

**Alumna: Laura Loreiro**

03/05/2021

Playground

## Seguridad informática

¿Podemos pensar en una cuarta revolución industrial? Aunque en la historia de la humanidad podemos definir claramente tres revoluciones industriales, lo cierto es que existe una cuarta y, es precisamente, la que estamos viviendo en la actualidad, gracias a la aparición de las tecnologías de información y las comunicaciones (TIC), junto con Internet.

En las últimas dos décadas, las TIC han adquirido un valor en dimensiones que nunca antes había ocurrido en la historia, generando profundas transformaciones en todos los ámbitos socioeconómicos y, por supuesto, de la mano aparecieron conductas ilícitas cometidas sobre los datos, la información, los programas y todo aquel recurso tecnológico susceptible de ser manipulado ilícitamente.

La seguridad informática, o ciberseguridad, es una disciplina que se encarga de proteger la integridad y la privacidad de los datos y toda la información que se encuentre alojada en un sistema informático. La idea principal es que se pueda evaluar la seguridad de los sistemas de cómputo y redes para, posteriormente, protegerlos de los ataques informáticos que se pueden llevar a cabo a los sistemas.

Pero, ¿esto fue siempre así? A lo largo de la historia, esta seguridad se ha ido transformando, gracias a los controles y auditorías sobre los sistemas, explotando las vulnerabilidades que se puedan encontrar en los mismos. Se han implementado medidas de seguridad física y lógicas en conjunto con la seguridad en Internet.

Por otro lado, sería fantástico poder analizar de forma particular cuál es el impacto que ha causado en la sociedad, en sus normas jurídicas y éticas. Además, reconocer e identificar los delitos informáticos y las consecuencias legales que implican el no acatarlos.

Bien, ha llegado el momento de adentrarnos en el estudio de este maravilloso mundo de seguridad.

## Ciberseguridad

La seguridad informática se enfoca en la **protección de la infraestructura computacional** y todo lo vinculado con la misma, especialmente, en la información que se transmite a través de las redes de computadoras. Para minimizar todos los riesgos a la infraestructura y a la información se han creado a lo largo de la historia múltiples métodos, como estándares, protocolos, reglas, herramientas y obviamente leyes informáticas.

Debemos tener en cuenta que la seguridad informática únicamente se va a centrar en el medio de comunicación por el cual va a viajar la información. No debemos confundir este término con el de seguridad de la información, ya que esta última puede estar en diferentes medios y no solo en los medios informáticos.

Bajo este último concepto, la seguridad informática va a identificar, eliminar vulnerabilidades y proteger de ataques maliciosos a los equipos de cómputo, servidores, redes informáticas y todo aquel medio informático por el cual se transmita información.

Malware, es un malicious software, tienen como objetivo filtrarse y dañar o robar. Virus, trojanos, gusanos

Virus, es un tipo de malware, cuyo objetivo es copiarse, destruir o inhabilitar archivos o programas.

La mayoría de estos virus se adhieren a los archivos ejecutables, no tiene la capacidad de afectar a otros dispositivos al menos que lo pasemos por medio de un hardware, por eso son de poca infección porque se replican a sí mismos solos dentro del mismo dispositivo

Cuando las pc se empiezan a conectar a la red aparecen los gusanos, se copia a sí mismo y utiliza la red para copiar a otras pc, tienen mayor capacidad de infección

Trojanos, no causan daños por sí mismos, tienen cosas ocultas, son programas sin licencias, requieren de la

ejecución del usuario; el troyano puede crear backdoors es un software para que una persona pueda entrar en forma remota

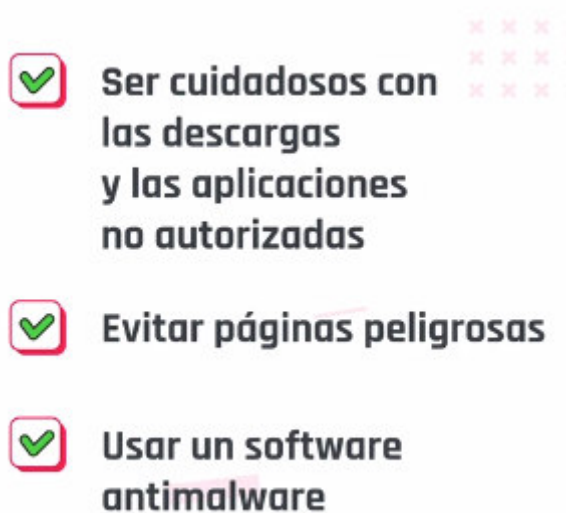
Adwares cuyo objetivo, es bombardear nuestro dispositivo con publicidad, generalmente vienen dentro de troyanos

En la red hay amenazas informáticas, spywares, no daña los dispositivos pero roba información, su objetivo es mantenerse oculto para robar la mayor cantidad de información, puede ingresar por troyanos.

