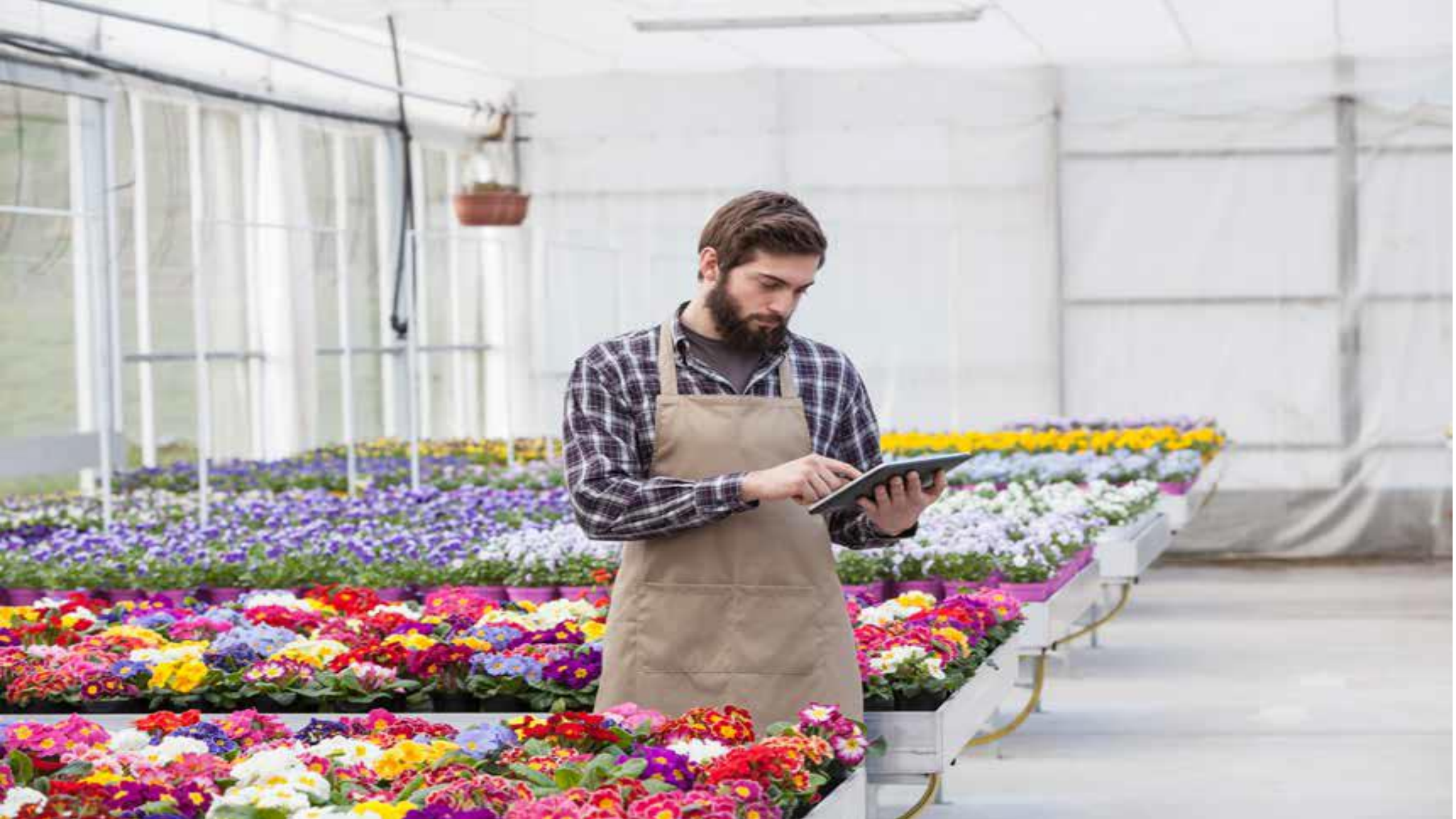


Pymes: en la mira de los ciberdelincuentes

El acelerado desarrollo de las tecnologías de la información y la comunicación que se ha dado en las últimas décadas, ha multiplicado las alternativas de interacción y conexión entre las personas y su entorno, masificando el uso de dispositivos que permiten enviar y recibir información de manera inmediata y en tiempo real.

