E-book

Microsoft Security

Los 4 mayores riesgos de ciberseguridad en una PyME

La importancia de una protección 360°

¿Por qué la seguridad es importante para las PyMEs?

La mayoría de las empresas latinoamericanas coincide en que la ciberseguridad es una preocupación y una prioridad para su negocio. **La sofisticación y los tipos de ciberataques están evolucionando a un ritmo rápido. Los ataques cibernéticos son cada vez más populares y las soluciones de antivirus del pasado no suelen ser suficientes para proteger la totalidad del negocio ante esta nueva realidad.**

Si bien muchas pequeñas y medianas empresas toman medidas para asegurar su negocio como políticas, entrenamientos y gestión centralizada, el 37% de las empresas ha experimentado algún problema de ciberseguridad a lo largo de su existencia[1].

De allí que dar máxima prioridad a los temas de seguridad digital se vuelve clave para el éxito y el futuro de esas compañías, así como el de nuestra región: las PyMEs representan el 90% de las empresas de América Latina, generan más de la mitad de los empleos y una cuarta parte del PBI[1], son el motor de nuestra economía.

[1] El impacto del COVID-19 en la cultura y operación de las PyMEs de Latinoamérica

La tecnología juega un rol clave para prevenir las amenazas de ciberseguridad, detectar las brechas y recuperar los datos del negocio. No obstante, las personas que forman parte de la empresa deben conocer los riegos más comunes y contribuir a un negocio seguro.

Este e-book te invita a explorar - por medio de una narrativa que simula casos reales - qué caminos adoptar para asegurar la información en tu empresa. También busca enumerar la tecnología disponible, accesible para pequeñas y medianas empresas, que te ayudará a prevenir, mitigar y lidiar con un ataque cibernético. Aprende a proteger los datos y la infraestructura de tu negocio; y controla el acceso de los empleados y sus dispositivos.

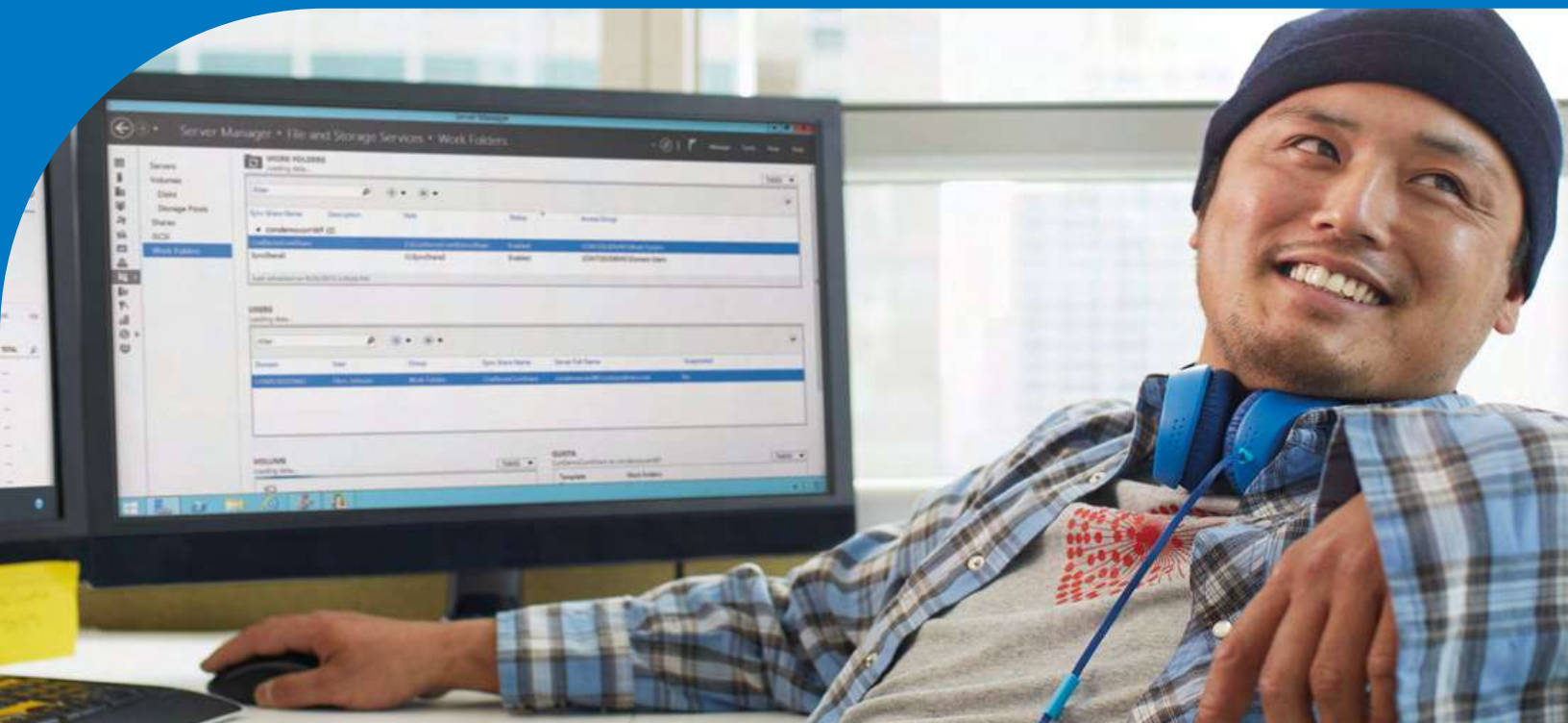
¡Conoce los riesgos más comunes de ciberseguridad de una PyME!

