1. Introducción a la Ciberseguridad

1. Conceptos Fundamentales de Ciberseguridad

1.1 Introducción

En la actualidad, la palabra “ciberespacio” se usa en muchos contextos y no siempre está claro lo que este término significa y describe.

Vamos a empezar comparando diferentes definiciones de ciberespacio de forma que podamos establecer unas nociones comunes de lo que tratamos de definir.

Hay muchos otros términos que se basan en el ciberespacio:

- Ciberseguridad.
- Cibercrimen.
- Ciberguerra.
- Ciberterrorismo.

De ahí la importancia de esta definición inicial.

Podríamos trabajar con varias definiciones, pero esto nos acarrearía problemas. Por ejemplo, si una definición se enfoca sólo en el hardware (ordenadores, dispositivos móviles, dispositivos de red,…), pero ignora los datos y otra definición hace lo contrario, la conclusión de una parte no tendría significado para la otra.

La situación empeora cuando muchos documentos hablan del ciberespacio sin ni siquiera definirlo. Uno de estos documentos es el “Information Security Strategy for Protecting the Nation” del Information Security Policy Council de Japón.

De la gran cantidad de definiciones existentes del término ciberespacio podemos extraer un conjunto de términos que son los más usados en ellas:

- Actividades
- Aplicaciones
- Comunicación
- Humano
- Hardware
- IT/ICT
- Información
- Interconexión
- Internet
- Red
- Servicios
- Social
- Virtual

Estos términos los podemos dividir en tres categorías:

- Tangibles:

    - Hardware
    - IT/ICT
- Intangibles:
    - Información
    - Actividades
    - Aplicaciones/Servicios
    - Social/Humano
    - Virtual
- Relacionados con la red:
    - Internet
    - Red
    - Interconexión
    - Comunicación

Prácticamente todas las definiciones de ciberespacio incluyen **elementos tangibles**. Esto implica que el ciberespacio no puede existir sin elementos tangibles.

También, todas las definiciones incluyen información. Esta información pueden ser datos almacenados, señalización entre procesos y/o dispositivos, o el contenido que se está transmitiendo.

El ciberespacio incluye elementos tangibles, pero también es virtual.

Veamos algunas de estas definiciones:

Oxford English Dictionary:

"The space of virtual reality; the notional environment within which electronic communication (esp. via the Internet) occurs."

Cyber Security Strategy (Australia):

"Cyber security refers to the safety of computer systems – also known as information and communications technologies (or ICT)."

Cyber Security Strategy for Germany:

"Cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace."

The UK Cyber Security Strategy:

"Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services."

European Union, Glossary:

"Word invented by the writer William Gibson in his play "le Neuromacien". It describes the virtual space in which the electronic data of worldwide PCs circulate."

Y la que usaremos en nuestro curso, **ISO/IEC 27032 Guidelines for cybersecurity**:

"The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."

1.2 Naturaleza del Ciberespacio

Dada la complejidad de definir un término como ciberespacio, vamos a abordar su naturaleza dividiéndolo en 4 capas:

- **Personas**: Quienes participan en la ciberexperiencia, comunicándose, trabajando con información, tomando decisiones, llevando a cabo planes, transformando la naturaleza del ciberespacio trabajando con sus servicios y capacidades.
- **Información**: Almacenada, transmitida y transformada en el ciberespacio.
- **Bloques lógicos**: Constituyen los servicios y dan soporte a la naturaleza de la plataforma del ciberespacio.
- **Física**: Da soporte a los bloques lógicos.

No son los ordenadores los que crean el ciberespacio, sino la interconexión, que se realiza en las cuatro capas que hemos descrito.

Capa Física:

- Ordenadores.
- Servidores.
- Cables.
- Fibra.
- Transmisión por radio.
- …

Capa Lógica:

El ciberespacio está construido a partir de componentes que proporcionan servicios, y estos servicios están diseñados de forma que puedan combinarse para formar servicios más complejos.

Entre los **servicios de nivel más bajo** podemos tener los entornos de ejecución de programas, los mecanismos de transporte de datos (protocolos), los estándares para el formato de datos.

Sobre estos bloques básicos se construyen **aplicaciones** como procesadores de texto, bases de datos o la Web.

Combinando las aplicaciones anteriores obtenemos servicios más complejos. Por ejemplo, uniendo una base de datos con la Web obtenemos generación dinámica de contenidos.

Sobre la web dinámica se han desarrollado otros servicios más complejos, como Facebook, que a su vez es una plataforma sobre la que se desarrollan otras aplicaciones.

La naturaleza del ciberespacio es la continua y rápida evolución de nuevas capacidades y servicios, basados en la creación de nuevas construcciones lógicas sobre los fundamentos físicos.

Podemos decir que el ciberespacio es **recursivo**, plataformas sobre plataformas sobre plataformas…

Capa de Información:

Hay muchos aspectos que influyen en el ciberespacio, pero claramente, la creación, captura, almacenamiento y procesado de información es fundamental en esta experiencia.

La información en el ciberespacio puede tomar muchas formas:

- Música y vídeo que compartimos.
- Registros de empresas.
- Páginas de WWW.
- Libros online y fotografías.
- Información sobre información (metadatos)
- Información creada y recopilada mientras buscamos información (Google)

La información ya no sólo se almacena de forma estática, sino que se crea de **forma dinámica** continuamente. Las páginas web se crean bajo demanda y se personalizan para el usuario, basándose en componentes de información almacenados en bases de datos.

