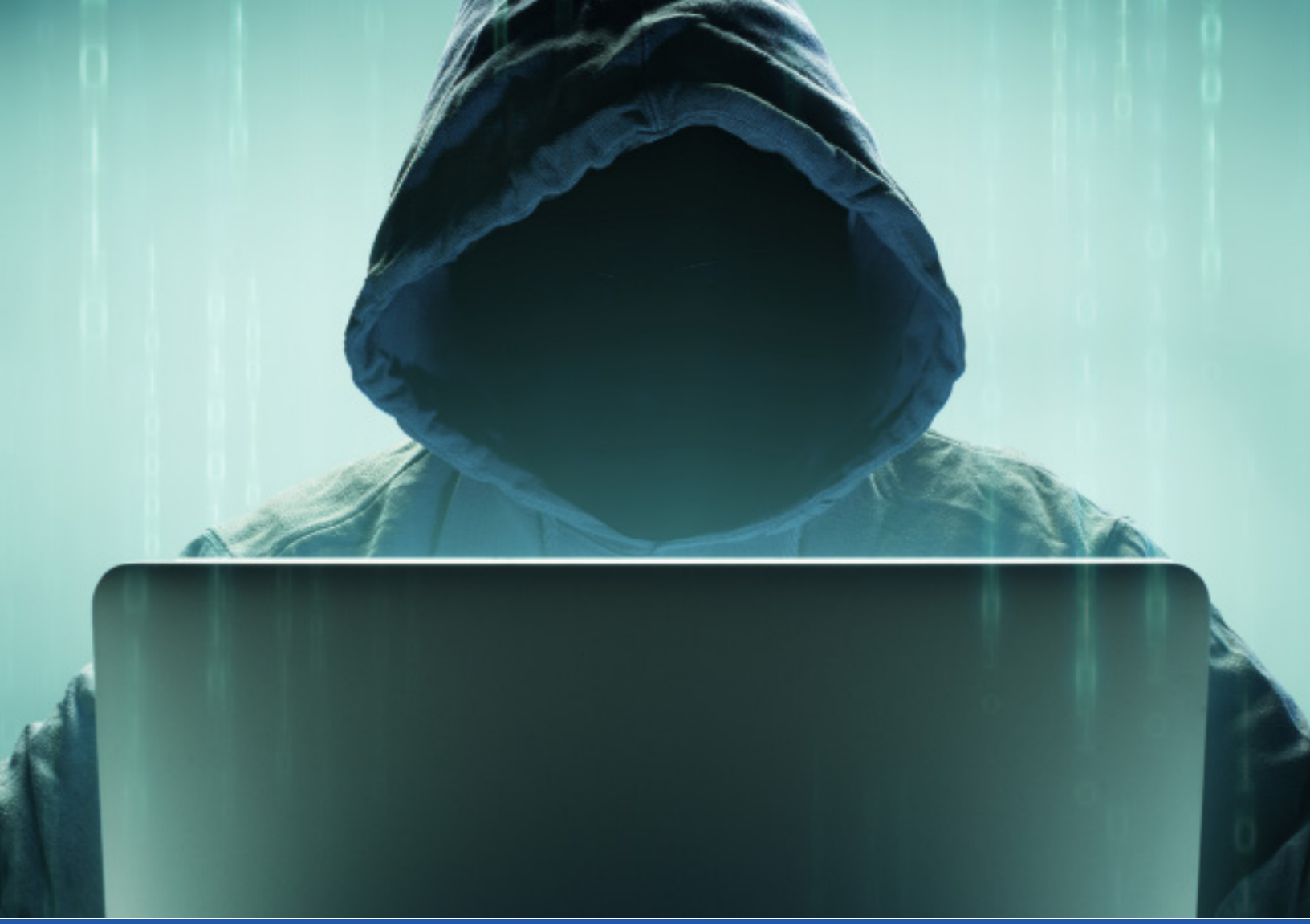


Consejos para la prevención del ransomware

Ontrack®

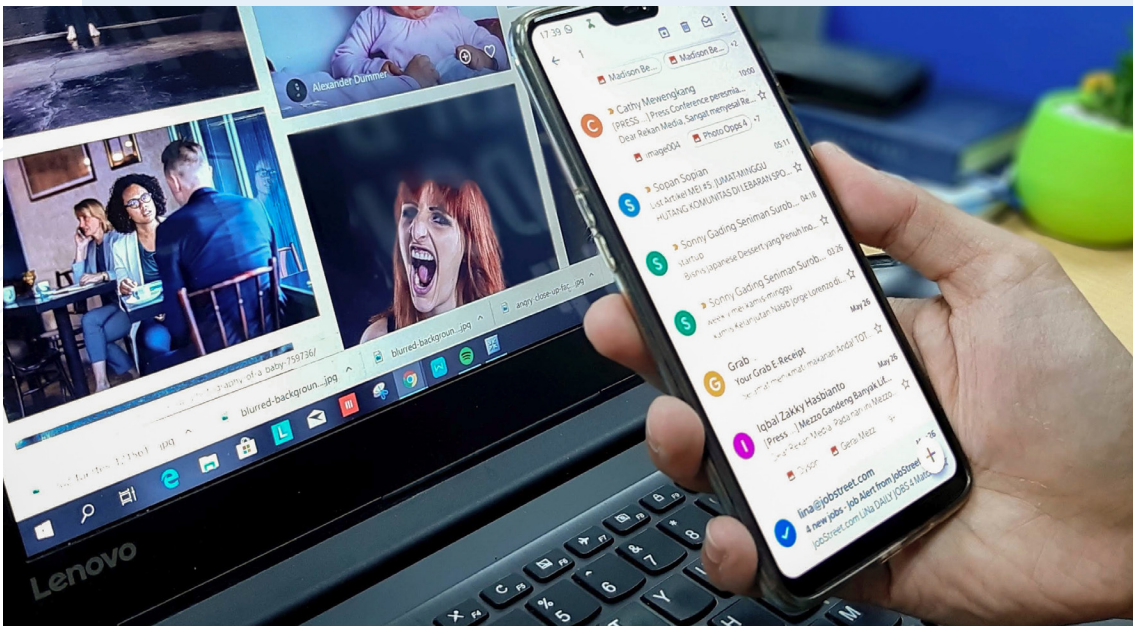
1. La seguridad del correo electrónico es fundamental

Según McAfee, el correo electrónico de **suplantación de identidad** continúa siendo una de las principales formas de acceso de los virus de ransomware, especialmente en los casos de ataques orientados. Por lo tanto, resultará esencial para todo aquel que administra una red o se conecta a Internet proteger esta vía primaria de vulnerabilidades.

La mayor parte de los usuarios inician un ataque de ransomware al abrir lo que parece un correo electrónico normal y que en realidad alberga el virus dentro de un documento, una foto, un video u otro tipo de archivo. La mayor parte de los hackers actuales **no necesitan de muchos conocimientos** para insertar un malware en un archivo. Existen numerosos artículos y tutoriales de YouTube con instrucciones paso a paso para hacerlo.

Teniendo siempre presente esto, siempre debes **evitar abrir un correo electrónico de un remitente desconocido**. Si recibes un correo electrónico de origen desconocido, informa de esta situación al equipo de IT o de asesores de seguridad de tu compañía inmediatamente.

Recuerda: Siempre será la decisión correcta mantener seguros los datos y sistemas de IT de tu compañía.



