TIEMPO DE SEGUROS

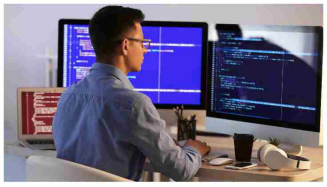
Home Noticias Entrevistas Columnistas Análisis de casos TDS ZOOM PODCAST

Home / Gacetillas - Home Principal

LA CIBERSEGURIDAD PREOCUPA AL 25% DE LOS EMPRESARIOS

Según el último IBR de Grant Thornton, en Argentina, 1 de cada 4 líderes del mercado identifica a los ciber incidentes como una limitación clave a la hora de hacer negocios.

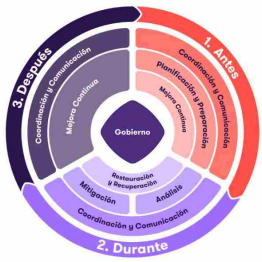
GACETILLAS, HOME PRINCIPAL | 14 NOV 2024



Twitter Facebook LinkedIn

En un contexto global cada vez más digitalizado, los riesgos cibernéticos emergen como una de las principales preocupaciones para los líderes empresariales. De acuerdo con el último International Business Report (IBR) de Grant Thornton, en Argentina, **1 de cada 4 líderes del mercado medio (25%) identifica a los ciber incidentes como una limitación clave a la hora de hacer negocios.**

A nivel global, esta preocupación afecta a la mitad de los líderes empresariales, lo que refleja el creciente reconocimiento de los ataques informáticos como una amenaza real y urgente. Este fenómeno está impulsando una tendencia alcista de redoblar las inversiones en tecnología para reducir su vulnerabilidad, no solo como un medio para mejorar la productividad, sus datos y operaciones, sino también como una estrategia defensiva frente a los riesgos digitales.



Un desafío más allá de las pérdidas económicas inmediatas

Datos del Fondo Monetario Internacional (FMI) señalan que el impacto en las operaciones por incidentes cibernéticos se ha cuadruplicado desde 2017, alcanzando los USD 2.500 millones (1). Cuando las empresas son víctimas de ataques, además de enfrentar daños financieros y consecuencias legales, sufren un impacto directo sobre su reputación ya que, la confianza de clientes y aliados se ve afectada, y la imagen de la organización queda en entredicho, lo que puede tener efectos duraderos.

"Esta situación va de la mano con los cambios en las formas de relacionamiento de las compañías con sus clientes, proveedores, empleados, y sería esperable que se incrementen en el futuro", comenta **Cristian Bertone, socio de BRS Servicios Financieros y líder de IT Advisory de Grant Thornton Argentina**. *"La multiplicación de canales digitales, sumado a la falta de percepción del riesgo, las exigencias de menor fricción del usuario y la velocidad de adopción de nuevas tecnologías, ponen a las organizaciones en una encrucijada"* añade.

Desde la pandemia, los ciberataques se han triplicado y sofisticado. Ya no basta con que solo los equipos de TI sean los responsables de prevenir y contener las amenazas. Los líderes empresariales y sus equipos deben comprender los riesgos y tomar medidas preventivas más estrictas para estar preparados y actuar rápidamente, ante potenciales ataques.

IA y la ciberseguridad

En el tercer trimestre de 2024, a nivel global, el **69% de las empresas del mercado medio planea invertir en tecnología de la información** durante los próximos 12 meses. De este porcentaje, el 66% señala que será en inteligencia artificial (IA). *"Dado el contexto que estamos viviendo, **es importante mantener una mentalidad abierta y no negarse a la innovación** que pueden traer aparejadas estas nuevas herramientas"*, comenta **Bertone.**

Conocerlas y seguir su evolución es clave para mitigar y prevenir riesgos, al tiempo que puede facilitar las defensas. Por ejemplo, **la IA puede volver más sofisticados los ataques a la vez que permite optimizar procesos de control y análisis.** El Informe de Riesgos Globales 2024 del Foro Económico Mundial (2) indica que las consecuencias negativas de los avances de la IA y las capacidades tecnológicas relacionadas ingresaron al ranking de gravedad de riesgo percibido en el largo plazo (10 años), ubicándose en el 5° puesto para los sectores público y privado.

"Con nuestros equipos venimos observando desde hace tiempo la disponibilidad de herramientas de desarrollo de software que permiten gestionar alarmas, optimizar códigos, corregir errores de programación o traducir de un código a otro", destaca **Bertone.** ***"El proceso de parametrización de estas herramientas es clave, al igual que sus posteriores testeos, para asegurar que el uso de IA verdaderamente aporte valor y permita alcanzar los objetivos que se tienen en mente al realizar estas inversiones en nuevas herramientas"***.

La IA también puede ser utilizada para elaborar un sistema de gestión de vulnerabilidades que permita llevar más allá a la empresa. Grant Thornton Luxemburgo, por ejemplo, desarrolló con un equipo diverso de expertos en ciberseguridad, ingenieros informáticos y estrategas comerciales un sistema de gestión de vulnerabilidades basado en IA. Este, no solo señala vulnerabilidades basándose en métricas de riesgo tradicionales, sino que también alinea esos riesgos con las prioridades comerciales de la empresa, mejorando la eficiencia general y el enfoque estratégico.

