

Guía para evitar infecciones de ***RANSOMWARE***

Versión 1.1

Septiembre 2018

Este trabajo está licenciado bajo

[Licencia Reconocimiento-Compartir Igual 4.0 España \(CC BY-SA 4.0 ES\)](https://creativecommons.org/licenses/by-sa/4.0/es/)



Contenido

Información de la Guía.....	4
Licenciamiento	4
Colaboradores	4
Resumen Ejecutivo	4
Introducción	6
El negocio del <i>ransomware</i>	11
Un negocio como cualquier otro	11
Mercado e innovación	11
Grado de madurez.....	13
Cómo evitar infectarse	14
1. Hacer backup periódico de la información.....	14
2. Concientizar y entrenar a los usuarios	15
3. Aplicar un modelo de mínimo privilegio	16
4. Segmentar la Red.....	17
5. Revisar recursos compartidos y unidades externas	18
6. Utilizar soluciones antivirus	19
7. Utilizar antispam, firewall y filtro de contenido	20
Filtrado a nivel de firewall	20
Filtrado web (proxy)	21
Filtrado de nodos TOR	21
Filtrado de correos	22
8. Mostrar las extensiones de los archivos	23
9. Filtrar archivos con extensiones peligrosas	24
10. Inventariar y controlar aplicaciones	25
11. Instalar actualizaciones del sistema operativo y aplicaciones.....	26
12. Deshabilitar ejecución de archivos temporales.....	27
13. Deshabilitar escritorio remoto	29
14. Restaurar el sistema	30

15.	Desactivar las macros y ActiveX en las herramientas de ofimática	31
16.	Deshabilitar servicios de scripting y consolas	32
17.	Bloquear publicidad y ventanas emergentes	33
18.	Desactivar Autorun/Autoplay	34
19.	Apagar conexiones inalámbricas	35
20.	Instalar herramientas de terceros.....	36
	¿Cómo funcionan?.....	36
21.	Proteger el MBR	38
22.	Aislar el equipo infectado	39
23.	Deshabilitar o eliminar protocolos obsoletos	40
24.	Gestionar sistemas operativos obsoletos.....	41
	Recuperación de archivos cifrados.....	42
	Proceso de pago	44
	Aspectos legales	46
	Responsabilidad Penal	46
	Responsabilidad Civil	49
	Conclusión	53

Información de la Guía

Licenciamiento

La **Guía para evitar infecciones de RANSOMWARE** es de uso gratuito.

Esta Guía llega a usted bajo [Licencia Reconocimiento-Compartir Igual 4.0 España \(CC BY-SA 4.0 ES\)](#), así que puede copiar, distribuir y difundir este trabajo, adaptarlo y utilizarlo comercialmente, pero todo lo que atribuya, altere, transforme o amplíe sobre este trabajo, deberá distribuirse sólo bajo la misma licencia o similar a ésta.

Colaboradores

Agradecemos la colaboración de esta guía a:

- Cristian Borghello - @seguinfo - [Segu-Info](#)
- Marcelo Temperini - @mgitemperini - [AsegurarTe](#)
- Mauro Gioino - @maurog11 - [Equipo AntiRansom](#)
- Nicolás Gustavo Bruna - @thinkthenclick - [Smartfense](#)
- Matías Sequeira - @matiasasequeira - [Equipo AntiRansom](#)
- Maximiliano Macedo - @ydea2 - [AsegurarTe](#)
- Walter Heffel - [Segu-Info](#)

Resumen Ejecutivo

En los últimos años, son cada vez más comunes los titulares del tipo *“Empresa X debió pagar ‘rescate’ por sus datos”* u *“Organización Pública Y no puede prestar atención porque su información fue secuestrada”*.

Parece que las organizaciones están preparadas para enfrentar distintos tipos de incidentes físicos como cortes de energía e inundaciones, pero sigue siendo común que toda la infraestructura de datos sea privada de funcionamiento porque alguien hizo clic en un enlace malicioso o abrió un archivo adjunto de un correo electrónico dañino. Debido a esto muchas organizaciones luchan contra el malware y en particular contra el **RANSOMWARE**.

Este documento está destinado a ser una completa guía de **Defensa en Profundidad** basada en una lista de verificación, con el fin de evitar infecciones con *ransomware* y, en última instancia crear procedimientos adecuados para la recuperación de la información.

Dada la prevalencia de los sistemas operativos Windows como objetivo (de más del 90%) del *ransomware*, la guía está orientada en gran medida hacia dicho entorno y, aunque fue diseñada para ser agnóstica, no siempre se podrán aplicar todos los controles en todos los casos.

Introducción

Un *ransomware* (del inglés *ransom*, rescate y *ware*, software) es un tipo de malware que restringe o bloquea el acceso a determinados componentes o archivos del sistema infectado, y pide un “rescate” para liberarlos.

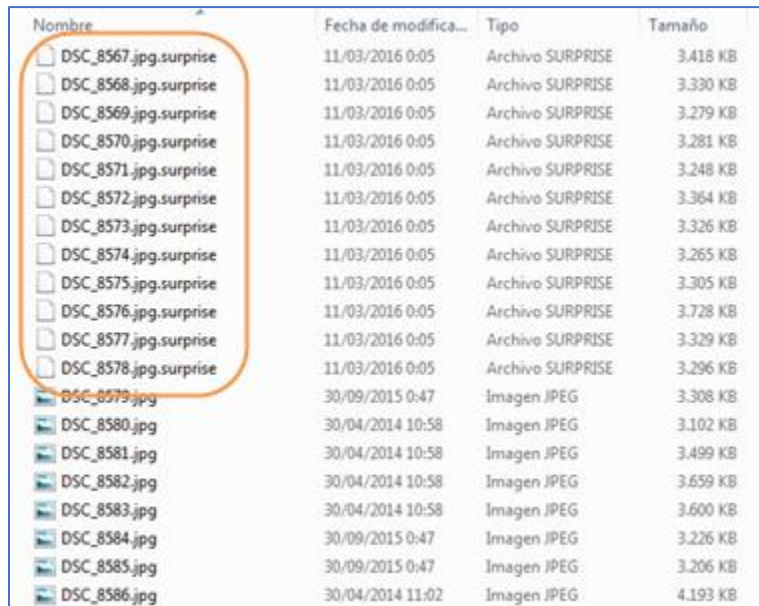
Algunos tipos de *ransomware* cifran¹ archivos sensibles del sistema operativo y otros cifran archivos del usuario, ofimática, bases de datos, etc. coaccionando al propietario a pagar el rescate que permitirá descifrarlos. Luego del cifrado, los archivos originales se eliminan de forma segura para que no puedan ser recuperados por métodos tradicionales.

El *ransomware* afecta a empresas, gobiernos, infraestructuras críticas e incluso a usuarios domésticos, y las consecuencias incluyen:

- pérdida temporal o permanente de información sensible o confidencial;
- interrupción de las operaciones de la organización;
- pérdidas financieras incurridas para restaurar los sistemas y archivos, o en el peor de los casos, por el pago del rescate;
- potencial daño a la reputación de la organización;
- responsabilidad penal o civil (que será analizado en el apartado de aspectos legales).

¹ En el contexto de este documento se utiliza “cifrar” como sinónimo del término “encriptar”.

Esta imagen muestra un proceso de infección, donde parte de los archivos ya se encuentran cifrados y eliminados:



Nombre	Fecha de modifica...	Tipo	Tamaño
DSC_8567.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.418 KB
DSC_8568.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.330 KB
DSC_8569.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.279 KB
DSC_8570.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.281 KB
DSC_8571.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.248 KB
DSC_8572.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.364 KB
DSC_8573.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.326 KB
DSC_8574.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.265 KB
DSC_8575.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.305 KB
DSC_8576.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.728 KB
DSC_8577.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.329 KB
DSC_8578.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.296 KB
DSC_8579.jpg	30/09/2015 0:47	Imagen JPEG	3.308 KB
DSC_8580.jpg	30/04/2014 10:58	Imagen JPEG	3.102 KB
DSC_8581.jpg	30/04/2014 10:58	Imagen JPEG	3.499 KB
DSC_8582.jpg	30/04/2014 10:58	Imagen JPEG	3.659 KB
DSC_8583.jpg	30/04/2014 10:58	Imagen JPEG	3.600 KB
DSC_8584.jpg	30/09/2015 0:47	Imagen JPEG	3.226 KB
DSC_8585.jpg	30/09/2015 0:47	Imagen JPEG	3.206 KB
DSC_8586.jpg	30/04/2014 11:02	Imagen JPEG	4.193 KB

Imagen 1 - Proceso de cifrado de un *ransomware*

El *ransomware* suele cifrar la información en todas las unidades, tanto las locales del sistema operativo como las mapeadas a otros equipos. Esto incluye cualquier unidad asignada a discos externos, USB, unidades de red y en la nube. Esta situación se vuelve crítica cuando el equipo infectado está conectado a un servidor de archivos o a un sistema responsable de realizar [backup](#), ya que se cifrarán los archivos originales y las respectivas copias de seguridad.

En general, el cifrado de los *ransomware* actuales suele ser imposible de revertir ya que se utiliza una combinación de algoritmos de criptografía [simétrica](#) y [asimétrica](#), y cada archivo es cifrado con una clave única. Finalmente, el malware deja una “nota de rescate” en el escritorio del usuario y/o en archivos en distintas carpetas del sistema (en inglés o en varios idiomas), de forma tal que la víctima conozca el procedimiento para recuperar sus archivos secuestrados.