Las empresas no son ajenas a esta realidad: hoy los negocios se realizan en el ecosistema digital y global. A través del ciberespacio viajan datos fundamentales para la operación de las compañías y en los servidores, los data centers y en la nube se almacena información confidencial. Esto incentiva la competitividad entre las empresas.

Un ejemplo de un ecosistema digital es internet. Esta tecnología se ha convertido en una herramienta imprescindible para las empresas del mundo en cualquier campo de acción. Se ha transformado en un espacio muy útil para ampliar los mercados, estar en comunicación permanente con las personas, almacenar información y recolectar los datos personales de clientes actuales y potenciales.

Sin embargo, la actividad en la red conlleva riesgos, como el cibernético, que aumenta en la medida en que se descubren novedosas formas de vulnerar la información.

¿Qué es el riesgo **cibernético?**

El riesgo cibernético se refiere a cualquier riesgo que proviene del uso de información electrónica y su transmisión, incluye el daño físico que puede ser causado, el fraude cometido por el robo de información, cualquier responsabilidad proveniente del almacenamiento, disponibilidad, integridad y confidencialidad de datos, la cual normalmente se encuentra relacionado con individuos, compañías o el mismo gobierno

Las causas de este riesgo van desde los ataques cibernéticos, los virus informáticos y los correos malintencionados, hasta los errores humanos, los empleados que buscan recibir beneficios de manera fraudulenta, el uso inadecuado de información por parte de los proveedores, entre otros.

Los riesgos cibernéticos no solo se suscriben a amenazas tecnológicas o a objetivos de los ciberdelincuentes. Su materialización no siempre pretende generar este tipo de impactos u obtener beneficios económicos o financieros. Algunos ataques son motivados, por ejemplo, por un acto de venganza, por despedir a un empleado, la emoción de causar daños o el reto personal e intelectual de un ataque exitoso.

¿Cómo se ve afectada una pyme por un ciberataque?

Las pequeñas y medianas empresas son una parte importante de la infraestructura económica y cibernética de los países. Sin embargo, para algunas, la seguridad de su información, sistemas y redes, no es su principal prioridad. Generalmente, no cuentan con los recursos para invertir en seguridad de la información de la misma forma en que las empresas más grandes pueden hacerlo, lo que las hace más vulnerables a los ciberdelincuentes.

En este sentido, las pymes se pueden ver afectadas por un evento cibernético de varias formas:

- Perder dinero.
- Servir de acceso a objetivos más destacados por medio de su rol o sus productos y servicios en una cadena de suministro.
- Perder información crítica para administrar su negocio.
- Sufrir daños reputacionales que afecten la confianza de sus clientes.
- Perder ingresos como consecuencia de la interrupción de su actividad.
- Recibir sanciones de entes de control y vigilancia como consecuencia del mal uso de la información.
- Ser demandadas o recibir reclamaciones por parte de personas afectadas debido al mal uso de la información.

Los anteriores ejemplos son la evidencia de que un incidente de seguridad de la información puede ser perjudicial para clientes, empleados, socios, proveedores e, incluso, puede afectar la continuidad de las pymes.

Estas son algunas cifras globales que muestran como los cibercriminales están atacando a las organizaciones menos protegidas:

58 % de las víctimas de ataques de *malware* están categorizados como pymes y el **92.4 %** de estos ataques se reciben vía correo electrónico.

En el 2017 los ciberataques representaron al segmento pymes un impacto promedio de USD **$ 2,235,000**.

60 % de empresas pymes del mundo indican que los ciberataques están siendo más severos y cada vez más sofisticados.

1 de cada 5 pymes es víctima de delitos cibernéticos.

