CÁMARA DE COMERCIO SUIZO ARGENTINA

HOME > NOTICIAS CCSA

GRANT THORNTON: DIGITALIZACIÓN AUMENTA LA EXPOSICIÓN A CIBER AMENAZAS

Mar 4, 2022 | Noticias, Noticias Socios

Los proyectos de digitalización dejan a las firmas vulnerables con la frecuencia incremental de los incidentes cibernéticos. Frente a esta realidad, **Eduardo Diego, Gerente de Sistemas en Grant Thornton Argentina,** dice: *"La transformación digital se convirtió en una necesidad para que las Empresas puedan seguir realizando negocios en el mundo actual. Pero dicha transformación requiere del acompañamiento de toda la organización. No solo se trata de cambiar sistemas y/o procesos, sino que se debe trabajar fuertemente en mejorar los esquemas de seguridad y en capacitar al personal para no minimizar los riesgos a los que este cambio los puede enfrentar".* En ese sentido, el ejecutivo enfatiza en la importancia de que las empresas tengan especialistas en seguridad de la información o contraten servicios especializados que definan acciones a realizar

para minimizar los riesgos e, incluso, para estar preparados para su resiliencia en el supuesto de sufrir algún evento grave que afecte la operación. *"Si bien los cambios a implementar pueden significar una mayor inversión, no hacerlo puede llevar a perder participación en algunos negocios ya que, cada vez más, las empresas exigen a sus proveedores que estén alineados a los nuevos paradigmas."*

Diego sostiene que la pandemia fue la chispa que aceleró el ritmo hacia la digitalización y mejoró las prácticas y enfoques para muchas empresas. No obstante ello, asegura que estos cambios organizacionales dejaron muchas puertas abiertas para los ataques cibernéticos, haciendo mucho más daño y siendo mucho más costosos.

La cibernética es una prioridad estratégica

"*Las amenazas cibernéticas solo aumentarán a medida que las herramientas y métodos más sofisticados estén ampliamente disponibles para los amenazadores*" es la proclama del reporte 2022 del **Foro Económico Mundial (WEF)** sobre la ciberseguridad global. Al respecto, **Diego** remarca: *"El informe va más allá al examinar las ideas sobre el estado de la resiliencia cibernética, las brechas de percepción entre los ejecutivos, la amenaza del secuestro de datos, el riesgo en torno a las pequeñas y medianas empresas (PYME) y la necesidad de una regulación clara para apoyar los intercambios de información."*

La encuesta del **WEF** arrojó que el 81% de los participantes creen que, entre muchos factores que impulsan la ciberseguridad como una prioridad estratégica y que la transformación digital en curso está impulsando mejoras en la resiliencia cibernética. *"La aceleración de la digitalización, impulsada por la pandemia y los cambios posteriores en los enfoques de trabajo, ha puesto de relieve la ciber resiliencia"*, apunta.

Por otra parte, el estudio también demuestra que el 87% de los ejecutivos planean mejorar su protección organizacional mediante el fortalecimiento de políticas, procesos y estándares de resiliencia sobre cómo involucrar y administrar a terceros. *"El aumento del riesgo de la digitalización debe mitigarse con la concientización de los equipos de liderazgo senior"*, indica.

Las brechas de la percepción aumentan los riesgos

El informe también pone de relieve que las brechas de percepción entre los ejecutivos centrados en la seguridad, como los directores de seguridad de la información, y los ejecutivos de negocios, los directores ejecutivos. *"Esto explica por qué los profesionales de la seguridad se quedan fuera de las decisiones comerciales que afectan a la ciberseguridad y dejan a las empresas vulnerables."*

Las brechas fueron divididas en tres áreas:

- **La cibernética es una prioridad en la decisión empresarial:** el 92% de los ejecutivos de negocios estuvieron de acuerdo en que la resiliencia cibernética está integrada en las estrategias de gestión de riesgos empresariales, mientras que solo el 55% de los líderes encuestados estuvieron de acuerdo.
- **La alta Dirección apoya la Ciberseguridad:** el 84% de los profesionales creen que la resiliencia cibernética es considerada una prioridad para las empresas, pero solo el 68% ve la resiliencia

cibernética como una parte importante de su gestión general de riesgos.