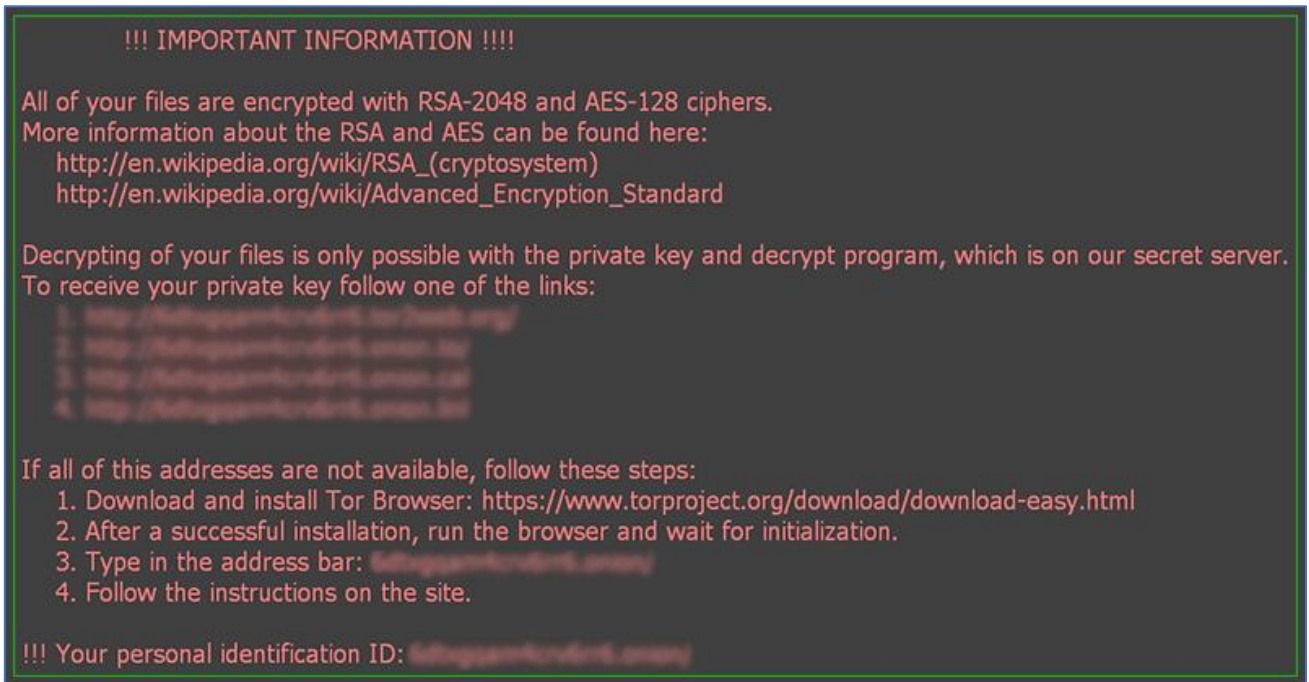


Imagen 2 - Nota de rescate típica de un *ransomware*

En algunas ocasiones, los errores de programación introducidos en el malware permiten desarrollar una aplicación para encontrar la contraseña, descifrar y recuperar los archivos, sin pagar. Pero, con excepción de aquellos tipos de malware que tienen errores en su desarrollo, la única forma de descifrar los mismos es pagando el rescate para obtener las contraseñas correspondientes.

Al realizar el mismo, generalmente en la [criptomoneda Bitcoin](#) o [Monero](#), el delincuente envía (o no) la/s contraseña/s para que la víctima pueda descifrar los archivos.

Ante todo, se recomienda NO PAGAR

Algunos *ransomware* conocidos y ampliamente difundidos son:

- Alphacrypt
- Cerber
- Chimera
- CryptorBit
- CryptoDefense
- CryptoLocker
- CryptoWall
- GandGrab
- Locky
- LowLevel04
- OphionLocker
- Petya

Guía para evitar infecciones de RANSOMWARE

- Nemucod
- NotPetya
- Ransom32
- TeslaCrypt
- Torrentlocker
- VaultCrypt
- WannaCry
- CryptXXX

[Esta página](#), creada por [Mosh](#), mantiene una lista actualizada de los *ransomware* conocidos, sus principales características y las [extensiones de archivos](#) utilizadas por los mismos. A continuación, se muestra una línea de tiempo, simplemente para dar una idea del nivel de crecimiento que han logrado los *ransomware* en los últimos años.

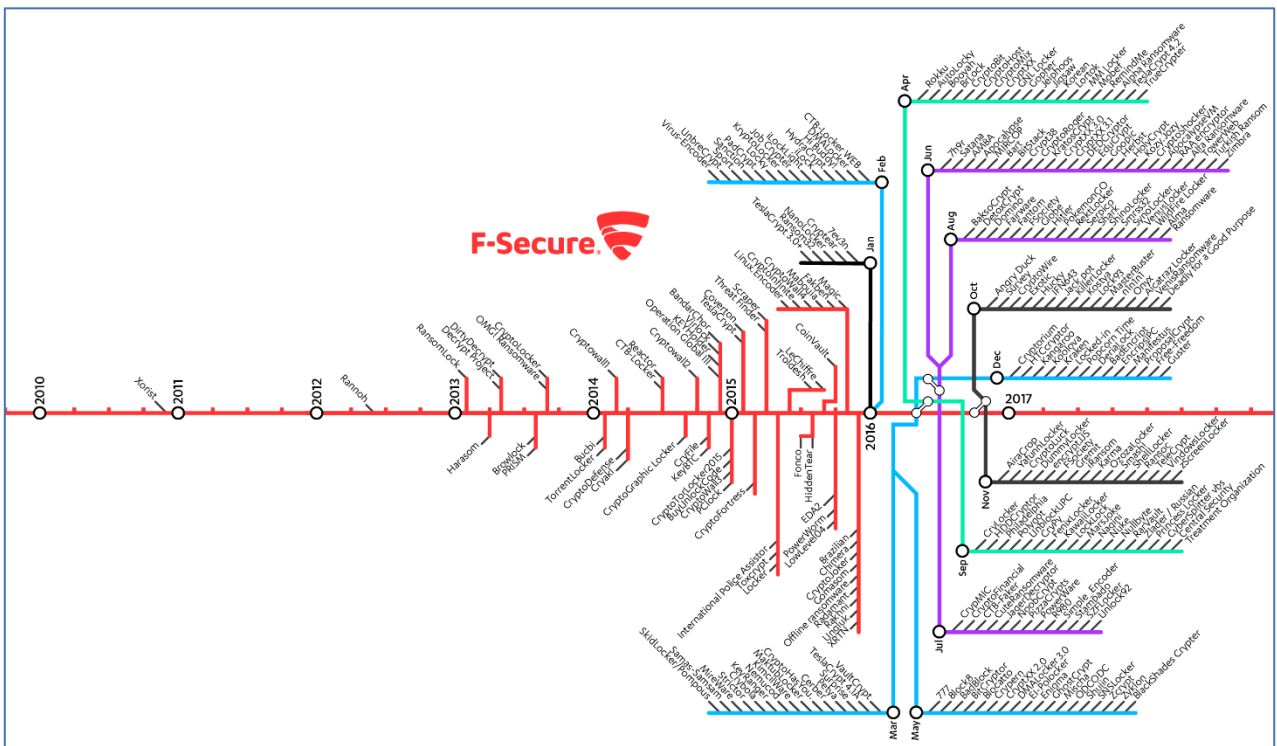


Imagen 3 - Línea de tiempo de *ransomware* - Fuente: F-Secure
<https://labsblog.f-secure.com/2017/04/18/ransomware-timeline-2010-2017/>

Actualmente el *ransomware* se puede encontrar tanto en sistemas operativos de escritorio como Windows, Linux y Mac OS, como así también en sistemas operativos móviles como ser Android, iOS y Windows Mobile. Los dispositivos de [IoT \(Internet of Thing\)](#) también están siendo alcanzados por esta amenaza, lo cual dará lugar a infecciones en televisores, refrigeradores y hasta en automóviles.

La presente guía tiene como objetivo dar a conocer distintas contramedidas que se pueden utilizar para disminuir el riesgo de potenciales

infecciones de *ransomware* o, dado el caso, intentar disminuir su impacto mediante la recuperación de los archivos afectados.

Más información

- [*Ransomware: una guía de aproximación para el empresario \(INCIBE\)*](#)
- [*Countries with highest share of users attacked with ransomware from 2017 to 2018*](#)
- [*The worst types of ransomware attacks*](#)
- [*A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time*](#)
- [*Ransomware Overview*](#)

El negocio del *ransomware*

Business is Business

Un negocio como cualquier otro

La motivación de la mayoría de los ciberdelincuentes es clara: **ganar dinero**. Ésta, es la misma motivación de una organización con fines de lucro (y mafiosa) y, de hecho, las bandas criminales se asemejan cada vez más a ellas en cuanto a su funcionamiento.

Si se analiza brevemente, dentro del negocio del *ransomware* existen distintos grupos de ciberdelincuentes los cuales compiten entre sí en cuanto a la calidad, precio, reputación e innovación de sus productos. Poseen áreas de atención al cliente, las cuales son consideradas el factor más importante de su negocio, y sus productos/servicios van lentamente migrando hacia la nube, como es el caso del [Ransomware-as-a-Service \(RaaS\)](#) -por analogía al [Software as a Service \(SaaS\)](#)-. Continuamente, los atacantes están buscando aumentar su rentabilidad y disminuir los riesgos a los que se exponen utilizando servicios que le garanticen el anonimato.

Si bien el dinero no guía a todos los atacantes, como ser grupos de [Hacktivismo](#) o [Ciberterrorismo](#), el grado de profesionalización y organización de los mismos sigue siendo alto.

Mercado e innovación

El negocio del *ransomware* existe porque hay un mercado cada vez más demandante del servicio. Por un lado, los ciberdelincuentes ganan dinero distribuyendo sus códigos maliciosos y cobrando los correspondientes rescates. Por el otro, ganan dinero vendiendo sus propios *ransomware* para que un tercero pueda utilizarlos, de la misma manera que una empresa legítima de software vende sus productos. Un tercer modelo implica que el proveedor del servicio de *ransomware* cobra a sus clientes un porcentaje de los rescates (\$) pagados por las víctimas.

