# Prevención de Ataques

Trabajo para la asignatura de Servidores Web de Altas Prestaciones de la Universidad de Granada.


Participantes:

- Inmaculada Cobo Ariza
- Sandra Ibáñez Rodríguez

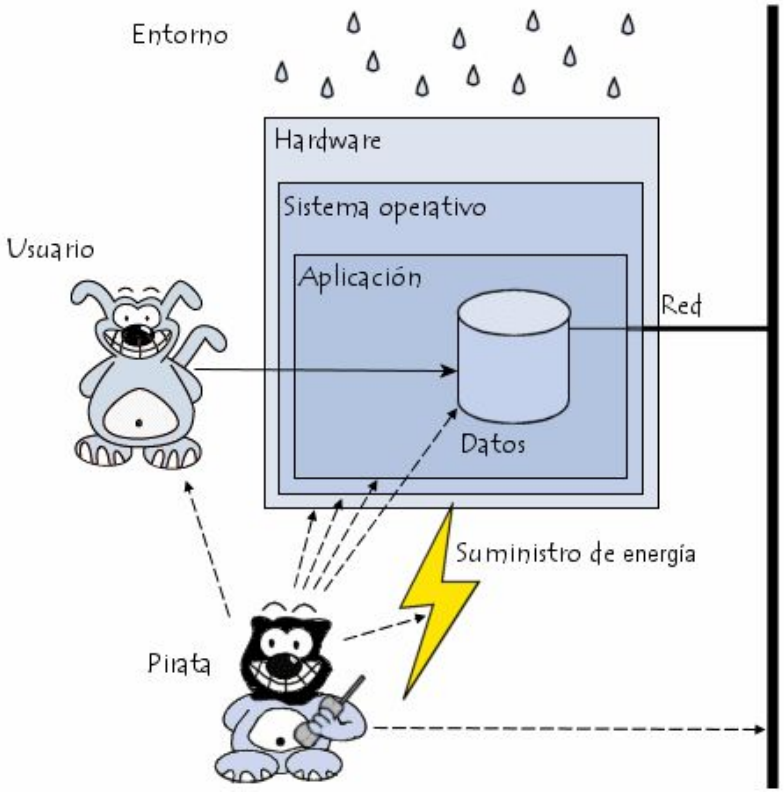
# 1. Introducción

Seguramente todos hayamos escuchado hablar de un ataque informático, además recientemente ha habido uno en grandes dimensiones. Antes de empezar, veamos algunas definiciones previas.

Un **ataque informático** es un intento organizado e intencionado por una o más personas para causar daño o problemas en un sistema informático o red. Su objetivo es tomar el control del sistema, desestabilizarlo o dañarlo y las causas pueden ser desde espionaje hasta para ganar dinero.

Se considera **delito informático** toda aquella actividad criminal, que encuadra en tipos ya conocidos como el robo, el hurto o la falsificación, involucra al medio informático para cometer ese comportamiento delictivo. [4]

Los “piratas informáticos”, que son los encargados de realizar estos ataques, aprovechan las debilidades o los fallos en el software o hardware para entrar en el sistema y causar un efecto negativo en este.




Uno de los aspectos muy importantes es asegurar nuestro sistema. En el tema 6 de la asignatura se ha hablado de la importancia de asegurar un sistema web, pero podemos aplicarlo a cualquier sistema ya que se debe intentar evitar que cualquier hacker malicioso realice cualquier acción que afecte a nuestro sistema.

Si bien las soluciones de seguridad han mejorado notablemente la experiencia del usuario, no existe una aplicación que brinde el 100% de protección frente a la amplia diversidad de problemas potenciales a los que se expone cotidianamente el hacer uso de las tecnologías.

Más adelante, veremos aspectos de seguridad que resultan fundamentales para evitar que los sistemas operativos sufran algún tipo de amenaza.

