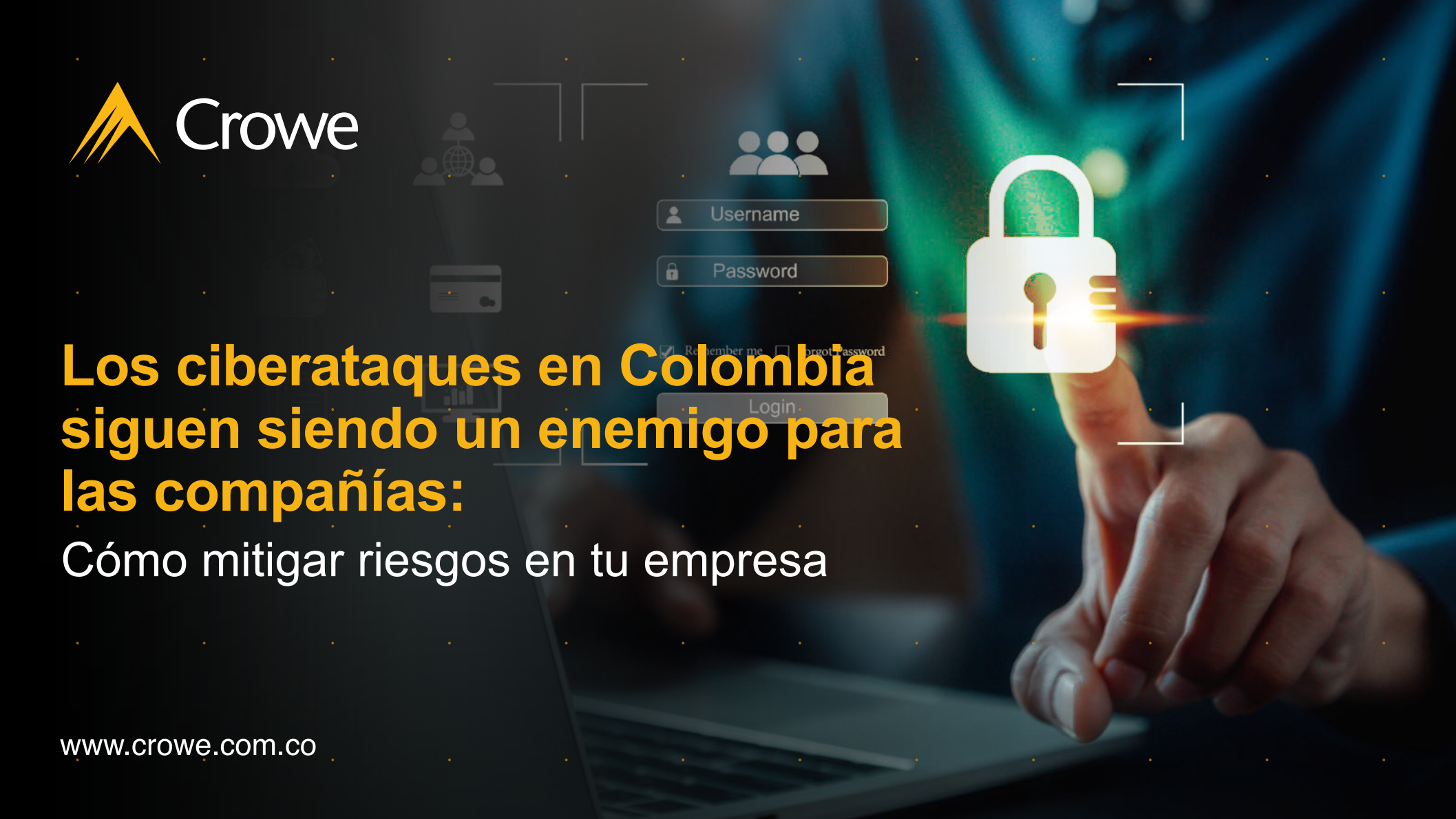
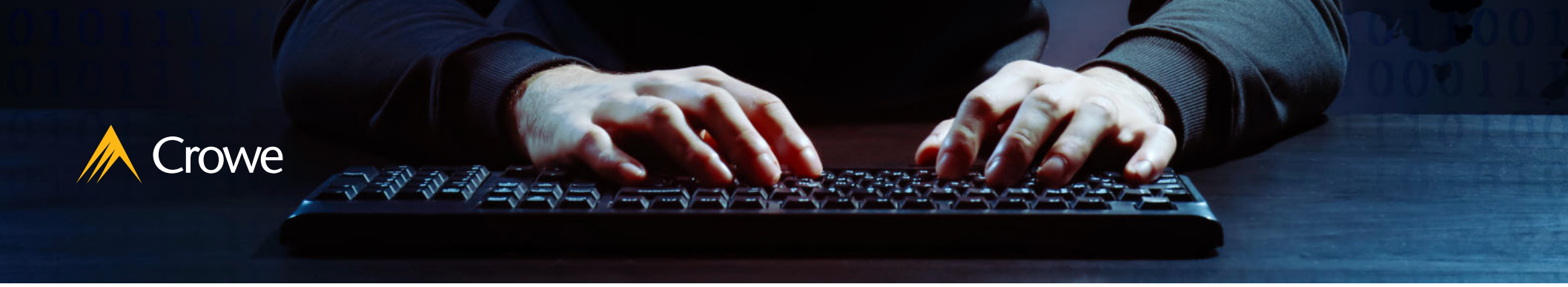
Crowe

