Deloitte.

Tendencias de Ciberseguridad en América Latina

Junio 2018

Tendencias de Ciberseguridad en América Latina

En los últimos años hemos visto grandes cambios en temas de ciberseguridad, en el cual se ha incrementado las amenazas, ataques debido a que las nuevas tecnologías y la era digital en la que nos enfrentamos, y a pesar del aumento de la inversión en seguridad de la información que han realizado las organizaciones, estas continúan sufriendo brechas de seguridad.

El estudio se realizó a

150 organizaciones

distribuidos en **12 países**

a nivel de América Latina y el Caribe

El **70%**

de las organizaciones afirma no tener certeza de la efectividad de su proceso de respuesta ante incidentes de ciber seguridad.

Y sólo un

3%

realizar simulaciones para probar sus capacidades efectivas de respuesta ante un ciberataque.

Así mismo **4 de cada 10** organizaciones **sufrieron un incidente de ciber seguridad en los últimos 24 meses**, con ello se puede observar que la problemática de ciber riesgos y seguridad de la información y riesgos continúan en aumento.

Razón por la cual las organizaciones en América Latina están **incrementando sus presupuestos** dedicados gestionar ciber riesgos y seguridad de la información.

Es importante resaltar que los ejecutivos de ciber riesgos y seguridad de la información han sido pieza clave para lograr que sus organizaciones vean la función de ciberseguridad como un área clave ante la digitalización de los negocios y de amenazas emergentes,

logrando con ello que

89%

de las organizaciones **asigne una importancia muy alta a la gestión de ciber riesgos** en un contexto cada vez más digital de los negocios.

Las organizaciones deben considerar que la digitalización de sus negocios y el incremento de la sofisticación de los ataques requieren el desarrollo de nuevas capacidades, observando que el

45% de las organizaciones se siente muy protegida respecto a los ciber riesgos, sin embargo la madurez de ciertas prácticas clave en la gestión de ciber riesgos como ser monitoreo, respuesta ante incidentes y ciber inteligencia, puede indicar un grado de optimismo mayor al que dichas capacidades ameritarían.

Y a pesar que el

93%

de las organizaciones cuenta con un software antivirus

solo el **12%** utiliza tecnologías adicionales al tradicional anti-virus,

es por ello que en el contexto de ciber amenazas actual, las organizaciones deben contar con diferentes tecnologías destinadas a proteger su información y sus sistemas contra amenazas del tipo malware o código malicioso.

Y de acuerdo a lo anteriormente descrito nuestra práctica de Cyber ha considerado que la función de Gestión de ciber riesgos y seguridad de la información está evolucionando hacia un nuevo paradigma que incluye cuatro componentes centrales y estratégicos:

Gobierno

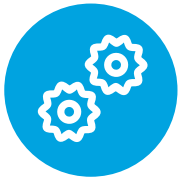
Establece la visión y estrategia, roles y responsabilidades de la función de gestión de ciber riesgos y seguridad de la información, considerando las necesidades del negocio, leyes, regulaciones y recursos humanos y tecnológicos.

Seguro

Se enfoca en la protección de la información y la tecnología que soportan los procesos clave del negocio, implementando controles adecuados al riesgo y a las amenazas propias de la organización.

Vigilante

Busca establecer una cultura en toda la organización que permita estar atentos a las amenazas y desarrollar la capacidad de detectar patrones de comportamiento que puedan detectar o predecir un ataque a la información.



Resilente

Significa tener la capacidad de controlar rápidamente el daño y movilizar los recursos necesarios para minimizar el impacto, incluyendo costos directos y disrupción del negocio, así como también daños a la reputación y a la marca.

Es importante que las Organizaciones verifiquen la efectividad de sus capacidades de protección, monitoreo y respuesta, a fin de no solo mejorarlo, sino de asegurar que funcionarán adecuadamente cuando se requieran. Es por ello que el propósito principal de nuestra práctica de Deloitte es proporcionar a los clientes confianza para progresar en el mundo digital, haciendo avanzar a la sociedad, y no solo presentar los riesgos si no también la posibilidad e innovación que este tiene para implementar programas y herramientas de ciberseguridad. Y con ello mantenerse seguro, vigilante y Resiliente.

Nuestro Equipo

Emilio Sandoval
Socio de Consultoría
esandoval@deloitte.com

Evelyn Donis
Gerente de Risk Advisory
edonis@deloitte.com

Herberth Vargas
Gerente de Risk Advisory
hevargas@deloitte.com

 2384 6500  deloitte.com/gt  @deloittegt

Deloitte.