Ontrack®

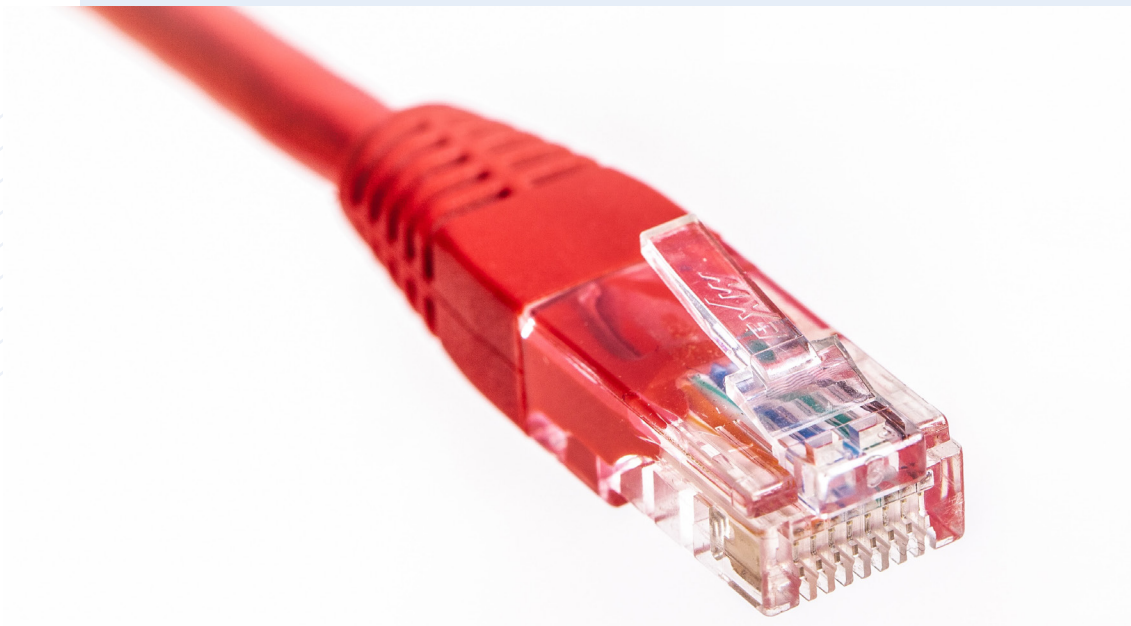
2. Protege tu red y tu entorno de IT

Sin dudas, la infección por ransomware de una computadora es un problema serio. Pero si se propaga a toda la red, no solamente puede transformarse en una pesadilla para el departamento de IT, sino que puede poner en peligro a toda la compañía.

Las compañías que no lo hayan hecho ya, deberían evaluar la implementación de un **software de seguridad de datos** que examine todos los correos electrónicos ingresantes antes de que los reciba el destinatario.

Dicha solución reducirá dramáticamente las probabilidades de que un virus se extienda por dentro de la red de la compañía. Además, los administradores y gestionadores de IT deben evaluar la implementación de un software de seguridad de red que monitoree automáticamente la red y sus archivos en búsqueda de amenazas. La solución también debe alertar a los administradores, si detecta que un ataque de ransomware está intentando cifrar grandes cantidades de archivos en la red.

Por último, aunque no menos importante: Siempre **actualiza tu software y sistemas operativos** con los parches más recientes, en cuanto estén disponibles. Como mencionamos repetidamente, los hackers solamente pueden alcanzar el éxito en sus ataques cuando las políticas de seguridad de datos de la víctima ofrecen vulnerabilidades.



3. Capacitación de los empleados

Incluso los usuarios de computadora más experimentados entran en pánico cuando se dan cuenta de que se enfrentan a un ataque de ransomware. Por lo tanto, resulta importante que **todos los empleados de una compañía sepan exactamente qué hacer** asi ocurre un ataque de ransomware, incluso los directores de IT y los ejecutivos de alto nivel.

Los protocolos para actuar ante un ataque de ransomware deben no solamente ser parte del plan de continuidad de negocios de los expertos de IT o los puestos superiores, sino que en todas las oficinas deben ser visibles y comprensibles las recomendaciones precisas de qué hacer si ocurre una infección. Las mismas pueden ser simples, pero efectivas, como las siguientes:

- Desconecta las computadoras de Internet y de la red interna.
- Intenta apagar el dispositivo de manera adecuada o llama inmediatamente al departamento de IT/ seguridad de IT.

El personal de administración y de seguridad de IT debe informarse de forma continua con respecto a los más recientes desarrollos del ciberdelito y la ciberseguridad.

Por lo tanto, debería ser una necesidad imperiosa para estos empleados capacitarse y actualizarse continuamente con respecto a las últimas novedades y los más recientes desarrollos en ese espacio y estar al tanto de los puntos débiles de las redes o las soluciones de software.

Ontrack®

4. Protege el Protocolo de Escritorio Remoto (RDP) de tu organización

Si tu organización no necesita utilizar un RDP, es conveniente reemplazarlo con una solución más segura. Si esto no es posible, entonces deben implementarse las siguientes **medidas**:

- Utiliza una VPN para acceder al RDP de tu organización, ya que esto crea una conexión segura entre los empleados de la organización y la Internet. Todo el tráfico de datos se envía a través de un túnel virtual cifrado, lo que debería evitar que los cibercriminales puedan acceder al sistema por fuerza bruta.
- Asegúrate de contar con una autenticación de dos factores.
- Aquellos empleados que trabajen en servicios internos importantes deben contar con el máximo acceso requerido para poder desempeñar su tarea. Cualquier empleado que acceda a respaldos o sistemas críticos debe implementar una autenticación de dos factores.
- Implementa un plan de recuperación ante desastres, que esté actualizado, para asegurarte de contar con una copia de respaldo de todos tus datos críticos en caso de que se vea afectado tu RDP.

Ontrack®

5. Asegúrate de contar con una copia de respaldo actualizada

Protegerse también significa contar con una copia de respaldo de los datos. Una copia de respaldo altamente segura resulta un elemento crucial dentro de la preparación para enfrentar un ataque por ransomware. Debes probar tu copia de respaldo exhaustivamente de forma frecuente y, lo que es más importante, la restauración de los datos debe resultar fácil.

