CYBER READINESS
INSTITUTE

La necesidad urgente de mejorar la preparación cibernética de las pequeñas y medianas empresas

Una propuesta para la Administración Biden

"A medida que el mundo se vuelve más dependiente e inmerso en la revolución informática, también se acelera el ritmo de las intrusiones, interrupciones, manipulaciones y robos. El avance tecnológico está sobrepasando la seguridad y seguirá haciéndolo si no cambiamos el modo en que afrontamos e implementamos las estrategias y prácticas de ciberseguridad. Los recientes ataques en los que dispositivos de consumo de uso habitual se pusieron en peligro por un uso maligno han dejado muy claro que ahora vivimos en un mundo mucho más interdependiente".

— Comisión para la mejora de la ciberseguridad nacional, Informe sobre la seguridad y el crecimiento de la economía digital, 1 de diciembre de 2016

Casi cinco años después, esas palabras siguen siendo ciertas. Continuamos atrapados en un horrible juego de Whack-A-Mole con nuestros enemigos cibernéticos. Pero ahora el entorno digital es más amplio y no sabemos dónde se producirá el próximo ciberataque. Lo que sí sabemos con certeza es que ocurrirá. El descubrimiento de las acciones de importantes enemigos, a través de los peligros de SolarWinds y Microsoft Exchange, se produce cuando salimos de un año de pandemia y de operaciones comerciales remotas que vieron un espectacular aumento de los ataques de ransomware contra hospitales, escuelas y otras infraestructuras esenciales. Nos encontramos en un punto de inflexión y existe la necesidad urgente de actuar.

info@cyberreadinessinstitute.org

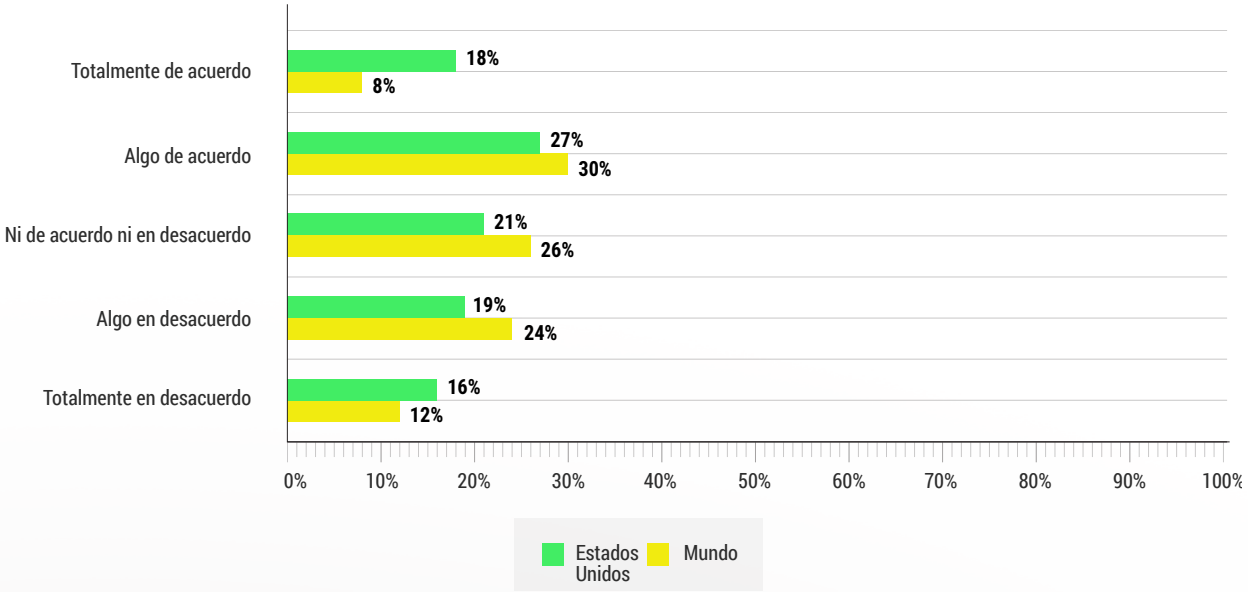
Los eventos SolarWinds y Microsoft Exchange, sorprendentemente expansivos y sofisticados, fueron solo síntomas de los desafíos a los que nos enfrentamos. Las medidas correctivas, por ejemplo, actualizar y parchear nuestro software, cambiar las contraseñas y eliminar el código maligno no son suficientes. Debemos reconocer y solucionar nuestra incapacidad de promover comportamientos seguros e implementar las políticas necesarias para fortalecer nuestras defensas cibernéticas, para que nuestra nación esté preparada para la cibernética.

Los eventos SolarWinds y Microsoft Exchange pusieron en peligro a decenas de pequeñas y medianas empresas (pymes) que tienen vínculos fundamentales con las cadenas de suministro y la economía de nuestra nación. Las pymes son el objetivo de los ataques cibernéticos porque a menudo carecen de recursos para invertir en herramientas y formación de ciberseguridad. El propósito de este Libro Blanco es proporcionar a la Administración Biden medidas específicas para mejorar la resiliencia y la preparación cibernética de las pymes de los Estados Unidos.

Aunque no podemos acabar con las intrusiones cibernéticas, existen medidas básicas que podemos tomar para proteger a nuestros ciudadanos, empresas e infraestructuras esenciales. Si nos centramos en el papel que desempeña el comportamiento humano en los ataques con éxito y ofrecemos a las pymes las herramientas y los recursos necesarios para mejorar su preparación cibernética, podemos construir una base sólida y resistente para la ciberseguridad.