- **Encontrar profesionales de ciberseguridad es una tarea difícil:** la encuesta encontró que al 59% de todos los encuestados les resultaría difícil responder a un incidente debido a la escasez de habilidades. El reclutamiento y la retención de talento fueron identificados por la mayoría como la parte más desafiante, pero los ejecutivos de negocios parecen menos conscientes de las brechas que sus ejecutivos de IT que perciben su capacidad para responder a un ataque con personal adecuado como una de sus principales vulnerabilidades.

Para el gerente de sistemas **en Grant Thornton Argentina**, *"las firmas deberían tener objetivos para reducir estas brechas a través de una comunicación efectiva y estableciendo marcos de seguridad a sus decisiones empresariales."*

El secuestro de datos encabeza las preocupaciones de amenazas

"Muchos de los líderes cibernéticos enfatizan que el secuestro de datos es peligroso y amenazante para la evolución de la seguridad pública". La encuesta confirmó que los ataques de secuestro de datos están a la vanguardia de las mentes de los líderes cibernéticos; son muy conscientes de este tipo de ataques, con el 50% de los encuestados indicando que el secuestro de datos es una de sus mayores preocupaciones entre las amenazas cibernéticas.

La ingeniería social y los ataques que se producen desde el interior de la organización fueron respectivamente las preocupaciones del segundo y tercer lugar para los líderes de IT cibernéticos. *"Las firmas deberían asegurase de tener las medidas adecuadas para reducir el riesgo de estas amenazas cibernéticas, a menudo empiezan educando a sus empleados y promoviendo el entendimiento del riesgo principal"*, asegura.

Las PYME ponen en peligro la seguridad de las organizaciones

El 88% de los encuestados se preocupan por la ciber resiliencia de las PYMEs que operan en sus cadenas de suministros, redes de socios y su ecosistema. *"Las firmas pueden mirar un mapa de cómo es que sus sistemas de seguridad interactúan con otras compañías e identificar sus debilidades. Después pueden colaborar con las PYMEs para reducir la amenaza de comprometer la seguridad."*

Eduardo Diego, Gerente de Sistemas en Grant Thornton Argentina, recomienda fomentar el intercambio de información y la colaboración. *"La encuesta a su vez demostró que hay una demanda de los profesionales cibernéticos de IT para una regulación clara que fomenta el intercambio de información y colaboración. Estos tipos de intercambios son valiosos, ya que el 90% de los encuestados señaló que la información de grupos externos de intercambio y/o socios proporcionan información procesable."*

Ante este panorama, ¿qué pueden hacer las firmas? *"Las empresas deben comprender lo que significa la seguridad y la resiliencia para ellas, especialmente si están sobrellevando una transformación digital. Los reguladores y los consumidores se centran cada vez más en los riesgos de amenazas y ataques, haciendo que la cibernética sea una prioridad comercial"*, concluye.

Temáticas: Amenazas cibernéticas | Brechas | Cámara de Comercio Suizo Argentina (CCSA) | Ciber resiliencia | Cibernética | Ciberseguridad | Eduardo Diego | Foro Económico Mundial | Grant Thornton Argentina | Pandemia | Proyectos de digitalización | PYME | Riesgos | Secuestro de datos | Sistemas | WEF

Sorry, no posts matched your criteria.

PRÓXIMOS EVENTOS

MARZO 2022

MAR 08 2022

ESTRATEGIAS DE PODER. CLAVES PARA EL LIDERAZGO FEMENINO

MAR 10 2022

¿ES CUMPLIBLE EL ACUERDO QUE SE FIRME CON EL FMI?

MAR 17 2022 - ABR 28 2022

LIDERAZGO MUJERES: ENTRENAMIENTO Y COACHING FEMENINO

NOTICIAS RECIENTES

GRANT THORNTON: DIGITALIZACIÓN AUMENTA LA EXPOSICIÓN A CIBER AMENAZAS

¿QUÉ METODOS DE FORMACIÓN EN EL

Temas

730 Aniversario | ABB Group | Acciones Positivas – 730 Aniversario | Adecco Argentina | América Latina | Argentina

EMPLEO IDENTIFICA ADECCO ARGENTINA?