Riesgo 1

Protección de datos sensibles

Contoso es una PyME con tres años de experiencia. La empresa empezó con una sola persona, María Vázquez, CEO y fundadora, y hoy ya cuenta con 25 empleados.

Para celebrar el tercer aniversario de la compañía, se planeó durante meses el lanzamiento de un nuevo producto. Todos estaban muy entusiasmados por ver el resultado de este proyecto, pero, al guardar información confidencial en un archivo compartido sin tomar los cuidados necesarios, se filtraron las especificaciones técnicas del producto, y ahora corría el riesgo de caer en las manos de un competidor.



Riesgo 1

Protección de datos sensibles

¿Por qué sucedió?

Durante el fin de semana previo al lanzamiento, Fernando Rodríguez, uno de los gerentes responsables del proyecto, descargó una aplicación que contenía un troyano: un malware que permitió a un grupo de hackers navegar por la red corporativa y robar la información del archivo compartido. Como su contraseña era muy simple y no tenía protección para el acceso a la red de Contoso, dejó una inmensa brecha para que los criminales actuaran sin contratiempos.

¿Cómo podría haberse evitado?

Si Fernando Rodríguez hubiera escuchado los consejos y buenas prácticas del entrenamiento de seguridad impartido por Ariel Domínguez, director de TI de Contoso, que recomendó a todos los colaboradores que activaran en los archivos confidenciales **Azure Information Protection Premium P1** , los mecanismos de esta tecnología hubieran mitigado el ataque.

No solo eso: si Fernando hubiera adoptado una **contraseña más fuerte** y la hubiera **cambiado cada 90 días**, habría hecho más difícil la tarea de los cibercriminales.

Riesgo 2

Protección en la nube

María Vázquez, CEO de Contoso, hizo una reunión con todos los empleados de la empresa para prepararlos para una de las fechas más importantes del año: el Black Friday. Se esperaba que la compañía superara su récord de ventas del año pasado. Todos salieron muy animados con el desafío y trabajaron muy duro para preparar la plataforma de ventas... pero horas antes de que empezara el evento, el e-commerce de Contoso cayó y los nervios quedaron a flor de piel...

Riesgo 2

Protección en la nube

¿Por qué sucedió?