Casos reales

1 Ataque con *ransomware*

Un bufete de abogados en España fue atacado con un ransomware: este es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de quitar esta restricción.

Los socios del bufete, para cuidar su reputación y la información propia y de sus clientes, enviaron un comunicado a sus usuarios en el que les contaban que habían sido víctimas de un ciberataque que podría comprometer los datos de sus clientes y proveedores. Además, les pidieron que si recibían algún mensaje sospechoso en relación con su firma de abogados, bien por contenido o por su remitente, ignoraran cualquier hipervínculo insertado en el mismo y los pusieran en conocimiento con la mayor brevedad.

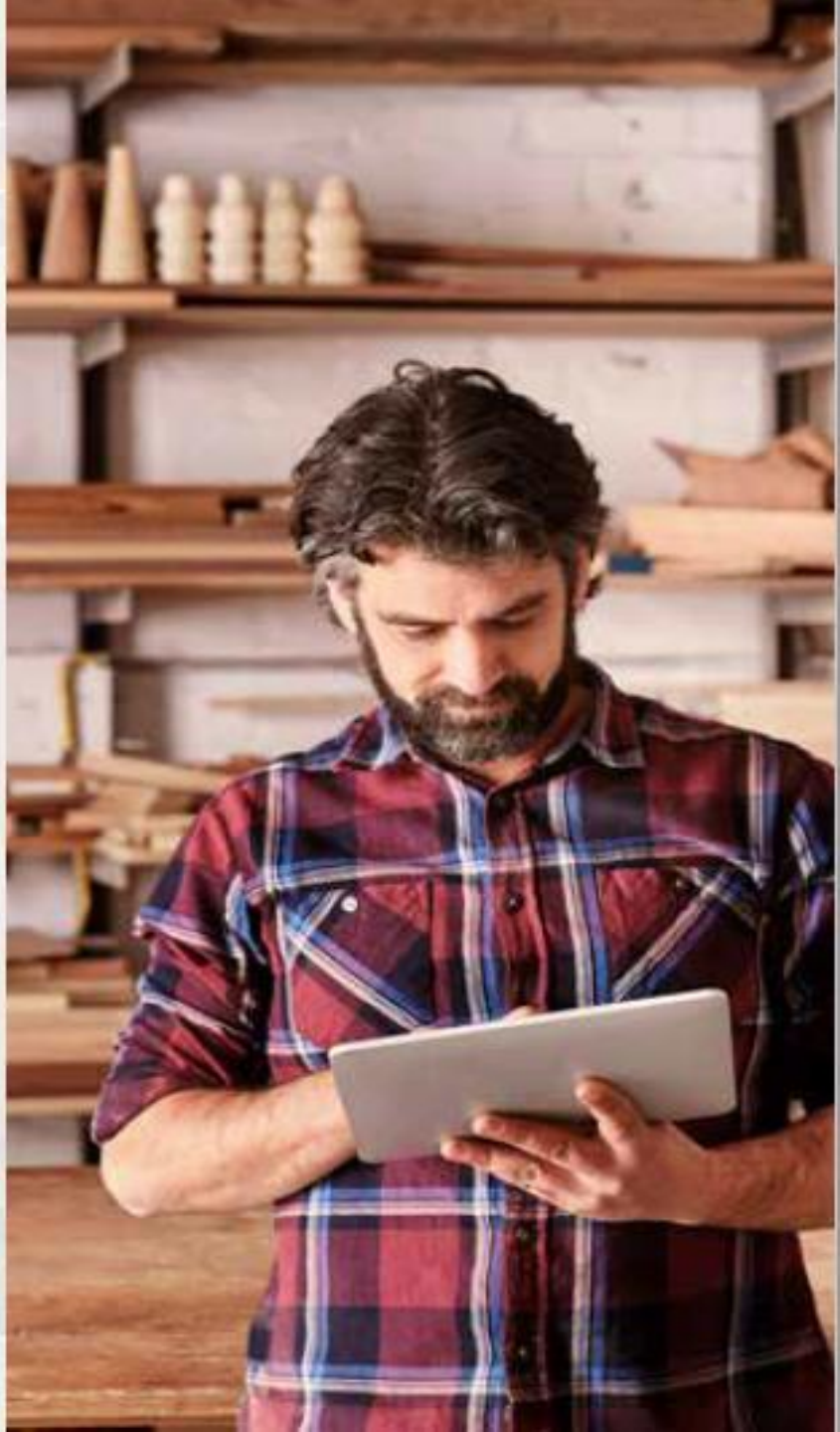
https://cincodias.elpais.com/cincodias/2017/11/02/legal/1509643523_493854.html