Esto significa que si te atacan con cualquier forma de malware, podrás **reconstruir tu sistema** rápida y efectivamente. De ser posible, asegúrate de que tu sistema de respaldo no esté conectado a tu red (o que solamente esté conectado el tiempo estrictamente necesario), lo que evitará que tu respaldo también se vea afectado por el malware.

Implementa un plan de recuperación y respaldo para todos los datos críticos, utilizando la estrategia 3-2-1:
3 - Mantener un mínimo de tres copias de los datos.
2 - Almacenar los datos en dos tipos de dispositivos distintos.
1 - Mantener protegida una copia de los respaldos fuera de las instalaciones.

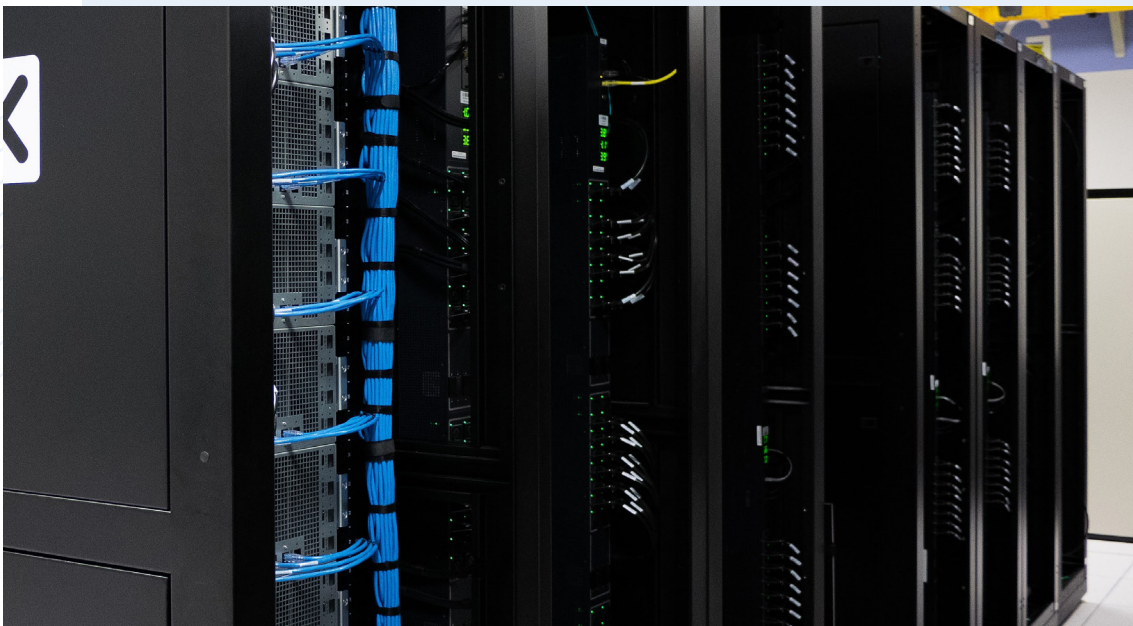
Prueba las copias de respaldo de forma regular para garantizar una adecuada configuración, lo que atenuará el impacto de una filtración de datos y acelerará el proceso de recuperación.

Desconecta los respaldos críticos de la red (brecha de aire) para lograr una protección máxima.

Implementa sistemas de archivos con copia al escribir (NetApp WAFL – Linux ZFS) o características WORM en sistemas o dispositivos NAS.

Aplica los parches a los sistemas operativos, software de respaldo, seguridad y antivirus críticos tan pronto como sea posible.

Implementa una continua capacitación en ciberseguridad para usuarios y administradores, a fines de identificar correos de suplantación de identidad.



Ontrack®

¿Qué hacer si sufres una infección por ransomware?

Si por una u otra razón el ransomware supera tus defensas, debes hacer lo siguiente:

- **¡Nunca pagues el rescate!**
  Pagarle los criminales no garantiza que recuperarás tus datos. En muchos casos (y definitivamente si es un *ranscam* o un *wiper*) no recuperarás tus datos, ¡lo que te dejará sin datos y con mucho menos dinero!
- **No intentes descifrar los datos tú mismo.**
  Algunos especialistas en computación pueden ser capaces de recuperar datos perdidos, pero esto es riesgoso. Si algo sale mal, puedes destruir tus datos para siempre.
- **¡Prueba tu copia de respaldo!**
  Aún en caso de perder la copia de respaldo luego de un ataque de ransomware, no hay que descartar nunca la posibilidad de la recuperación. Las soluciones posibles dependen del tipo de sistema de almacenamiento o dispositivo y del tipo de ransomware.

Ontrack®
C. Anabel Segura 7 - 1ª Planta,
Oficina B, 28108 Alcobendas, Madrid
24/7 900 112 012
www.ontrack.com/es