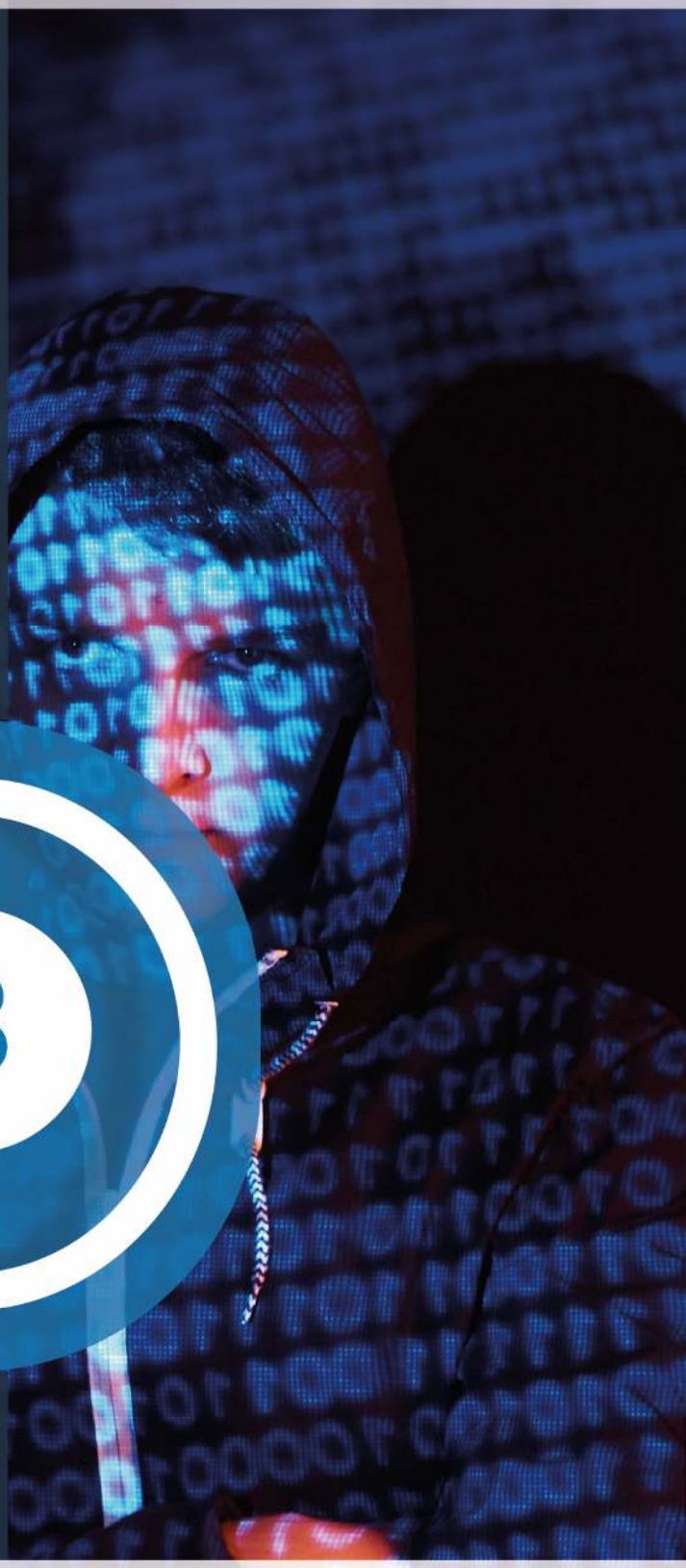
VALUATIVE SAS NIT 830.121.091-0 Oficinas a nivel Nacional
info@valuative.co - www.valuative.co

EL CYBER SEGURO LOS RIEGOS CIBERNETICOS

UN ENFOQUE PARA SUSCRIPCION Y ATENCION DE RECLAMO CRITERIOS Y CONCEPTOS



A – DIFERENCIAS ENTRE SEGUROS CIBERNETICOS Y CONTRA DELITOS

3

B – TENDENCIAS DEL CIBERCRIMEN EN COLOMBIA

VALUATIVE
LIDERES EN INVESTIGACIÓN Y PROTECCIÓN PATRIMONIAL

Cra. 7 No.156 - 10 Of.1607 /Torre Krystal
Centro Empresarial North Point
Bogotá D.C., Colombia
PBX.: +57(1) 390 2846
info@valuative.co