También podemos ayudar a promover la fortaleza y supervivencia de las empresas. Dado que, según la Alianza nacional de ciberseguridad, el 60% de las pymes que sufren una vulneración cibernética desaparecerán en el plazo de un año, es vital para las pymes, y para todos nosotros, que se conciencien y preparen para la cibernética.

Solo el 18% de las pymes de EE. UU. confían (“están totalmente de acuerdo”) en que su organización está preparada para un incidente cibernético.



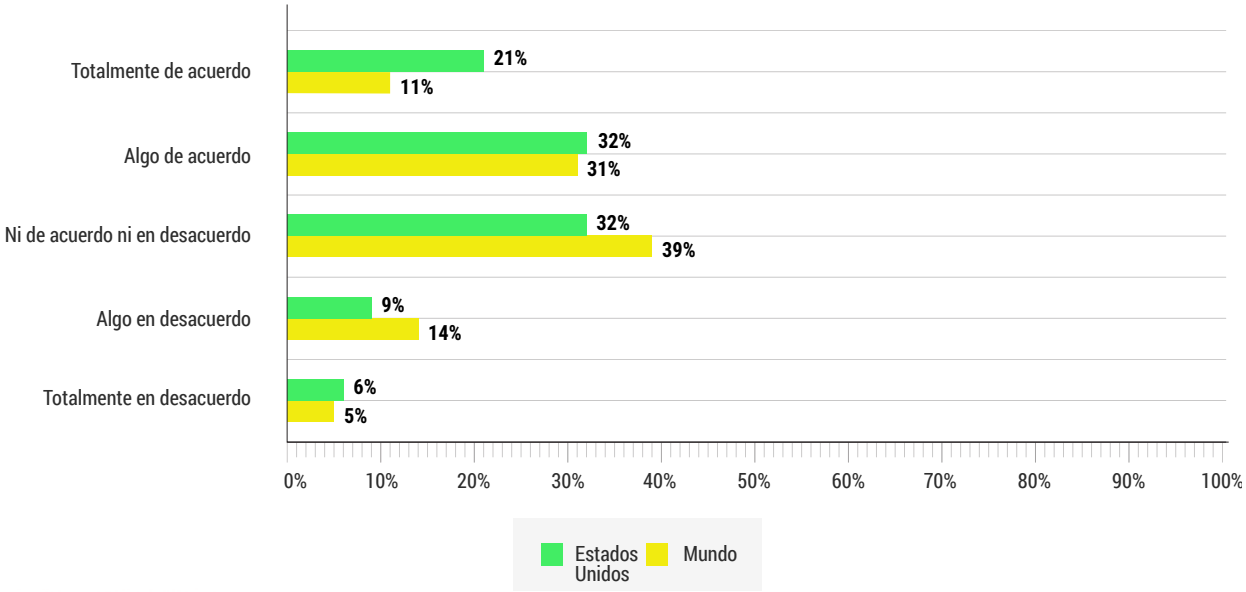
Pregunta: ¿En qué medida está de acuerdo en que su organización está preparada para un incidente cibernético y sabría cómo responder?

Fuente: Encuesta mundial del Cyber Readiness Institute a pequeñas y medianas empresas, enero de 2021

Entorno y desafíos para la ciberseguridad

La pandemia de la COVID-19 desató una fiebre mundial para permitir las operaciones remotas a los trabajadores, empresas y agencias gubernamentales. Aunque las empresas y la sociedad se beneficiarán de esta transformación digital, han aumentado las vulnerabilidades en todo el mundo y en todos los sectores industriales. En ningún lugar nuestra exposición es mayor que entre las pymes. No obstante, muchas pymes no tienen los recursos financieros o el talento humano necesarios para afrontar los desafíos de la ciberseguridad y ven poca rentabilidad de la inversión en gastar sus escasos recursos en ciberseguridad. De acuerdo con un estudio del CRI de 2021, solo el 21% de las pymes confía en que el tiempo y el dinero que invierte su organización en ciberseguridad reducirá su riesgo. La mayoría de las pymes están mucho más inseguras sobre el valor de invertir en ciberseguridad. Entre tanto, muchas grandes organizaciones ni siquiera han establecido requisitos de ciberseguridad básicos para sus proveedores pymes o apenas están empezando a afrontar el problema.

Solo el 21% de las pymes de EE. UU. confían (“están totalmente de acuerdo”) en que el tiempo y el dinero invertidos en ciberseguridad reducen sus riesgos.



