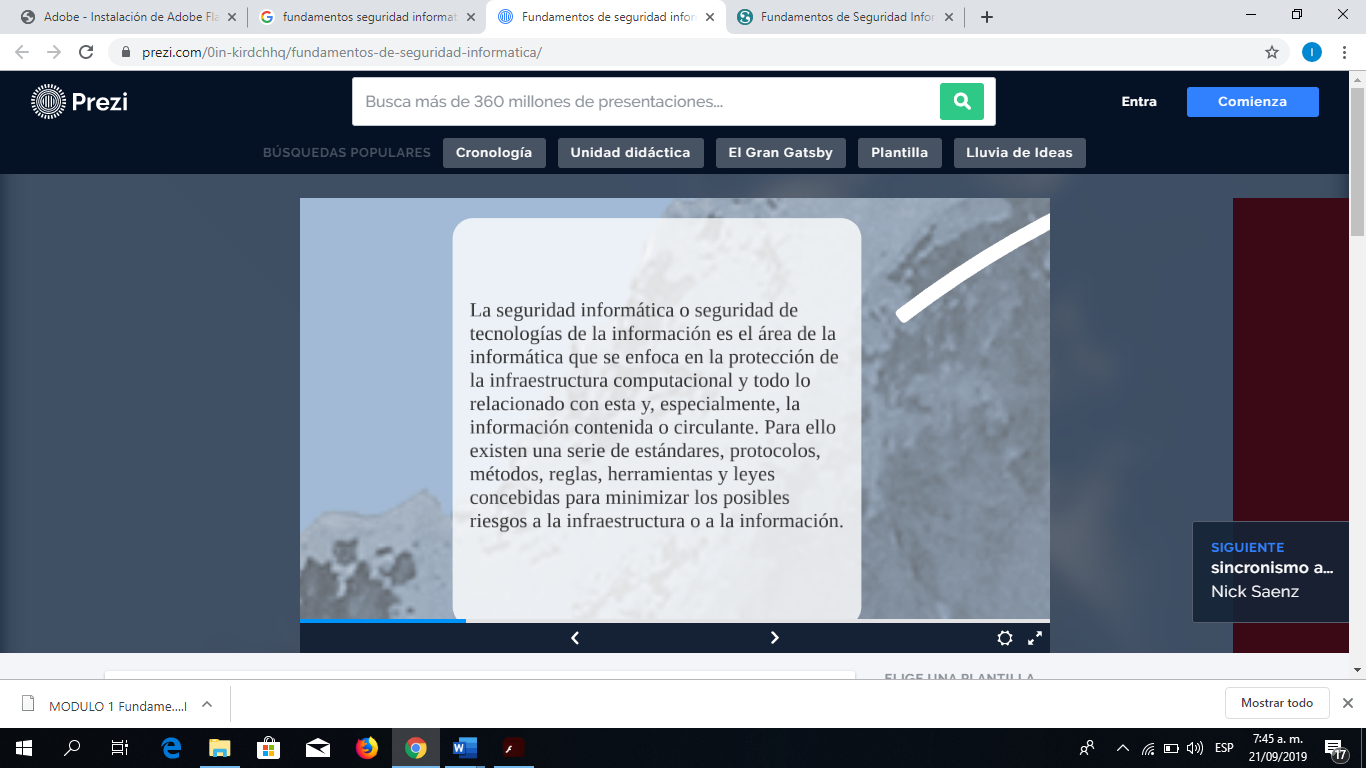
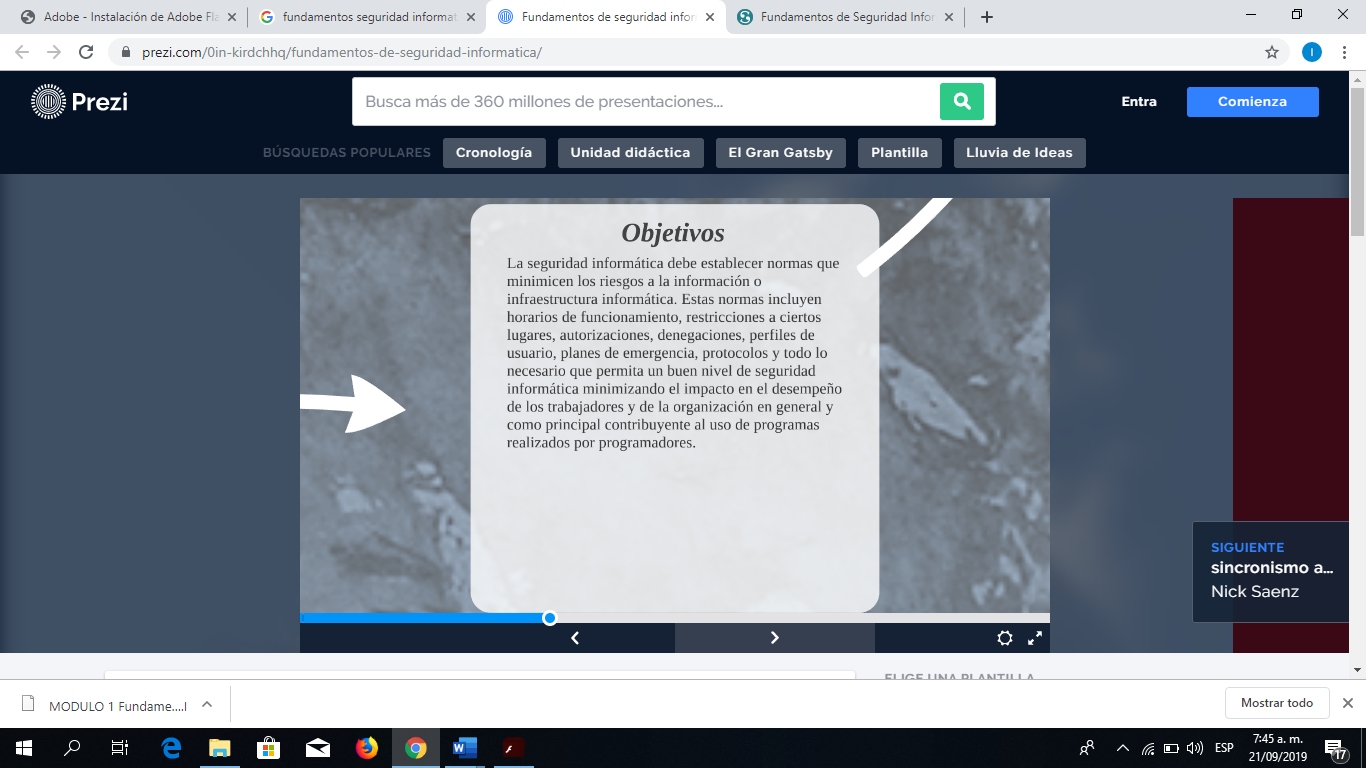