VALUATIVE
LÍDERES EN INVESTIGACIÓN Y PROTECCIÓN PATRIMONIAL

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

EL CYBER SEGURO
LOS RIEGOS CIBERNETICOS

A – DIFERENCIAS ENTRE SEGUROS CIBERNETICOS Y CONTRA DELITOS

B – TENDENCIAS DEL CIBERCRIMEN EN COLOMBIA

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

INTRODUCCION

Debido a que vivimos y trabajamos en un mundo que depende de las computadoras, todas las organizaciones corren el riesgo de ser víctimas de los ciberdelincuentes y deben tomar medidas para proteger los datos críticos. Los ciberdelincuentes son expertos en encontrar infinitas formas de infiltrarse en las computadoras y robar tanto fondos como datos. Es importante comprender en qué se diferencian las coberturas de **Cyber Risk** y **Computer Crime** y la protección que ofrecen.

El seguro contra **riesgos cibernéticos** es una protección contra el robo de información que los delincuentes utilizan para perpetuar el fraude. Los números de seguro social, los números de tarjetas de crédito o los registros médicos robados les permiten realizar compras no autorizadas, obtener medicamentos recetados para revenderlos, presentar facturas médicas fraudulentas e incluso revender la información robada a otros delincuentes. Una póliza de riesgo cibernético lo protege de demandas de terceros y cubre el costo de investigar la violación de datos, notificar a los clientes sobre la violación y brindar servicios de monitoreo de crédito. No cubre el robo de dinero o valores.

El crimen cibernético ocurre cuando los piratas informáticos transfieren fondos ilegalmente o hacen que el banco transfiera fondos por medios fraudulentos. Una política de delitos comerciales debe ofrecer protección contra delitos informáticos y fraude en transferencias de fondos como opciones estándar. Si la empresa tiene fondos de clientes, es fundamental que verifique que esos fondos también estén protegidos por la póliza.

Desafortunadamente, los empleados a veces responden a correos electrónicos de personas que se hacen pasar por clientes o proveedores de confianza, lo que se conoce como "**phishing**". Estos impostores inducen a los empleados a transferir fondos o proporcionar información. Es importante entender que los fondos transferidos voluntariamente a terceros mediante incentivos fraudulentos pueden no estar cubiertos. La empresa es responsable de determinar la autenticidad de dichas solicitudes.

Por otro lado, la cobertura de ingeniería social es **un respaldo** a la **póliza de delitos comerciales** que protege contra tales estafas. Aunque generalmente está sublimitado a

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

$250,000, es posible que existan límites más altos para riesgos específicos. Es posible que pueda obtener un acuerdo por separado para la cobertura de robo mediante estafas de suplantación de identidad y phishing.

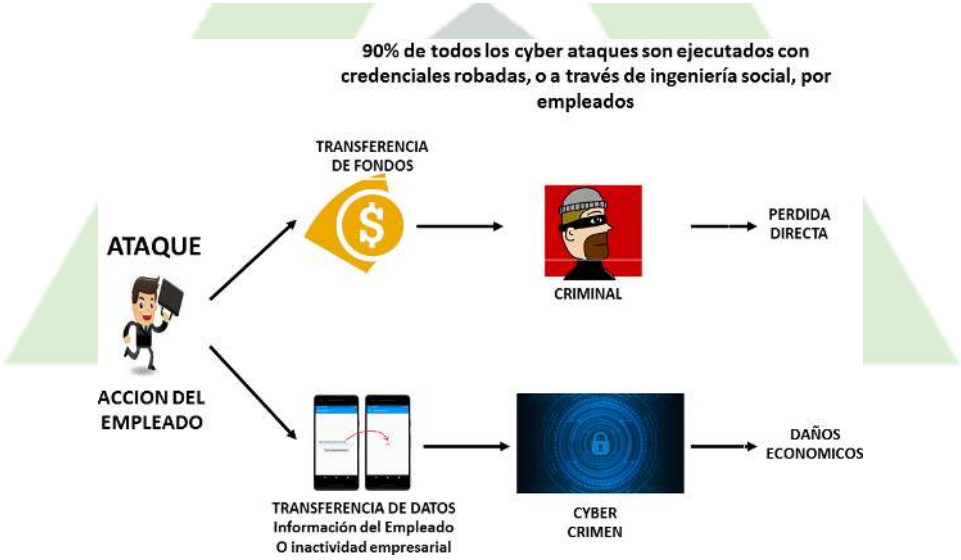
Sin importar el tamaño de una organización o la cantidad de información del cliente almacenada en el sistema informático, necesita la protección adecuada.