## Virus

Antes de comenzar, introduciremos la definición de virus y veremos algunos de los más importantes.
Los **virus** son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin el permiso o conocimiento del usuario. Estos, por lo general, infectan otros archivos del sistema con la intención de modificarlos para destruir de manera intencionada archivos o datos almacenados en tu computador.
Como podemos ver en [5], el primer virus informático se llamaba Creeper y consistía en el mensaje “Soy una enredadera…¡atrápame si puedes!” que aparecía en varios ordenadores en el año 1971. Este programa, se replicaba a sí mismo y se difundió por la red.
Veamos algunos de los virus más importantes y la forma de prevenirlos.

1. **Troyanos**: suelen ser los más peligrosos, ya que no hay muchas maneras de eliminarlos. Sin que lo sepamos, los podemos tener instalados en nuestro ordenador y que estén capturando la información que intercambiamos por la red, debido a que tienen un truco que hacen que nuestro sistema operativo los vea como un producto oficial de alguna de las compañías.
   Para evitarlos, es necesario contar con una buena protección de antivirus y analizar nuestro sistema de forma frecuente. Además, es recomendable evitar la descarga de contenidos desde páginas desconocidas o de dudosa reputación.
   En la siguiente imagen se muestra un ejemplo de cómo aparecería un ataque troyano en nuestro sistema.


2. **Worms o gusanos**: como hemos mencionado anteriormente con el virus Creeper, tienen la propiedad de duplicarse a sí mismo. Se ejecutan cuando se inicia el

sistema operativo ya que están registrados en un archivo.exe y ocupan parte de la memoria haciendo que el ordenador se vuelva más lento. Lo normal es que usen medios masivos como el correo electrónico. A diferencia de los troyanos, los gusanos si pueden ser eliminados.
Los métodos de prevención son iguales que los de cualquier virus, entre ellos, mantener el sistema operativo actualizado, disponer de un antivirus, evitar páginas dudosas, evitar instalar aplicaciones ilegales o ejecutar archivos de los que no confiemos, etc.

## 2. Causas de los ataques informáticos

Como ya hemos mencionado anteriormente, las causas pueden ser desde espionaje hasta para ganar dinero. Veamos algunos de los motivos por los que los piratas informáticos deciden atacar sobre algún sistema:

- Para obtener acceso al sistema
- Para robar información, ya sean secretos industriales o propiedad intelectual.
- Para recopilar información personal de algún usuario o de una organización.
- Para obtener información de cuentas bancarias.
- Para afectar al funcionamiento del sistema.
- Para usar los recursos del sistema del usuario, por ejemplo, la red cuando el sistema tiene un ancho de banda considerable.

## 3. Consecuencias de los ataques informáticos

Podemos distinguir entre varios tipos de daños que se presentan en un sistema informático, siendo unos más graves que otros. A continuación, explicaremos brevemente algunos de ellos ordenándolos desde menos a más importante.

- **Daños triviales**: estos virus se pueden remover y eliminar en tan solo unos segundos o minutos.
- **Daños menores**: comunes al virus “Jerusalén”, el cual consiste en borrar, los viernes 13,  todos los programa que se intenten usar después de que el virus haya infectado el sistema. Decimos que son menores porque el problema se solucionaría volviendo a instalar dichos programas.
- **Daños moderados o mayores**: ocurren cuando los piratas consiguen que el virus formatee el disco duro del sistema. Este daño comienza a ser más grave porque puedes perder información. Para resolverlo se tendría que volver a instalar el sistema operativo. En el caso de que podamos recuperar la información diremos que son moderados y en el caso de perderla, diremos que son mayores.
- **Daños severos**: en estos tipos de virus, el usuario no sabe cuando los datos son los correctos o han sido modificados.
- **Datos ilimitados**: en algunos casos, el virus consigue obtener la clave del administrador del sistema y existe una tercera persona que consigue acceder al sistema y hacer lo que quiera.