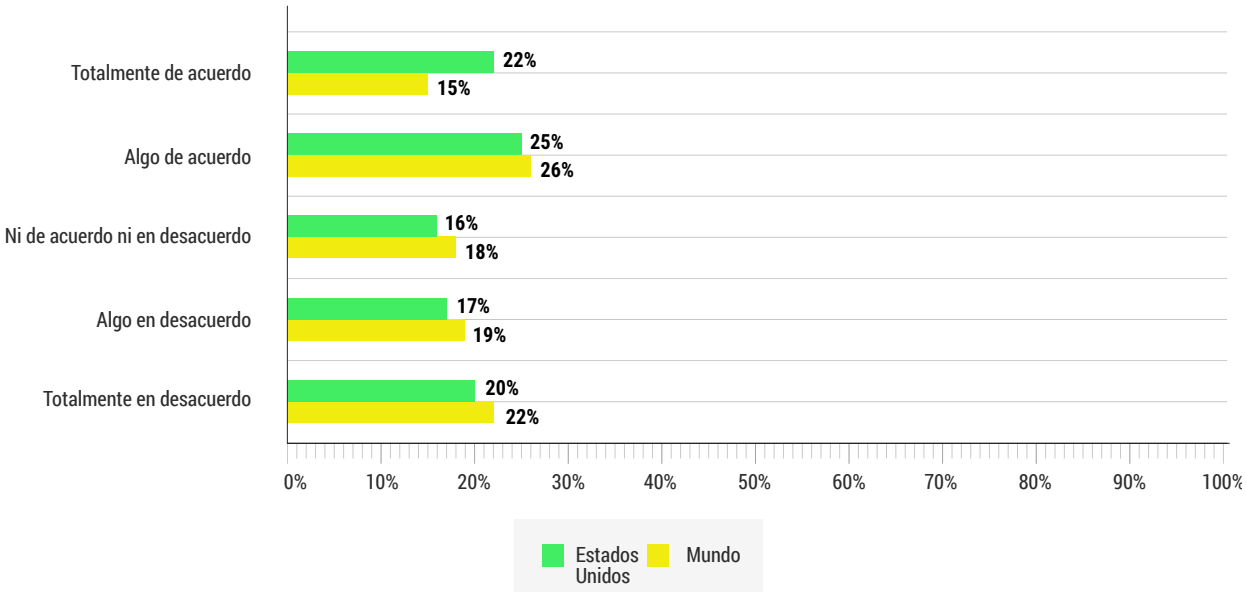
Pregunta: ¿En qué medida está de acuerdo en que el tiempo y el dinero que su organización invierte en ciberseguridad están reduciendo sus riesgos?

Fuente: Encuesta mundial del Cyber Readiness Institute a pequeñas y medianas empresas, enero de 2021

info@cyberreadinessinstitute.org

Existen muchas amenazas para las pymes, pero el ransomware, phishing y robo de credenciales (robo de contraseñas) se encuentran entre los más graves. Se espera que estas amenazas aumenten a medida que los sectores siguen realizando todas las operaciones en línea debido a la pandemia de la COVID-19 y a la naturaleza cambiante del trabajo. Este rápido cambio ha creado brechas en la resiliencia cibernética, porque las empresas, sobre todo las que tienen menos recursos, luchan por mantenerse al día. Estas crecientes vulnerabilidades están siendo explotadas de modo fácil y frecuente por actores malignos.

Solo el 22% de las pymes de EE. UU. confían ("están totalmente de acuerdo") en que tienen un empleado o un equipo de empleados con una clara responsabilidad en materia de ciberseguridad.



Pregunta: ¿En qué medida está de acuerdo con la siguiente afirmación? "Tenemos un empleado o equipo de empleados con una clara responsabilidad en nuestra ciberseguridad"

Fuente: Encuesta mundial del Cyber Readiness Institute a pequeñas y medianas empresas, enero de 2021

Las consecuencias de un riesgo de ciberseguridad no solo son relevantes para la empresa afectada, sino que también exponen a otras empresas de su cadena de suministro. Puesto que más de dos tercios de las grandes empresas subcontratan una parte de sus funciones y permiten el acceso de terceros a sus datos, una protección cibernética insuficiente entre las pymes también puede tener consecuencias para las empresas más grandes. **Un informe de 2020 elaborado por Accenture encontró que hasta el 40% de las violaciones cibernéticas son indirectas, lo cual significa que eligen eslabones débiles de las cadenas de suministro o ecosistemas empresariales.**

Recomendaciones

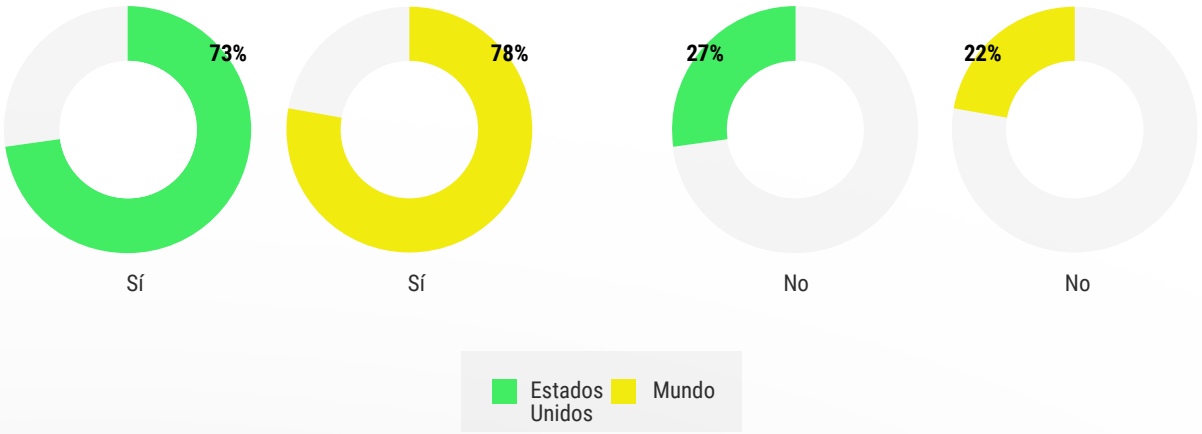
La ciberseguridad de las pymes de Estados Unidos es fundamental para el funcionamiento sin restricciones de nuestras instituciones públicas y privadas y el bienestar económico de nuestra nación. A continuación, se incluyen cinco recomendaciones para ayudar a que las pymes de Estados Unidos estén preparadas para la cibernética.

