicios son los necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las Administraciones públicas.

Además, el mantenimiento de la ciberseguridad es una de las funciones propias del Centro Nacional de Inteligencia (CNI), según establece el artículo 4 b) de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

Finalmente, debemos mencionar el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Esta norma tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales y establecer un sistema de notificación de incidentes, además de un marco institucional para su aplicación y la coordinación entre autoridades competentes y con los órganos de cooperación relevantes en el ámbito comunitario. Como es sabido, este Real Decreto-ley se aplica a los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, así como a los servicios de la sociedad de la información en el sentido recogido en la letra a) del anexo de la Ley 34/2002,

de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Sobre estas cuestiones ha venido a pronunciarse el Tribunal Constitucional en su sentencia 142/2018, de 20 de diciembre de 2018, en relación con el recurso de inconstitucionalidad 5284-2017 interpuesto por el Presidente del Gobierno respecto de la Ley 15/2017, de 25 de julio, de la Agencia de Ciberseguridad de Cataluña, sobre las competencias en materia de telecomunicaciones, defensa y seguridad pública[3].

De la citada sentencia y de la normativa que invoca, a modo de resumen, extraemos las consecuencias más significativas:

- La ciberseguridad, como sinónimo de la seguridad en la red, es una actividad que se integra en la seguridad pública, así como en las telecomunicaciones. A partir de su conceptuación como conjunto de mecanismos dirigidos a la protección de las infraestructuras informáticas y de la información digital que albergan, fácilmente se infiere que, en tanto que dedicada a la seguridad de las tecnologías de la información, presenta un componente tuitivo que se proyecta específicamente sobre el concreto ámbito de la protección de las redes y sistemas de información que utilizan los ciudadanos, empresas y administraciones públicas, (FJ 1).
- La ciberseguridad se incluye en materias de competencia estatal en cuanto, al referirse a las necesarias acciones de prevención, detección y respuesta frente a las ciberamenazas, afecta a cuestiones relacionadas con la seguridad pública y la defensa, las infraestructuras, redes y sistemas y el régimen general de telecomunicaciones, (FJ 1)[4].

Todas estas cuestiones han encontrado definitiva consolidación en el Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021, en el que la ciberseguridad pública se configura como parte integrante de la Seguridad Nacional, al encuadrar el ciberespacio dentro de los objetos materiales de la seguridad exigible a los espacios

[3] BOE, núm 22, viernes 25 de enero de 2019.
[4] Efectivamente, la citada sentencia TC 142/2018, señala que "*la seguridad pública es, en principio, competencia exclusiva del Estado ex artículo 149.1.29 CE, precepto constitucional que pone de manifiesto que ya en él se establecen salvedades («sin perjuicio de») que, en cierto sentido, vienen a modular la exclusividad de la competencia estatal, proclamada en el párrafo inicial del artículo 149 CE*", añadiendo que "*la competencia exclusiva del Estado en materia de seguridad pública no admite más excepción que la que derive de la creación de las policías autónomas*" (STC 104/1989, de 8 de junio, FJ 3).

comunes globales e integrando el modelo de gobernanza de la ciberseguridad en el marco del Sistema de Seguridad Nacional.

1.3 Las dimensiones de la ciberseguridad.

Como hemos señalado en otros trabajos[5], la ciberseguridad es un concepto poliédrico que puede estudiarse desde diferentes puntos de vista, atendiendo precisamente a las garantías exigibles a la información tratada o los servicios que deben ser preservados.

El Esquema Nacional de Seguridad (ENS), siguiendo la metodología MAGERIT de análisis y gestión de riesgos[6]- establece cinco dimensiones de seguridad: *Confidencialidad*, *Integridad*, *Autenticidad*, *Trazabilidad* y *Disponibilidad*, a las que nosotros hemos añadido una más, de carácter genérico: *Conformidad Legal.*

El cuadro siguiente muestra las definiciones de estas dimensiones, así como su aplicabilidad a la información tratada o los servicios prestados por los sistemas de información de que se trate.

DIMENSIÓN DE LA CIBERSEGURIDAD	DEFINICIÓN	APLICABILIDAD
Confidencialidad	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a	Información

[5] Galán Pascual, Carlos Manuel. *El Derecho a la Ciberseguridad*, en *Sociedad Digital y Derecho*. Varios autores. BOE, 2018.
[6] MAGERIT versión 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

	individuos, entidades o procesos no autorizados.	
Integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.	Información
Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.	Información y Servicios
Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.	Información y Servicios
Disponibilidad	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.	Información y Servicios
Conformidad legal	Propiedad o característica de las tecnologías, productos, soluciones o servicios que sustentan las operaciones, para mantenerse permanentemente alineados con lo dispuesto en la legislación nacional, europea o internacional que resulte de aplicación.	Sistemas de Información, en su conjunto.

Naturalmente, dependiendo de la aplicación o del servicio concreto de que se trate, ciertas dimensiones de seguridad cobrarán más importancia que las restantes. En el caso de las telecomunicaciones, todas ellas, en mayor o menor medida, constituyen los elementos esenciales de la ciberseguridad en el ámbito de los servicios de telecomunicaciones, como se verá a lo largo de este capítulo.