Los ciberataques en Colombia siguen siendo un enemigo para las compañías:

Cómo mitigar riesgos en tu empresa



www.crowe.com.co



En los últimos años, Colombia ha visto un aumento en el número de ciberataques a empresas de todos los tamaños. Según el informe de amenazas globales de Fortinet, revela que América Latina fue el objetivo de más de 360 mil millones de intentos de ciberataques en el año 2022 y Colombia recibió 20.000 millones de ellos, revelando un crecimiento del 80 % frente al 2021. Las empresas se han visto afectadas por piratas informáticos y han sufrido violaciones de datos, lo que puede tener consecuencias financieras y de reputación a largo plazo.

El destructivo malware “Wiper” aumentó en más del 50%, mientras que las cadenas de suministro de los cibercriminales se fortalecen en complejidad y sofisticación para contrarrestar las defensas en evolución, según FortiGuard Labs.

En Colombia fueron hackeadas 34 empresas durante el año 2022, 133% más que el año pasado, entre ellas grandes compañías como EPM, EPS Sanitas, Fiscalía General, Viva Air y la Universidad Javeriana, quienes fueron las más afectadas, trayendo consigo un impacto negativo en la reputación organizacional, pero inicialmente, una gran afectación a miles de usuarios afectados por las empresas prestadoras de servicios, como las EPS.

En Colombia la ciberseguridad se ha vuelto cada vez más importante en los últimos años debido a la prevalencia del delito cibernético, pues esta, es la práctica de proteger redes, sistemas, computadoras y datos de intentos o ataques maliciosos. Los ciberataques a empresas se han vuelto comunes, y los piratas informáticos buscan acceso a información confidencial y aprovechan redes vulnerables para ingresar a robar información confidencial. Como resultado, es esencial que las organizaciones tomen medidas para protegerse contra tales ataques.

De acuerdo con el Informe Global de Brecha de Habilidades en Ciberseguridad de 2023, la cantidad de organizaciones que experimentaron cinco o más infracciones aumentó en un 53 por ciento de 2021 a 2022, afirmando que, esto sería producto de que muchos equipos de ciberseguridad en las empresas cuentan con poco personal, una alta sobrecarga laboral y la suma de trabajar bajo presión, pues cada vez la ciberseguridad se ha convertido en un punto clave para las compañías.

Empresas que han sido Hackeadas

Fuente: Sondeo LR/Gráfico: LR-AL

¿Cómo pueden las empresas protegerse mejor de los ciberataques?

El primer paso para protegerse mejor de los ciberataques es comprender los tipos de amenazas más comunes y cómo se pueden prevenir o mitigar. Si bien ninguna solución única protegerá contra todas las amenazas, existen varias medidas que las organizaciones pueden tomar para reducir el riesgo de ser atacadas.