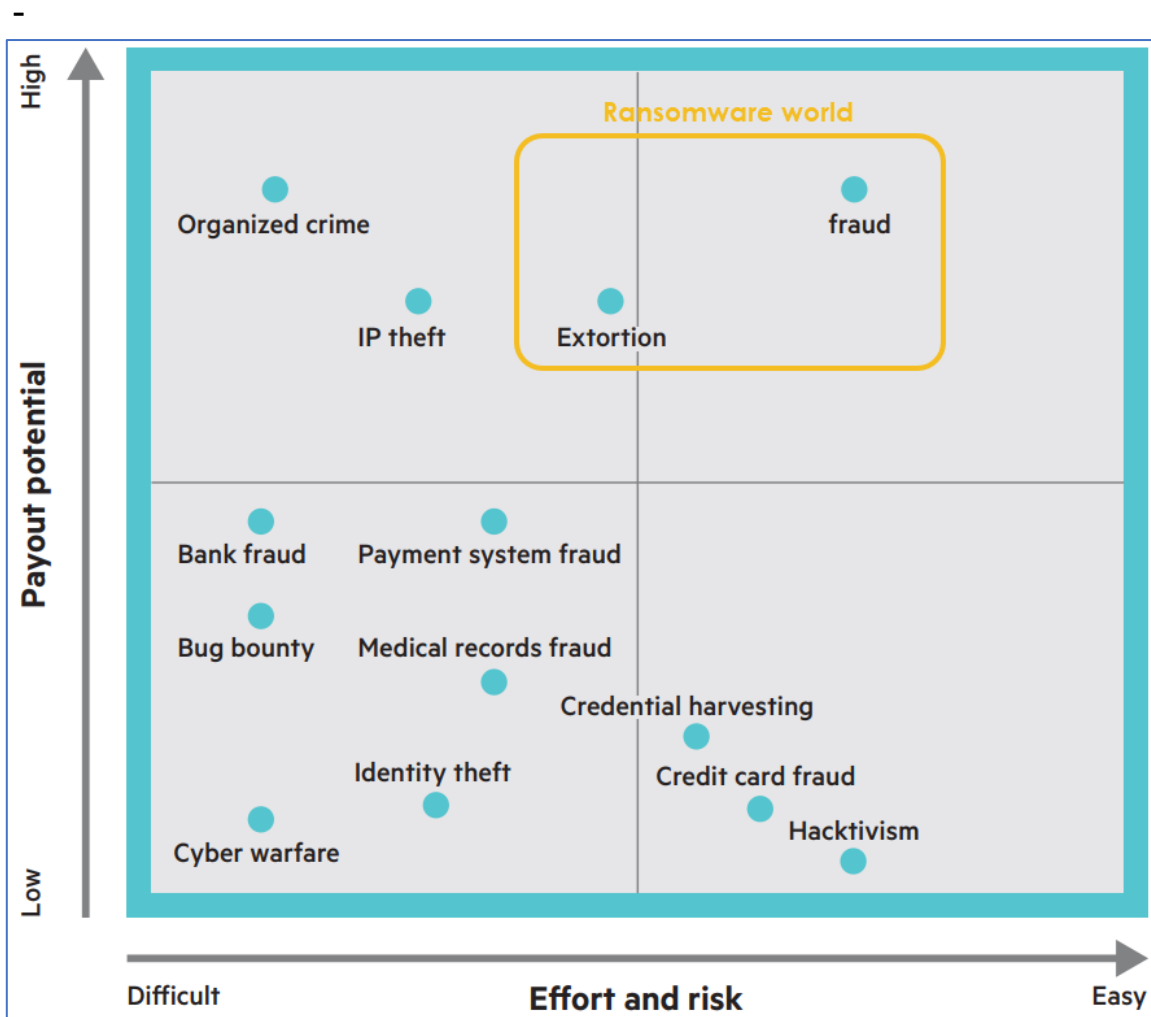


Imagen 4 - Modelos de negocio del cibercrimen

Al igual que en organizaciones legítimas, es un negocio que promueve la innovación y la mejora continua de sus productos y servicios. En el caso del *ransomware*, como cualquier otro software (legítimo o no), su evolución fue naturalmente hacia la nube. A su vez, los ciberdelincuentes seguirán aprovechando los avances tecnológicos como oportunidades, como ser el auge de las tecnologías móviles e IoT y cualquier innovación tecnológica que depare el futuro, para seguir creciendo y perfeccionando sus ataques.

Como todo mercado, el del *ransomware* es guiado por la oferta y la demanda de productos, y debido a que la cantidad de productos de *ransomware* no deja de subir, éstos se vuelven cada vez más accesibles. A su vez, los ciberdelincuentes buscan la manera de diferenciarse de la competencia haciendo campañas de marketing profesionales, como es el caso de

[ransomware Philadelphia](#), de manera de lograr ventajas competitivas que le permitan mantener o aumentar su cuota de mercado.

Grado de madurez

Teniendo en cuenta la evolución que ha tenido el *ransomware* a lo largo del tiempo, se puede afirmar que el negocio se encuentra en una etapa de neto crecimiento, la rentabilidad del mercado es cada vez mayor y la cantidad de productos y servicios van perfeccionando la calidad de los ataques, a la par que lo hacen las herramientas y servicios de anonimato que le permiten a los delincuentes tomar menores riesgos a cambio de proteger sus -cada vez mayores- ganancias económicas.

Más información

- [The Business of Hacking: Business innovation meets the business of hacking - HP](#)
- [Ransomware as a Service, demuestra la capacidad comercial de los ciberdelincuentes](#)
- [Estadísticas alarmantes dan a conocer la epidemia mundial de Ransomware](#)

Cómo evitar infectarse

Las balas de plata no existen...

Ninguna de las siguientes medidas es efectiva por sí sola y deben utilizarse en conjunto como parte de una estrategia de seguridad en capas y por niveles, de forma tal que cada una de ellas contribuya a hacer más robusto y seguro el sistema y la red.

1. Hacer backup periódico de la información

El backup es una medida reactiva, no ayuda a no infectarse, pero es tan importante que se ha decidido incluirla primero en la lista. La única y más importante herramienta contra el *ransomware* son las copias de seguridad.

Si un malware cifra o daña los archivos, recuperar el último backup es la mejor alternativa. De esta forma, se evita perder información o tener que pagar el rescate por los datos.

Las copias de seguridad deben ser realizadas *off-site*, y las unidades utilizadas para realizar el backup **no deben estar mapeadas en la red** para evitar que los archivos de respaldos sean alcanzados por el *ransomware*.

Los procesos de backup y recuperación deben ser probados periódicamente y deben estar apropiadamente documentados.

A su vez, los usuarios de la organización deberían ser concientizados respecto a dichos procesos, lo cual se relaciona con el punto a continuación.

Más información

- [Guía práctica de backup para usuarios finales](#)
- [Las 10 preguntas clave antes de hacer backup](#)
- [NIST SP 800-34 - Contingency Planning Guide for Federal Information Systems](#)
- [NIST SP 800-184 - Guide for Cybersecurity Event Recovery](#)

2. Concientizar y entrenar a los usuarios

Una de las principales puertas de entrada del *ransomware* son los usuarios con hábitos y comportamientos negligentes, debido a la falta de información sobre las amenazas actuales.

Por este motivo, se recomienda llevar adelante un proceso de concientización y entrenamiento de todos los usuarios de la organización. El objetivo es que aprendan y comprendan los riesgos asociados al uso de recursos informáticos e Internet, y desarrollen hábitos y comportamientos que les permitan realizar un uso responsable y seguro de los mismos.

El proceso de concientización debería ser acordado por el área de RRHH y de Seguridad de la Información de la organización, o en su defecto una consultora especializada en el tema, y ser un proceso proactivo y de mejora continua. Esto último indica que, además de planear e implementar un proceso de concientización, se debe estar en condiciones de evaluar periódicamente los hábitos y comportamientos de los usuarios para así poder, a partir de los resultados obtenidos, realimentar y mejorar dicho proceso.

Más información

- [Cómo desarrollar una capa de seguridad orientada al usuario](#)
- [¿Seguimos desconfiando del usuario final o hacemos algo al respecto?](#)

3. Aplicar un modelo de mínimo privilegio

Si todos los procesos necesarios para realizar las tareas de un usuario se ejecutan con la mínima cantidad de privilegios posible, será más difícil para un software malicioso que se ejecute en el entorno de dicho usuario, ya sea infectar el equipo como propagarse a otros.

El uso de permisos administrativos facilita la ejecución de aplicaciones dañinas y la instalación de malware. Un usuario “administrador” (o “*root*”) sólo debería ser utilizado cuando se necesite realizar una tarea que lo requiera, autorizado por personal superior y auditado de forma periódica.

Por lo tanto, para disminuir el riesgo de una infección por *ransomware*, cada usuario debe ser capaz de acceder sólo a la información y recursos que sean necesarios para el desempeño de sus tareas autorizadas.

Cada usuario, además debería ingresar a los sistemas a través de su identificación unívoca de usuario y contraseña. Si se *loguea* de esta manera y se cumple el modelo del mínimo privilegio, sólo tendrá acceso a la información y datos que necesita, dentro de su perfil y a ningún directorio sensible del sistema operativo, lo cual minimiza el impacto de una posible infección.

Para simplificar, este concepto se resume en decir que la cantidad de usuarios “*administrador/root*” debería ser mínima dentro de una organización.

Más información

- [Guía para implementar el modelo de mínimo privilegio en Windows Server 2016, Windows Server 2012 R2, Windows Server 2012](#)
- [Principio del mínimo privilegio en Oracle Linux](#)
- [Seguridad de ficheros en Linux](#)
- [Listas de control de acceso en Linux](#)

4. Segmentar la Red

La segmentación de la red a través de VLAN² y ACL³ permite controlar el tráfico entre redes de distinta relevancia (por ejemplo, la LAN de usuarios y la LAN de los servidores). Segmentar una red no evita que un ataque de *ransomware* tenga acceso a los sistemas, pero será de mucha ayuda para limitar la infección y lograr que el malware permanezca aislado sólo en el segmento de red que ha comprometido, y así no se extienda por toda la organización. Es particularmente importante para las organizaciones que mantienen sistemas legados, que ya no pueden recibir actualizaciones de seguridad.

Así como puede realizarse la segmentación física/lógica de la red, también es posible segmentar infraestructuras virtualizadas a través de tecnologías de segmentación propias de este tipo de entornos (como [VMware NSX](#) y [Microsoft Hyper-V Network Virtualization](#)).

² VLAN (Red de Area Local Virtual, por sus siglas en inglés): método para crear redes lógicas independientes dentro de una misma red física.

³ ACL (Lista de Control de Acceso, por sus siglas en inglés): forma de determinar los permisos de acceso apropiados a un determinado objeto para lograr la separación de privilegios.

5. Revisar recursos compartidos y unidades externas

Periódicamente se deben realizar revisiones de recursos compartidos (unidades de disco, impresoras, carpetas, etc.) y unidades externas (pendrives, tarjetas de memoria, discos rígidos, etc.) conectadas a los equipos, con el objetivo de determinar si es necesario que permanezcan compartidos o no y, de ser necesario establecer los permisos mínimos para un correcto desempeño.