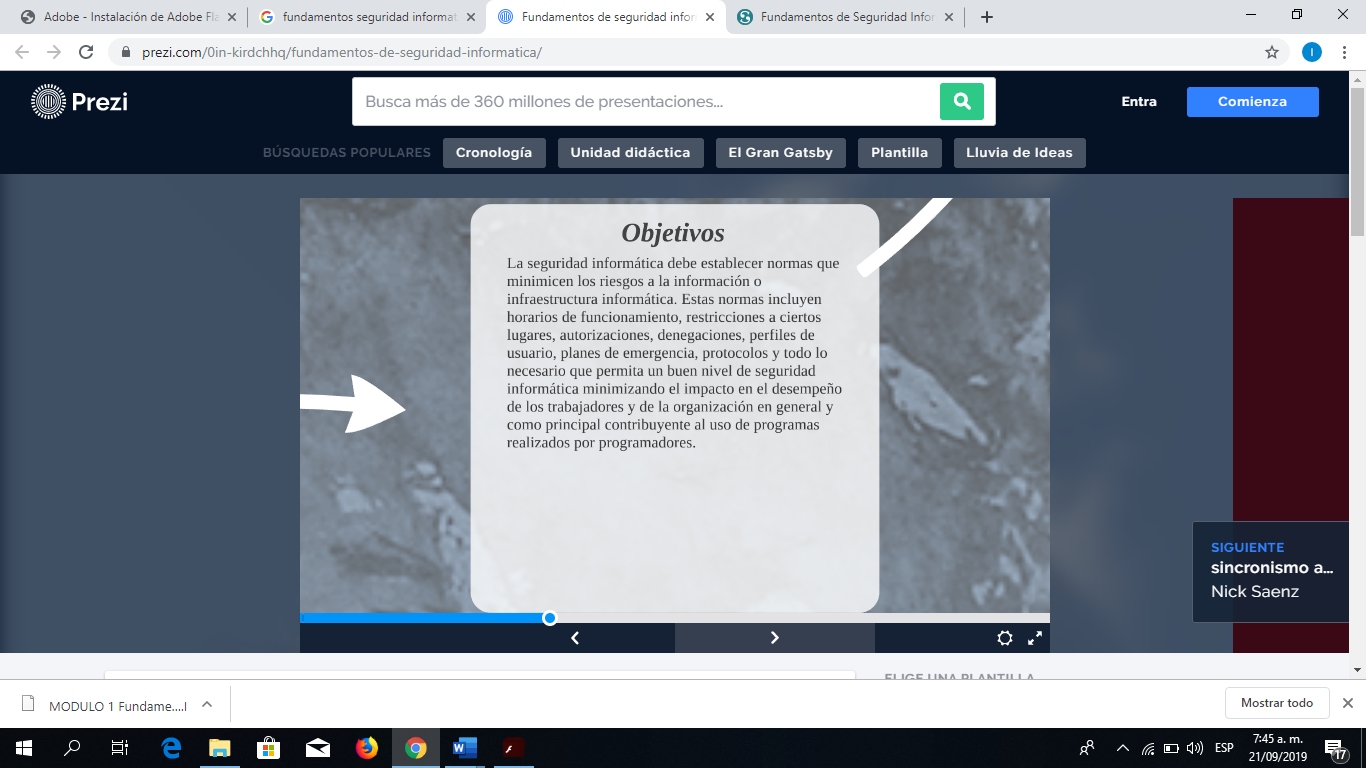
Significado de Seguridad informática







