



Seguridad Informática en el sector Salud

¡Porque la seguridad es de todos!

Ataques por Malware

Los ataques por *malware* se sirven de programas maliciosos cuya funcionalidad **consiste en llevar a cabo acciones dañinas en un sistema informático y contra nuestra privacidad**. Generalmente, buscan robar información, causar daños en el equipo, obtener un beneficio económico a nuestra costa o tomar el control de su equipo.

Dependiendo del *modus operandi*, y de la forma de infección, existen distintas categorías de *malware*. **Las medidas de protección**, por el contrario, **son muy similares para todos ellos**.

Virus

Los virus se encuentran dentro de la categoría de *malware* y **están diseñados para copiarse a sí mismos y propagarse a tantos dispositivos como les sea posible**.



¿Cómo se propaga o infecta? Proliferan infectando aplicaciones, a través del correo electrónico u otros servicios web, y pueden transmitirse por medio de dispositivos extraíbles, como memorias USB o archivos adjuntos, incluso a través de conexiones de red.

¿Cuál es su objetivo? Pueden llegar a modificar o eliminar los archivos almacenados en el equipo. Son capaces de dañar un sistema, eliminando o corrompiendo datos esenciales para su correcto funcionamiento.

Adware

Se trata de un **software malicioso** diseñado **para mostrarnos anuncios no deseados de forma masiva**.



Spyware

Este *malware* **se instala en nuestros equipos y comienza a recopilar información, supervisando toda su actividad para luego compartirla con un usuario remoto**. También es capaz de descargar otros *malware* e instalarlos en el equipo.



¿Cómo se propaga o infecta? Al navegar por páginas webs no seguras, pueden aparecer mensajes en forma de anuncios o *pop-ups* que, al hacer clic, descarguen este tipo de *malware*. También es común que se ejecuten como programas adicionales durante la instalación de un *software*.

¿Cuál es su objetivo? Una vez que el *malware* logra instalarse, puede llevar a cabo numerosas acciones, como controlar el dispositivo de forma remota, realizar capturas del contenido de aplicaciones y servicios como el correo electrónico o redes sociales.

Troyanos

Suelen camuflarse como un software legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.





Seguridad Informática en el sector Salud

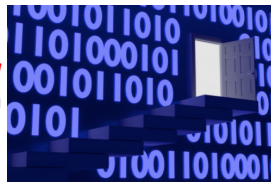
¡Porque la seguridad es de todos!

¿Cómo se propaga o infecta? Se propagan por medio de archivos adjuntos en correos electrónicos o desde páginas webs poco fiables, escondiéndose tras descargas de juegos, películas o aplicaciones no legítimas.

¿Cuál es su objetivo? La mayoría de los troyanos tienen como objetivo controlar nuestro equipo, robar los datos, introducir más *software* malicioso en el equipo y propagarse a otros dispositivos.

Backdoors

Es un troyano que **abre una puerta trasera** en el sistema de tu computadora y permite que un hacker remoto tome el control de tu equipo sin que lo sepas



¿Cómo se propaga o infecta? Por lo general se propagan por medio de archivos adjuntos en correos electrónicos o desde páginas webs poco fiables, escondiéndose tras descargas de juegos, películas o aplicaciones no legítimas.

¿Cuál es su objetivo? Su objetivo es conseguir crear una puerta trasera en nuestro sistema con la que controlar el equipo poco a poco y, finalmente, robar información.

Ransomware

Tipo de *malware* que **consigue tomar el control del dispositivo para cifrar el acceso al mismo y la información**. Para recuperar el control y toda la información, nos exigirá el pago de un rescate.



¿Cómo se propaga o infecta? se propagan por medio de archivos adjuntos en correos electrónicos o desde páginas webs poco fiables, escondiéndose tras descargas de juegos, películas o aplicaciones no legítimas.

¿Cuál es su objetivo? Cuando el *malware* se ejecuta, se van cifrando todos los archivos y carpetas del dispositivo, impidiendo el acceso a ellos sin una clave. Una vez completada su tarea, el atacante nos envía otro correo con las instrucciones para el pago y el posterior envío de la clave para descifrar el equipo.

Fuente: *INCIBE y la Oficina de Seguridad del Internauta (OSI).*

Te invitamos a tomar las siguientes medidas preventivas:

- **NO abrir archivos adjuntos** ni abrir enlaces que provengan de correos de destinatarios desconocidos, que alerten sobre cobros jurídicos, demandas o similares y en caso de recibirlo, se debe reportar de inmediato al correo de Seguridad de tu institución o al área de informática, adjuntando el correo sospechoso.
- No descargue contenido multimedia por redes de intercambio tales como Ares.
- Apagar el equipo de cómputo cuando termine su jornada laboral, no solo previene que sea blanco de un ataque, sino que mejora el rendimiento, ahorra energía y previene el desgaste innecesario de este.
- Evitar ingresar a páginas de orígenes desconocidos.

Comité editorial

Claudia Gallego – Clínica Antioquia
Clemencia Mejía – Clínica Medellín Grupo Quirón Salud
Dany Ospina – Clínica el Rosario
Tatiana Flórez – Organización VID