## 4. Tipos de ataques informáticos.

Antes de describir cómo prevenir los ataques informáticos, conviene explicar un poco qué tipos de ataques informáticos existen, ya que, en algunos casos, para bloquear estos ataques dependiendo del tipo que sean, será necesario usar unas medidas u otras. Podemos realizar una clasificación del siguiente modo:

- **Acceso físico**: para poder realizar este tipo de ataques, el pirata informático debe tener acceso a las instalaciones y a los equipos que quiere atacar. Para realizarlos, puede interrumpir el suministro eléctrico, apagar directamente algún equipo, usar algún USB infectado, robar el disco duro, monitorizar el tráfico de red, etc.
- **Denegaciones del servicio**: el objetivo es interrumpir el funcionamiento normal de un servicio, pueden ser, o por las debilidades del protocolo TCP/IP (protocolo de control de transmisión o protocolo de Internet) o por las vulnerabilidades del software del servidor.
- **Intrusión**: para realizar estos ataques, el atacante puede realizar un análisis de los puertos, realizar un ataque malintencionado (virus, gusanos, troyanos) o aprovechar una vulnerabilidad en una aplicación al enviar una solicitud específica. En estos últimos, a veces consiguen acceder al sistema con derechos de aplicación.
- **Ingeniería social**: en algunas ocasiones, el propio usuario, ya sea por ignorancia o a causa de un engaño, genera una vulnerabilidad en el sistema brindando información al pirata informático.
- **Puertas trampa**: en algunos programas, su diseñador deja puertas traseras ocultas que le dejan acceso en todo momento a dicho programa.

### Ataques de tipo lógico

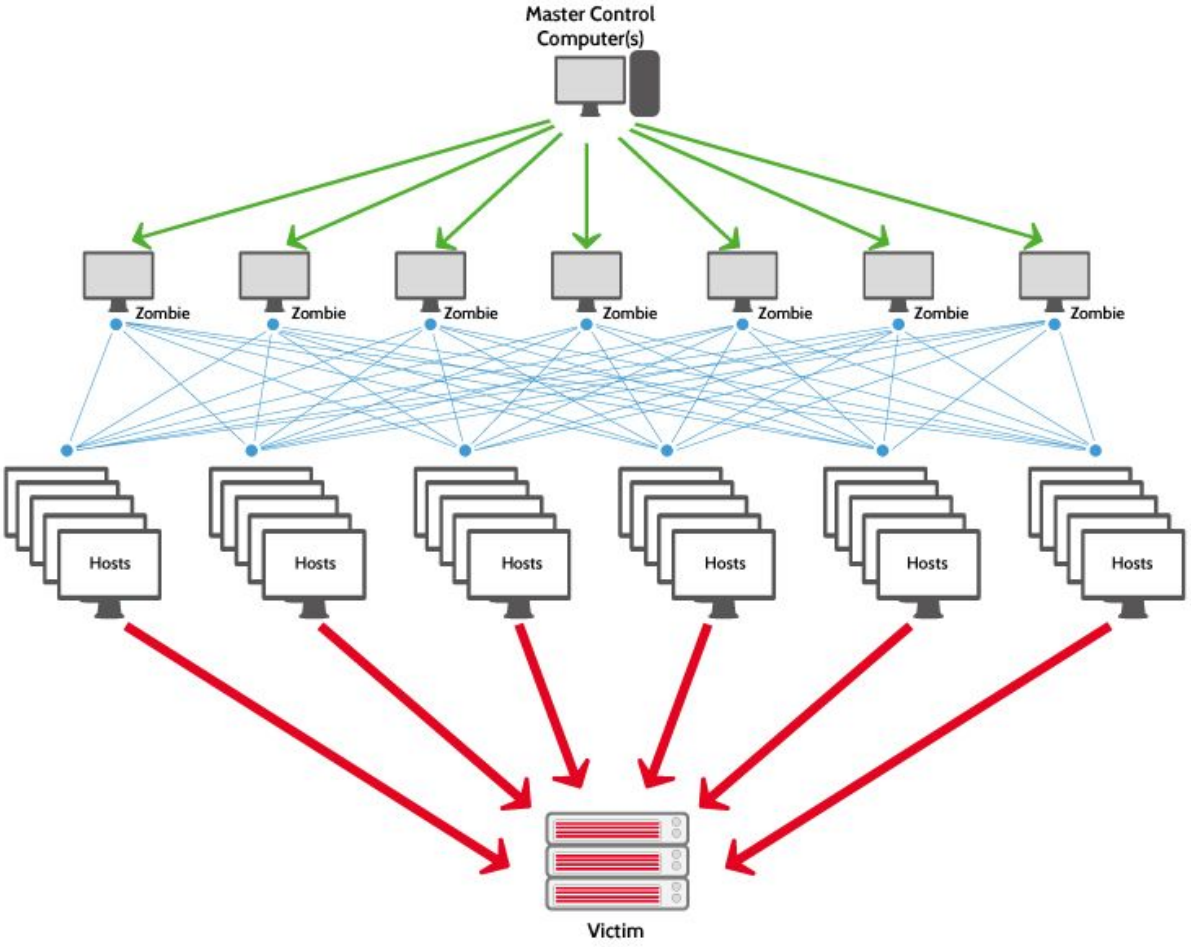
Si nos centramos en los ataques de tipo lógico podemos distinguir entre los siguientes:

- **Trashing o cartoneo**: consiste en recolectar información a partir de material descartado, con la finalidad de obtener datos que sirvan como información para cometer fraudes. Puede ser de dos tipos, el trashing físico consiste en recolectar información de papeles, diskettes o discos compactos. El trashing lógico consiste en recolectar información de la computadora, ya sea en la papelera de reciclaje, en el historial de navegación o en los archivos que se almacenan en las cookies. Puede parecer una tontería, pero el hecho de apuntar el usuario y contraseña en un papel y después arrojarlo a la basura, puede resultar una oportunidad para el atacante para poder entrar al sistema. [3]
- **Monitorización**: este tipo de ataque se realiza para observar a la víctima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceder a su sistema.
- **Ataques de autenticación**: en estos tipos de ataques se intenta engañar al sistema de la víctima para poder entrar.
- **Modificación**: se puede dar como tampering o data diddling (modificación desautorizada de los datos o el software instalado en el sistema de la víctima) o borrado de huellas.

## Ataques más comunes

A continuación se muestran los tipos de ataques más comunes o importantes.

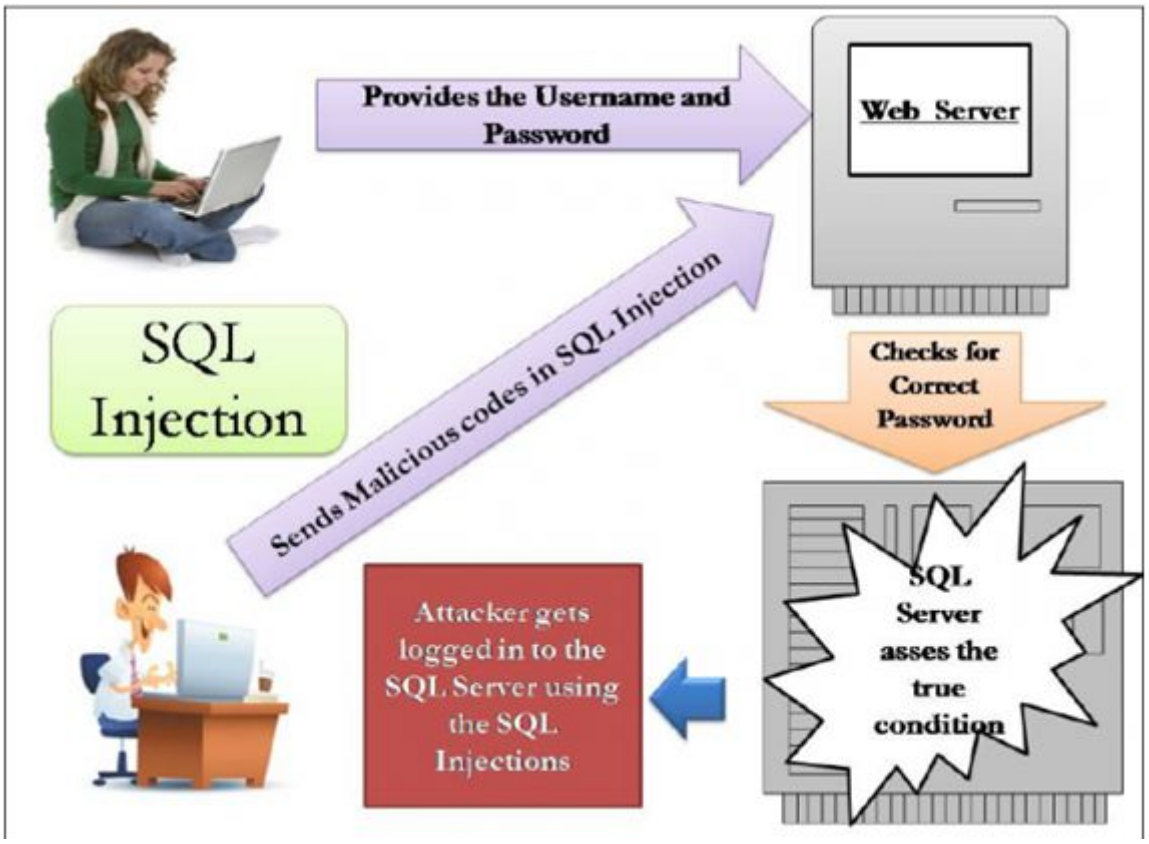