En caso de detectar dispositivos que no correspondan o que no sean utilizados, deberán ser desconectados/deshabilitados, de forma tal que si ocurre una infección, se evite la propagación del malware por la red de la organización, minimizando el impacto en otros equipos.

Más información

- [Administración de almacenamiento y recursos compartidos en Windows Server](#)
- [Montar y desmontar una unidad extraíble automáticamente en Windows 7 con Mountvol](#)

6. Utilizar soluciones antivirus

Es recomendable utilizar (al menos) dos antivirus: uno en dispositivos ubicados en el [perímetro](#) de la red -firewall y correo corporativo- y otro para los clientes internos y estaciones de trabajo. Para evitar el pago de licencias adicionales, se puede utilizar un producto pago y uno gratuito u *Open Source*.

Nota: en la estación de trabajo sólo debe instalarse un antivirus.

Debido al dinamismo del malware, es normal que los antivirus se “tomen” un promedio de 48 hs para reaccionar ante un nuevo tipo de amenaza como es el *ransomware* actual. Cuanto más tiempo pase desde la aparición de un nuevo tipo de malware, mayor es la posibilidad de detección por parte del producto.

Ningún antivirus es infalible, pero tener dos o más productos en distintos niveles de la organización multiplica la posibilidad de detección.

La mayoría de los antivirus actuales permiten analizar el interior de archivos comprimidos en busca de malware. Estos archivos serán analizados siempre y cuando el archivo no posea contraseña.

En el caso de Windows 10 (ediciones 2018 en adelante), se puede utilizar la protección de carpetas específica contra *ransomware*, configurando esta opción dentro del Centro de Seguridad de Windows Defender.

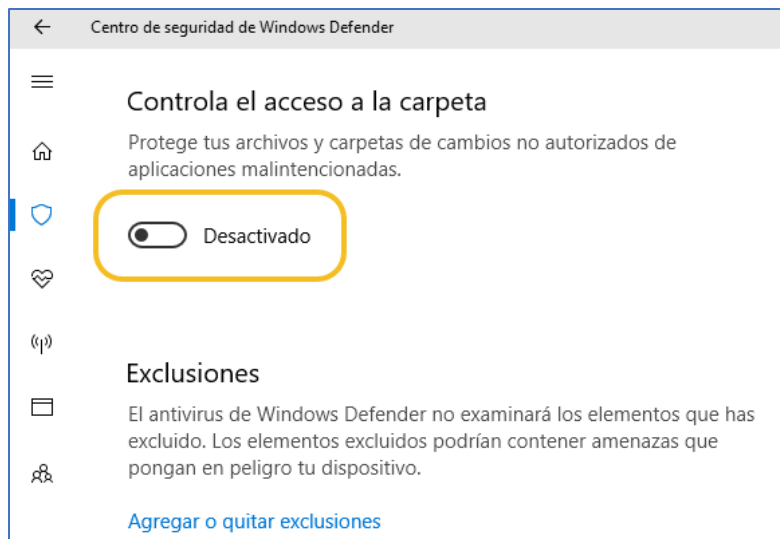


Imagen 5 - Centro de seguridad de Windows Defender

Más información

- [Protección contra *ransomware* en Windows 10](#)

7. Utilizar antispam, firewall y filtro de contenido

A continuación, se mencionan diferentes herramientas y recomendaciones de filtrado para proteger la infraestructura y evitar que la amenaza llegue a los usuarios.

El filtro de contenido se puede realizar en forma manual desde el cliente de correo o bien desde el servidor de correo corporativo, [firewall](#), proxy o [UTM](#), dependiendo lo que la organización decida.

Filtrado a nivel de firewall

Generalmente, el *ransomware* debe comunicarse con un [centro de Comando y Control](#) (C&C) a través de Internet, para enviar las contraseñas de cifrado y recibir instrucciones. El uso de firewall es fundamental (aunque tampoco es una herramienta infalible) en el bloqueo de este canal de comunicación entre el malware y su C&C.

Para el *ransomware*, por lo tanto, es importante hacer foco en el filtrado de conexiones salientes (sin descuidar las conexiones entrantes) para evitar que se comunique con dicho C&C.

Los *firewalls* actuales permiten configurar listas blancas y negras de sitios webs y aplicaciones que se conectan a Internet. A través de listas blancas, se pueden permitir dominios/puertos utilizados, por ejemplo, para actualizaciones de software y de los sistemas operativos que maneja la organización.

Los *firewalls* tipo [appliance](#) permiten configurar opciones de tráfico de red, listas blancas y negras de sitios webs y aplicaciones que se conectan a Internet. A través de los filtros de contenido y las listas negras se pueden bloquear los sitios utilizados para propagar el malware y los archivos ejecutables del *ransomware*, que intentan conectarse al C&C. Con las listas blancas se puede permitir sólo dominios utilizados para las actualizaciones del software y del sistema operativo de la organización

Filtrado web (proxy)

Se debe bloquear la conexión a sitios web:

- Según su geo-localización, como por ejemplo el tráfico proveniente de Asia y otros países de Europa del Este.
- Según su dominio de nivel superior. En [Spamhaus](#) se encuentra un listado de dominios sospechosos por naturaleza.
- Según el contenido/finalidad del sitio: spam, phishing, evasión de proxy, pornografía, y otras categorías de sitios web considerados innecesarios para las operaciones normales de la organización.
- Cuando sea posible, servicios de correo electrónico personal (Gmail, Outlook, Yahoo), sitios de intercambio de archivos (Drive, Dropbox, OneDrive), redes sociales, mensajería instantánea, entre otros. De ser necesario, se pueden agregar excepciones especiales a una cantidad acotada de personas, de acuerdo a su responsabilidad dentro de la organización.

Filtrado de nodos TOR

Si se dispone de un Proxy, Firewall o cualquier otro sistema de seguridad perimetral, será posible añadir reglas para bloquear accesos hacia nodos de la red [TOR](#).

Para facilitar el bloqueo, existe una [lista de nodos hoja](#) dependiendo de su IP pública, y también se pueden agregar [una lista de direcciones](#), que se actualiza cada 30 minutos y permite identificar nodos TOR.

Si se administra un servidor web, se puede efectuar este mismo tipo de restricción mediante los archivos de configuración propios del *webserver*.

Más información

- [Bloquear accesos desde TOR](#)
- [Blocking Tor Browser in Cisco ASA](#)
- [Block TOR en Forefront TMG](#)

Filtrado de correos

Los módulos que se deberían configurar en los servidores o *gateway* de correo (en un caso ideal), son los módulos:

- Antispam, para filtrar o bloquear cualquier tipo de correo basura.
- Filtrado del contenido, para analizar y bloquear malware o archivos ejecutables, analizar archivos comprimidos, bloquear URLs maliciosas, entre otras.

El servicio *antispam*, debe configurarse para bloquear (como mínimo) cualquier tipo de archivo ejecutable o comprimido. Existen soluciones gratuitas y de pago e incluso algunos productos antivirus ofrecen la posibilidad de incorporar estos filtros a su solución tradicional de detección. Dos soluciones antispam Open Source son [Radical Spam](#) y [Mail Cleaner](#).

En determinados dispositivos, se dispone del módulo de [DLP \(Data Loss Prevention\)](#) para prevenir que información confidencial/importante de la organización sea enviada hacia el exterior de la misma.

8. Mostrar las extensiones de los archivos

En el caso de utilizar sistema operativo Windows, se debe tener en cuenta que, de manera predeterminada, oculta las [extensiones](#) para tipos de archivos conocidos (*.EXE*, *.TXT*, *.SCR*, etc.). Esto es un problema porque, un método tradicional de propagación de malware consiste en utilizar extensiones dobles para engañar al usuario. Por ejemplo, si el archivo se llama *file.pdf.exe* o *archivo.docx.scr*, Windows mostrará *file.pdf* o *archivo.docx*.

Es recomendable entonces activar la visualización de la extensión de los archivos para que sea más fácil detectar archivos maliciosos con doble extensión.

Esta medida debería ser contemplada a su vez dentro del proceso de concientización y entrenamiento, mencionado previamente, para que los usuarios sepan qué es una extensión, qué extensiones son peligrosas, y, efectivamente, que un archivo con doble extensión es un archivo potencialmente riesgoso. De otra manera, no servirá de nada mostrar las extensiones ocultas de un archivo si un usuario igualmente termina haciendo doble clic sobre el mismo.

Más información

- [Cómo mostrar u ocultar las extensiones de nombre de archivo en el Explorador de Windows](#)
- [Mostrar extensiones a través de GPO](#)

9. Filtrar archivos con extensiones peligrosas

El filtro de contenido se puede realizar desde el cliente de correo o bien desde el servidor de correo corporativo, el firewall, el proxy o el UTM, dependiendo de lo que la organización decida.

Aquellas organizaciones que dispongan de la administración de su servidor de correo podrían filtrar archivos adjuntos con [extensiones peligrosas](#) (ejecutables y *scripts*) a través de [listas negras](#). Dependiendo del tamaño de la organización, se puede implementar [listas blancas](#) aunque, a mayor tamaño, mayor complejidad.

En el caso que sea necesario intercambiar archivos comprimidos, se puede utilizar una cuarentena temporal. Por ejemplo, un administrador debería autorizar el ingreso de los archivos recibidos o estos se pueden “estacionar” 24/48 hs para dar tiempo a que el antivirus pueda actualizar su base de datos de firmas.

Inicialmente, se deberían bloquear al menos los siguientes tipos de archivos:

- BAT
- CMD
- COM
- CPL
- DLL
- EXE
- JAR
- JS / JSE
- LNK
- MSI
- PIF
- PS1
- SCR
- VBE / VBS
- ZIP / RAR / 7z (y otros comprimidos)

Más información

- [Archivos adjuntos de emails con extensiones peligrosas](#)
- [Cómo evitar infectarse con archivos JS adjuntos y ransomware](#)

10. Inventariar y controlar aplicaciones

Es recomendable realizar relevamientos periódicos de las aplicaciones utilizadas por los usuarios, para adquirir una visibilidad completa del software instalado en toda la infraestructura de la organización.

De esta manera será posible determinar la presencia de herramientas no autorizadas o innecesarias que podrían estar conectándose a internet y convirtiéndose, por lo tanto, en una fuente de riesgo para la organización. De la misma forma, podrá detectarse la ausencia de actualizaciones en el software autorizado, y podrá actuarse en consecuencia. Las actualizaciones se tratan en profundidad en el siguiente punto de esta guía.