RIESGOS CIBERNETICOS Y DELITOS INFORMATICOS ¿CUAL ES LA DIFERENCIA?

A medida que el seguro cibernético se convierte en la norma para muchas empresas, existe una confusión cada vez mayor sobre las diferencias entre las coberturas contra el delito y las cibernéticas.

EN RESUMEN: Las **pólizas de delitos** cubren la pérdida directa de los fondos, ya sea por maleficencia, deshonestidad de los empleados o ingeniería social, mientras que las **pólizas cibernéticas** cubren los daños económicos que surgen por una falla en los controles de seguridad o privacidad de la red que pueden causar pérdidas indirectas.

Incluso a medida que los ciberdelincuentes y sus tácticas se vuelven más complejas, la mayoría de **los ataques cibernéticos de ciberdelincuentes se ejecutan mediante ingeniería social**.



VALUATIVE
LÍDERES EN INVESTIGACIÓN Y PROTECCIÓN PATRIMONIAL

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

EL SEGURO INTEGRAL CONTRA DELITOS

En un entorno comercial cada vez más sofisticado, más empresas corren el riesgo de sufrir pérdidas a causa de actividades delictivas. Las amenazas tradicionales de robo y hurto fueron superadas por los eventos de delitos de cuello blanco y en el mundo actual la atención se centra ahora en los delitos cibernéticos. Las diferentes categorías de riesgos de fraude coexisten y son omnipresentes sin importar el tipo de industria o la escala del negocio.

Las reclamaciones típicas de seguros contra delitos implican deshonestidad de los empleados, malversación de fondos, falsificación, robo, fraude en Internet o cibernético, fraude en transferencias de fondos, falsificación y otros actos delictivos. Los esquemas y estafas son extensos y aprovechan los eslabones débiles en la gestión del riesgo de fraude, los procesos de auditoría y cumplimiento.

Los siguientes ejemplos son eventos de fraude comunes que afectan a todas las empresas:

- Un empleado que establece proveedores fantasmas o empleados fantasmas con el único propósito de robar dinero de la empresa.
- Transferencias de fondos no autorizadas
- Empleado en connivencia con una parte externa para la apropiación indebida de activos Compañía que recibe dinero falso
- Robo de inventario mientras se encuentra en tránsito o en las instalaciones (almacén), que a menudo involucra la colusión de empleados y terceros
- Piratería informática y fraude cibernético relacionado
- Informe de gastos de fraude de los empleados
- Falsificación de documentación financiera como cheques, giros bancarios, transferencias telegráficas y cartas de crédito.

Con la mayor sofisticación de los riesgos de fraude, los seguros tradicionales de infidelidad, dinero o tránsito ya no son soluciones efectivas de transferencia de riesgos.

Características clave del seguro

El seguro contra delitos protege a una empresa de la pérdida de dinero, valores, inventario u otra propiedad resultante de eventos de fraude.

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

El seguro contra delitos brinda cobertura contra:

- La pérdida directa por actos deshonestos o fraudulentos cometidos por los empleados o terceros
- La pérdida de dinero, valores o propiedad, ya sea en las instalaciones o en tránsito.
- Falsificación de instrumentos negociables como cheques y por pérdidas derivadas de terceros
- Delitos informáticos, incluido el fraude por transferencia de fondos.

Organizar una póliza contra delitos " adecuada para cada propósito "requiere experiencia y conocimientos incomparables, teniendo en cuenta que las diferentes aseguradoras tienen variaciones sutiles de redacción entre la deshonestidad de los empleados y el lenguaje de robo o el lenguaje de pérdida descubierta y pérdida sostenida que pueden tener un impacto significativo en la cobertura.