2 Pérdida de información por un virus informático

Afixcal es una pyme especializada en asesoría fiscal, contable, laboral y legal que sufrió un ciberataque en 2015: un virus se infiltró en su servidor y provocó la pérdida de los datos de más de 200 clientes.

El virus entró en un PDF remitido por un desconocido. Este archivo se abrió desde uno de los ordenadores de la empresa y de ahí pasó a todo el servidor. El resultado: se perdieron los datos de los clientes en los que la empresa había estado meses trabajando.

El dueño de la empresa afirma que con un simple virus se pueden perder años de trabajo en minutos. En este caso, tuvieron la suerte de rehacer todo el trabajo antes de la presentación de impuestos. En el caso contrario, más que el daño por la pérdida de información, tendrían que afrontar el cobro de las sanciones por no presentar los impuestos de todos sus clientes a tiempo. Esto les hubiera costado $75 000 euros en multas más $50 000 euros adicionales, valor del salario de los empleados que tendrían que volver a realizar el trabajo.



A esto se hubiera sumado la posible pérdida de clientes potenciales quienes, al enterarse de la situación, podrían buscar la asesoría de otra empresa.

https://www.reasonwhy.es/actualidad/digital/la-pyme-esta-preocupada-por-los-ciberataques-2017-05-15

3 Bases de datos infectadas con *malware*

Rokenbok Education es una empresa de juguetes en Estados Unidos que sufrió un ataque mientras se acercaba la temporada navideña: sus bases de datos fueron infectadas con un *malware*. Los ciberdelincuentes encriptaron los archivos de la empresa y les pidieron a sus dueños mucho dinero a cambio de devolverles el acceso. La empresa, que se dedica a los juegos basados en robótica y construcción, perdió miles de dólares en ventas durante dos días. Lo peor de todo es que este no era el primer ataque que recibían: la empresa ya se había visto afectada por un ataque de negación de servicio que tumbó su sitio web.

Su director afirma que las compañías pequeñas suelen enfocarse más en los ingresos que en la protección y eso es un gran riesgo: reducen el presupuesto de seguridad, sus sistemas son obsoletos o cuentan empleados negligentes. Todo esto es explotado por los ciberdelincuentes, quienes cada vez realizan ataques más sofisticados.

Rokenbok Education, en vez de pagar el rescate, reconstruyó sus sistemas clave por medio de un proceso que duró cuatro días.