En el caso de Microsoft por ejemplo, [AppLocker](#) es una funcionalidad incorporada por defecto en Windows Server 2008 R2 y Windows 7. Permite crear reglas para permitir o denegar la ejecución de aplicaciones basándose en las identidades de los archivos y especificar qué usuarios o grupos pueden ejecutar esas aplicaciones. Por lo tanto, se recomienda habilitar AppLocker y, especificar las aplicaciones y herramientas conocidas que podrían causar un incidente en la red.

Más información

- [Uso de Applocker](#)
- OCS- Software de gestión de inventario de activos (hardware y software)
- [Understanding inventory, configuration and IT asset management](#)
- [NIST SP800-167 - Guide to Application Whitelisting](#)

11. Instalar actualizaciones del sistema operativo y aplicaciones

El aprovechamiento de [vulnerabilidades](#) y [exploits](#) es un factor común en la mayoría del malware. Los delincuentes se aprovechan de los *bugs* y falta de actualizaciones en el sistema operativo y en aplicaciones tradicionales como navegadores (Internet Explorer, Edge, Firefox, Chrome y Safari), Java, Flash Player y Adobe Reader, entre los más populares.

Todas las aplicaciones instaladas deberían actualizarse lo antes posible, sea a través de una configuración/herramienta automática o manualmente a través del sitio oficial del fabricante.

Se debe tener en cuenta que ciertos navegadores comenzaron a bloquear por defecto Java y Flash Player desde el año 2017 y, debido a la gran cantidad de vulnerabilidades que se les han hallado, cuando sea posible se debería [desinstalar Java](#), [Flash Player](#) y Adobe Reader. En el caso de las dos primeras, en general no son necesarias y la última podría ser reemplazada por una equivalente, tal como [Foxit Reader](#).

Para usuarios avanzados podría ser posible filtrar Javascript, Java, Flash y otros *plugins* el navegador a través de la extensión [NoScript](#) (para Firefox) y [ScriptSafe](#) (Chrome).

Más información

- [Guía práctica de actualización de Windows](#)
- [Desinstalar Flash Player](#)
- [Desinstalar Java](#)

12. Deshabilitar ejecución de archivos temporales

Al evitar el uso de permisos administrativos, los archivos descargados por el usuario se almacenan en carpetas locales y temporales de su perfil. En Windows, algunas de ellas son:

- %AppData%\
- %LocalAppData%\
- %LocalAppData%\Temp\
- %ProgramData%\
- %Temp%\
- %userprofile%\
- %WinDir%\temp\
- %WinDir%\SysWow\

El malware suele ejecutarse casi siempre en alguno de estos directorios. Por lo tanto, se deben bloquear los permisos de ejecución sobre los mismos para que los archivos dañinos no se puedan ejecutar. Para bloquear el acceso a estos directorios, se pueden utilizar las directivas de restricción de software local o las GPO de *Active Directory* ("secpol.msc").

Por ejemplo, se podría bloquear la siguiente lista:

- %AppData%*.exe
- %AppData%**.exe
- %LocalAppData%*.exe
- %LocalAppData%**.exe
- %LocalAppData%\Temp*.zip*.exe
- %LocalAppData%\Temp\7z**.exe
- %LocalAppData%\Temp\Rar**.exe
- %LocalAppData%\Temp\wz**.exe
- %ProgramData%*.exe
- %Temp%*.exe
- %Temp%**.exe
- %userprofile%*.exe

- %WinDir%\temp*.exe
- %WinDir%\SysWow*.exe

A esta lista se pueden incorporar los tipos de archivos (y extensiones) mencionados anteriormente.

En la siguiente imagen, se muestra una regla de configuración local donde se restringe la ejecución de archivos .exe en el directorio %AppData%.

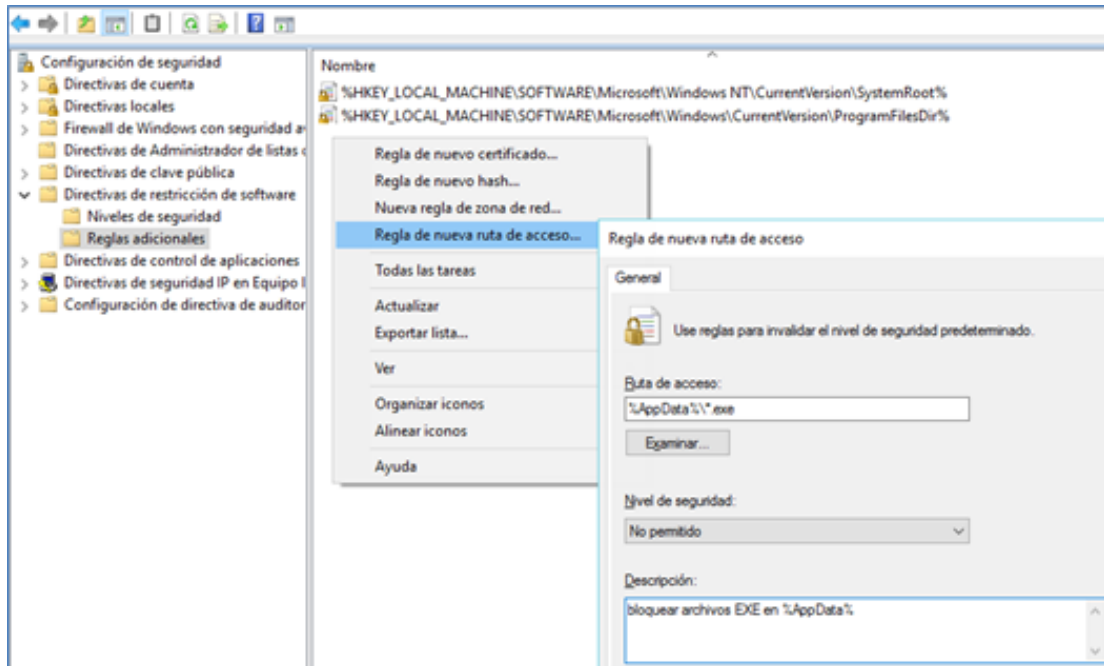


Imagen 6 - Configuración de seguridad

En el caso de tener la necesidad de ejecutar aplicaciones legítimas desde estos directorios, se debe crear una excepción para la regla correspondiente.

Los usuarios de Linux deberían tener las mismas consideraciones en el directorio `~/tmp` y con el perfil propio del usuario (`~/`). En el caso de [Mac OS](#), además se debería proteger `~/Library/`, en donde este sistema operativo almacena los archivos de configuración de las aplicaciones instaladas.

Más información

- [Administrar las directivas de restricción de Software](#)
- [Archivos temporales en Windows](#)

13. Deshabilitar escritorio remoto

En aplicaciones de [escritorio remoto como RDP](#) (nativo de Windows), VNC o [TeamViewer](#), es común la infección a través del aprovechamiento de vulnerabilidades y el uso de contraseñas débiles. Cuando sea posible, estas aplicaciones deberían ser deshabilitadas y, de requerirse un acceso remoto, se recomienda la implementación de una [VPN](#), cuya configuración se limite sólo a los equipos necesarios dentro de la red corporativa.

En el marco de un modelo de defensa en profundidad, se propone fortalecer (proceso de *hardening*) las conexiones RDP con el cifrado de las comunicaciones a través de certificados digitales basados en PKI (X.509), preferentemente emitidos por una entidad certificante (CA) externa de confianza (Symantec, Comodo, Goddady, etc). Otra posibilidad es usar [Remote Desktop Web Client](#) o [Remoto Desktop Service \(RDS\)](#).

Adicionalmente, se recomienda aplicar los siguientes controles sobre las conexiones de escritorio remoto:

- Establecer una contraseña robusta;
- habilitar el [doble factor de autenticación \(2FA\)](#) (cuando sea posible);
- utilizar las últimas versiones disponibles con todas las actualizaciones y parches.

Más información

- [Ejemplo de ransomware propagado por Teamviewer](#)
- [Cómo deshabilitar Escritorio remoto mediante Directiva de grupo](#)
- [Segundo factor de autenticación en Teamviewer](#)
- [Segundo factor de autenticación en RDP](#)
- [Segundo factor de autenticación en VNC](#)

14. Restaurar el sistema

Los sistemas operativos Windows tienen la funcionalidad “Restaurar sistema”, la cual permite recuperar el sistema operativo a un estado anterior a un incidente. Quien administre un dominio, a través de una GPO podrá habilitar/deshabilitar el servicio [Volume Shadow Copy](#) (“vssvc.exe” - “Instantáneas de volumen” en español) en los equipos de red que se considere apropiado proteger.

Sin embargo, es importante hacer notar que, el *ransomware*, también utiliza dicho servicio para eliminar las copias de seguridad, por lo tanto, será útil sólo en el caso que el malware no las haya eliminado. De todas formas, la mejor recomendación es tenerlo habilitado, para aumentar las probabilidades de recuperar el sistema afectado.

Dado que Linux no dispone de un servicio nativo como Windows, una alternativa similar es utilizar [Timeshift](#), [rsnapshot](#), [BackInTime](#) o [TimeVault](#). En el caso de Mac OS se puede utilizar la aplicación [Time Machine](#), que permite hacer copias de seguridad o restaurar completamente el sistema operativo.

Más información

- [Realizar una copia de seguridad de tu PC y restaurarla](#)
- [Guía sobre CTBLocker \(I\)](#)
- [Guía sobre CTBLocker \(y II\)](#)

15. Desactivar las macros y ActiveX en las herramientas de ofimática

Una de las técnicas de propagación utilizada por el *ransomware*, son los documentos adjuntos maliciosos de ofimática (DOCX, XLSX, ODT, etc.) enviados como adjuntos a través de correos electrónicos. Estos documentos contienen [macros](#) que son ejecutadas automáticamente al abrir el documento.

Posteriormente, la macro descarga y ejecuta un archivo EXE, que es el verdadero troyano/*ransomware* que infecta el sistema.

Incluso, en el último tiempo [han aparecido otras técnicas \(*macro-less*\)](#) que hacen posible la ejecución de malware sin necesidad de abrir una macro en el documento.

