MARSH

# ¿Está siendo víctima de un ransomware? Cómo prepararse ante esta situación

La transformación tecnológica va a un ritmo vertiginoso y está modificando drásticamente el entorno empresarial global. Este crecimiento también aumenta la exposición al riesgo relacionado con la tecnología y la ciberseguridad. Esto deriva irremediablemente a pérdidas económicas, en ocasiones notables. La última investigación de Marsh al respecto se presentó en el informe *The Changing Face of Cyber Claims*, que aprovecha el conocimiento recopilado de los datos de reclamaciones de Marsh Continental Europe, la experiencia y el conocimiento de Wavestone y CMS, para examinar formas prácticas de gestionar y mitigar tanto los riesgos como las reclamaciones ciber, incluyendo **profundos y detallados análisis de ransomware.**

La dilatada experiencia en este campo sitúa a Marsh en posición de **ofrecer las mejores prácticas para ayudar a las empresas** a **comprender, medir y gestionar** el riesgo de ser víctima de un ransomware.

## 1. Conocimiento: ¿de qué estamos hablando?

Los ataques ransomware tienen como objetivo secuestrar los datos y equipos de una empresa cifrándolos (imposibilitando el acceso si no se dispone de la contraseña para descifrarlos) y, de este modo, extorsionar a la víctima pidiendo un pago de rescate a cambio. Este tipo de ataque se ha vuelto muy popular en todo el mundo.

En 2019, registramos un aumento del 100% en los ataques de ransomware en toda nuestra cartera europea de reclamaciones ciber. Y este aumento se debe en parte, a que hace unos años el conocimiento para realizar estos ataques quedaba reducido en unos pocos, pero actualmente, es alarmantemente preocupante la sencillez con la que se puede comprar un ransomware en la Deep Web por un precio similar al de un desayuno en una cafetería.

Los ataques son cada vez más **frecuentes,** ayudados por nuevas tipologías de ransomwares y malwares

La **severidad** de los incidentes está aumentando drásticamente, afectando a la actividad operacional y resultados financieros: solicitud de rescates, gastos asociados, tiempo inoperativo... están incrementándose exponencialmente.

El teletrabajo se ha convertido en el objetivo del phishing con el envío de emails con **contenido relacionado con el COVID19.**

Con el incremento de trabajadores teletrabajando en **entornos menos seguros en materia de ciberseguridad**, los ataques son cada vez más exitosos.

Según el análisis de siniestros realizado por Marsh, el **67% de los ataques son maliciosos.**

El número de siniestros declarados de tipo ransomware se **duplicó** durante el 2019.


La duración media de una **interrupción de actividad** derivada de un ciber **ataque básico** es de hasta **1 semana hasta la recuperación completa** de la actividad.

La interrupción derivada de un **ciber ataque sofisticado** puede ser de **3-4 semanas** hasta que se restauran los sistemas principales y de **6 semanas** hasta que se recuperan los datos.

FUENTE: The Changing Face of Cyber Claims 2020

MARSH & McLENNAN COMPANIES

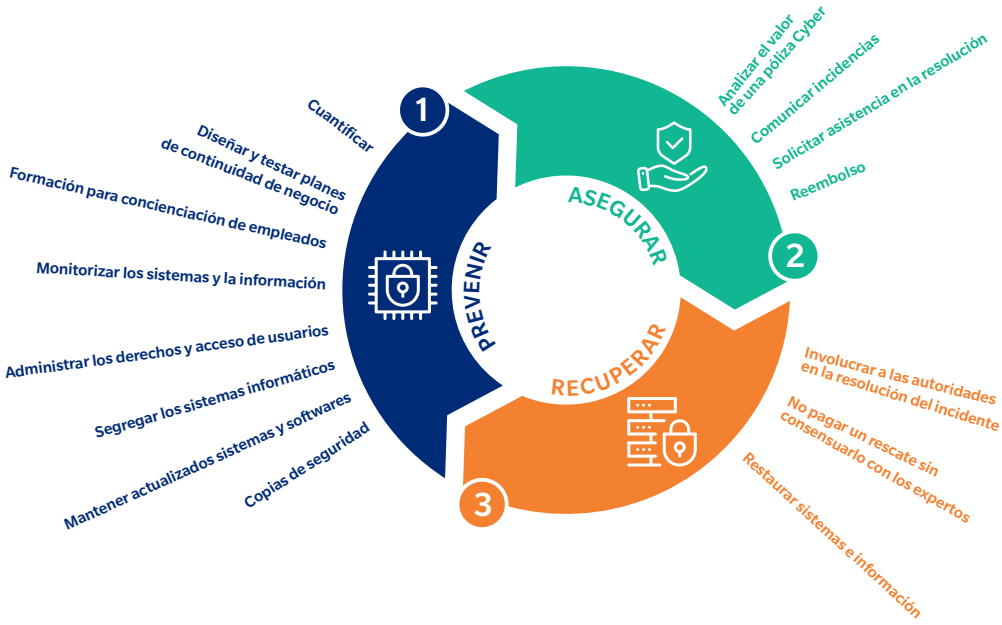
## 2. Valoración: Cuál es el precio de sufrir un ransomware