La ciberseguridad en el sector bancario

En Argentina, el Equipo de Respuesta ante Emergencias Informáticas Nacional (CERT.ar) evidenció que en 2023 el **sector de las finanzas fue el mayor blanco de los ciberataques,** con el 31% de los incidentes registrados.

Desde hace tiempo que el Banco Central de la República Argentina (BCRA) trabaja en pos de la Ciber resiliencia y **ha establecido una serie de lineamientos y requisitos obligatorios** para hacer frente a los ciberincidentes y limitar los riesgos.

"La Com. A7724 del BCRA que se emitió en 2023, por ejemplo, actualizó los requisitos obligatorios que deben implementar las entidades financieras de Argentina para la gestión de sistemas y tecnologías de la información. Incorporó nuevos controles y temáticas a considerar, asegurando que todas las entidades cuenten con prácticas efectivas para el control interno y la gestión de riesgos de su entorno operativo de tecnología y seguridad de la información", comenta **Fabián Bogado, Director de IT Advisory de Grant Thornton Argentina.**

El BCRA también ha establecido lineamientos para la respuesta y recuperación ante ciberincidentes (RRCI) que deben ser aplicados antes, durante y después del mismo. *"Si bien éstos están dirigidos a entidades financieras, proveedores de servicios de pago que ofrecen cuentas de pago e infraestructuras del mercado financiero; pueden ser adoptados por cualquier institución o compañía ya que revisten un carácter general"*, destaca **Bertone.**

Cómo estar ciber-protegido

Uno de los aspectos clave para abordar los riesgos digitales es adoptar una estrategia integral. La seguridad informática dejó de ser simplemente un desafío para el equipo de TI y crear una cultura de ciberseguridad en toda la empresa podría evitar grandes perjuicios ya que, según Harvard Business Review, el 80% de los ataques cibernéticos se deben a errores humanos (3).

En este sentido Bertone destaca que "adoptar un enfoque holístico para gestionar los riesgos digitales y contar con el respaldo de la alta dirección puede ser crucial para asegurar la protección de la empresa". Esta perspectiva no solo minimiza el riesgo de ataques, sino que también facilita la respuesta a incidentes cuando ocurren. Además, incorporar expertos en ciberseguridad permite que las empresas gestionen los riesgos con mayor eficacia y puedan cumplir con las regulaciones emergentes.

La ciberseguridad preocupa al 25% de los empresarios **14/11/2024**
Argentina - Tiempo de Seguros (Online) [Online] Tier:N/D Circulación: 184 Audiencia 184
P. -- 0 cm² 7034 cc N/D N/D Sin autor Ref.: 568105998

[...] Según el último IBR de Grant Thornton, en Argentina, 1 de cada 4 líderes del mercado identifica a los ciber incidentes como una limitación clave a la hora de hacer negocios. En un contexto global cada vez más digitalizado, los riesgos cibernéticos emergen como una de las principales preocupaciones para los líderes empresariales. De acuerdo con el último International Business Report (IBR) de Grant Thornton, en Argentina, 1 de cada 4 líderes del mercado medio (25%) identifica a los ciber incide [...]

Según el último IBR de Grant Thornton, en Argentina, 1 de cada 4 líderes del mercado identifica a los ciber incidentes como una limitación clave a la hora de hacer negocios. En un contexto global cada vez más digitalizado, los riesgos cibernéticos emergen como una de las principales preocupaciones para los líderes empresariales. De acuerdo con el último International Business Report (IBR) de Grant Thornton, en Argentina, 1 de cada 4 líderes del mercado medio (25%) identifica a los ciber incidentes como una limitación clave a la hora de hacer negocios.

A nivel global, esta preocupación afecta a la mitad de los líderes empresariales, lo que refleja el creciente reconocimiento de los ataques informáticos como una amenaza real y urgente. Este fenómeno está impulsando una tendencia alcista de redoblar las inversiones en tecnología para reducir su vulnerabilidad, no solo como un medio para mejorar la productividad, sus datos y operaciones, sino también como una estrategia defensiva frente a los riesgos digitales.

Un desafío más allá de las pérdidas económicas inmediatas

Datos del Fondo Monetario Internacional (FMI) señalan que el impacto en las operaciones por incidentes cibernéticos se ha cuadruplicado desde 2017, alcanzando los USD 2.500 millones (1). Cuando las empresas son víctimas de ataques, además de enfrentar daños financieros y consecuencias legales, sufren un impacto directo sobre su reputación ya que, la confianza de clientes y aliados se ve afectada, y la imagen de la organización queda en entredicho, lo que puede tener efectos duraderos.