- **Denial of Service (DoS)**:  la Denegación de Servicio (DoS) o Denegación de Servicio Distribuida (DDoS), es un ataque a un sistema de computadoras o red que causa con un servicio o recurso sea inaccesible a los usuarios. Normalmente provoca la pérdida de la conectividad con la red. Estos ataques se generan mediante la saturación de los puertos con muchos flujos de información, provocando la sobrecarga y que, éstos, no puedan seguir prestando su servicio.
  El DDoS es una ampliación de este ataque ya que lo que logra es generar un gran flujo de información desde varios puntos de conexión. El proceso es el siguiente, un hacker instala un agente o demonio en numerosos host. El hacker envía un comando al maestro, el cual reside en cualquiera de los host infectados. Por último, el maestro se comunica con los agentes que residen en otros servidores para comenzar el ataque.




- **Ataque de Fuerza Bruta**: en criptografía se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso. En el caso de que se quiera averiguar una contraseña, se probarían todas las combinaciones posibles hasta conseguir la correcta. Es una de las técnicas más habituales de robo de contraseñas en Internet

puesto que no se necesitan grandes conocimientos en seguridad informática. Además, existen programas que realizan este trabajo de forma automática, por ello, algunas páginas web tienen los llamados captchas, como vemos en la siguiente imagen, que intentan detectar si es una persona humana o un software informático.