Ariel Domínguez, director de TI de Contoso, le recomendó a María un proveedor de nube poco confiable, que no contaba con las capas de seguridad necesarias para evitar caídas como esa. Por el Black Friday, un grupo de hackers infectó al servidor con un software malicioso. Eso hizo que no solo Contoso, sino una centena de clientes, quedaran sin acceso a sus plataformas de venta.

¿Cómo podría haberse evitado?

Si María hubiera seguido el consejo de Silvia Gutiérrez, programadora senior de Contoso, que durante la reunión del Black Friday sugirió la implementación de **Defender for Cloud**, -una solución de Microsoft - la empresa hubiera contado con una protección en la nube alineada a un sistema robusto de recuperación ante desastres. Esto los hubiera ayudado no solo a restablecer la plataforma, sino también hubiera evitado el ataque en primer lugar (con las herramientas de monitoreo que brinda la tecnología).

Riesgo 3

Protección de identidades

Guillermo Suárez, director financiero de Contoso, disfrutaba de sus vacaciones con su familia cuando recibió una llamada de María Vázquez. Le informaba de unas transacciones atípicas hechas por él durante la madrugada. Asustado, Guillermo contestó que no había sido responsable de ninguna operación financiera en los últimos diez días. María colgó la llamada, mientras Ariel Domínguez, director de TI de Contoso, informaba que la empresa podría haber sido víctima de un nuevo ataque de hackers...

Riesgo 3

Protección de identidades

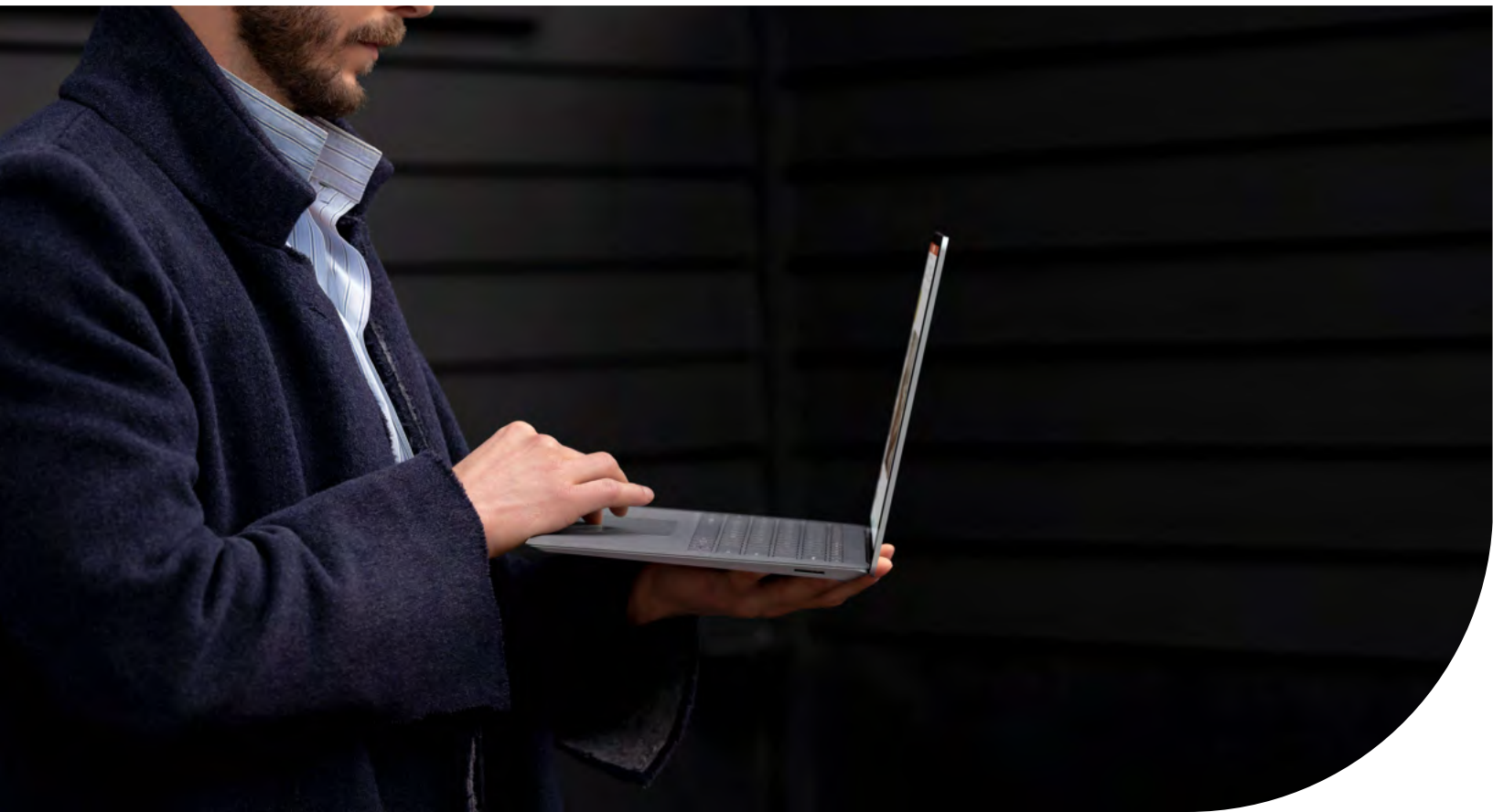
¿Por qué sucedió?