- Crear una campaña nacional de concienciación para fomentar la preparación cibernética de las pymes
- Crear un Centro de recursos de ciberseguridad para las pymes dentro del gobierno federal
- Conceder créditos fiscales para animar a las pymes a que inviertan en ciberseguridad
- Establecer una colaboración pública/privada para definir unos estándares de ciberseguridad mínimos
- Crear “escuadrones cibernéticos” financiados por el gobierno, en colaboración con colegios comunitarios y universitarios

Crear una campaña nacional de concienciación para fomentar la preparación cibernética de las pymes

Como nación, tenemos un largo historial de uso de campañas de concienciación pública para salvar vidas y cambiar comportamientos, desde incendios forestales o el uso del cinturón de seguridad, hasta los anuncios de “Si ve algo, diga algo” posteriores al 11 de septiembre. Ahora es el momento de organizar una campaña nacional de concienciación que se centre en el papel del comportamiento humano en la ciberseguridad y eduque a todos sobre las medidas que nos protegerán a todos. Existe el apoyo público para una campaña del gobierno: más del 60% de las pymes de EE. UU. y del mundo, en una encuesta del CRI de 2021, creen que el gobierno debería organizar una campaña nacional de concienciación pública para promover la preparación cibernética.

Más del 70% de las pymes de EE. UU. desean que el gobierno haga más para ayudar a que las organizaciones de la cadena de suministro estén preparadas para la cibernética



Pregunta: ¿Debería el gobierno ofrecer más apoyo para ayudar a mejorar la ciberseguridad de su organización y de otras de la cadena de suministro?

Fuente: Encuesta mundial del Cyber Readiness Institute a pequeñas y medianas empresas, enero de 2021

info@cyberreadinessinstitute.org

La ciberseguridad es un tema complejo que no se reduce fácilmente a un simple mensaje. Una campaña de servicio público eficaz se debe centrar en un único tema de ciberseguridad básico, por ejemplo, el uso de contraseñas seguras. Centrarse en un solo tema con un mensaje recurrente sencillo ayudará a proteger a las pymes frente a uno de los métodos preferidos por los piratas informáticos.

Crear un Centro de recursos de ciberseguridad para las pymes dentro del gobierno federal

Una campaña nacional de concienciación centrada en la preparación cibernética lógicamente remitirá a las pymes a una lista de recursos públicos y privados disponibles. En la actualidad, esos recursos están dispersos en varias agencias gubernamentales, que a veces dan consejos que son demasiado técnicos para muchos propietarios de empresas que no tienen personal informático interno o que subcontratan la ciberseguridad. Considerando la labor en curso por parte de la Agencia de seguridad de infraestructura y ciberseguridad (CISA) para las pymes, recomendamos que la CISA sea la agencia mejor situada para encargarse de la gestión de los recursos de ciberseguridad para las pymes. La agencia encargada de gestionar los recursos también debería tener como misión principal la tarea de simplificar los conceptos relacionados con la ciberseguridad para hacerlos accesibles y comprensibles para los propietarios de las empresas.

Conceder créditos fiscales para animar a las pymes a que inviertan en ciberseguridad

Para fomentar las inversiones de las pymes en ciberseguridad, el gobierno federal debería ofrecer incentivos en forma de créditos fiscales. El Departamento del Tesoro, en colaboración con la Administración de pequeñas empresas (SBA) y la CISA, deberían establecer directrices sobre los requisitos necesarios para los créditos fiscales para la inversión de las pymes en ciberseguridad. Aunque los créditos fiscales disminuirán la cantidad de ingresos tributables que recauda el gobierno, una mejor ciberseguridad reducirá el daño económico provocado por los atacantes cibernéticos y tendrá un efecto neto positivo en la seguridad, fortaleza y resiliencia de la economía digital.

Colaborando con otras agencias y solicitando las opiniones del sector, el Departamento del Tesoro puede establecer requisitos para que las empresas indiquen si han tomado medidas para la preparación para el ciberespacio antes de recibir cualquier crédito fiscal. Estos estándares deberían exigir educación y formación en ciberseguridad para que los empleados reúnan los requisitos del crédito. La educación debería recalcar la necesidad de crear una cultura de la ciberseguridad en el lugar de trabajo. La concienciación sobre los riesgos que implican las infracciones cibernéticas y los comportamientos que reducen estos riesgos deberían estar integrados en las acciones de todos, desde los empleados hasta la dirección de la empresa, para que los empleados comprendan sus responsabilidades y se tomen medidas para garantizar que la organización esté preparada para la cibernética.

Establecer una colaboración pública/privada para definir unos estándares de ciberseguridad mínimos

Ya no podemos confiar en las fuerzas del mercado o en medidas voluntarias para mejorar la ciberseguridad de nuestras instituciones públicas y privadas. En la actualidad, “primero en llegar al mercado” triunfa sobre “seguro en el mercado”. Las fuerzas del mercado dan prioridad a los beneficios sobre la seguridad y permiten las vulnerabilidades que nuestros enemigos aprovechan con facilidad. Esta estructura no es aceptable y debe cambiar. Debemos crear estándares que den prioridad a la seguridad en el mercado. En consonancia con una campaña eficaz de educación y concienciación, los estándares de seguridad del mercado servirán para que los consumidores den prioridad también a la seguridad.

Establecer estándares mediante la colaboración del gobierno y el sector es fundamental para proteger las cadenas de suministro. Hemos establecido con éxito regulaciones que mejoran la seguridad de nuestras carreteras, atención sanitaria y sistemas financieros. Debemos establecer unos estándares mínimos de ciberseguridad.

No existe una solución única que valga para todos para preparar a las organizaciones para que estén listas para la cibernética. El número de empleados, el sector, los conocimientos técnicos y las capacidades financieras son solo algunos de los factores que varían en función de cada empresa. Pero el gobierno y el sector pueden trabajar juntos para establecer estándares, centrados en un método de gestión de riesgos, que tengan en cuenta esos factores.