Rootkits, son un conjunto de software tienen acceso al dispositivo en modo sistema o kernel, logran esconderse de softwares antimalware o antivirus

Botnet, es una red de robots, ataca a una red de pc para ser controladas, todas al mismo tiempo

Ransomeware o software de secuestro, secuestran a empresas.

- 
- ✓ **Ser cuidadosos con las descargas y las aplicaciones no autorizadas**
  - ✓ **Evitar páginas peligrosas**
  - ✓ **Usar un software antimalware**

## Protección de la información

### Fallas

Una falla, también conocida como bug, es un error en un programa o sistema operativo que desencadena un resultado indeseado.

El término bug viene desde 1947 cuando Grace Hooper, mientras, estaba programado el Mark II, descubrió que un insecto (bug) había provocado un error en unos de los relés electromagnéticos.

En el desarrollo del software existen muchos tipos de fallas, pero en general se pudieron establecer unos tipos generales de bugs según su comportamiento.

### Vulnerabilidades

## Tipos de fallas

Nombre	Descripción
<b>Heisenbug</b>	Basados en el principio de incertidumbre de Heisenberg se denominan a aquellos bugs que alteran o desaparecen su comportamiento al tratar de depurarlos.
<b>Bohrbug</b>	Nombrados así por el modelo atómico de Bohr, es una clasificación de un error de software inusual que siempre produce una falla al reiniciar la operación que causó la falla.
<b>Mandelbug</b>	Llamado así por el matemático Benoit Mandelbrot, un mandelbug es un fallo con causas tan complejas que su comportamiento es totalmente caótico.
<b>Schroedinbugs</b>	Son errores que no aparecen hasta que alguien lee el código y descubre que, en determinadas circunstancias, el programa podría fallar. A partir de ese momento, el "Schroedinbug" comienza aparecer una y otra vez.

Una vulnerabilidad es una debilidad o fallo de un sistema informático que puede poner en riesgo la integridad, confidencialidad o disponibilidad de la información.

La evaluación o detección de vulnerabilidades permite reconocer, clasificar y caracterizar los ajustes de seguridad.

### Pasos para detectar una vulnerabilidad

Si bien no existe un método único para detectar vulnerabilidades, es posible armar una serie de ítems a tener en cuenta para considerar nuestra información segura.

- Evaluar cómo está constituida la red e infraestructura de la empresa.
- Delimitar quien puede y debe acceder a la información confidencial.
- Probar que las copias de seguridad realizadas funcionen.
- Identificar las partes mas sensibles y esenciales del sistema
- Realizar auditorías del estado de la seguridad informática.

### Clase Sincrónica

Virus,

Gusanos, para atacarlo hay que apagar toda la red y limpiar compu por compu.

### Secuestro de datos

<https://www.pagina12.com.ar/291148-los-hackers-publicaron-finalmente-la-informacion-robada-a-la>

### Exposición

<https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/programacion-declarativa/>

<https://dosideas.com/noticias/actualidad/487-los-lenguajes-especificos-de-dominio>

### Actividad

Grupo 3:

<https://thehackernews.com/2021/04/alert-theres-new-malware-out-there.html>



#### **Micro desafíos**

Deberán leer cada una de las noticias asignadas y responder en un documento (ustedes deben abrirlo) las siguientes consignas:

- ¿Qué tipo de amenaza es?  
Saint Bot es un troyano relativamente nuevo.
- ¿Cómo comienza y cómo se propaga esta amenaza?  
Saint Bot se envía a través de correos electrónicos de phishing que contienen archivos adjuntos ZIP, que a su vez contienen archivos LNK. Cuando se abre, el archivo LNK apunta a una URL de descarga, donde extrae y ejecuta un cargador de PowerShell inicial en la carpeta %TEMP%. Este cargador luego descarga y ejecuta dos archivos EXE, el primero de los cuales es un script por lotes que intenta deshabilitar Windows Defender, mientras que el otro contiene Saint Bot. Una vez ejecutado, Saint Bot soltará varios scripts para controlar sus otros componentes, incluida una copia de ntdll que utiliza en lugar de la versión legítima. A continuación, realiza una verificación de emulación y una verificación de ubicación para determinar en qué lugar se encuentran los sistemas afectados, y se cancela si parece estar en algún miembro de la Comunidad de

Estados Independientes. Se crea una clave de registro Ejecutar para garantizar la persistencia.

Saint Bot intentará ponerse en contacto con una de varias direcciones de comando y control (C2) codificadas y enviará información del sistema a cualquier servidor que responda. Las URL de descarga para nuevas cargas útiles se le pasan desde el servidor C2.

- ¿Hay más de una amenaza aplicada ?  
Sí, dentro del troyano se encuentra un spyware con la finalidad de robar la información presente en la computadora, dando actualización constante al bot. ↑

3	<a href="https://thehackernews.com/2021/04/alert-theres-new-malware-out-there.html">https://thehackernews.com/2021/04/alert-theres-new-malware-out-there.html</a>
---	---

Ingeniería social

<https://www.youtube.com/watch?app=desktop&v= qcW81eke6U>

<https://www.youtube.com/watch?v=dQw4w9WgXcQ>