1. Utilizar contraseñas seguras

Uno de los pasos más importantes es utilizar contraseñas seguras tanto para los sistemas internos como para los externos. Las contraseñas deben ser complejas, únicas y cambiarse periódicamente para garantizar la máxima protección. También es importante utilizar la autenticación de dos factores, que requiere un código o token independiente además de la contraseña.

2. Monitorización de actividades

Monitorear las actividades en redes y sistemas puede ayudar a identificar actividades maliciosas tan pronto como ocurren es crucial. Los equipos de seguridad deben realizar un seguimiento de toda la actividad de los usuarios, incluidos los inicios de sesión y el acceso a datos confidenciales. También deben estar atentos a cualquier comportamiento sospechoso que pueda indicar un posible ataque.

3. Implementar herramientas de seguridad

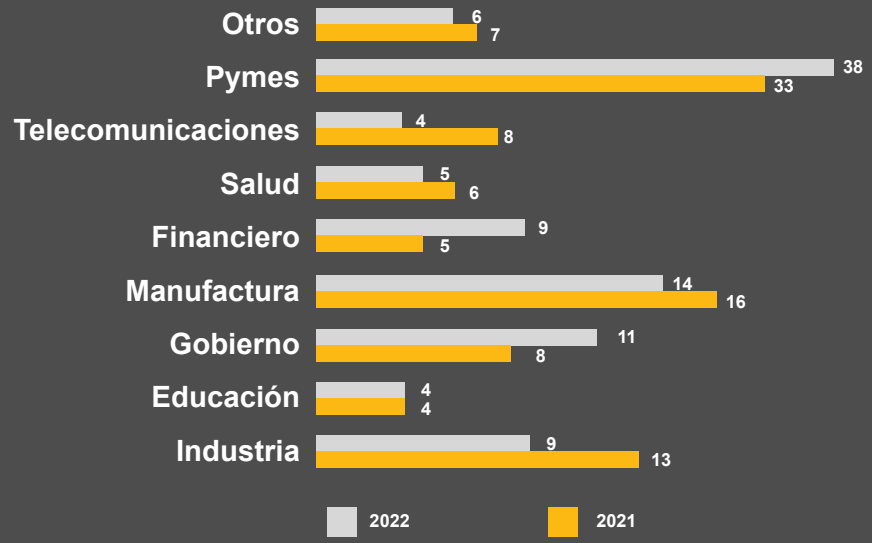
Es importante que las organizaciones puedan implementar herramientas de seguridad, como firewalls y software antivirus, para proteger sus sistemas de ataques maliciosos asegurarse de que todos los sistemas y aplicaciones se actualicen periódicamente para protegerlos contra vulnerabilidades conocidas.

4. Formación de los empleados

Finalmente, las organizaciones deben brindar capacitación en seguridad a los empleados para asegurarse de que comprendan la importancia de proteger sus datos y redes; enseñarles acerca de los procedimientos adecuados para identificar amenazas potenciales, así como también cómo responder en caso de un ataque. Además, deben conocer las mejores prácticas para el uso de contraseñas y otras medidas de seguridad.

Con la implementación de estas medidas, las empresas pueden reducir significativamente el riesgo de sufrir un ciberataque. La seguridad de los sistemas es una tarea continua, por lo que deben realizarse evaluaciones periódicas para garantizar que los medios de seguridad estén al día y funcionando correctamente. Es importante tener en cuenta el costo de la implementación y mantenimiento de estas medidas; sin embargo, una buena seguridad es una inversión que puede evitar grandes pérdidas en el futuro.

Sectores más afectados 2021-2022



Fuente: Informe Anual de Ciberseguridad de la Cámara Colombiana de Informática y Telecomunicaciones, CCIT

Prevenir las violaciones de la privacidad es esencial en una compañía

Además de estas medidas técnicas y preventivas para reducir los riesgos de ciberataques, las empresas deben tener en cuenta sus responsabilidades legales relativas a la protección de los datos personales. Esto significa cumplir con una serie de estándares y regulaciones para garantizar que se mantienen estrictas políticas de privacidad y seguridad. Todo esto garantiza que los datos personales de los usuarios estén protegidos en todo momento.