Crear “escuadrones cibernéticos” financiados por el gobierno, en colaboración con colegios comunitarios y universitarios

Ya existe un programa del gobierno financiado mediante becas concedidas por la National Science Foundation, CyberCorps: Scholarship for Service. No obstante, ese programa está diseñado para contratar y formar a los profesionales informáticos y directores de ciberseguridad para puestos en agencias federales, estatales y locales. Un nuevo programa de “escuadrones cibernéticos” aumentaría el flujo de talento disponible para las pymes y también facilitaría la participación de diferentes disciplinas y experiencia en la creación de culturas de preparación cibernética entre las pymes.

Los “escuadrones cibernéticos” pueden solucionar varios problemas que dificultan los esfuerzos de las pymes para prepararse para la cibernética, incluida la escasez de talento y la falta de recursos financieros. Un programa de “escuadrones cibernéticos”, inspirado en el Cuerpo de Paz, o una campaña similar a la iniciativa educativa de Ciencia, Tecnología, Ingeniería y Matemáticas (S.T.E.M.) permitirá a los estudiantes tener interés en emprender la ciberseguridad como una carrera profesional además de ofrecer una conexión con sus comunidades locales.

En cooperación con los colegios comunitarios y universidades, los estudiantes en prácticas con experiencia en varias disciplinas recibirían formación adicional sobre el papel que desempeña el comportamiento humano para lograr que las pymes sean seguras, temas como la administración de contraseñas, la actualización del software y la concienciación sobre el phishing, que no se tratan en muchos programas de ciberseguridad. Se enviarían “escuadrones cibernéticos” a la comunidad para ayudar a las pymes locales a mejorar su preparación cibernética. Al principio, el programa se centraría en ayudar a las empresas propiedad de minorías con fondos insuficientes.

Conclusión

Estas recomendaciones y medidas subrayan la necesidad de una colaboración público/privada urgente para solucionar las graves vulnerabilidades que ponen en riesgo nuestra seguridad nacional y nuestro bienestar económico. **Ahora, más que nunca, necesitamos una colaboración proactiva e intencionada y una acción colectiva entre el gobierno y la industria.**

Los eventos cibernéticos del año pasado demuestran cómo nuestros enemigos cibernéticos son cada vez más sofisticados a la hora de identificar y explotar nuestras vulnerabilidades y debilidades. Debemos reforzar nuestras capacidades de defensa cibernética además de seguir invirtiendo en nuestra ofensiva.

Las pymes necesitan acceso a recursos de ciberseguridad que sean prescriptivos y accesibles. Los recursos, herramientas y técnicas para las pymes requieren un método diferente al que necesitan las grandes empresas. El objetivo es el mismo, crear una empresa protegida y sana, pero el camino para conseguirlo es diferente. No podemos limitarnos a reducir las herramientas y técnicas empleadas por las grandes corporaciones a versiones más pequeñas para las pymes.

Debemos ser proactivos a la hora de apoyar a las pymes para que se conviertan en una fortaleza de nuestro ecosistema, no en un punto débil. Deben volverse más resistentes y estar preparadas cibernéticamente para garantizar que nuestra nación tenga una base sólida y una cultura de seguridad.

