



# Módulo I

# Conceptos base para el análisis de la ciberseguridad

---

JONATHAN E. HERNÁNDEZ FUENTES



## Dispositivo Electrónico

Es todo aquel dispositivo, conformado por un **Hardware y Software**, suministrado por una fuente de energía, interna o externa, para cumplir una función específica, capaz de ser programable, **procesar datos**, almacenarlos, visualizarlos, redireccionarlos.

JONATHAN E. HERNÁNDEZ FUENTES



## Mundo Real

Es el lugar donde vivimos, coexistimos, a través de la **percepción real de nuestros sentidos**, el estado real de lo que nos rodea tal y como existe y no tal como puede parecer o imaginarse, la realidad entonces supone lo que es y no lo que supone ser, hablando materialmente.

JONATHAN E. HERNÁNDEZ FUENTES



## Mundo virtual

(ciberespacio)

En contraposición al termino anterior, se hace referencia a **algo no físico**, que no existe en el mundo real, es decir **solo existe en la interconexión**, de las tecnologías de información y comunicación por medio de los dispositivos electrónicos; un espacio no físico que puede ser creado mediante lenguajes de programación y así poder interactuar.

JONATHAN E. HERNÁNDEZ FUENTES



## Mundo Real

En el mundo real somos

**PERSONAS**



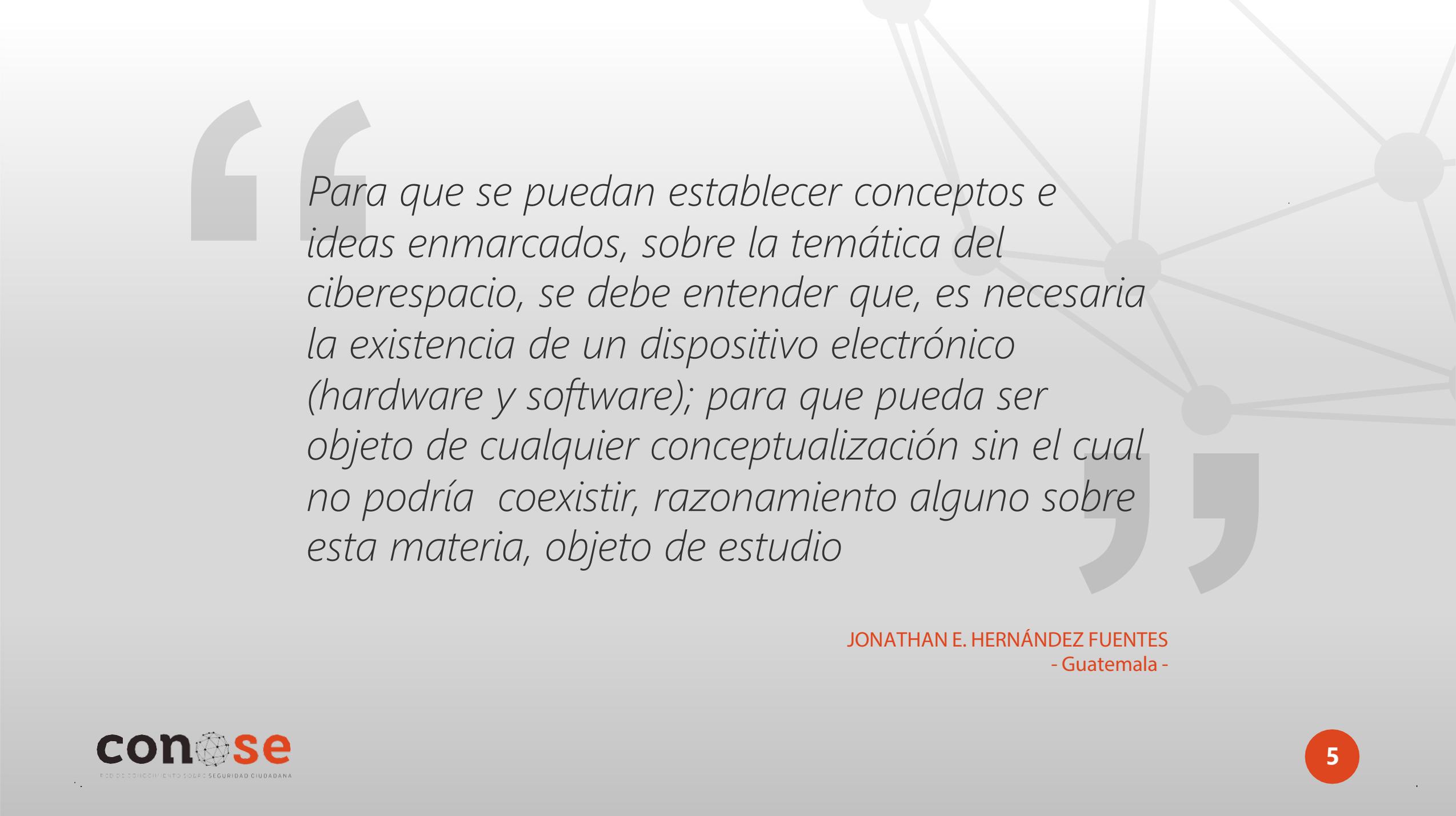
## Mundo virtual

(ciberespacio)

En el mundo virtual somos

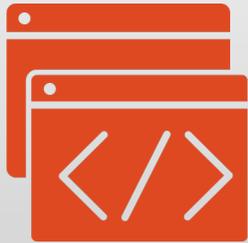
**USUARIOS**





*Para que se puedan establecer conceptos e ideas enmarcados, sobre la temática del ciberespacio, se debe entender que, es necesaria la existencia de un dispositivo electrónico (hardware y software); para que pueda ser objeto de cualquier conceptualización sin el cual no podría coexistir, razonamiento alguno sobre esta materia, objeto de estudio*

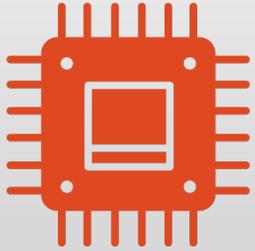
JONATHAN E. HERNÁNDEZ FUENTES  
- Guatemala -



