MARSH

ENCUESTA DE RIESGO CIBERNÉTICO ARGENTINA 2020

REPORTE DE CORTESÍA

MARSH & McLENNAN COMPANIES

El riesgo cibernético ha pasado del robo de datos y la preocupación por la privacidad a esquemas más sofisticados que pueden interrumpir la operación en empresas, industrias, cadenas de suministro y naciones, costándole a la economía miles de millones de dólares en cada sector.

Y la crisis por el COVID-19 ha puesto en cuarentena a prácticamente todos los países, llevando a los sistemas de salud al límite y generado que la economía mundial haya entrado en una recesión sin precedentes.

Análisis

A pesar de que el Riesgo Cibernético se ha vuelto más complejo y desafiante a raíz de la pandemia, los resultados de la encuesta muestran que algunas empresas son conscientes del incremento en los ciberataques y, en algunos casos, han realizado esfuerzos adicionales.

No obstante, se siguen observando empresas en las que esta situación no se ha manifestado aún. Esta situación podría deberse en parte a una cuestión presupuestaria, aunque también a la falta de mecanismos y procedimientos necesarios para detectar situaciones sospechosas que puedan sugerir un ataque, de manera oportuna.

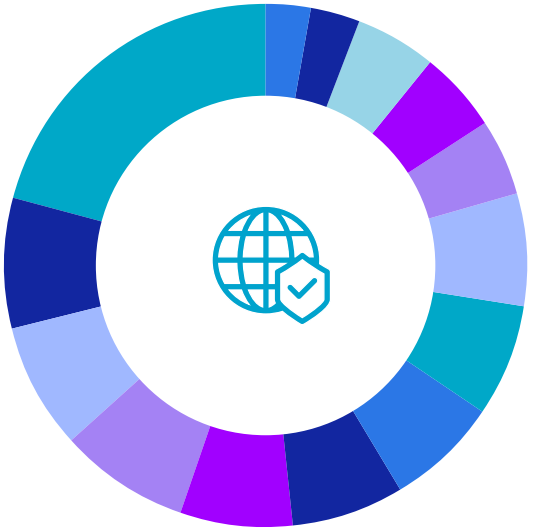
Se observa un bajo nivel de adopción del seguro de Riesgo Cibernético como un medio para transferir este tipo de riesgos. Con el paso de la pandemia han cambiado su percepción sobre la posibilidad de adquirir uno.

Las compañías han reevaluado sus prioridades de ciberseguridad con el fin de enfocar sus esfuerzos en implementar controles para mejorar la protección de datos, la seguridad de acceso remoto, la continuidad del negocio y la concientización en seguridad.

Encuesta Argentina

56% De las empresas facturan más de USD20 millones al año

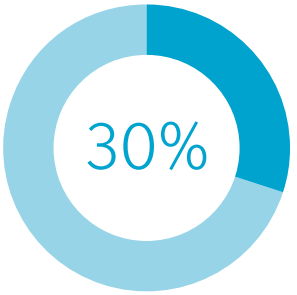
Distribución por actividad:



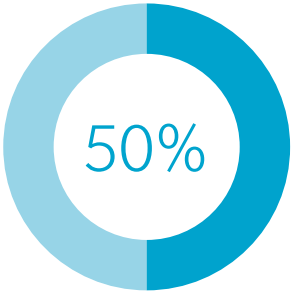
- **3%** Fundación | Institución educativa
- **3%** Minería
- **5%** Energía
- **5%** Logística y Transporte
- **5%** Química
- **7%** Alimentos y bebidas
- **7%** Construcción
- **7%** Farma | Laboratorio
- **7%** Petróleo y Gas
- **7%** Minoristas y mayoristas
- **8%** Agricultura
- **8%** Comunicaciones, Media y Tecnología
- **8%** Metalúrgica
- **21%** Otros

Prevalencias Argentina

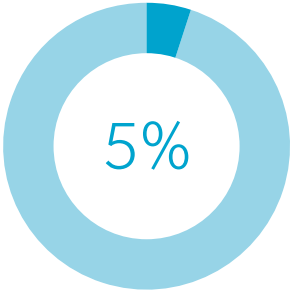
De las empresas encuestadas que reconocen una alta dependencia a la tecnología, nos encontramos con que:



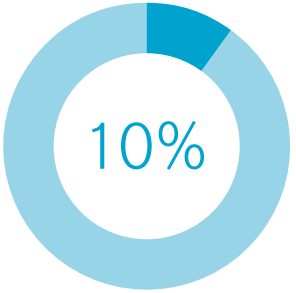
Posee un plan de respuesta a incidentes cibernéticos