En conclusión, nunca se debería abrir un archivo de ofimática que haya sido recibido por correo electrónico, ya sea porque le resulta sospechoso (por ej. escrito en otro idioma), porque no lo espera o porque es un remitente desconocido y, si se abre, nunca se debe permitir la ejecución de macros, siempre que sea posible denegarlo. En última instancia, también es válido comunicarse con el remitente para confirmar la veracidad del documento recibido.

Por su parte, los [ActiveX](#) permiten realizar distintos tipos de acciones sobre el sistema operativo, lo cual también podría ser utilizado para infectarlo.

Se recomienda desactivar las macros y ActiveX a través de GPO o manualmente en la herramienta ofimática utilizada.

Más información

- [Cómo evitar el *ransomware* en macros mediante Políticas de Grupo en Office 2016](#)
- [Locky malware, lucky to avoid it](#)
- [Plan security settings for VBA macros for Office 2013](#)
- [GPO to enable Excel 2007 and 2010 Macro's](#)

16. Deshabilitar servicios de scripting y consolas

Se han popularizado campañas de spam que [contienen archivos adjuntos](#) comprimidos como ZIP y RAR con archivos VBS ([VisualBasicScript](#)) o JS ([JavaScript](#)). Si el usuario ejecuta el script adjunto, posteriormente se descarga y ejecuta el malware (.EXE) que suele ser un *ransomware*.

Los sistemas operativos Windows, por defecto abren archivos de scripts con la aplicación *Windows Based Script Host (WSH)*. Por lo tanto, la recomendación es deshabilitar el servicio en cuestión a través de una política de grupo (GPO) o localmente. De la misma forma se recomienda deshabilitar o desinstalar *Windows Power Shell* y *CMD* ya que la mayoría de los usuarios no requieren estas herramientas.

Para los casos donde no sea posible deshabilitar dichos servicios, se recomienda - previo análisis para evitar falencias en el funcionamiento de los sistemas/procesos de la organización - configurar la apertura de los archivos de scripts con un editor de texto.

Más información

- [Cómo evitar infectarse con archivos JS adjuntos y ransomware](#)
- [To run scripts using the Windows-based script host](#)
- [How to Enable and Disable PowerShell V2 on Windows 8](#)
- [Disable the command prompt](#)
- [Disabling Windows Script Host](#)

17. Bloquear publicidad y ventanas emergentes

Es común encontrar malware incrustado en publicidades de sitios web, ya que estos tercerizan sus espacios para mostrar publicidad relacionada con el contenido de la página web. Esta técnica se denomina [Malvertising](#) (*Malware + Advertising*) y, por lo tanto, con tan solo visitar un sitio con estas características, se puede infectar el sistema de la víctima de forma automática.

La medida de protección a aplicar, es instalar un complemento en el navegador para bloquear las ventanas emergentes y la publicidad. Dos bloqueadores efectivos y gratuitos son [Adblock](#) y [Adblock Plus](#), los cuales funcionan en cualquier navegador y pueden ser instalados a través de una GPO. Además, se puede complementar la funcionalidad de los bloqueadores, configurando en el navegador el bloqueo de las ventanas emergentes.

Más información

- [Bloquear ventanas emergentes en Chrome](#)
- [Bloquear ventanas emergentes en Firefox](#)
- [Bloquear ventanas emergentes en Internet Explorer](#)
- [Bloquear ventanas emergentes en Opera](#)

18.Desactivar Autorun/AutoPlay

Desde el lanzamiento de Windows Vista (año 2006), el servicio de "[Autorun/AutoPlay](#)" de medios de almacenamiento externos, como USB y CD, se encuentra desactivado por defecto, pero en versiones anteriores se encuentra activado. En algunas ocasiones (todavía), es posible encontrar malware que se propaga a través de dispositivos USB utilizando esta función y por lo tanto, debe ser desactivada.

A través del uso de GPO o manualmente en un equipo local, se puede desactivar este servicio, de forma tal que el archivo *autorun* no se ejecute automáticamente cuando se inserta un dispositivo externo.

Más información

- [Desactivar Autorun en Windows desde la GPO](#)

19. Apagar conexiones inalámbricas

En los dispositivos móviles (teléfonos, tablets y notebooks), cuando sea posible se debe deshabilitar el uso de redes inalámbricas (*bluetooth*, infrarrojo y Wi-Fi) porque se disminuye el riesgo de propagación de malware a través de dispositivos que se conectan automáticamente y sobre los que generalmente no se tiene un control adecuado.

20. Instalar herramientas de terceros

Las herramientas *anti-ransomware* son una medida adicional de seguridad que funcionan a la par de las soluciones antivirus. Los proveedores de gran parte de estas herramientas son empresas de seguridad especializadas en antivirus que dejan estas herramientas disponibles a la comunidad de manera gratuita. En general, las mismas han surgido como vacuna de alguna variante de *ransomware* y luego fueron evolucionando, hasta convertirse en una solución aplicable a diversas variantes.

¿Cómo funcionan?

Este tipo de soluciones, mayoritariamente reaccionan ante un comportamiento anómalo propio del funcionamiento de los distintos tipos de *ransomware*. Otras, crean carpetas en la unidad de disco C con caracteres especiales, como señuelo, de modo que, al iniciar el proceso cifrado, el código malicioso arrancará por los archivos de dichas carpetas, y en consecuencia le dará tiempo a la herramienta de detectar y detener el cifrado.

En otros casos, es posible seleccionar los directorios a proteger del *ransomware*, para evitar que los archivos que contienen sean cifrados. De esta manera, se consigue una protección proactiva.

Algunos ejemplos de este tipo de herramientas son:

- [AntiRansom](#) es una aplicación de seguridad desarrollada especialmente por [Security by Default](#) para detectar este tipo de malware en Windows. Si bien se ha discontinuado no deja de ser interesante su revisión.
- [CryptoPrevent](#) es una aplicación de seguridad para Windows diseñada originalmente por [d7xTech](#) para prevenir la infección de [CryptoLocker](#) que surgió a fines de 2013 y actualmente proporciona protección contra una amplia gama de *ransomware* y otros tipos de malware.
- [BDAntiransomware](#) es una “vacuna” lanzada por [BitDefender](#) para brindar protección contra versiones de las familias *CTB-Locker*, *Locky* y *TeslaCrypt*.
- [Latch Antiransomware Tool](#) es una herramienta publicada por [Eleven Paths](#) que añade una capa de autorización sobre carpetas “protegidas”, de forma que deniega cualquier tipo de operación de escritura o

borrado de los archivos. De la misma forma, [Windows 10 permite un control similar sobre carpetas](#) previamente definidas por el usuario.

- [Kaspersy NoRansom](#) es un conjunto de herramientas para descifrar varios tipos de *ransomware*.
- Avast ha publicado [Ransomware Decryption Tools](#).
- MalwareHunterTeam ha desarrollado la herramienta [ID-Ransomware](#) que permite identificar varios tipos de malware.
- [PowerShell y Bash también pueden utilizarse para detectar la modificación de ciertos archivos señuelos](#) en Windows y Linux.
- Lista de otras [herramientas para ransomware particulares](#).

Por otro lado, es importante mencionar a la iniciativa [NoMoreRansom](#) lanzada por la [National High Tech Crime Unit](#) de la policía de Países Bajos, el [European Cybercrime Centre de Europol](#) y las compañías de ciberseguridad [Kaspersky Lab](#) y [McAfee](#), que tiene el objetivo de ayudar a las víctimas de *ransomware* a recuperar sus datos cifrados sin tener que pagar rescate.

NoMoreRansom también ha publicado una [lista](#) que permite buscar rápidamente el tipo de *ransomware* que ha afectado un sistema y comprobar si existe una solución o herramienta de descifrado disponible.

Más información

- [Herramientas de descifrado de NoMoreRansom](#)
- [Control de carpetas en Windows 10](#)

21. Proteger el MBR

El [MBR \(Master Boot Record\)](#) consiste en código ejecutable almacenado en el primer sector (sector 0) de un disco duro, el cual inicia el arranque (*Boot Loader*) del sistema operativo. El MBR también contiene información sobre las particiones del disco y su sistema de archivo.

Teniendo en cuenta que el MBR se ejecuta antes que el propio sistema operativo, puede ser manipulado por un *ransomware* para ganar persistencia en el equipo. Por ejemplo [HDDCryptor](#), [Petya](#) y [Satana](#) explotan esta vulnerabilidad.

Para prevenir la modificación del sector 0 de todos los dispositivos conectados a un sistema, se puede utilizar la herramienta [MBRFilter](#), la cual brinda una protección a nivel del sistema operativo.

22. Aislar el equipo infectado

En el caso de sospechar haber ejecutado un *ransomware*, desconectar la red y apagar el equipo puede disminuir la tasa de archivos infectados. Esto no es una solución, pero es preferible tener algunos archivos cifrados y no todos. Sin embargo, se debe prestar especial atención a este procedimiento porque algunas variantes de *ransomware* eliminan de manera parcial los archivos luego de cada reinicio.

Como medida adicional, se puede retroceder la hora en el reloj de la BIOS porque algunos *ransomware* dan un tiempo limitado para realizar el pago. Obviamente esto no ayuda a recuperar los archivos cifrados.

Es decir, este procedimiento representa un riesgo porque que el sistema podría no volver a arrancar por los daños ocasionados por el malware.

23. Deshabilitar o eliminar protocolos obsoletos

En las organizaciones suelen encontrarse activados protocolos obsoletos, no recomendados por las buenas prácticas internacionales (por ej. FTP, TELNET, etc.) o que la organización no utiliza y nadie se ha percatado de esta situación.

Estos protocolos deberían ser reemplazados por versiones actualizadas para solucionar vulnerabilidades de seguridad, o directamente retirados debido a que no son requeridos en los procesos normales de negocio.

Un ejemplo de esta situación es la implementación del protocolo [SMBv1](#) en ambientes Windows. Cabe recordar que SMBv1 es uno de los vectores de infección utilizados por el *ransomware* Wannacry para diseminarse a través de la red. Mantener esta versión del protocolo se justifica en muy pocos casos:

- Cuando aún existen equipos con Windows XP o Server 2003, en virtud de un acuerdo de soporte personalizado;
- existe software de administración antiguo o programas legados que exigen a los usuarios navegar a través de una lista maestra de “vecindad de red” (*network neighborhood*);
- existen impresoras multifunción con *firmware* antiguo, usadas con el fin de “escanear para compartir”.