COBERTURA OTORGADA POR UNA POLIZA DE RESPONSABILIDAD CIBERNETICA

Las Empresas utilizan computadoras para enviar, recibir o almacenar **datos electrónicos**. Dichos datos pueden incluir proyecciones de ventas, registros de impuestos y otra información propiedad de la empresa. Si los datos se pierden, son robados o dañados debido a una brecha de seguridad, podría ser muy costoso reemplazarlos o restaurarlos.

El sistema informático también puede contener datos confidenciales que pertenecen a otras partes, como clientes, empleados o proveedores. Si los datos se pierden o son comprometidos por un pirata informático, los propietarios pueden demandar a la empresa por daños. La empresa también podría incurrir en gastos de notificación sustanciales. Prácticamente, los estados tienen leyes que requieren que las empresas informen a las personas cuya información personal se ha visto comprometida en una violación de datos. Puede proteger un negocio contra los costos asociados con las violaciones de datos comprando una póliza de responsabilidad cibernética.

El seguro de responsabilidad cibernética cubre las pérdidas financieras que resultan de violaciones de datos y otros eventos cibernéticos. La mayoría de pólizas cibernéticas incluyen coberturas

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

tanto propias como de terceros. Algunas coberturas pueden incluirse automáticamente mientras que otras están disponibles "a la carta".

Las coberturas propias pagan los gastos en los que incurre directamente la empresa como resultado de la infracción, como el costo de informar a sus clientes sobre un ataque de piratas informáticos. Las coberturas de terceros se aplican a reclamaciones contra la empresa por parte de personas o empresas que han resultado lesionadas como consecuencia resultado de sus acciones o falta de actuación. Por ejemplo, un cliente demanda por negligencia después de que un pirata informático roba sus datos personales de su sistema informático y los publica en línea.

Coberturas First Party [Primera persona]

Estos son los tipos de coberturas de primera persona que probablemente encontrará en una póliza de responsabilidad cibernética. Estas coberturas pueden estar sujetas a un deducible.

- **Pérdida o daño de datos electrónicos**: cubre el costo de reemplazar o restaurar datos electrónicos o programas dañados, destruidos o robados en una violación de datos, ya sea que los datos pertenezcan a la empresa o/a otra persona. Las pérdidas deben ser el resultado de un peligro cubierto, como un ataque de piratas informáticos, un virus o un ataque de denegación de servicio. Las políticas también pueden cubrir el costo de contratar expertos o consultores para ayudar a preservar o reconstruir los datos.
- **Pérdida de ingresos y gastos adicionales**: cubre las pérdidas de ingresos que sufre y los gastos adicionales en los que incurra para evitar o minimizar el cierre del negocio después de que el sistema informático falle debido a un peligro cubierto. Algunas pólizas, cubren las pérdidas de ingresos de dependientes. Estas son pérdidas de ingresos que sufre cuando se ha violado el sistema del proveedor de red propio.
- **Extorsión cibernética**: se aplica cuando un pirata informático irrumpe en el sistema informático y amenaza con cometer un acto nefasto, como dañar los datos, introducir un virus, iniciar un ataque de denegación de servicio o liberar datos confidenciales a menos que pague una suma específica. La cobertura generalmente se extiende a cualquier pago de extorsión que realice y a los gastos en los que incurra para responder a la demanda.
- **Costos de notificación**: cubre el costo de notificar a las partes (voluntariamente o según lo requiera la ley) afectadas por una violación de datos. También puede cubrir el costo de brindar servicios de monitoreo de crédito y establecer un centro de llamadas.

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

- **Daño a la reputación**: algunas pólizas cubren los costos en los que incurre en marketing y relaciones públicas para proteger la reputación de la empresa luego de una violación de datos. Esta cobertura puede denominarse **Manejo de Crisis**.

Coberturas de Responsabilidad de terceros

Las coberturas de responsabilidad que ofrece una póliza cibernética suelen operar por **reclamación**. La cobertura generalmente se aplica a daños o acuerdos que resulten de reclamos cubiertos, así como al costo de defensa. Los costos de defensa podrían reducir el límite del seguro.