Desconoce el impacto financiero de un evento cibernético



Contrata un seguro de Cyber



Percibe un incremento en ciberataques durante la pandemia

Recomendaciones ante el Riesgo Cibernético

Christian Rada
Especialista en riesgos Cibernéticos
Marsh Argentina

Edson Villar
Líder de consultoría de riesgos en
Marsh Latinoamérica

Un análisis post pandemia

Los atacantes aprovechan nuestra mayor dependencia de las herramientas digitales durante el aislamiento social y la incertidumbre de esta crisis. En tiempos como los actuales, todos los integrantes de una familia pasan más tiempo conectados ya sea para trabajar remotamente, estar informados, entretenidos (descarga de streaming), conectarse con amigos o tomar clases virtuales, así como para jugar en red o en las redes sociales. Las empresas y organizaciones del sector público y privado combinan políticas de teletrabajo con trabajo presencial, y muchas interacciones laborales se están dando a través de videollamadas y chats. El aislamiento y distanciamiento social exponen a las personas a pasar más tiempo online, corriendo el riesgo de caer en el acceso "gratuito" a sitios web o ingresar en enlaces equivocados donde se abren las puertas a posibles ataques, solicitudes de información de tarjetas de crédito o la instalación de aplicaciones de visualización.

En el caso de personas conectadas desde su casa, la exposición es mayor porque en muchos casos no cuentan con medidas de seguridad tan controladas como tienen en la oficina. Las empresas están en riesgo si los empleados no tienen la capacitación y concientización necesaria sobre las precauciones que deben tomar o cómo se debe trabajar. Si bien las empresas están implementando adecuadas medidas de seguridad, las Pymes representan un objetivo muy buscado por los hackers, ya que no cuentan con tantos recursos y presentan pocas herramientas de protección, corriendo el riesgo que sus empleados sean víctimas de phishing, que se produce cuando acceden a algún correo que no debían atender, o activan un enlace que descarga un malware o ransomware.

Los ataques cibernéticos no descansan

Los ataques más comunes son el Phishing, Malware, Social Engineering y Denial of Services.

En los ataques de Phishing los ciberdelincuentes crean cuentas de correo electrónico y páginas web que se mimetizan con las oficiales, lo que dificulta que los usuarios distingan entre la página segura y la creada para conseguir datos de forma fraudulenta. Hoy está muy de moda el phishing temático sobre COVID19.

Los ciberdelincuentes desarrollan webs creadas o campañas de sms que utilizan ganchos informativos sobre ayudas que se están poniendo en marcha desde las diferentes administraciones, sobre aspectos sanitarios suplantando entidades o directamente proponiendo al receptor del mensaje su colaboración en campañas de recaudación de fondos para luchar contra el COVID19. Por ejemplo simulan ser algún organismo de salud e incitan a los destinatarios de los correos a dar click en un link con la excusa de acceder a las nuevas indicaciones de salud y piden una donación, para robar dinero o información personal.

El malware o software malicioso es una categoría de software diseñado para infiltrarse y dañar un sistema de información sin ser detectado. Entre los malwares más utilizados, están los troyanos (programas diseñados para ingresar en los sistemas de seguridad y permitir el acceso a otros archivos maliciosos), los spyware (programas que espían un dispositivo para obtener información privada y que pueden instalar otros softwares maliciosos) y los ya famosos ransomwares, que secuestran la información de valor de un dispositivo, con el fin de solicitar una transferencia en criptomoneda o monedas digitales a modo de rescate.

- Por otro lado Social Engineering es cuando se explotan las vulnerabilidades humanas de los empleados para eludir las medidas de seguridad de una empresa y obtener datos confidenciales. Para los delincuentes cibernéticos estos métodos son relativamente rápidos y fáciles de implementar. Las técnicas de Social Engineering van desde la solicitud de ayuda, simular una urgencia y hasta la extorsión real.

- El uso de ataques Denial of Services por parte de los delincuentes cibernéticos intenta comprometer la accesibilidad de los servicios de Internet, como el acceso a un sitio web. La inaccesibilidad del sitio puede causar grandes pérdidas económicas a las empresas.

Cómo se previene ataques

Un buen paso inicial para entender este nuevo escenario consiste en validar si se han implementado las capacidades adecuadas y evaluar el nivel de madurez en términos de Ciberseguridad en la empresa, en base a un estándar. El National Institute of Standards and Technology (NIST) ha desarrollado un Marco de Trabajo de Ciberseguridad muy completo que orienta a las empresas en las capacidades que deberían tener para enfrentar los retos de Ciberseguridad y las estructura en cinco funciones clave:

1.Identificar: Identificación de los activos, capa de gobierno, y prácticas de gestión de ciber-riesgo en la organización y en la cadena de suministro.