EL PACHÓN: PLANIFICACIÓN DE SU PROGRAMA COMUNITARIO 2022 EN CALINGASTA

HOLCIM ARGENTINA: CUARTA EDICIÓN DEL PROGRAMA "JÓVENES PROFESIONALES"

SIKA: RÉCORD EN VENTAS Y BENEFICIOS, CRECIENDO EN TODAS LAS REGIONES

Calingasta Cambio climático CCSA (Cámara de Comercio Suizo Argentina) Clariant COVID-19 Cámara de Comercio Suiza en el Perú Cámara de Comercio Suizo Argentina (CCSA) Cordoba Desarrollo sostenible Economía circular Empresas y Entidades Ernesto Kohen Firmenich Fundación Holcim Argentina Gilbert Ghostine Glencore Pachon Grant Thornton Argentina Habilitación Postural Funcional Heinrich Schellenberg Holcim Argentina I+D Innovación KPMG Argentina Lorice Scalise María Silvia Abalo MCI Argentina Nestlé Argentina Omega Pandemia Responsabilidad y acción social Ricardo Arriazu Roche Argentina Salud San Juan Sika Argentina Sostenibilidad Suiza Sustentabilidad Trabajo

CÁMARA DE COMERCIO SUIZO ARGENTINA

MENU

LA CAMARA

SERVICIOS

NOTICIAS

SOCIOS

CONTACTO


CONTACTO
Av. Leandro N. Alem 1074, piso 10, CABA.
(5411) 4311 7187
info@suiza.org.ar
EN LAS REDES
Facebook
Twitter
LinkedIn
Youtube

Mar 4, 2022 | Noticias Noticias Socios Los proyectos de digitalización dejan a las firmas vulnerables con la frecuencia incremental de los incidentes cibernéticos.Frente a esta realidad, Eduardo Diego, Gerente de Sistemas en Grant Thornton Argentina, dice: "La transformación digital se convirtió en una necesidad para que las Empresas puedan seguir realizando negocios en el mundo actual. Pero dicha transformación requiere del acompañamiento de toda la organización. No solo se trata de cambiar sistemas y/o procesos, sino que se debe trabajar fuertemente en mejorar los esquemas de seguridad y en capacitar al personal para no minimizar los riesgos a los que este cambio los puede enfrentar" . En ese sentido, el ejecutivo enfatiza en la importancia de que las empresas tengan especialistas en seguridad de la información o contraten servicios especializados que definan acciones a realizar para minimizar los riesgos e, incluso, para estar preparados para su resiliencia en el supuesto de sufrir algún evento grave que afecte la operación. "Si bien los cambios a implementar pueden significar una mayor inversión, no hacerlo puede llevar a perder participación en algunos negocios ya que, cada vez más, las empresas exigen a sus proveedores que estén alineados a los nuevos paradigmas."

Diego sostiene que la pandemia fue la chispa que aceleró el ritmo hacia la digitalización y mejoró las prácticas y enfoques para muchas empresas. No obstante ello, asegura que estos cambios organizacionales dejaron muchas puertas abiertas para los ataques cibernéticos, haciendo mucho más daño y siendo mucho más costosos.

La cibernética es una prioridad estratégica

" Las amenazas cibernéticas solo aumentarán a medida que las herramientas y métodos más sofisticados estén ampliamente disponibles para los amenazadores" es la proclama del reporte 2022 del Foro Económico Mundial (WEF) sobre la ciberseguridad global. Al respecto, Diego remarca: "El informe va más allá al examinar las ideas sobre el estado de la resiliencia cibernética, las brechas de percepción entre los ejecutivos, la amenaza del secuestro de datos, el riesgo en torno a las pequeñas y medianas empresas (PYME) y la necesidad de una regulación clara para apoyar los intercambios de información."

La encuesta del WEF arrojó que el 81% de los participantes creen que, entre muchos factores que impulsan la ciberseguridad como una prioridad estratégica y que la transformación digital en curso está impulsando mejoras en la resiliencia cibernética. "La aceleración de la digitalización, impulsada por la pandemia y los cambios posteriores en los enfoques de trabajo, ha puesto de relieve la ciber resiliencia" , apunta.