Acerca del Cyber Readiness Institute

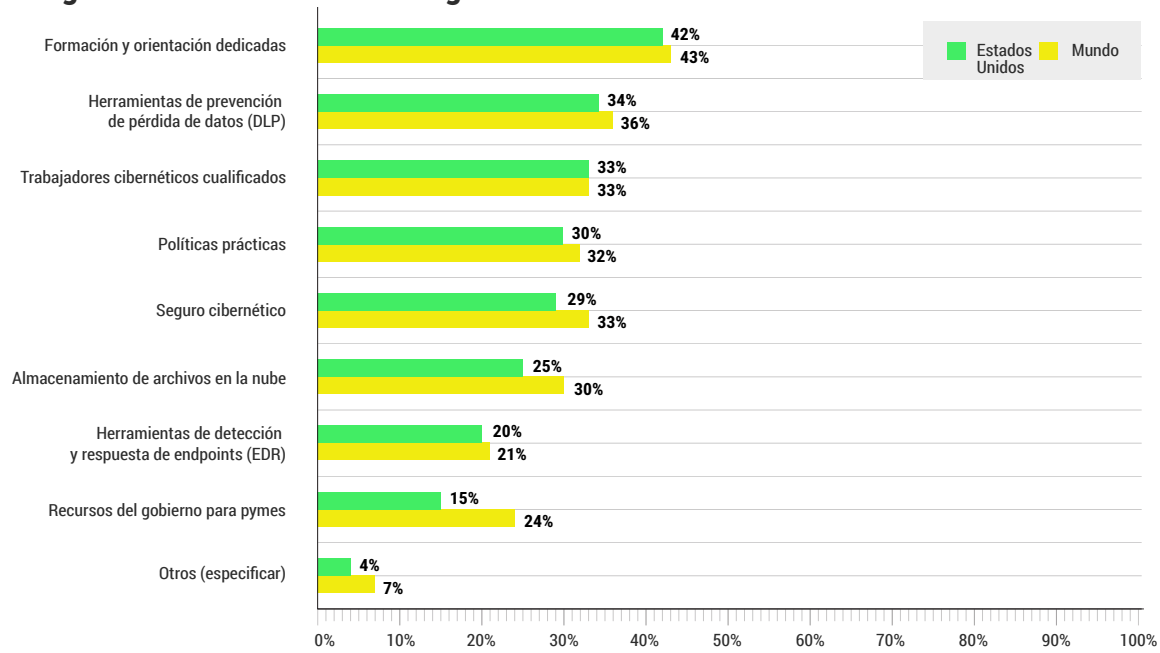
CYBER READINESS INSTITUTE

El Cyber Readiness Institute es una iniciativa sin fines de lucro que reúne a líderes empresariales de todos los sectores y zonas geográficas para compartir recursos y conocimientos que impulsan el desarrollo de herramientas de ciberseguridad gratuitas para las pequeñas y medianas empresas (pymes). El CRI fue cofundado por los Directores Generales de The Center for Global Enterprise, Mastercard, Microsoft y PSP Partners, como una medida de seguimiento de la labor de la Comisión para la mejora de la ciberseguridad nacional. Nuestros miembros también incluyen a ExxonMobil, General Motors y Principal. Nuestro objetivo es promover la preparación cibernética de las pymes para mejorar la seguridad de las cadenas de suministro mundiales. Los recursos del CRI se centran en el comportamiento humano y ponen de relieve la formación y concienciación de los empleados. Para obtener más información, visite www.BeCyberReady.com.

Apéndice

Encuesta mundial sobre ciberseguridad del Cyber Readiness Institute*, enero de 2021

La mayoría de las pymes necesitan formación y orientación específicas para que su organización sea más cibersegura.

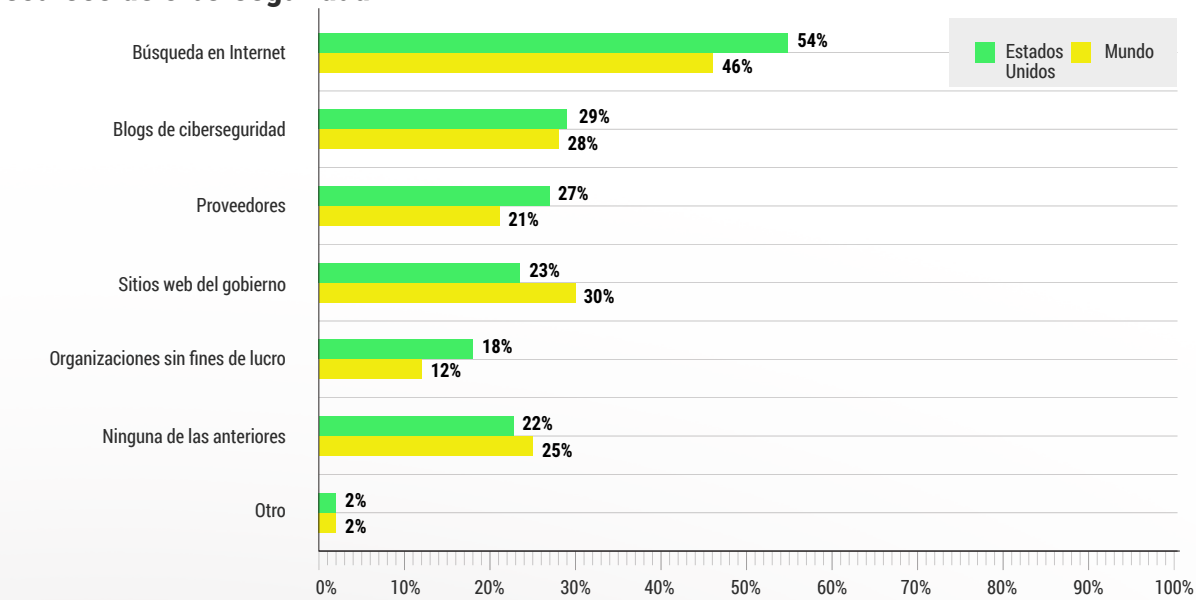


Pregunta: ¿Cuáles de las siguientes cosas necesita para que su organización sea más segura? (seleccione todas las que correspondan)

Fuente: Encuesta mundial del Cyber Readiness Institute a pequeñas y medianas empresas, enero de 2021

**Tamaño de la encuesta: Estados Unidos son 576 y el mundo son 517*

La mayoría de las pymes confían en las búsquedas en Internet para encontrar recursos de ciberseguridad.