Luis Gómez, interno de Contoso hace dos meses, sufrió un ataque ransomware por correo electrónico con la técnica de phishing. Esto infectó su dispositivo y brindó acceso al sistema de la empresa.

Los hackers llegaron a las informaciones financieras de Guillermo Suárez, jefe inmediato de Luis, y utilizaron sus datos para transacciones bancarias.

¿Cómo podría haberse evitado?

Si Contoso hubiera contado con una estrategia Zero Trust, donde cada acceso es verificado en tiempo real, las identidades de ambos, Guillermo y Luis, hubieran estado protegidas al ser notificados del ataque a Luis de forma inmediata. Todo esto con **Azure Information Protection Premium P1**, incluido en la suite de **Microsoft 365 Business Premium**, esto habría detectado un acceso inusual desde sus usuarios y hubiera hecho bloqueos preventivos para evitarlo.



Riesgo 4

Protección de dispositivos

Todos llegaron a trabajar después de un feriado y fin de semana largo, pero al intentar abrir los archivos, estaban encriptados. Nadie logró iniciar sus tareas, y parecía que las energías recuperadas empezaban a desvanecerse. Otro día caótico en la vida de los empleados de Contoso...

Riesgo 4

Protección de dispositivos

¿Por qué sucedió?

Ana Ruíz, directora de Recursos Humanos, cambió su dispositivo antes del fin de semana y no siguió las políticas de la empresa, ni instaló debidamente las nuevas soluciones de seguridad. Esta brecha en la protección de su dispositivo hizo que todo el sistema de Contoso se viera afectado...

¿Cómo podría haberse evitado?

Si Ana hubiera seguido las políticas de seguridad e instalado la nueva solución de la empresa, **Microsoft Defender for Business**, como le recomendó Ariel Domínguez, este hubiera sido un día productivo de trabajo después de un poco de descanso.

Conclusiones y próximos pasos

Cuando se trata de defenderse de un ciberataque, las empresas deben considerar su patrimonio digital. Este incluye todos los activos que necesitan proteger y se ve un poco diferente de lo que era hace 5 o 10 años: ahora somos responsables de proteger un conjunto de tecnologías propias y ajenas, como por ejemplo los dispositivos móviles que son propiedad de los usuarios y acceden a los datos corporativos. Cualquiera de estos puede ser un punto de vulnerabilidad.

En temas de seguridad, ya no se puede establecer un perímetro alrededor de la organización, se debe pensar en vez, en prevenir, detectar y recuperar teniendo en cuenta el ecosistema completo. Adoptando una protección 360º que abarque la protección de identidades, datos, aplicaciones y dispositivos, ya sean locales, en la nube o en dispositivos móviles.

Microsoft Security