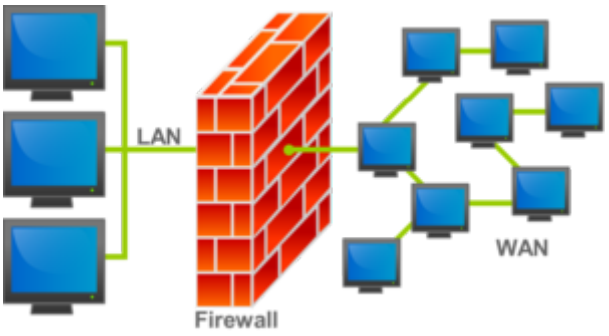

- **SQL Inyection**: es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos. Uno de los principales problemas de este ataque es que, además de obtener información de la base de datos, tal como contraseñas o usuarios, también puede eliminarla y dejarla inservible.
  Este tipo de intrusión normalmente es de carácter malicioso, dañino o espía, por tanto, es un problema de seguridad informática que debe tener en cuenta el programador para prevenirlo.




## 5. Cómo prevenir los ataques

Como ya hemos visto, existen numerosas formas de atacar algún sistema informático y cabe destacar que el peligro es mayor de lo que la gente cree. Veamos algunas recomendaciones, tanto físicas como lógicas, para mantener el sistema seguro.

- Actualizar regularmente el sistema operativo y el software instalado en su equipo, poniendo especial atención en las actualizaciones del navegador web. Como ya hemos visto, cualquier fallo en nuestro sistema, será una oportunidad para un pirata informático para entrar y producir un ataque.
- Instalar un antivirus y analizar con este tanto el sistema, como los dispositivos de almacenamiento de datos tales como USBs o discos duros externos. También es recomendable analizar los archivos nuevos, sobretodo los descargados de internet.
- Instalar un Firewall o Cortafuegos con el fin de restringir accesos no autorizados de Internet. Un Firewall o Cortafuegos es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado. En la siguiente imagen vemos un esquema de donde se localizaría el cortafuegos en una red de ordenadores.




- También es recomendable tener instalado algún tipo de software anti-spyware, para evitar que se introduzcan programas espías destinados a recopilar información del usuario.
- Si queremos mantener segura una empresa por ejemplo, no es recomendable dejar las estaciones de trabajo sin vigilancia durante largos periodo de tiempo y es recomendable restringir el acceso a estas zonas en las que estén los sistemas informáticos.
- Guardar copias de seguridad de toda la información en una zona segura, limitando también el acceso a esta zona.
- Colocar los cables de las redes dentro de las paredes o bajo suelos y techos para que no se pueda acceder a ellos de una forma fácil para dañarlos.
- La vigilancia es otro mecanismo de seguridad con lo que se pueden utilizar guardias de seguridad para controlar el acceso a un recinto o emplear alarmas en caso de riesgo.
- Acceso controlado mediante claves únicas, lector de huella digital y/o de córnea, cámaras de vigilancia, etc.
- Asegurarse de poner el centro de cómputo en un lugar no muy alto ni tan bajo debido a los riesgos que corren los equipos ya sea en caso de inundaciones, incendios, terremotos, etc. En el caso de incendio es bueno tener el gas que consigue dejar la sala sin oxígeno para que el incendio no se propague.
- La limpieza también mantiene protegidos a los equipos, ya que el polvo puede provocar tanto daños físicos como lógicos en los equipos.

Podemos centrarnos también en la forma de navegar por internet y en la utilización de correo electrónico. La recomendaciones son las siguientes:

- Utilizar contraseñas seguras, compuestas por mínimo ocho caracteres, combinando números, letras y símbolos y distinguiendo entre mayúsculas y minúsculas. Es conveniente modificar las contraseñas con frecuencia, en especial si se usan equipos públicos en lugar de privados.
- Es recomendable navegar siempre por páginas web seguras, en especial si se van a realizar compras online o se va a facilitar información confidencial. Para reconocer las páginas web seguras, estas deben empezar con https:// en lugar de http://. Además en la barra de navegación debe aparecer un icono de un candado cerrado, el cual indica que la página tiene un certificado digital que confirma la autenticidad de la página.
- Hay que ser cuidadoso al usar programas de acceso remoto. Estos programas suponen una gran ventaja ya que puedes acceder a otro ordenador aunque esté situado a kilómetros de distancia pero esto puede poner en peligro la seguridad del sistema.
- Bloquear direcciones web maliciosas, por ejemplo, existen casos de descarga de música, programas o películas que terminan siendo malware.
- No clicar en enlaces que resulten sospechosos. Se debe ser precavido antes de seguir un enlace al navegador, en el correo, en la mensajería instantánea o en una red social. Los mensajes falsos que acompañan pueden ser muy convincentes con el fin de captar la atención del usuario y redirigir a páginas maliciosas.
- Hay que prestar especial atención a lo que se descarga de un navegador ya que algunos antivirus no pueden combatir todas las amenazas.