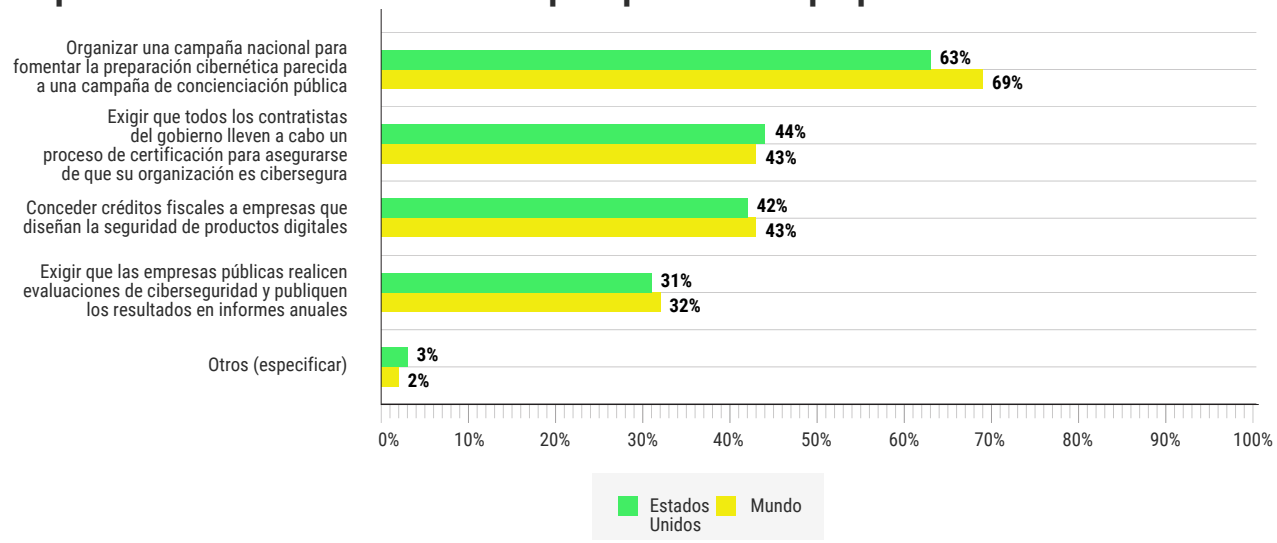


Pregunta: ¿Cuáles de las siguientes fuentes ha visitado para encontrar recursos de ciberseguridad para su organización?

Fuente: Encuesta mundial del Cyber Readiness Institute a pequeñas y medianas empresas, enero de 2021

info@cyberreadinessinstitute.org

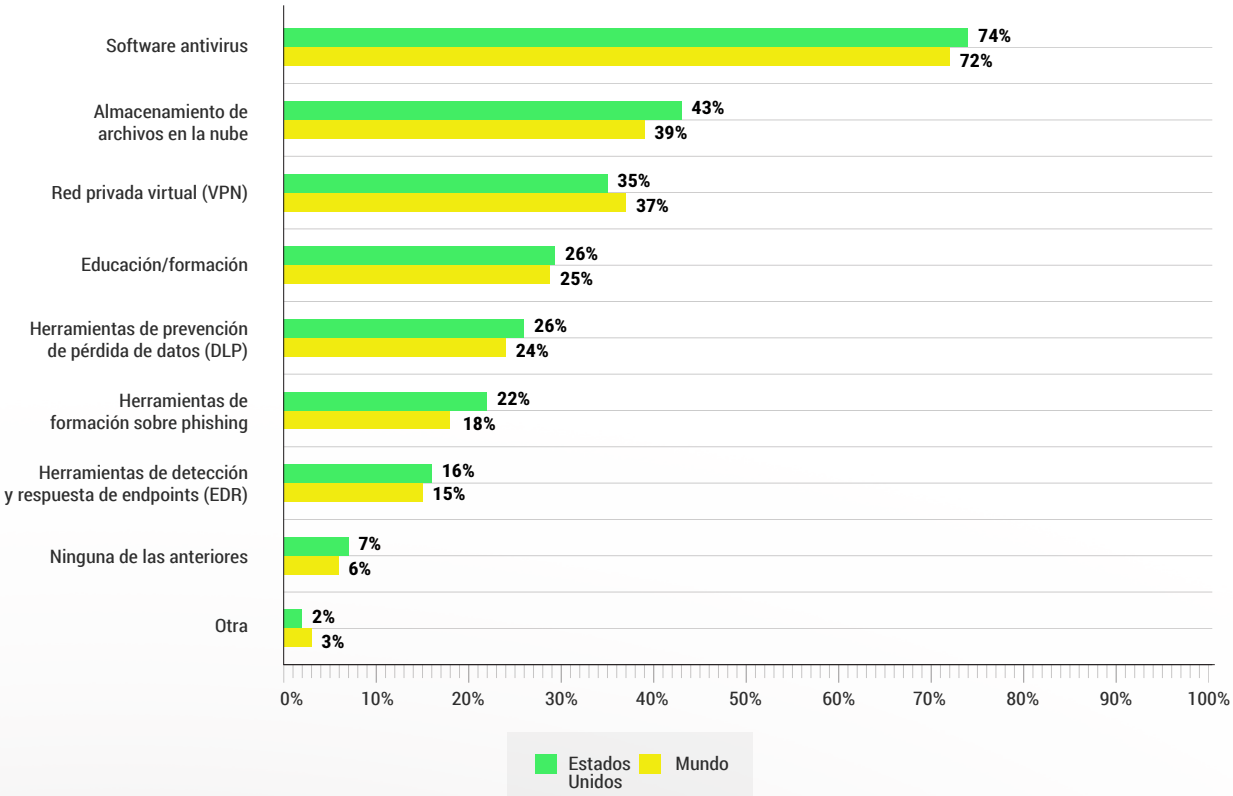
Más del 60% de las pymes de Estados Unidos quieren que el gobierno organice una campaña nacional de concienciación para promover la preparación cibernética.



Pregunta: ¿Cuáles de las siguientes medidas debería adoptar el gobierno?

Fuente: Encuesta mundial del Cyber Readiness Institute a pequeñas y medianas empresas, enero de 2021

El software antivirus, el almacenamiento de archivos en la nube y la red privada virtual (VPN) son las tres herramientas de ciberseguridad principales en las que confían las pymes.