**Diferenciamos los ataques en dos:**

- **Ransomware no dirigido**. Enviado aleatoriamente a millones de direcciones de correo electrónico y principalmente golpeando a las pymes y a individuos. El mecanismo es sencillo y la cantidad del rescate no parece desorbitada (con un promedio de alrededor de 300 euros, en bitcoin) pero el retorno de la inversión para los atacantes es enorme, debido al alto número de víctimas que paga el rescate. El volumen por tanto, es la clave en este tipo de ataque.
- **Ransomware dirigido**. Estos ataques, mucho menos numerosos, son preparados con mucha antelación por los atacantes, por lo general gracias a la ingeniería social. Las grandes empresas son objetivo (> 500M de facturación) y los ciber criminales aprietan el gatillo en el peor momento posible para la empresa, buscando la máxima afectación en las operaciones. Estamos hablando de rescates de hasta varias docenas de millones de euros.

## 3. Gestión: prevenir, asegurar y recuperar

**El siguiente esquema puede ayudar a proteger sus activos de estas amenazas:**




### PREVENIR

**En este caso, prevenir es mejor que curar**

1. **Copias de seguridad:** el propósito de la mayoría de ransomware es evitar que acceda a sus datos y pagar por su recuperación. Es esencial para su negocio hacer copias de seguridad regulares y mantenerlas seguras. Revise periódicamente la información almacenada y la precisión del proceso de copias de seguridad y, guarde las copias en una unidad de almacenamiento no conectada a su red ordinaria.
2. **Mantener actualizado el software y los sistemas:** su sistema de información es vulnerable y sus puntos débiles son utilizados por los piratas informáticos para difundir el ransomware y cifrar sus datos. Al mantenerlos actualizados de forma constante, el nivel de seguridad global de su empresa aumenta notablemente.
3. **Segregar sistemas de información**: algunas partes de sus sistemas de datos e información son más críticas o sensibles que otras. Asegúrese de que estos elementos cuenten con medidas de seguridad adicionales.
4. **Administrar los derechos y el acceso de los usuarios**: no todos los empleados o terceros necesitan el mismo nivel de acceso en sus sistemas. La correcta gestión de cuentas y mantenimiento de las mismas es un factor clave.
5. **Supervisar su sistema y sus datos:** para que pueda detectar lo antes posible cualquier comportamiento anormal en sus sistemas, lo que significa tiempos de reacción más rápidos y una mayor prevención de daño.
6. **Aumentar la conciencia del personal:** haz de tus profesionales tu mejor defensa contra las amenazas. Entre un 20% y un 35% de los empleados caen en un phishing, y el atacante únicamente necesita que un único profesional abra el archivo malicioso. En general, queda un largo camino que recorrer en este aspecto y debe ser uno de los pilares de un plan de ciberseguridad.
7. **Diseñar y probar un plan de continuidad de negocio:** los ataques son desestabilizadores. No estar preparado significa fracasar: la mejor manera de lidiar con los ataques es preparándose, incluyendo la configuración de la planificación y los procedimientos de respuesta a incidentes. Pruebe el plan de continuidad de forma periódica, realice simulaciones de ataques y compruebe que su plan realmente le permitiría volver a la normalidad de sus operaciones.
8. **Cuantificar:** cuantifique su exposición al riesgo, averigüe cuánto podría costarle un ciberataque. Esto le ayudará a gestionar el riesgo en el comité ejecutivo justificando las inversiones que requiere el plan de mitigación para su empresa, así como una transferencia del riesgo residual a terceros.

