AGIS
Asociación Guatemalteca de Instituciones de Seguros

Edición no. 6, diciembre 2021 | agis.com.gt

Perspectiva Aseguradora

Ciberseguridad: nuevas soluciones para nuevos tiempos

OPINIÓN ASEGURADA
Los ciberseguros y su importancia en un futuro pospandemia

INNOVACIÓN Y DESARROLLO
Desarrollo de seguros cibernéticos: riesgos, coberturas, beneficios y evolución.

SEGUROS EN DATOS
Crecimiento de los ciber-seguros y ampliación de coberturas

PERSPECTIVA INTERNACIONAL
Lecciones de “WannaCry”: el ataque de *ransomware* más extenso de la historia.

BOLETÍN DE NOTICIAS
Resumen de los más importante de las últimas semanas

Contenido

Opinión asegurada

Los ciberseguros y su importancia en un futuro pospandemia

Ing. Christian Nölck

En estos últimos años, en los que el mundo ha cambiado sustancialmente a una actividad tecnológica más fuerte derivado de las nuevas condiciones de vida tras la pandemia, innovar en el campo digital para atender a los clientes de una forma más ágil y remota y el cuidar las plataformas informáticas cobra una relevancia muy grande.

Los ataques cibernéticos son una realidad en nuestro país y en el mundo, y pueden poner en riesgo la estabilidad de una empresa, comprometer operaciones vitales del giro de negocios y datos sensibles de una compañía, con consecuencias económicas enormes. De esa cuenta, contar con un seguro de ciberriesgo puede protegerla con una indemnización ante diferentes ataques tecnológicos, pues se estima que un 60% de las empresas atacadas no logran recuperarse de un ataque informático grave.

Según varios estudios (Ponemon Institute y Osterman Research), 1 de cada 5 empresas se enfrentó a un tiempo de inactividad de 25 horas o más después de los ataques de *ransomware* el año pasado. Muchos de ellos tuvieron que apagar sus sistemas durante más de 100 horas. El Ponemon Institute indica que la mayoría de las amenazas son causadas por empleados. El 54% de las filtraciones de datos son culpa de colaboradores que por descuido ingresan a correos electrónicos y sitios web sospechosos. Asimismo, según estimaciones de Cybersecurity Ventures, el costo mundial de ataques de *ransomware* en 2017 fue de US$ 5 mil millones, más de 15 veces el costo solo dos años antes (US$ 325 millones).

De esa cuenta, el seguro de ciberataques ha sufrido muchos cambios en los últimos años, se innova constantemente para conocer y entender cómo ayudar a las empresas en estos riesgos a nivel internacional. En Guatemala, aún hay mucho por desarrollar en el ramo, pues todavía no existe regulación aprobada al respecto a excepción de la creación de la Comisión Nacional de Ciberseguridad mediante el acuerdo gubernativo 200-2021.

Como gremio, consideramos que hay un camino por recorrer en investigación y desarrollo de coberturas, así como de capacitación en prevención y manejo de incidentes. Pero, sin duda, es uno de los elementos que las organizaciones y personas debemos de ir gestionando por el riesgo que conlleva.

Ing. Christian Nölck
Presidente

“Aún hay un camino por recorrer en investigación y desarrollo de coberturas, así como de capacitación en prevención y manejo de incidentes. Pero, sin duda, es uno de los elementos que las organizaciones y personas debemos de ir gestionando por el riesgo que conlleva”.

Innovación y desarrollo:

Josemaría Echeverría

Desarrollo de seguros cibernéticos: riesgos, coberturas y beneficios.

Acompañando el desarrollo del comercio cibernético y la vida digital impulsada en parte por la pandemia derivada del COVID-19, se han diversificado los riesgos para las empresas e instituciones que se manejan en el mundo digital.

El riesgo principal que afrontan varias instituciones son los ciberataques. Estos consisten en maniobras ofensivas y dañinas que tienen como objetivo desestabilizar redes, destruir estructuras digitales, o utilizar, exponer o robar información sensible. Si bien es cierto que los ciberataques de mayor dimensión han estado relacionados con organizaciones que se enfocan en guerras informáticas o ciberterrorismo, también se dan casos de individuos que prefieren atacar empresas e instituciones que les supongan un beneficio económico a manera de extorsión o venta de datos.

Para empresas e instituciones gubernamentales las consecuencias pueden ser devastadoras tanto en funcionamiento como en rentabilidad. Estas consecuencias varían no solo entre tipos, sino las instancias dañadas y los montos. Según estimaciones periodísticas se calcula que sólo en México los daños de los ataques superaban los US$ 8 mil millones en 2019. Si bien es cierto que los daños suelen ser triviales o menores, los ataques bien dirigidos suelen borrar información relevante o robarla permanentemente, inhabilitar equipos completos o incluso ataques industriales a larga escala.