2. Proteger: Procesos, tecnología y entrenamiento al personal, para que la organización pueda hacer frente a un ciber-incidente.

3.Detectar: Equipo, herramientas y procesos de detección de amenazas.
4.Responder: Capacidades para reaccionar frente a un ciberincidente de manera oportuna y con el menor impacto.
5.Recuperar: Procesos para la restauración de servicios afectados ante un ciberincidente, en los tiempos esperados.

Asimismo, existen tres puntos esenciales que los líderes de las organizaciones deben tener en cuenta al momento de elaborar una estrategia de ciberseguridad:

- Apoyo e involucramiento de la alta gerencia, y la participación de toda la organización.

- Conocimiento de los riesgos y el nivel de exposición.

- Siempre orientar las acciones teniendo como premisa que un ciberincidente es inminente.

Esto permitirá a las organizaciones incorporar las capacidades más importantes en el momento correcto y hacer frente a las ciberamenazas que acechan hoy en día.

- Se pueden realizar acciones preventivas para mitigar el riesgo de un ataque siguiendo las siguientes recomendaciones:

- Proteger con antivirus y actualizar el sistema de los equipos que se tenga en casa o en la oficina.

- Utilizar contraseñas fuertes combinando números, letras mayúsculas, minúsculas y símbolos.

- Utilizar protocolos de seguridad.

- Concientizar y capacitar a los empleados en seguridad informática.

- Comprobar la autenticidad de enlaces y perfiles. Es muy común sufrir ataques a través de phishing mediante el cual se intenta adquirir información confidencial de forma fraudulenta, normalmente a través del email. Hoy en día en las redes sociales se crean perfiles falsos para captar estos datos, sobre todo por medio de cuentas no oficiales de empresas con el fin de engañar.

- Evitar dar datos personales en cualquier tipo de página web que no sea confiable.

- No descargar contenido pirata en la red ya que podrían ser una fuente de introducir programas maliciosos en el sistema y así poder realizar un ataque. Aunque la descarga sea legal es necesario comprobar previamente que el sitio web no es sospechoso.

- Realizar una copia de seguridad para poder recuperar la información pérdida ante un ataque.

- No hacer click en enlaces que resulten sospechosos.

- Desconfiar los correos de remitentes desconocidos y en todo caso no responder, eliminarlos o enviarlos al departamento de seguridad informática.

1 EL RANSOMWARE

El ransomware, ha sido una amenaza que ha venido afectando al mundo satisfactoriamente desde el año 2005.

2 SOFTWARE MALICIOSO

Este tipo de software malicioso, cifra o encripta los archivos de un equipo para posteriormente pedir un rescate para la devolución de la información.

3 SOFISTICACIÓN Y AGRESIVIDAD

En los últimos años se ha podido observar un incremento en el nivel de sofisticación y agresividad de estas amenazas.

4 IDENTIFICACIÓN DE MALWARE

Aproximadamente **1 de cada 3** muestras de malware identificadas en 2018, tenían como objetivo el cifrado de equipos para el posterior cobro de extorsiones.

5 ¿CÓMO FUNCIONA UN ATAQUE DE RANSOMWARE?

El usuario recibe un correo electrónico que solicita descargar el software malicioso. 92% de los casos de malware es entregado a través de correo electrónico.

Un usuario dentro de la red ejecuta el software malicioso que recibió en el correo electrónico. El malware cifra los archivos en la PC infectada y exige el pago de un rescate para que el usuario pueda recuperarlos.

En algunos casos, el ransomware aprovecha vulnerabilidades en los sistemas para reproducirse por la red y afectar a otros equipos, e incluso a terceros interconectados. 57% de las brechas de datos se ejecutaron debido a falta de actualizaciones de vulnerabilidades conocidas.

¿CÓMO PODEMOS RESOLVERLO?

ENTENDIMIENTO

- Evaluación de ciber-riesgos.
- Análisis de madurez y cumplimiento.
- Asesoría estratégica en la gestión del ciber-riesgo.

CUANTIFICACIÓN

- Análisis de la susceptabilidad a un ciberataque.
- Estimación analítica del costo de una brecha de datos.
- Cuantificación del impacto de una brecha de seguridad.

GESTIÓN

- Definición de la estrategia de ciberseguridad.
- Desarrollo de planes de respuesta ante ciberincidentes.
- Simulación de escenarios de ciber-crisis.
- **Asesoría para adquisición de Seguro Cyber.**

MARSH

MARSH & McLENNAN COMPANIES