Por eso, tomar decisiones de monitoreo y prevención de posibles ciberataques se ha convertido en un proceso importante para las compañías que quieran disminuir su posibilidad de ser atacados y que en los ciberataques roben información privada.

En primer lugar, es importante que las organizaciones cuenten con un plan integral de respuesta a incidentes. Este plan debe incluir los pasos a seguir en caso de un ataque, cómo aislar los sistemas afectados y notificar a las autoridades pertinentes. Además, debe identificar funciones y responsabilidades claras para responder a incidentes y describir procedimientos para realizar análisis forenses del sistema y recuperar datos.

Al tomar estas medidas, las organizaciones pueden asegurarse de estar preparadas para responder rápida y eficazmente a los ciberataques. Con las medidas de seguridad adecuadas se logran proteger los datos y redes de ataques maliciosos.

Además, las organizaciones también deberían practicar un seguimiento continuo de sus redes, lo que implica escanear periódicamente los

sistemas en busca de signos de actividad maliciosa, así como monitorear el acceso a datos confidenciales. Asimismo, las empresas deberían utilizar soluciones de gestión de registros para rastrear la actividad de los usuarios en sus redes y detectar posibles amenazas. Al tomar estos pasos, las organizaciones pueden asegurarse de poder identificar y responder rápidamente a cualquier amenaza potencial.

La ciberseguridad es una medida esencial para organizaciones de todos los tamaños en Colombia y en el mundo, con las medidas de seguridad adecuadas, las empresas pueden proteger sus datos y proteger su reputación. Lo que afirma que, para lograr este objetivo, brindar capacitaciones en seguridad a los empleados, contar con un plan integral de respuesta a incidentes y practicar el monitoreo continuo de sus redes y datos, les permite estar preparados ante cualquier situación y garantizar que sus sistemas estén seguros y protegidos contra ataques cibernéticos.

Además de estas medidas de seguridad, las organizaciones también deben asegurarse de mantenerse actualizadas sobre las últimas tendencias y mejores prácticas de ciberseguridad. Las empresas pueden utilizar recursos como blogs, informes de la industria y foros en línea para mantenerse informados sobre las últimas amenazas y aprender cómo proteger mejor sus redes y datos. Al mantenerse al tanto de las tendencias actuales, las organizaciones pueden prepararse mejor para los ciberataques.

Asimismo, es importante establecer políticas de seguridad estrictas y claras para garantizar que todos los usuarios cumplan con las normas de

seguridad disminuyendo la posibilidad de una exposición al riesgo y a mantener la integridad y el buen funcionamiento del sistema de información.

Aunque no es un proceso sencillo, se ha convertido en una tarea imprescindible para garantizar la continuidad de los negocios y el buen funcionamiento de las operaciones. Pues la implementación de estas medidas también puede mejorar la percepción de la empresa ante terceros, ya que demuestra su compromiso con el cumplimiento de las leyes. Si bien puede requerir una inversión significativa de recursos, los beneficios obtenidos a largo plazo justifican la implementación de planes eficaces de seguridad cibernética.

¡Contáctenos!

Sede Central Internacional

Crowe Global - New York City
515 Madison Avenue
8th Floor, Suites 9006--9008
New York, NY-10022
United States of America
MAIN +1.212.808.2000
Contactus@Crowe.org

Colombia

Bogotá D.C.

Carrera 16 # 93-92
Edificio Crowe
PBX +57.1. 605.9000
Contacto@Crowe.com.co

Barranquilla

Calle 77B # 57-103 Oficina 608
Edificio Green Towers
PBX +57.5.385.1888
Barranquilla@Crowe.com.co

Cali

Carrera 100 # 5-169 Oficina 706
Unicentro – Centro de Negocios
PBX +57.2.374.7226
Cali@Crowe.com.co

Manizales

Carrera 23 C # 62-06, Oficina 705
Edificio Forum Business Center
PBX +57.6.886.1853
Manizales@Crowe.com.co

Medellín

Avenida Las Palmas # 15 B 143 - Piso 5
Edificio 35 Palms Business Tower
PBX +57.4.479.6606
Medellin@Crowe.com.co

Smart decisions. Lasting value.

Jaime Mendieta
Gerente de Transformación Digital & TI

Contáctanos