Como ya hemos mencionado anteriormente, el correo electrónico y la mensajería instantánea es una de las herramientas más utilizadas para llevar a cabo estafas o atacar con algún virus. Es primordial prevenir potenciales infecciones a través de estos medios empleando buenas prácticas que permitan controlar de manera eficaz las necesidades de seguridad. Por lo que es recomendable:

- No abrir mensajes de remitentes desconocidos. A veces, simplemente con abrir el mensaje, nos infectan con algún tipo de virus.
- Desconfiar de correos en los que entidades bancarias o sitios de venta online, solicitan contraseñas o información confidencial.
- No difundir mensajes de correo con contenido dudoso y que piden ser reenviados a todos los contactos ya que estos pretenden captar direcciones de correo de usuarios a los que después se les enviarán mensajes con virus. Estas cadenas de mensajes han dejado de ser tan famosas como antes, ya que no se utiliza tanto el correo electrónico.
- Tener un software anti-spam para detectar el correo basura.

Si nos centramos en los ataques anteriormente mencionados, las formas de prevenirlos son las siguientes:

- Para protegernos de un ataque DoS o DDoS, es primordial tener los antivirus actualizados y monitorizar la actividad anómala dentro de nuestra red. Además de las prevenciones lógicas y físicas anteriormente comentadas.
- Para protegernos de un ataque de fuerza bruta es imprescindible establecer políticas de contraseñas que sean lo suficientemente estrictas. Es importante también

establecer medidas de seguridad que puedan ayudar a evitar cualquier posible intento de ataque usando, por ejemplo, bloqueo por IP o captchas.

- Para evitar ataques de SQL Injection lo principal es no confiar en la entrada del usuario.

# 6. Algunos ejemplos importantes

## Ataques recientes

### WannaCry

En primer lugar, vamos a explicar un poco el reciente ataque informático “ransomware” llamado “WannaCry”. Este ataque es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de quitar esa restricción.
Como podemos ver en [11], este ataque se produjo el 12 de mayo de 2017 y afectó a grandes empresas españolas, entre ellas Telefónica, Iberdrola y Gas natural, además de afectar a otros países, convirtiéndose en un ataque de escala mundial. Según los últimos datos, ha habido más de 300.000 máquinas afectadas en 150 países. En la siguiente imagen se muestran los países afectados por él.

Los computadores afectados han sido los que no habían aplicado las últimas actualizaciones de seguridad en los ordenadores del sistema operativo Windows. Estos tenían sus archivos codificados y les aparecía un mensaje en pantalla que exigía un rescate de 300 dólares en bitcoins a cambio de descodificar los archivos.

### EternalRock

Al igual que el anterior, es un ataque de tipo ransomware pero mucho más potente y difícil de detectar. Este ataque consigue entrar en los equipos, espiarlos y esparcirse por ellos. La principal diferencia con WannaCry es que este avisaba de la infección a los usuarios mientras que, EternalRock permanece oculto e inactivo en un primer momento.

### Subtítulos maliciosos

Es un software malicioso camuflado en los subtítulos. Entramos a nuestra plataforma de streaming, reproducimos una película y elegimos los subtítulos. Esta acción puede llegar a afectarnos ya que se ha descubierto una vulnerabilidad en estas plataformas populares como VLC, Kodi, Popcorn-Time o Stremio. Este ataque toma el control total de nuestro dispositivo, teniendo acceso a toda nuestra información y pudiendo instalar más software malicioso.