Qué es Seguridad informática:

La seguridad informática es un conjunto de herramientas, procedimientos y estrategias que tienen como objetivo**garantizar la integridad, disponibilidad y confidencialidad de la información de una entidad en un sistema**.

La seguridad informática se caracteriza por la protección de datos y de comunicaciones en una red asegurando, en la medida de lo posible, los tres principios básicos:

* **La integridad de los datos**: la modificación de cualquier tipo de información debe ser conocido y autorizado por el autor o entidad.
* **La disponibilidad del sistema**: la operación continua para mantener la productividad y la credibilidad de la empresa.
* **La confidencialidad**: la divulgación de datos debe ser autorizada y los datos protegidos contra ataques que violen este principio.

La seguridad informática es una disciplina o rama de la Tecnología de la información, que estudia e implementa las amenazas y vulnerabilidades de los sistemas informáticos especialmente en la red como, por ejemplo, virus, gusanos, caballos de troya, ciber-ataques, ataques de invasión, robo de identidad, robo de datos, adivinación de contraseñas, intercepción de comunicaciones electrónicas, entre otros.

Tipos de seguridad informática

La seguridad informática suele dividirse en tres clases:

Seguridad de *hardware*

Hardware es la parte física de un ordenador o sistema informático. Está formado por los componentes eléctricos, electrónicos, electromecánicos y mecánicos, tales como circuitos de cables y luz, placas, memorias, discos duros, dispositivos periféricos y cualquier otro material en estado físico que sea necesario para hacer que el equipo funcione.

La seguridad de *hardware* implica tanto la protección física como el control del tráfico de una red y el escáner constante de un sistema. Algunos ejemplos de seguridad informática de *hardware* son los cortafuegos de hardware, servidores proxys y claves criptográficas para cifrar, descifrar y autentificar sistemas, copias de seguridad, bancos de baterías para los cortes de electricidad, etc.

### Seguridad de software

### Software es un término informático que hace referencia a un programa o**conjunto de programas**de cómputo, así como**datos, procedimientos y pautas que permiten realizar distintas tareas en un sistema informático.**

La seguridad de software se dedica a bloquear e impedir ataques maliciosos de hackers, por ejemplo. La seguridad de software es parte del proceso de la implementación de un programa, trabajo de ingenieros informáticos, para prevenir modificaciones no autorizadas que cause el mal funcionamiento o violación de la propiedad intelectual del programa en sí.

**Hacker** es una voz del inglés para referirse a una **persona o a una comunidad que posee conocimientos en el área de informática y se dedica a acceder a sistemas informáticos para realizar modificaciones en el mismo**. Los hackers también son conocidos como “piratas informáticos”

### Seguridad de red

En informática, como redes se designa un **conjunto de equipos o dispositivos conectados entre sí para el intercambio de recursos** (como hardware o software) y de información.

Las redes informáticas se pueden clasificar según su tamaño (cantidad de equipos conectados), velocidad de transferencia y alcance de la red (distancias geográficas), internet.

La seguridad informática en la red es aplicada a través del hardware y el software del sistema. La seguridad en la red protege la facilidad de uso, la fiabilidad, la integridad, y la seguridad de la red y de los datos. Algunos componentes que ayudan en este aspecto son: los antivirus, antispyware, cortafuegos que cortan el acceso no autorizado, redes privadas virtuales (VPN) y sistema de prevención de intrusos (IPS).

Virus

que son [**programas**](https://definicion.de/software/) que se copian en forma automática y que su objetivo es afectar el normal funcionamiento de una [**computadora**](https://definicion.de/computadora/), sin el consentimiento del usuario.

en el sentido estricto del término, los virus informáticos son programas que pueden replicarse y ejecutarse por sí mismo. En su accionar, suelen reemplazar archivos ejecutables del [**sistema**](https://definicion.de/sistema/) por otros infectados con el código maligno. Los virus pueden simplemente molestar al usuario, bloquear las redes al generar tráfico inútil o, directamente, destruir los datos almacenados en el disco duro del ordenador.

Entre las herramientas más usuales de la seguridad informática, se encuentran los **programas antivirus**, los cortafuegos o firewalls, la encriptación de la información y el uso de contraseñas (passwords).