## Software

Programas informáticos que sirven para realizar tareas específicas. Cualquier herramienta que instalemos o utilicemos en nuestro ordenador es un ejemplo de software, como el navegador, el correo electrónico, un juego o cualquier otra aplicación que ofrezca alguna funcionalidad concreta.

OFICINA DE SEGURIDAD INTERNA.ES



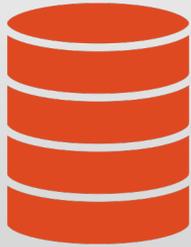
## Hardware

Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

# CONCEPTOS BÁSICOS

Las personas, las organizaciones y los gobiernos son **víctimas habituales de los ciberataques**. Por lo que se hace referencia a términos y conceptos a los que no estamos familiarizados como ciberseguridad, ciberataques, ciberdelincuentes, etc.

Por lo que se hace necesario abordarlos, definirlos y así lograr identificarlos, **creando un marco de seguridad, prevención y protección de los datos**.



## Dato

Dato (en plural datos o como un sustantivo en masa) es cualquier secuencia de uno o más símbolos a los que se les da significado mediante actos específicos de interpretación, por medio de software o bien por un analista. Los datos o dato (una sola unidad de datos) requieren una interpretación para convertirse en información.

Un dato puede definirse como la representación simbólica de algo dentro de un sistema informático. Recordemos que los datos no necesariamente tienen que ser numéricos, ya que estos pueden estar conformados por signos y hasta por letras que guardan una significación con respecto a un conjunto.

Los datos en informática describen hechos o sucesos que pueden ser interpretados como ordenes de un usuario, a un sistema de computadora o la respuesta del propio sistema a los comandos ingresados por el usuario.



# Información

La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

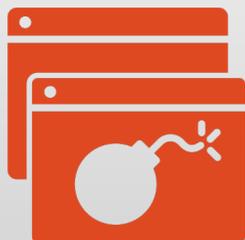
Es el conjunto de datos que configuran un mensaje que emite un emisor y que se pretende llegue al receptor para que quede informado. Siempre se lleva a cabo a través de un canal que es el que uno a ambos interlocutores han elegido.