Sin embargo, aunque la recuperación después de uno de estos ataques puede ser costosa, la implementación y desarrollo de seguros cibernéticos presenta una opción rentable y segura para proteger negocios e instituciones.

Los seguros cibernéticos normalmente cubren incidentes de seguridad de datos, que pueden incluir robo de datos personales, así como incidentes generalizados en la red, ataques contra datos de proveedores o terceras partes o incluso ataques terroristas. También incluyen coberturas de responsabilidad civil por violación a la privacidad, por daños a multimedia y publicidad y gastos de defensa, fianzas y conflictos de interés. De hecho, hay algunos que van más allá y llegan a cubrir interrupciones de negocio, extorsiones cibernéticas, gastos derivados de la restitución de la imagen, sanciones legales o gastos de relanzamiento del negocio.

La era digital y los avances tecnológicos generan tantos retos como beneficios y no se puede ignorar que en este entorno de oportunidades existen riesgos nuevos, usualmente dirigidos a PYMES.

Más allá de los beneficios que especifican las diferentes pólizas, el asegurado cuenta con a la certeza de que sus ganancias no estén a la deriva de un cibercriminal. Según un informe de la aseguradora *AGCS, la principal preocupación del 50% de las empresas encuestadas es perder sus ingresos por un ciberataque. Esta perdida con un ciberseguro estaría cubierta así como también los costos de mantener un negocio mientras dure el ciberataque y su consecuente proceso de recuperación*. Por otro lado, y de cara a los consumidores y clientes, el hecho de presentar un plan en caso exista daños a terceros no es despreciable. La generación de confianza se vuelve una cadena de reacciones.

En 1998 empezaron a lanzarse las primeras "ciberpólizas" evolucionando y desarrollando las pólizas de responsabilidad civil. Luego en 2006, empieza a desarrollarse la cobertura para perdidas propias como la interrupción de la red, extorsiones cibernéticas y el secuestro de archivos digitales. Esto derivado de los ataques a Sony y la intervención en varias centrales nucleares de Irán.

Para 2013, la cantidad de aseguradoras ofreciendo seguros cibernéticos había crecido considerablemente. En este periodo los ataques más relevantes se dieron en Adobe y TARGET.

La industria fue evolucionando respondiendo también a la evolución y el crecimiento de riesgos, a tal punto que el Foro Económico Mundial reconoce como tercer riesgo más grande los ataques cibernéticos desde 2018 hasta hoy. La ciberseguridad en términos de seguros seguirá creciendo como un fenómeno imposible de ignorar.

Seguros en datos

Impacto de los ciberataques para empresas

Tanto los ataques de *ransomware* en tendencia, las tarifas altas de “rescate” y los cambios en las regulaciones, están impulsando el mercado de los seguros cibernéticos en los últimos años. De hecho, una apreciación popular entre las aseguradoras es que solo existen dos tipos de empresas: las que han sido victimas de ciberataques y las que lo serán en el futuro.

Según Howden en su reporte A Hard Reset, la principal amenaza que enfrentan las empresas son los ataques de *ransomware* que han aumentado en más del 200% de 2019 a finales de 2020, aumentando no solo el número de ataques sino también la gravedad de estos y el coste por empresa que en 2019 subió un 400%.

Consecuentemente, los ciberseguros también han crecido en los últimos años y este crecimiento sustancial ha representado para las aseguradoras y reaseguradoras una oportunidad de influir positivamente en el desarrollo empresarial de sus países. Las primas brutas emitidas se han duplicado año con año desde 2016 con una tasa de crecimiento anual compuesto del 22% y se prevé que para próximos años crezca a un ritmo del 23%.

Esta tendencia se ve respaldada también por la pandemia del COVID-19 que ha forzado en gran medida que las empresas migren a regímenes de comercio electrónico y, por tanto, propiciando que los ciberdelincuentes diversifiquen sus ataques, así como sus estrategias.

En términos de montos desembolsados debido a secuestro de datos, se presentó un crecimiento del 143%. Entre los países más afectados se encuentran Singapur con un aumento del 317%, Países Bajos con un 215%, México con un 357%, y Estados Unidos con un 235%.

Según datos de la OCDE, el 100% de las pólizas evaluadas cubren violaciones de datos y brechas en la seguridad de red, 95% cubre problemas de comunicación, y el 92% cubre daños a equipos tecnológicos y ciber-extorsión.

No obstante, a pesar de que el mercado de los ciberseguros presenta una tendencia al alza, el reto consistirá en concientizar de los riesgos de no contar con uno, sobre todo a pequeñas y medianas empresas.

Perspectiva internacional

Josemaría Echeverría

Lecciones de “WannaCry”: el ataque de *ransomware* más extenso de la historia.