## ASEGURAR

**Para ayudarle a superar una crisis y apoyar su recuperación financiera**

1. **Evaluar el valor sel seguro ciber:** el seguro ciber puede ofrecerle asistencia rápida durante y después del ataque, y también buscar una compensación por sus pérdidas financieras.
2. **Comunicación:** después de un evento de seguridad, las empresas necesitan recuperar la confianza de sus clientes, empleados y socios. Los especialistas en ciberseguridad cuentan con el expertise para ayudarle a reconstruir una reputación sólida.
3. **Obtenga asistencia:** muchas empresas no tienen los recursos internos ni la experiencia necesaria para gestionar un incidente de seguridad. Los proveedores de servicios especializados le ayudan a minimizar los daños y a volver a sus negocios lo más rápido posible. El análisis forense puede ayudarle a comprender la causa raíz de por qué el ataque tuvo éxito, tomar las medidas adecuadas para recuperarse y también ayudarle a estar más preparado en el futuro.
4. **Recibir un reembolso:** el seguro de ciberseguridad mitigará el impacto en el balance de pérdidas y ganancias de una empresa. Puede ayudarle a evitar una falta de beneficios o incluso la bancarrota en el caso de afectaciones graves.

## RECUPERAR

**¡Mejore de forma constante!**

1. **Involucrar a la autoridades pertinentes:** pueden ayudarle a investigar y recuperarse de un incidente. La mayoría de nuestros clientes en esa situación se han movido en esa dirección.
2. **No pague un rescate antes de escuchar a los expertos:** no hay garantía de que los criminales entregarán la clave del cifrado en caso de que realice el pago – ¡No olvidemos que son ladrones después de todo! Además, si se considera que su organización está dispuesta a pagar, probablemente fomentará más ataques, ya sea por el mismo grupo u otros, y serán aún más sofisticados.
3. **Restaure sus sitemas y datos:** lo mejor es restaurar su sistema y datos de fuentes de confianza y actualizar sus contraseñas. Es esencial comprobar que los datos que restaura son integros. Manténgase informado para asegurarse de que se encuentra en la mejor posición posible: puede obtener nuestros comentarios sobre las reclamaciones que hemos manejado este año consultando nuestro informe Changing Face of Cyber Claims, que recopila datos de toda Europa Continental.

Manténgase informado para asegurarse de que se encuentra en la mejor posición posible: puede leer nuestros comentarios sobre las reclamaciones que hemos gestionado este año, consultando nuestro informe *Changing Face of Cyber Claims*, que recopila datos de Europa Continental.

Para más información sobre seguros cibernéticos y otras soluciones de Marsh, visite marsh.com o póngase en contacto con:

**SARA MUÑOZ**
Technology & Cyber
Insurance Leader
sara.munozrubio@marsh.com

**NELIA ARGAZ**
Business Resilience & Cybersecurity
Consulting Practice Leader
nelia.argaz@marsh.com

### SOBRE MARSH

Marsh es el líder global en consultoría de riesgos y correduría de seguros. Con más de 35.000 empleados que trabajan en equipo para dar servicio a sus clientes en más de 130 países, Marsh ofrece a clientes comerciales e individuales, soluciones de riesgo basadas en el análisis de datos y servicios de asesoramiento.

Pertenece al Grupo Marsh & McLennan Companies (NSYE: MMC), un equipo global de empresas de servicios profesionales, que ofrece a sus clientes asesoramiento y soluciones de riesgo, estrategia y capital humano. Con unos ingresos anuales cercanos a los 17.000 millones de dólares y 76.000 empleados en todo el mundo, Marsh & McLennan Companies ayuda a sus clientes a navegar en un entorno cada vez más dinámico y complejo a través de cuatro empresas líderes en el mercado: Marsh, Guy Carpenter, Mercer y Oliver Wyman.

Síganos en Twitter @ MarshGlobal, en LinkedIn; Facebook YouTube o suscríbase a BRINK.