## Ataques importantes en la historia

### Creeper

Como ya hemos mencionado anteriormente, se trata del primer virus de la historia. El principal objetivo de este virus no era causar daño sino comprobar si se podía crear un programa que se moviera entre ordenadores. El virus mostraba un mensaje como el que se muestra en la siguiente imagen.


### Melissa

Este virus fue el primero que se transmitió vía correo electrónico en 1999. No fue demasiado destructivo pero logró propagarse y contagiar a millones de usuarios. De hecho, compañías como Microsoft, Intel o Lucent Technologies tuvieron que bloquear sus conexiones a Internet, cerrando temporalmente sus servidores de correo electrónico ya que el virus estaba obstruyendo el sistema.

### I love you

Una tesis de un joven de 24 años fue rechazada por la universidad ya que resultaba ser un virus capaz de infectar a más de 45 millones de computadores. El programa enviaba un correo electrónico que en su asunto mostraba las palabras “I love you” (te amo) y estaba

acompañado de un archivo adjunto bautizado “Una carta de amor para ti”. Al ejecutarse, el virus se enviaba a toda la lista de contactos del usuario.

### Slammer

Es un gusano informático que provocó una Denegación de servicio en algunos servidores de Internet e hizo dramáticamente más lento el tráfico de Internet en general. Se extendió rápidamente, infectando a la mayoría de sus 75.000 víctimas en diez minutos. Este ataque, no utilizó el lenguaje SQL, se aprovechó de un error de desbordamiento de buffer en los productos de motor de base de datos de Microsoft SQL Server.

### Virus CIH o Chernobyl:

En su momento fue considerado uno de los virus más peligrosos y destructivos, capaz de eliminar información crítica del usuario e incluso sobrescribir el sistema BIOS, impidiendo el arranque del equipo.

## 7. Conclusión

Como hemos podido comprobar a lo largo de este documento, la seguridad informática es una necesidad, no solo porque los virus y otros tipos de malware puedan resultar molestos, sino porque además pueden provocar graves daños y serias pérdidas a las empresas y a los usuarios.
La seguridad informática tiene como principal objetivo la conservación de la integridad de la información y el equipo en sí. Otra cuestión muy importante es el valor de la información en sí, los datos como las cuentas bancarias, fotos o gustos, deben ser protegidos ya que cabe la posibilidad de que alguien haga un mal uso de ello.

## Referencias.


[1] https://es.wikipedia.org/wiki/Ataque_inform%C3%A1tico
[2] http://es.ccm.net/contents/17-introduccion-a-los-ataques
[3] http://www.seguridadinformatica.unlu.edu.ar/?q=taxonomy/term/23
[4] http://www.confirmasistemas.es/es/contenidos/canal-basics/que-es-el-trashing
[5] https://www.xataka.com/historia-tecnologica/la-historia-de-creeper-el-primer-virus-informatico-jamas-programado
[6] https://rootear.com/windows/gusano-informatico-windows
[7] http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack
[8] http://www.tutorialesonline.info/seguridad-informatica-que-es-un-ataque-de-fuerza-bruta/
[9] https://es.wikipedia.org/wiki/Inyecci%C3%B3n_SQL
[10] http://seguridadinformatica-umex.blogspot.com.es/p/objetivo-este-blog-estacreado-con-la_29.html
[11] https://es.wikipedia.org/wiki/WannaCry
[12] https://www.xataka.com/seguridad/mas-potente-que-wannacry-y-sin-avisar-asi-es-eternalrock-un-nuevo-malware-que-usa-aun-mas-exploits-de-la-nsa
[13] http://www.enter.co/chips-bits/seguridad/los-10-virus-mas-famosos-de-la-historia-disi-2010/