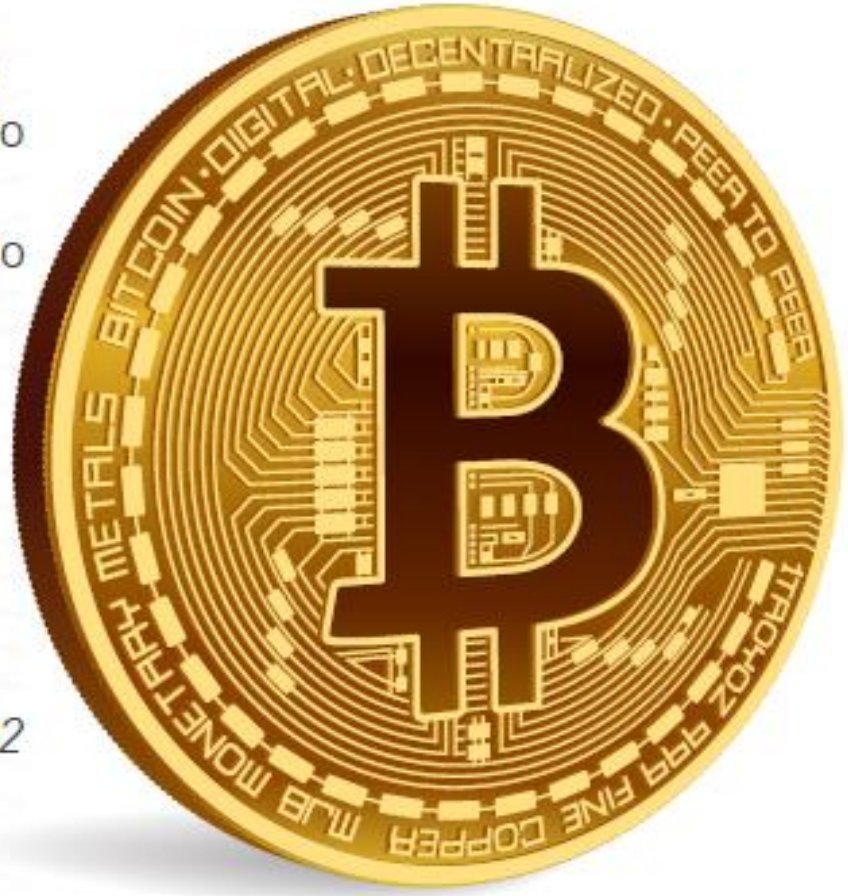
https://www.nytimes.com/es/2016/01/28/las-empresas-pequenas-tambien-pueden-ser-hackeadas/

4 Extorsión cibernética

Un director técnico de Barcelona, dueño de una pyme, sufrió una extorsión cibernética de la que pudo librarse pagando. Lo primero que vio en su pantalla fue un mensaje de los ciber delincuentes en el que le indicaban que sus datos habían sido encriptados y que para recuperarlos tenía que hacer una transferencia en bitcoins.

El director técnico tuvo que desembolsar $2744 euros a los delincuentes en la red, a pesar de que la Policía le aconsejó denunciar y nunca pagar.

https://elpais.com/internacional/2017/05/13/actualidad/1494682135_104939.html



Con tu seguro de protección digital podrías respaldarte a través de las siguientes coberturas

sura
SEGUROS, TENDENCIAS Y RIESGOS

Protección Digital

Asistencia

Pérdidas propias

- Recuperación de activos digitales
- Interrupción del negocio
- Extorsión cibernética
- Transacciones electrónicas

Responsabilidad Civil

- Responsabilidad por violación de privacidad o confidencialidad
- Responsabilidad por virus informático
- Responsabilidad por publicación de contenido digital

Manejo de crisis

- Gastos forenses
- Protección de la reputación
- Gastos de investigación oficial
- Gastos de defensa
- Gastos de emergencia
- Op: Gastos de notificación y monitoreo

Bibliografía y referencias

- “Verizon Data Breach Investigations Report” del 2018
- Ponemon Institute sobre el estado de ciber seguridad en Pymes del 2017.
- IRM Cyber Risk Executive Summary. The Institute of Risk Management. 2014
- Small Business Information Security: The Fundamentals. National Institute of Standards and Technology. Celina Paulsen / Patricia Toth. 2016
- https://gestion.pe/tecnologia/cinco-pymes-victima-delitos-ciberneticos-microsoft-73780

Si estas interesado conocer mas acerca de la solución de protección digital que ofrecemos, déjanos tus datos:

https://forms.office.com/r/dtT7dU13g1

Si tienes dudas adicionales sobre esta y otras soluciones puedes contactar a:

Guillaume Emmanuel Fernandes
Cel:3185363684
Asesor de Seguros Sura