- **Responsabilidad de privacidad y seguridad de la red**: cubre reclamos contra la empresa por actos negligentes, errores u omisiones que resultan en un ataque de denegación de servicio, acceso no autorizado, introducción de un virus u otra violación de seguridad del sistema informático. También cubre reclamos que alegan que no se protegieron adecuadamente los datos confidenciales almacenados en el sistema informático. Los datos pueden pertenecer a clientes, clientes, empleados u otras partes.
- **Responsabilidad** por medios electrónicos: el **seguro de responsabilidad por medios electrónicos** cubre demandas en contra de la por actos como difamación, y calumnia, infracción de derechos de autor, invasión de la privacidad o infracción del nombre de dominio. Generalmente, estos actos están cubiertos solo si son el resultado de su publicación de datos electrónicos en Internet.
- **Procedimientos regulatorios**: cubre las multas o sanciones impuestas a la empresa por las agencias reguladoras que supervisan las leyes de violación de datos. También cubre el costo de contratar a un abogado para que ayude en la respuesta a un procedimiento reglamentario.

Las pólizas de responsabilidad cibernética protegen el negocio de reclamos y gastos resultantes de una violación de datos.

Las políticas no están estandarizadas y contienen terminología única.

La mayoría de las pólizas son flexibles, por lo que pueden elegir las coberturas que se desee, acorde con la actividad de cada empresa.

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

TENDENCIAS DEL CIBERCRIMEN EN COLOMBIA

De algunas fuentes disponibles en la Internet, hemos extractado las siguientes noticias vinculadas con Delitos Informáticos, de la siguiente manera:

ABRIL DE 2012 – Fuente: El Espectador

Unos 338 mil millones de dólares se gastaron en 2010 para contrarrestar ciberataques.

¿Cuánto le costaría a una empresa o a un banco ser víctima de un delito informático? En costos de hardware seguramente nada, a menos que alguien se robara físicamente algún equipo de cómputo. Pero en términos de información confidencial que podría ser usada para extorsión o robo, o por proyectos confidenciales que van a manos de la competencia, o en cuestiones de confianza de los clientes, las pérdidas pueden ser millonarias.

De acuerdo con la firma de seguridad informática Kaspersky, más del 80% de los códigos maliciosos son desarrollados con el fin de robar información bancaria, y hay ataques semanales a los sistemas web de los bancos en la región.

"Si bien los bancos normalmente tienen un fuerte enfoque en seguridad, no están exentos de sufrir ataques maliciosos o algún robo de información interna por un empleado descontento o un ejecutivo que se va a la competencia. Las pérdidas que esto genera pueden ser grandes en términos económicos, pero son exponenciales en lo que se refiere a la confianza de sus clientes", comenta Andrés Velázquez, Presidente y Fundador de MaTTica.

Los costos relacionados con delitos informáticos pueden ir desde un aumento en la inversión en sistemas y personal de seguridad, hasta la cobertura de indemnizaciones, campañas de imagen, pérdida de competitividad ante el mercado, baja de acciones, etcétera. **Sin embargo, el ejecutivo subraya que las peores pérdidas pueden llegar de aquellos delitos que no se detectan o que se dejan sin investigar.**

"La manera de detectar a los insiders [se refiere a la persona o personas que debido a su posición dentro de una corporación, normalmente en los órganos de dirección, gozan del conocimiento de información confidencial o privilegiada acerca del estado financiero (o de cualquier índole) de una empresa; así como de las decisiones sobre el presente y decisiones futuras de una compañía.]

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

en una empresa es atraparlos mientras cometen un delito informático, o realizar una investigación a partir de una sospecha fundamentada. Y eso se puede hacer actualmente, gracias a la forensia informática. Siguiendo los procedimientos adecuados, podemos realizar investigaciones que ofrezcan pruebas digitales válidas, tanto en procesos administrativos como legales", indica Velázquez.

De acuerdo con el estudio de ciberdelito desarrollado por el Registro de Direcciones de Internet para América Latina y Caribe (**Lacnic**), **el phishing o robo de datos personales significa pérdidas anuales por unos US$93 mil millones de dólares, y afecta a unos 2.500 bancos que operan en la región,** en tanto los robos a cuentas de clientes suman otros US$761 millones de dólares.

