# Part 1

*Ciberseguridad es una de las ramas de software por las que estuve a punto de orientar mi carrera, es algo que lo tengo en mi día a día constante, asi como debates con diferentes amigos que trabajan en el sector, algunos con unos futuros brillantes.*

## ¿Qué es un ransomware?

Un ransomware es un tipo de software malicioso cuyo objetivo es bloquear el acceso al contenido/datos de la víctima a través de un proceso de codificación.

Sus objetivos principales suelen ser, tras la codificación de estos datos, proceder a la extorsión de la víctima pidiendo cantidades de dinero (generalmente en formato de cryptomoneda para evitar el rastreo) a cambio de la decodificación de sus datos.

Un ejemplo reciente es el caso del hospital de Barcelona que sufrió este ataque y tubo que ceder a un chantaje de 4millones de euros en bitcoin

<https://www.xataka.com/seguridad/hospital-clinic-barcelona-esta-cuerdas-ataque-ransomware-negociacion-rescate-nada>

## ¿Por qué son tan problemáticos?

Uno de los mayores problemas que tenemos a dia de hoy, no solo con los ransomware si no con cualquier tipo de virus es que la gran mayoría de antivirus que usamos son prácticamente inútiles contra un ataque planificado y dirigido. Ya que a no ser que trabajes con Antivirus en tiempo de ejecución o de comportamiento (software que tiene a ser tanto caro monetariamente como de uso de recursos) es extremadamente fácil colar este tipo de virus a los antivirus convencionales (que funcionan a nivel de disco) como McAffe, Windows Defender…

Si a esta problemática le sumas la facilidad de extorsión bajo este tipo de ataques y las grandes pérdidas que suponen para los negocios afectados consigues una receta para el desastre, más aún ahora que es tan complicado rastrear cierto tipo de currencies.

# Parte 2

## ¿Presentan problemas o riegos para los datos personales?

La respuesta corta es sí.

Los ransomwares representan un riesgo para los datos personales.

Aunque su función principal es codificar los datos, impidiendo el acceso a la entidad propietaria hasta que se pague un rescate, a menudo se acompañan de la extracción y robo de datos. Estos datos robados pueden venderse en la dark web o a diferentes empresas, y también pueden utilizarse para realizar chantajes en el futuro. Por lo tanto, el ransomware no solo bloquea el acceso a los datos, sino que también pone en peligro la privacidad y la seguridad de la información personal.

En el caso de las noticias mencionadas, ambas destacan la vulnerabilidad de sistemas críticos como el PYMEs y los sitemas críticos (como el ejemplo del hospital de Barcelona) ante ciberataques con ransomware ya que pueden desde interrumpir operaciones hasta exponer datos personales con altos riesgos que afectan a la seguridad y privacidad de las personas involucradas