Ninguna de estas cosas debería afectar al usuario final o al negocio. A menos que los administradores lo permitan o no gestionen las mitigaciones correspondientes.

Más información

- <https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>
- <https://support.microsoft.com/es-ar/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and>

24. Gestionar sistemas operativos obsoletos

Se considera “obsoleto” a cualquier software sin soporte del fabricante o cuyo ciclo de vida está próximo a expirar.

La idea primaria es analizar los riesgos derivados de mantener sistemas operativos obsoletos en equipos conectados a la red corporativa (por ej. Windows XP o Server 2003) y las posibilidades resultantes, si es que existen. Cuando una plataforma operativa llega al fin de su “vida útil” es altamente probable que deje de recibir actualizaciones por parte del fabricante. Con el paso del tiempo aparecen nuevas vulnerabilidades, las cuales no siempre son evaluadas ni parcheadas, aumentando la superficie de ataque de toda la red de la organización.

En algunos casos, como cajeros automáticos, ambientes industriales o aplicaciones embebidas, no es posible reemplazar el hardware y/o el sistema operativo “viejo”, con lo cual migrar a una versión más actual de la plataforma no suele ser una opción inmediata. Por ende, estos casos deben monitorearse en forma puntual y someterse a eventuales cambios, tales como evitar que se conecten a Internet, habilitar un firewall local, deshabilitar puertos o servicios ociosos, etc.

Recuperación de archivos cifrados

La eliminación del malware se puede realizar manualmente o a través de un antivirus. En cambio, la recuperación de los archivos cifrados depende del tipo de *ransomware* y versión del mismo ya que, a medida que este tipo de malware se ha ido perfeccionando, sus creadores han ido corrigiendo errores y han agregado nuevas funcionalidades que dificultan que los archivos sean recuperados.

Por ejemplo:

- Las primeras versiones de *CrypLocker*, *TeslaCrypt*, *Locky* y *AlphaCrypt* se podían recuperar utilizando las Shadow Copies de Windows y la herramienta [ShadowExplorer](#), pero las versiones actuales eliminan estas copias y ya no se pueden utilizar.
- Para las dos primeras versiones de *Locky* y *TeslaCrypt* era posible utilizar una herramienta de recuperación, pero versiones siguientes corrigieron errores y ya no es posible realizar este procedimiento.

Con las tecnologías actuales (dejando de lado la computación cuántica) no es posible romper el cifrado de 128+ bits simétricos y 1024+ bits asimétricos utilizados por el *ransomware*. Por ejemplo

- Para un algoritmo simétrico, se necesitan un par de horas para obtener una contraseña de 20 bits y años para una clave de 128 bits: ($2^{128} = 340282366920938463463374607431768211456$ claves posibles)
- Para un algoritmo asimétrico, una clave de 512 bits puede romperse fácilmente (en unos meses), pero una clave de 1024 o 2048 bits no es posible hacerlo en un tiempo razonable para el negocio.

La recuperación de los archivos eliminados de forma segura, posterior al cifrado, tampoco suele ser posible ya que el “borrado seguro” sobrescribe N veces la información, de forma que cualquier esfuerzo por reconstruir los archivos se vuelve infructuoso, no se puede aplicar a todos los archivos cifrados o no es viable en un tiempo razonable para aplicar en múltiples sistemas afectados.

De todos modos, antes de darlo todo por perdido, se pueden probar herramientas como [R-Studio](#), [Photorec](#) o [Recuva](#) (Windows) y [Foremost](#) o [TestDisk](#) (Linux) que podrían permitir la recuperación de algunos archivos.

Más información

- [TeslaCrypt and Alpha Crypt *ransomware* Information Guide and FAQ](#)
- [The Complete Guide to *ransomware*](#)
- [Cómo hacer borrado seguro de datos](#)

Proceso de pago

Ante todo, se recomienda NO PAGAR

Si todo lo anterior falla, y sólo si la organización decide hacerlo, se puede efectuar el pago del rescate. El pago no asegura resultados positivos ni la recuperación de los archivos, ya que siempre se estará negociando con delincuentes.

Además, pagar para descifrar los archivos, no significa que se haya eliminado la infección; incluso puede suceder que luego de recuperar la información, la misma sea cifrada nuevamente por el mismo malware.

El pago debe realizarse dentro de un plazo que generalmente no supera la semana luego de la infección. Este tiempo puede depender de una exigencia del delincuente o porque el sitio web, donde se brindan las instrucciones de pago, desaparece al ser dado de baja por la justicia o por el mismo criminal.

En algunos casos es posible recuperar algunos pocos archivos de forma gratuita como “prueba de vida”, para probar que el delincuente realmente dispone de las claves para descifrar los archivos.



Imagen 7 – Página con instrucciones para el pago de rescate

El rescate generalmente se exige en [Bitcoin](#) (u otra criptomoneda como [Monero](#)), lo cual hace muy difícil rastrear al delincuente y creador del malware. La cantidad de Bitcoin exigidos por los delincuentes depende del tipo de malware y puede ir desde unos pocos a cientos o miles de dólares.

Nota: [La cotización de Bitcoin](#) es muy variable (ha fluctuado entre 0,1 y 20.000 dólares desde 2008) pero su tendencia alcista hace que sea un negocio perfecto para el delincuente.

El lugar de pago también varía, pero generalmente se realiza en sitios de la Deep Web, lo cual también imposibilita el rastreo del delincuente.

Para el pago, se deben seguir las instrucciones presentadas en la página web o pantalla de bloqueo y enviar la cantidad exigida a la "*Bitcoin Address*", que es una [cadena de 26 a 35 caracteres](#) y que identifica la billetera del delincuente.

Luego del pago, el delincuente debería enviar por correo electrónico (u otro medio) una aplicación ejecutable (el descifrador) y las contraseñas necesarias para descifrar los archivos.

Más información

- [Ransomware: ¿Debes elegir si pagar o no un rescate? Te ayudo a decidirlo](#)

Aspectos legales

Ya se ha mencionado que entre las distintas consecuencias de una infección de *ransomware* podemos encontrar:

- pérdida temporal o permanente de información sensible o confidencial;
- interrupción de las operaciones de la organización;
- pérdidas financieras incurridas para restaurar los sistemas y archivos, o en el peor de los casos, por el pago del rescate;
- potencial daño a la reputación de la organización;
- responsabilidad penal o civil.

En el presente apartado, nos dedicaremos a analizar los distintos tipos de responsabilidades jurídicas que pueden derivarse de un caso de infección de *ransomware*.

Responsabilidad Penal

Los ataques de *ransomware* tienen cierta complejidad, así como también consecuencias en la responsabilidad penal. En materia de delitos informáticos, en la República Argentina la [Ley N° 26.388](#) ha modificado y agregado determinados tipos penales al Código Penal Argentino, incluyendo algunos de ellos que -de acuerdo al caso concreto- podrían ser aplicados a un ataque de *ransomware*.

En relación al bien jurídico afectado, en principio un ataque de *ransomware* afectaría dos de los tres pilares básicos de la seguridad de la información, que son la **disponibilidad** y la **integridad** de la información. Esta afirmación sería cierta siempre y cuando sólo se analicen las consecuencias del ataque en los sistemas de información.

Sin embargo, si se elige tener una mirada un más amplia sobre el hecho en sí, se podrían encontrar otros bienes jurídicos afectados, como ser el propio **patrimonio de la organización**, en el caso que la información afectada algún tipo de valor comercial para la víctima. Además, si se decidió por el pago del rescate, existe otro tipo de daño económico más directo causado por la erogación que implica recuperar la información secuestrada. Incluso,

suponiendo la difusión pública del incidente, podríamos considerar la afectación de la imagen y la marca como otro eventual daño del mismo delito.

A continuación, dejamos el listado de algunos de los tipos penales (Argentina) que podrían ser aplicables, dependiente del caso concreto:

- **Daño informático (art. 183 2do párrafo):** En la misma pena -prisión de quince días a un año- incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños. (Párrafo incorporado por art. 10 de la Ley N° 26.388, B.O. 25/6/2008)
- **Denegación de Servicios (art. 197):** Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida. (Artículo sustituido por art. 12 de la Ley N° 26.388, B.O. 25/6/2008)
- **Extorsión (art. 168):** Será reprimido con reclusión o prisión de cinco a diez años, el que con intimidación o simulando autoridad pública o falsa orden de la misma, obligue a otro a entregar, enviar, depositar o poner a su disposición o a la de un tercero, cosas, dinero o documentos que produzcan efectos jurídicos.
- **Estafa (art. 172):** Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño.
 - **Tipo especial de estafa (art. 173 inc. 16):** El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos. (Inciso incorporado por art. 9° de la Ley N° 26.388, B.O. 25/6/2008)

Como se puede observar del listado anterior, en Argentina existen distintas posibilidades desde lo penal para tipificar un caso de *ransomware*. Si bien el tipo penal básico aplicable sería el de **cracking o daño informático**, dependiendo de la estrategia probatoria y a las evidencias con las que se cuenten en el caso, podría aplicarse una o más figuras penales.

Nota: *el lector debería tener en consideración la adaptación de las figuras penales vigentes en el país donde ha ocurrido el incidente.*

En un caso interesante de jurisprudencia española ([Ver Texto Completo](#)), de fecha marzo 2016, se condena a una banda dedicada a la creación y propagación de *ransomware*, demostrando precisamente la amplitud de tipos penales que es posible aplicar a casos concretos. Este caso tuvo lugar a partir de la investigación realizada a nivel internacional y los usuarios afectados recibieron mensajes en los que aparecía el membrete falsificado de la policía española, solicitándoles el pago de una cantidad de 100 Euros por la presunta comisión de determinados ilícitos.

De dicha investigación se detuvo a 10 personas (7 de nacionalidad rusa y 3 de nacionalidad ucraniana), que fueron acusados por:

1. Un delito continuado de estafa, de los artículos 248, 250.6° y 74 del Código Penal Español (CPE), en concurso medial con el artículo 77, con un delito de daños informáticos del artículo 264, apartados 2 y 3.1 del referido cuerpo legal.
2. Un delito de blanqueo de capitales, del artículo 301 del CPE.
3. Un delito continuado de falsedad en documento mercantil, de los artículos 392.1 y 390.1°, 2° y 74 del CPE.
4. Un delito de pertenencia a organización criminal, del artículo 570 bis, apartados 1 y 2 c) del CPE y
5. Un delito contra la intimidad, del artículo 197.2 del CPE.