Los ataques *ransomware* de la variedad WannaCry (¿quieres llorar?) han sido ataques cibernéticos que se han llevado a cabo desde el 12 de mayo de 2017 en más de 150 países en todo el mundo. Estos han sido posibles usando el gusano informático del mismo nombre y se dirigieron al sistema operativo Windows de Microsoft.

La modalidad de este ataque es literalmente secuestrar los datos de la víctima, cifrándolos con una única vía de rescate que es pagar cuantiosas sumas vía Bitcoin para recuperar el acceso a estos datos, dándose incluso casos donde el rescate fue pagado, pero aún así no se recuperó la información.

Hasta 2019, este *ransomware* había afectado a más de 250,000 equipos en más de 150 países, siendo Rusia, Ucrania y Taiwán los más afectados. En términos de instituciones públicas, el Servicio Nacional de Salud de Gran Bretaña fue el más afectado y los casos más relevantes del sector privado fueron las infecciones de FedEx, Deutsche Bank, y las aerolíneas de LATAM.

Una de las preguntas más recurrentes es cómo se dan estas infecciones y la respuesta es más sencilla de lo que podría parecer. Normalmente el *ransomware* entra vía un correo electrónico de phishing y a partir de ahí el gusano informático infecta los equipos conectados a la misma red.

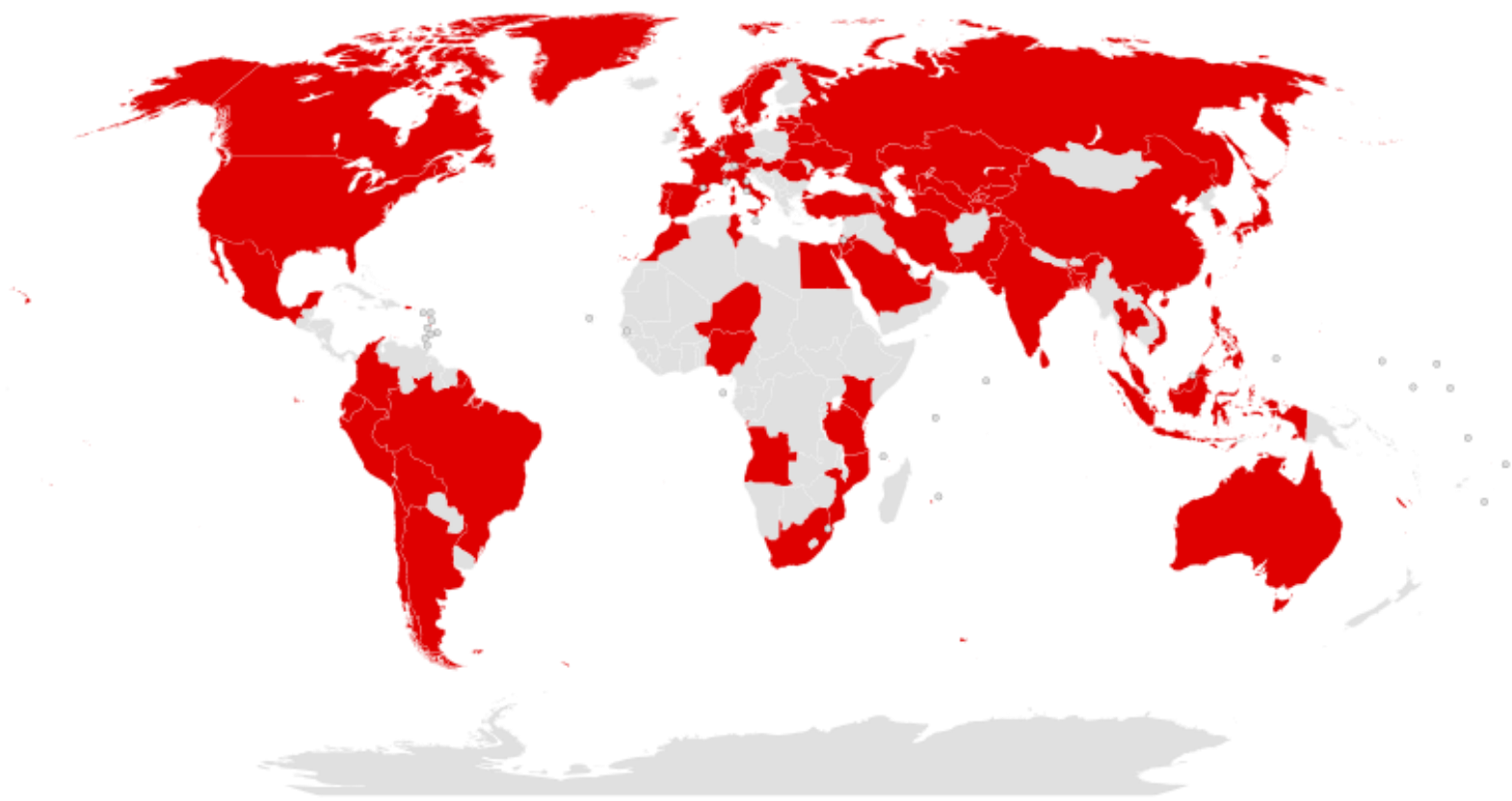
Como se mencionó anteriormente, el rescate de los datos secuestrados oscilaba entre los 300 y 500 dólares al inicio del ataque, para luego pasar de cifras desde 600 dólares hasta los 1,500 dólares. Para el caso del Servicio Nacional de Salud de GB (NHS), se estima que las perdidas fueron de más de 93 millones de libras esterlinas, sumando al estimado mundial de perdidas de 2017 de 4,000 millones de dólares.