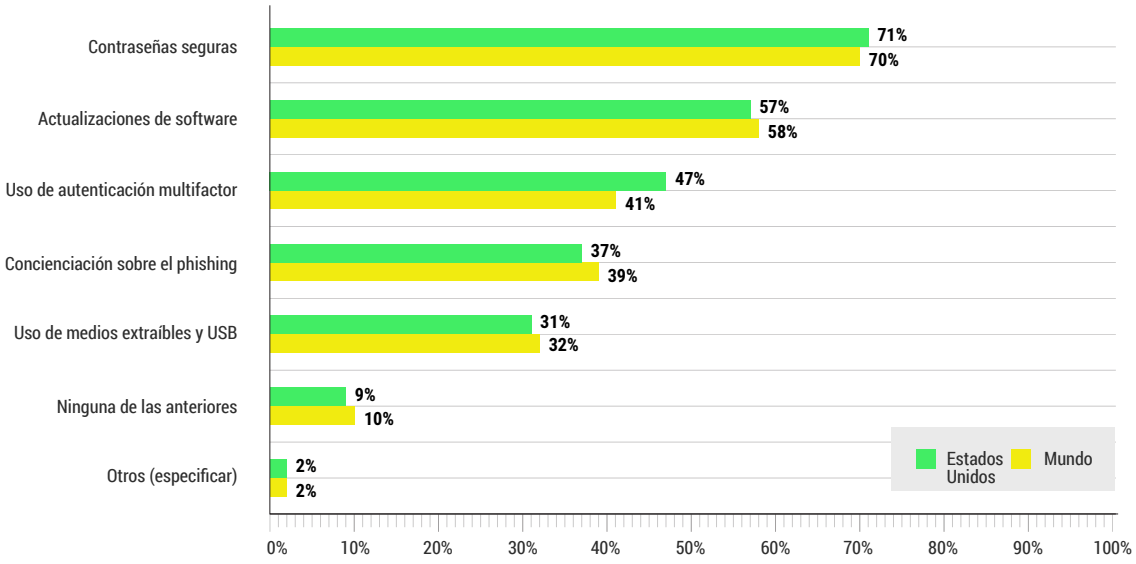


Pregunta: ¿Cuáles de las siguientes tecnologías y/o herramientas ha usado para ayudar a mantener la ciberseguridad de su organización?

Fuente: Encuesta mundial del Cyber Readiness Institute a pequeñas y medianas empresas, enero de 2021

info@cyberreadinessinstitute.org

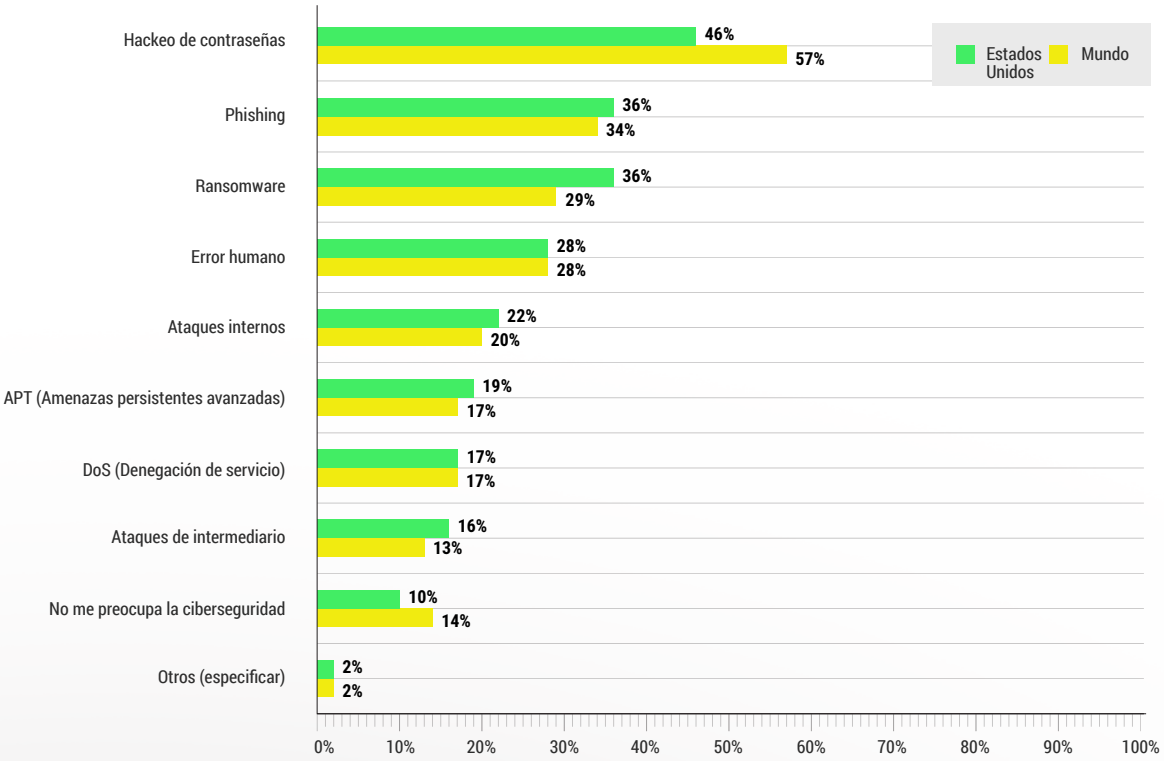
El 71% de las pymes de Estados Unidos afirman que sus empleados están entrenados para usar contraseñas seguras. PERO las contraseñas poco seguras siguen siendo la razón principal de los recientes ataques.



Pregunta: ¿Cuáles de los siguientes temas relacionados con la ciberseguridad están entrenados para afrontar los empleados de su organización?

Fuente: Encuesta mundial del Cyber Readiness Institute a pequeñas y medianas empresas, enero de 2021

El hackeo de contraseñas encabeza la lista de preocupaciones de ciberseguridad entre las pymes, además del phishing, el ransomware y el error humano.



Pregunta: ¿Qué es lo que más le preocupa en relación con la ciberseguridad de su organización?

Fuente: Encuesta mundial del Cyber Readiness Institute a pequeñas y medianas empresas, enero de 2021

info@cyberreadinessinstitute.org