Por otra parte, el estudio también demuestra que el 87% de los ejecutivos planean mejorar su protección organizacional mediante el fortalecimiento de políticas, procesos y estándares de resiliencia sobre cómo involucrar y administrar a terceros. "El aumento del riesgo de la digitalización debe mitigarse con la concientización de los equipos de liderazgo senior", indica.

Las brechas de la percepción aumentan los riesgos

El informe también pone de relieve que las brechas de percepción entre los ejecutivos centrados en la seguridad, como los directores de seguridad de la información, y los ejecutivos de negocios, los directores ejecutivos "Esto explica por qué los profesionales de la seguridad se quedan fuera de las decisiones comerciales que afectan a la ciberseguridad y dejan a las empresas vulnerables."

Las brechas fueron divididas en tres áreas:

La cibernética es una prioridad en la decisión empresarial: el 92% de los ejecutivos de negocios estuvieron de acuerdo en que la resiliencia cibernética está integrada en las estrategias de gestión de riesgos empresariales, mientras que solo el 55% de los líderes encuestados estuvieron de acuerdo.

La alta Dirección apoya la Ciberseguridad: el 84% de los profesionales creen que la resiliencia cibernética es considerada una prioridad para las empresas, pero solo el 68% ve la resiliencia cibernética como una parte importante de su gestión general de riesgos.

Encontrar profesionales de ciberseguridad es una tarea difícil: la encuesta encontró que al 59% de todos los encuestados les resultaría difícil responder a un incidente debido a la escasez de habilidades. El reclutamiento y la retención de talento fueron identificados por la mayoría como la parte más desafiante, pero los ejecutivos de negocios parecen menos conscientes de las brechas que sus ejecutivos de IT que perciben su capacidad para responder a un ataque con personal adecuado como una de sus principales vulnerabilidades

Para el gerente de sistemas en Grant Thornton Argentina "las firmas deberían tener objetivos para reducir estas brechas a través de una comunicación efectiva y estableciendo marcos de seguridad a sus decisiones empresariales."

El secuestro de datos encabeza las preocupaciones de amenazas

"Muchos de los líderes cibernéticos enfatizan que el secuestro de datos es peligroso y amenazante para la evolución de la seguridad pública". La encuesta confirmó que los ataques de secuestro de datos están a la vanguardia de las mentes de los líderes cibernéticos; son muy conscientes de este tipo de ataques, con el 50% de los encuestados indicando que el secuestro de datos es una de sus mayores preocupaciones entre las amenazas cibernéticas.

La ingeniería social y los ataques que se producen desde el interior de la organización fueron respectivamente las preocupaciones del segundo y tercer lugar para los líderes de IT cibernéticos. "Las firmas deberían asegurase de tener las medidas adecuadas para reducir el riesgo de estas amenazas cibernéticas, a menudo empiezan educando a sus empleados y promoviendo el entendimiento del riesgo principal" , asegura.

Las PYME ponen en peligro la seguridad de las organizaciones

El 88% de los encuestados se preocupan por la ciber resiliencia de las PYMEs que operan en sus cadenas de suministros, redes de socios y su ecosistema. "Las firmas pueden mirar un mapa de cómo es que sus sistemas de seguridad interactúan con otras compañías e identificar sus debilidades. Después pueden colaborar con las PYMEs para reducir la amenaza de comprometer la seguridad."

Eduardo Diego, Gerente de Sistemas en Grant Thornton Argentina, recomienda fomentar el intercambio de información y la colaboración "La encuesta a su vez demostró que hay una demanda de los profesionales cibernéticos de IT para una regulación clara que fomenta el intercambio de información y colaboración. Estos tipos de intercambios son valiosos, ya que el 90% de los encuestados señaló que la información de grupos externos de intercambio y/o socios proporcionan información procesable."

Ante este panorama, ¿qué pueden hacer las firmas "Las empresas deben comprender lo que significa la seguridad y la resiliencia para ellas, especialmente si están sobrellevando una transformación digital. Los reguladores y los consumidores se centran cada vez más en los riesgos de amenazas y ataques, haciendo que la cibernética sea una prioridad comercial" , concluye.