Entre las lecciones aprendidas podemos resaltar que en lo que se refiere a los costos económicos, el costo directo (es decir, aquel derivado del daño al *hardware* y el pago del rescate) es el menor en comparación con los costos indirectos como lo fueron la recuperación de la seguridad, costos reputacionales, legales y los financieros derivados. De hecho, un acierto dentro del ataque fue que no fueron muchas las victimas que pagaron y que esto sirvió para que los atacantes bajaran la intensidad de sus maniobras.

Otra lección no menos importante es que el diseño, implementación y revisión constante de una estrategia de ciberseguridad es necesaria para todas las empresas

Sin importar la industria en la que se manejen. Si bies es cierto que los atacantes también se actualizan diariamente, los parches de seguridad en actualizaciones en los sistemas operativos, los softwares antivirus y reglas y estatutos de desenvolvimiento en redes es vital para la seguridad institucional en internet.

Por último y probablemente la más evidente y más importante es la contratación de un seguro cibernético que si bien no evitará un posible ataque, proveerá la capacidad de resiliencia a estos y hará posible que las empresas puedan seguir en funcionamiento. Las consecuencias empresariales de estos ataques varían y van desde el rescate de datos, hasta consecuencias legales, pasando por problemas reputacionales que una buena póliza de seguro resolvería. Los ciberataques son una realidad que puede ser evitada y contrarrestada.



Países donde se reportaron ataques de WannaCry

“La estabilidad y prosperidad de nuestra sociedad tiene un mayor grado de dependencia de la seguridad y confiabilidad del ciberespacio, cualidades que pueden verse comprometidas por causas técnicas o agresiones como las que hemos vivido estos días”, Alfonso Mur

Mensaje lanzado a las victimas del ataque

Boletín de Noticias

Lo más importante del mes

Los precios de los ciberseguros se dispararon un 32% en medio de una pandemia digital

El *ransomware* es ahora la amenaza digital más grande que enfrentan empresas de todos los tamaños en el mundo y es por esto que los aseguradores les instan a contar con refuerzos en su seguridad cibernética.

El Reaseguro: clave para desbloquear el mercado de los ciberseguros

Las tendencias de digitalización han llegado para quedarse y conducirán irremediablemente a un aumento en los ciberataques. Ante esto y el crecimiento de los precios las aseguradoras primarias transfieren del 35% al 45% de las primas globales de ciber riesgo a las reaseguradoras.

Clima y Ciber se disputan el top de riesgos a futuro

AXA ha hecho pública la octava edición de su Informe de Riesgos Futuros. Este estudio mide y clasifica la evolución de la percepción de los riesgos emergentes según la opinión de un panel de expertos en gestión de riesgos

Las aseguradoras ven gestionable el aumento del riesgo en los ciberseguros

El ciberseguro ha sido rentable para las aseguradoras de Estados Unidos, pero las crecientes pérdidas relacionadas con las intrusiones en la red, los incidentes de suplantación de identidad y las denegaciones de servicio probablemente aumentarán el volumen de reclamaciones y el coste medio por siniestro en el futuro, según Fitch.

AGIS
Asociación Guatemalteca de Instituciones de Seguros

SÍGUENOS EN REDES SOCIALES

Contacto: info@agis.com.gt
www.agis.com.gt

ASEGURADORA GENERAL

El Roble Seguros y Fianzas

La Ceiba Aseguradora

BMI SEGUROS DE GUATEMALA

SEGUROS COLUMNA es MISEGURO

Bupa

assa

Ficohsa | Seguros

Aseguradora Confío
Seguro para toda la vida

Seguros MAPFRE | GUATEMALA

PAN AMERICAN LIFE GUATEMALA
Compañía miembro de Pan-American Life Insurance Group

Universales
Queremos que siempre estés bien

SEGUROS BANTRAB

ASEGURADORA GUATEMALTECA

Seguros Agromercantil Bam

SEGUROS G&T

ASEGURADORA RURAL
Te ayuda a crecer seguro y tranquilo