"Esta situación va de la mano con los cambios en las formas de relacionamiento de las compañías con sus clientes, proveedores, empleados, y sería esperable que se incrementen en el futuro", comenta Cristian Bertone, socio de BRS Servicios Financieros y líder de IT Advisory de Grant Thornton Argentina "La multiplicación de canales digitales, sumado a la falta de percepción del riesgo, las exigencias de menor fricción del usuario y la velocidad de adopción de nuevas tecnologías, ponen a las organizaciones en una encrucijada" añade.

Desde la pandemia, los ciberataques se han triplicado y sofisticado. Ya no basta con que solo los equipos de TI sean los responsables de prevenir y contener las amenazas. Los líderes empresariales y sus equipos deben comprender los riesgos y tomar medidas preventivas más estrictas para estar preparados y actuar rápidamente, ante potenciales ataques.

IA y la ciberseguridad

En el tercer trimestre de 2024, a nivel global, el 69% de las empresas del mercado medio planea invertir en tecnología de la información durante los próximos 12 meses. De este porcentaje, el 66% señala que será en inteligencia artificial (IA). "Dado el contexto que estamos viviendo, es importante mantener una mentalidad abierta y no negarse a la innovación que pueden traer aparejadas estas nuevas herramientas" , comenta Bertone.

Conocerlas y seguir su evolución es clave para mitigar y prevenir riesgos, al tiempo que puede facilitar las defensas. Por ejemplo, la IA puede volver más sofisticados los ataques a la vez que permite optimizar procesos de control y análisis. El Informe de Riesgos Globales 2024 del Foro Económico Mundial (2) indica que las consecuencias negativas de los avances de la IA y las capacidades tecnológicas relacionadas ingresaron al ranking de gravedad de riesgo percibido en el largo plazo (10 años), ubicándose en el 5° puesto para los sectores público y privado.

"Con nuestros equipos venimos observando desde hace tiempo la disponibilidad de herramientas de desarrollo de software que permiten gestionar alarmas, optimizar códigos, corregir errores de programación o traducir de un código a otro", destaca Bertone.

" El proceso de parametrización de estas herramientas es clave, al igual que sus posteriores testeos, para asegurar que el uso de IA verdaderamente aporte valor y permita alcanzar los objetivos que se tienen en mente al realizar estas inversiones en nuevas herramientas".

La IA también puede ser utilizada para elaborar un sistema de gestión de vulnerabilidades que permita llevar más allá a la empresa . Grant Thornton Luxemburgo, por ejemplo, desarrolló con un equipo diverso de expertos en ciberseguridad, ingenieros informáticos y estrategas comerciales un sistema de gestión de vulnerabilidades basado en IA. Éste, no solo señala vulnerabilidades basándose en métricas de riesgo tradicionales, sino que también alinea esos riesgos con las prioridades comerciales de la empresa, mejorando la eficiencia general y el enfoque estratégico.

La ciberseguridad en el sector bancario

En Argentina, el Equipo de Respuesta ante Emergencias Informáticas Nacional (CERT.ar) evidenció que en 2023 el sector de las finanzas fue el mayor blanco de los ciberataques, con el 31% de los incidentes registrados.

Desde hace tiempo que el Banco Central de la República Argentina (BCRA) trabaja en pos de la Ciber resiliencia y ha establecido una serie de lineamientos y requisitos obligatorios para hacer frente a los ciberincidentes y limitar los riesgos.

"La Com. A7724 del BCRA que se emitió en 2023, por ejemplo, actualizó los requisitos obligatorios que deben implementar las entidades financieras de Argentina para la gestión de sistemas y tecnologías de la información. Incorporó nuevos controles y temáticas a considerar, asegurando que todas las entidades cuenten con prácticas efectivas para el control interno y la gestión de riesgos de su entorno operativo de tecnología y seguridad de la información", comenta Fabián Bogado, Director de IT Advisory de Grant Thornton Argentina.

El BCRA también ha establecido lineamientos para la respuesta y recuperación ante ciberincidentes (RRCI) que deben ser aplicados antes, durante y después del mismo. "Si bien éstos están dirigidos a entidades financieras, proveedores de servicios de pago que ofrecen cuentas de pago e infraestructuras del mercado financiero; pueden ser adoptados por cualquier institución o compañía ya que revisten un carácter general", destaca Bertone.

Cómo estar ciber-protegido

Uno de los aspectos clave para abordar los riesgos digitales es adoptar una estrategia integral. La seguridad informática dejó de ser simplemente un desafío para el equipo de TI y crear una cultura de ciberseguridad en toda la empresa podría evitar grandes perjuicios ya que, según Harvard Business Review, el 80% de los ataques cibernéticos se deben a errores humanos (3).

En este sentido Bertone destaca que "adoptar un enfoque holístico para gestionar los riesgos digitales y contar con el respaldo de la alta dirección puede ser crucial para asegurar la protección de la empresa". Esta persepectiva no solo minimiza el riesgo de ataques, sino que también facilita la respuesta a incidentes cuando ocurren. Además, incorporar expertos en ciberseguridad permite que las empresas gestionen los riesgos con mayor eficacia y puedan cumplir con las regulaciones emergentes.