# Ciberseguridad

La ciberseguridad hace referencia a tecnologías, procesos y aprendizaje que ayudan a proteger los sistemas, las redes, los programas y los datos frente a ciberataques, daños y accesos no autorizados.

FUENTE: MICROSOFT



## Ciberataque

Se define normalmente como un intento de obtener acceso no autorizado a un equipo o sistema informático para causar daños.

FUENTE: MICROSOFT



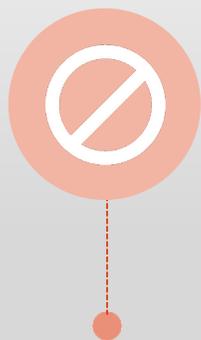
## Ciberdelincuente

Un ciberdelincuente es cualquier persona que lleva a cabo un ciberataque.

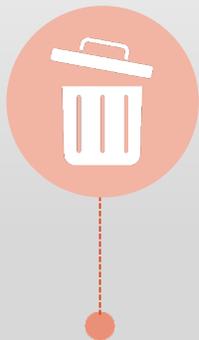
Los ciberdelincuentes se pueden encontrar en cualquier lugar, incluso dentro de una organización o institución, para causar daños desde dentro.

FUENTE: MICROSOFT

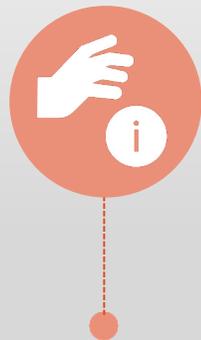
Un atacante puede usar personas, equipos, teléfonos, aplicaciones, mensajes y procesos del sistema para llevar a cabo un ataque. Estos atacantes podrían hacer lo siguiente:



Bloquear datos y procesos y exigir un rescate.



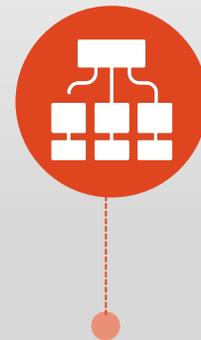
Quitar información vital para causar daños graves.



Robar información



Exponer públicamente información privada



Comprometer infraestructuras críticas



Detener la ejecución de procesos y sistemas empresariales vitales para provocar interrupciones y errores de funcionamiento.



Los individuos, las organizaciones, las instituciones y los gobiernos pueden ser víctimas de un ataque.



## Contraseñas

Claves que utilizamos para iniciar sesión o registrarnos en alguna aplicación o página web. Están formadas por una serie de caracteres (letras, números y caracteres especiales), que, en función de su complejidad, pueden hacerlas más seguras.

OFICINA DE SEGURIDAD INTERNA.ES



## Copia de seguridad

Copia de nuestros archivos y programas que puede almacenarse en otros dispositivos o soportes para evitar perder nuestra información en caso de fallo, pérdida o robo

OFICINA DE SEGURIDAD INTERNA.ES



## Antivirus

Programa que detecta cualquier amenaza, como los virus, y la elimina de nuestro dispositivo. Es necesario mantenerlo actualizado para que nos proteja correctamente, incluso de los virus más nuevos.

OFICINA DE SEGURIDAD INTERNA.ES



## Ingeniería Social

Estrategia de engaño que utilizan los ciberdelincuentes para ganarse nuestra confianza y conseguir que compartamos nuestros datos con ellos, como contraseñas o datos de nuestra tarjeta, o que les demos acceso a nuestros dispositivos.

OFICINA DE SEGURIDAD INTERNA.ES



## Phishing

Técnica donde los ciberdelincuentes se hacen pasar por otra persona o entidad a través del correo electrónico, como puede ser el banco, una red social o incluso un servicio público, para engañarnos y que realicemos alguna acción bajo cualquier excusa, generalmente acceder a una página fraudulenta o descargar un fichero infectado.

OFICINA DE SEGURIDAD INTERNA.ES

# ¡Gracias!

---