Se destaca que la investigación realizada para identificar y detener a la banda de cibercriminales, fue posible gracias a la denuncia de 390 víctimas (cuyos datos incluso constan en el texto completo del fallo), que, tras ser víctimas del ataque, decidieron realizar la correspondiente denuncia formal ante los órganos competentes y colaborar con la información que hizo posible llevar adelante la investigación.

Como puede observarse, desde el punto de vista del derecho penal material, existen múltiples tipos penales que es posible aplicar en estos casos, dependiendo de las posibilidades de prueba que se tengan desde la justicia. Sin embargo, los mayores desafíos para la justicia son los aspectos investigativos y probatorios, toda vez que más allá de los desafíos propios que implica la preservación y recolección de evidencia digital, la mayoría de las bandas de cibercriminales dedicadas al *ransomware*, operan desde diferentes países, haciendo necesario llevar adelante una investigación de índole internacional, solicitando cooperación a distintas empresas y Estados, para que sea posible identificar a los delincuentes y poder así, aplicar las

responsabilidades penales que correspondan. A estos aspectos procesales, deberíamos sumar los posibles obstáculos de investigación que implica la utilización de técnicas antirastreo o antiforenses utilizadas por las bandas de cibercriminales más organizadas y complejas.

En este contexto, en diciembre de 2017, a través de la Ley N° 27.741 [Argentina ha sancionado la aprobación del CONVENIO SOBRE CIBERDELITO del CONSEJO DE EUROPA](#) (más conocido como el Convenio de Cibercrimen de Budapest), el cual permite acceder a algunas herramientas de cooperación internacional que podrán ser de utilidad para las investigaciones complejas que este tipo de delitos demandan.

Se recomienda a quienes han sido víctimas de un ataque de *ransomware*, **realizar la denuncia formal lo más rápido posible ante una fiscalía competente** (dependiendo del lugar de residencia de la víctima), a fin de documentar la existencia del incidente y permitir a las fuerzas de la ley llevar adelante (o al menos analizar la viabilidad de) una investigación penal para dar con los autores del mismo. Adicionalmente a la denuncia, se recomienda evitar todo tipo de manipulación de los sistemas, a fin de no realizar una contaminación de la evidencia digital.

En el caso de no querer o poder realizar formalmente la denuncia, se recomienda al menos reportar el incidente al [Observatorio de Delitos Informáticos de Latinoamérica \(ODILA\)](#) que se encarga de realizar un seguimiento y estadísticas sobre la existencia de delitos informáticos en Latinoamérica, a través de la medición de la cifra negra de estos delitos.

Responsabilidad Civil

A diferencia del apartado anterior, donde se desarrollan las posibles responsabilidades penales que podrían aplicarse a quienes están detrás de un ataque de *ransomware*, aquí se intenta realizar un breve análisis sobre la posible responsabilidad civil de la propia organización que fue afectada por un ataque de este tipo, entendiendo que dicho incidente de seguridad habría sido posible a partir del incumplimiento de obligaciones legales (contractuales o normativas) en materia de seguridad de la información.

La pregunta clave aquí es: *¿Existe responsabilidad de la organización que sufre un incidente de seguridad de la información -ataque de ransomware- y que en consecuencia de ello genera daños a sus clientes finales?*

Es decir, se plantea el hipotético caso donde un usuario (EMPRESA B) es afectado por las consecuencias de un ataque de *ransomware* que tuvo la organización (EMPRESA A) prestadora de algún tipo de servicio (públicos o privados).

Entre los posibles daños que sufre la EMPRESA B se podría mencionar la falta de disponibilidad en el servicio, la pérdida o daño de información de uso comercial, la divulgación de información confidencial, etc. En definitiva, consecuencias informáticas que a su vez se traducen en consecuencias de índole económico, cuya gravedad dependen del tipo de actividades que desarrolle la empresa -que podría ser desde una clínica que se queda sin acceso a información de salud de sus pacientes, una entidad bancaria que no puede operar, o un municipio que no puede prestar sus servicios básicos, hasta un estudio jurídico-contable cuyas operaciones confidenciales con sus clientes son divulgadas-.

Para avanzar en una primera respuesta, se debe revisar las obligaciones legales asumidas por parte de la organización, entre las que se pueden encontrar en primer lugar aquellas impuestas por Ley, y en un segundo escalón aquellas asumidas de forma voluntaria a través de un contrato (es posible que existan las segundas sin que existan las primeras).

Primero se debe analizar la existencia de obligaciones legales en materia de seguridad de la información, tales como podrían ser las establecidas por la [Ley N° 25.326 de Protección de Datos Personales \(Argentina\)](#), particularmente detalladas en la Resolución 47/2018. Otro ejemplo de normativa que establece obligaciones en materia de seguridad de la información, es la [Comunicación "A" 4609](#) del Banco Central de la República Argentina, aplicable para el caso de las entidades financieras. Aquellas organizaciones que han emprendido algún proyecto de seguridad de la información que tiene como modelo la Norma [ISO 27001](#), podrán encontrar que la principal tarea en el dominio de "*Compliance*" es precisamente la identificación de toda la normativa aplicable a la organización, respuesta que dependerá exclusivamente del tipo de organización, la actividad que desarrolle y las jurisdicciones aplicables.

En Estados Unidos se ha considerado las consecuencias del *ransomware* en el ámbito de la salud, donde la normativa aplicable ([HIPAA](#)) a este tipo de información establece obligaciones legales a tener en cuenta para estos casos. Existen incluso debates acerca si un ataque de *ransomware* generaría o no lo que la citada normativa considera como un *breach*, definido como "*...the acquisition, access, use, or disclosure of Personal Health Information (PHI) in a manner not permitted under the [HIPAA Privacy Rule] which compromises the*

security or privacy of the PHI. En general se entiende que el cifrado de la información como consecuencia de un ataque de *ransomware* implica un *breach*, toda vez que para que ello suceda, la PHI previamente tuvo que ser accedida por un tercero que no debería haber tenido ese control, generando así una divulgación -*disclosure*- no permitida por la [HIPAA Privacy Rule](#).

Saliendo de la primera categoría de normativas aplicables que, como ya se ha analizado, dependerá exclusivamente del país, del tipo de actividad desarrollada y en algunos casos del tipo de organización (pública o privada), existe una segunda categoría que podría ser fuente de obligaciones para la organización: aquellas obligaciones asumidas voluntariamente, en virtud de la celebración de algún contrato en las cuales la organización (EMPRESA A) se compromete a respetar determinados estándares mínimos de seguridad de la información, o en su caso, a mantener los servicios en un nivel mínimo de prestación (generalmente a través de los SLA).

Si se observa con detalle, en la mayoría de los contratos de prestación de servicios de información, se pueden encontrar cláusulas relacionadas a las obligaciones asumidas en materia de seguridad de la información, como estos ejemplos:

- [Cláusula de Seguridad en AWS Amazon](#): (3.1 Seguridad de AWS). Sin limitación a lo dispuesto en la Sección 10 o a sus obligaciones contenidas en la Sección 4.2, implementaremos medidas adecuadas y razonables diseñados para ayudarle a asegurar Su Contenido contra pérdida, acceso o revelación accidental o ilícita.
- [Cláusula de Seguridad de Netflix](#): Contamos con medidas administrativas, logísticas, físicas y de gestión razonables para proteger su información personal contra pérdidas, robos y acceso no autorizado, uso y modificación. Lamentablemente, ningún sistema de seguridad es 100% seguro. De acuerdo con esto, no podemos garantizar la seguridad de su información.

Como se puede observar, la obligación de seguridad de la empresa proveedora (EMPRESA A) es la de **implementar medidas de seguridad razonables y adecuadas** para proteger la información del cliente (EMPRESA B). Desde este punto, y considerando el hipotético caso que la EMPRESA A ha sido víctima de un ataque de *ransomware* que afecta los intereses y provoca daños en la EMPRESA B, volvemos a realizar la pregunta que dio comienzo a esta sección: ***¿Es responsable la EMPRESA A por los daños ocasionados?***

El principio de respuesta a la misma, da lugar a un nuevo interrogante de segundo grado: ***¿Puede demostrar y probar la EMPRESA A que ha sido diligente en el tratamiento de la información, adoptando todas las medidas de seguridad adecuadas y razonables para evitar recibir un incidente de seguridad***

de esta magnitud (ransomware)? Incluso cabría preguntarse si en el estado actual de la seguridad de la información: ¿es posible considerar que una organización ha tomado medidas de seguridad razonables y aun así ha sido víctima de un ataque de *ransomware*?

Con la intención de no extendernos demasiado, se puede concluir en la importancia cada vez mayor que tiene a nivel mundial el concepto de **diligencia debida** en el cuidado y el tratamiento de la información, de forma que ante un incidente de seguridad (filtración, pérdidas o daños en la información), aquella organización que quiera evitar algún grado de responsabilidad civil, deberá acreditar, con la correspondiente documentación en materia de seguridad, así como la prueba de la existencia en los controles implementados, que existió un obrar de forma diligente y que se habían tomado medidas de seguridad adecuadas y razonables para esa información.

Conclusión

El *ransomware*, ha sido el protagonista de los últimos 3 años y probablemente, también lo sea en 2019.

Como se ha desarrollado durante el presente, del lado defensivo, técnicamente no es tan sencillo. Hay que implementar una estrategia de seguridad en capas progresiva de manera que el impacto para el normal funcionamiento de la organización sea lo más tenue posible.

Otro punto fundamental, que aún no estamos acostumbrados a identificar, es el tema legal que implican este tipo de ataques. Ser conscientes de las implicancias penales y civiles, es de suma importancia para estar al tanto de la situación actual en Argentina y cómo podría impactar a las partes involucradas.

Finalmente, desde nuestro lugar, queremos aportar nuestro granito de arena a la comunidad para ayudarlos a prevenir infecciones, con el objeto de disminuir la cantidad de casos y combatir entre todos al *ransomware*.

El presente trabajo ha sido desarrollado con el objetivo de brindar a la comunidad una guía simple a seguir a la hora de enfrentar la problemática del *ransomware*.

Todos los puntos de esta guía han sido resumidos y redactados en un lenguaje lo más simple posible, de manera que la misma pueda ser leída de manera fluida y con un tiempo de lectura mínimo.