Personas:

Las personas ya no son simples usuarios pasivos del ciberespacio. Las personas contribuyen a la Wikipedia y "twitean". Escriben en Facebok y establecen conexiones con otras personas en LinkedIn…

Los participantes en juegos multijugador "van" a su mundo virtual, conforman un rol (avatar), ganan dinero, hacen amigos, discuten sobre un gobierno y tienen un sentimiento de "realidad" de ese espacio virtual.

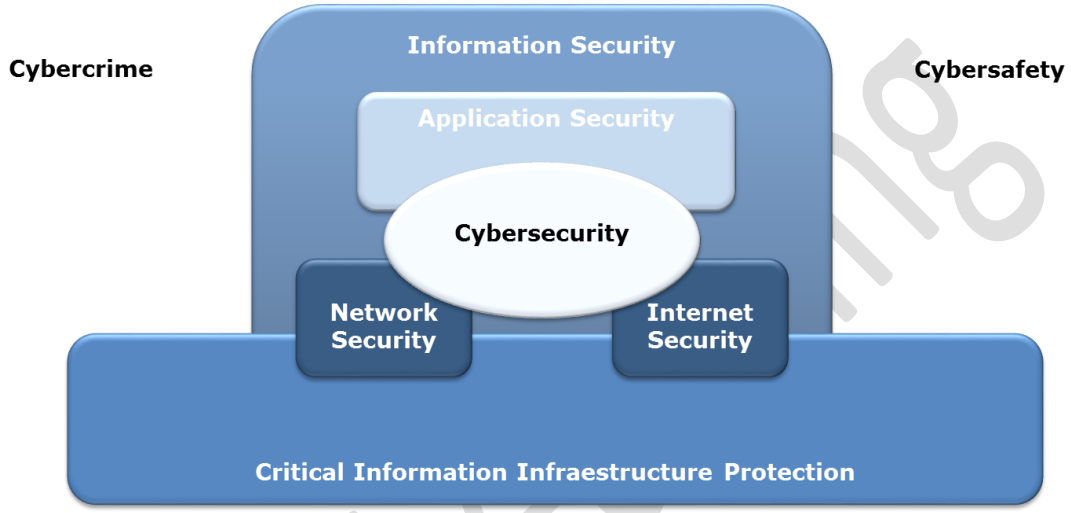
Todas las capas son importantes y si queremos entender la seguridad en el ciberespacio, no podemos enfocarnos sólo en una de ellas.

Los ataques pueden producirse en las 4 capas, desde la destrucción de componentes físicos a engañar a personas, pasando por comprometer elementos lógicos o corromper información.

1.3 Ámbito de la Ciberseguridad

La ciberseguridad se basa en la **seguridad de la información**, **seguridad de aplicaciones**, **seguridad de red** y la **seguridad de Internet** como bloques de construcción fundamentales.

La ciberseguridad es una de las actividades necesarias para CIIP (Critical Information Infrastructure Protection) y, al mismo tiempo, una protección adecuada de los servicios de infraestructura crítica contribuye a las necesidades básicas de seguridad (es decir, la seguridad, la fiabilidad y disponibilidad de la infraestructura crítica) para la consecución de los objetivos de la ciberseguridad.



La seguridad cibernética no es, sin embargo, sinónimo de seguridad de Internet, seguridad de red, seguridad de aplicaciones, seguridad de la información, o CIIP. Tiene un alcance único que requiere a las partes interesadas jueguen un papel activo con el fin de mantener, si no mejorar la utilidad y confiabilidad del ciberespacio.

Con mucha frecuencia se confunden los términos **ciberseguridad** y **seguridad de la información**.

Ambos conceptos tienen como objetivo conseguir y mantener las propiedades de la seguridad:

- Confidencialidad
- Integridad
- Disponibilidad

Sin embargo, el alcance global de Internet le da a la ciberseguridad un carácter único.

Mientras que la seguridad de la información se inició cuando la mayoría de los sistemas estaban aislados y raramente se atravesaban jurisdicciones, la ciberseguridad trabaja sobre amenazas globales e incertidumbre legal.

1. Las **leyes** creadas para la seguridad de la información son inadecuadas en la era de Internet.
2. La ciberseguridad tiene que lidiar con una arquitectura de Internet que hace prácticamente imposible **atribuir un ataque** a quien lo ha iniciado.
3. Debido a sus orígenes en los servicios militares y diplomáticos, la seguridad de la información suele centrarse en la **confidencialidad**. A pesar de que WikiLeaks ha

destacado la importancia de la confidencialidad, la ciberseguridad se centra también en la **integridad** y la **disponibilidad**.

Un **ciberataque** ocurre cuando una amenaza rompe con éxito los controles de seguridad (de los que hablaremos más adelante en el curso).

Las evidencias muestran que estos ataques están creciendo en sofisticación, frecuencia y gravedad.

Nuestra **creciente dependencia en el ciberespacio** pone a todos los gobiernos, empresas, organizaciones y usuarios individuales en el riesgo de fraude, sabotaje y vandalismo.