Asimismo, según cifras del estudio de McAfee Inc. y Science Applications International Corporation, 25% de las organizaciones han sufrido la paralización o atraso de una fusión o adquisición, o bien de la implementación de un nuevo producto o solución, a causa de una filtración de datos o por una amenaza creíble de filtración de datos.

Cabe mencionar que empresas e instituciones de todo el mundo gastaron 338 mil millones de dólares en 2011, para combatir ataques cibercriminales, dos tercios de los cuales fueron delitos de fraude económico, de acuerdo con números ofrecidos durante el Programa de Ciberseguridad y Cibercrimen de la ONU.

OCTUBRE DE 2015 – Fuente: Silicon week

Colombia es uno de los países más atacados de la región y los delitos informáticos relacionados con fraudes producen grandes pérdidas de dinero.

La **Asociación Bancaria de Colombia ha anunciado** las cifras sobre denuncias y pérdidas por fraudes relacionados por delitos informáticos durante 2014, cuando se registraron un promedio de **11 denuncias diarias de fraudes asociados a delitos** informáticos y dejando pérdidas financieras superiores a **80 mil millones de pesos** sólo durante el pasado año.

"Las cifras que tenemos de la Policía hablan de que la participación del total nacional es del **24% en Bogotá, 13% en Medellín, Cali 11% y Bucaramanga 6%",** de acuerdo con el presidente de

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

la Asociación Bancaria de Colombia, Santiago Castro que explicó que estas cifras se recopilaron hasta el día 30 de septiembre de este año.

El directivo recordó que hay un estudio reciente presentado por la Asociación que afirmaba que el 21.73% de los incidentes de delitos cibernéticos que se registran en toda América Latina, llegan desde **Colombia**, lo que hace de este uno de los países que está más en el punto de mira de los ciberdelincuentes a nivel global.

Asobancaria explicó que con la llegada de la Navidad suelen aumentar los fraudes y recomendó a los usuarios llevar a cabo una serie de prácticas como cambiar sus claves o tener cuidado sobre dónde o a quién se entregan las informaciones personales.

Septiembre de 2017 – Fuente: Dinero

Los sectores económicos más impactados por el cibercrimen en Colombia

La firma de seguridad informática **Digiware** reveló este martes cuáles son los sectores económicos más impactados por el cibercrimen en Colombia durante el 2017.

En un evento realizado en Bogotá, **la compañía dio a conocer que en Colombia se registraron 198 millones de ataques cibernéticos en el último año.**

Colombia participó con el **8,05% del total de los delitos informáticos de América Latina**, lo que equivale a pérdidas por más de US$6.179 millones.

Con estas cifras, Colombia es quinto en la clasificación latinoamericana en materia de ataques informáticos.

Por países, **Digiware mostró que Brasil es primero y representa el 25,13% de los ataques a nivel regional, seguido por México con 15,53%, Venezuela 11,91% y Argentina con 9,63%.**

De acuerdo a Digiware, Chile representa el 7,04% de las pérdidas regionales (US$5.404 millones), por encima de Perú con el 6,23% (US$4.782 millones) y Ecuador con 4,50% (US$3.456 millones)

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

El coronel del Centro Cibernético de la Policía, Freddy Bautista, **alertó que los fraudes vía mail son cada vez más comunes a pesar de que están "subestimados".**

Añadió que a través de diversas modalidades, las redes criminales realizan hurtos a diario que superan los $100 millones en Colombia a través del correo electrónico.

Nombró el caso de una empresa colombiana del sector metalúrgico que perdió más de Us$300.000 a través de un ataque de este tipo, que a pesar de ser uno de los más comunes, no pierden vigencia.

Digiware determinó que 5 de cada 6 **ciberdelitos** exitosos en la región se deben a la suplantación de usuarios digitales, vulnerabilidades en aplicaciones, falta de parcheo, malware avanzado, sistemas ineficientes de monitoreo.

Diariamente, en Colombia se producen en promedio **542.465 ataques informáticos**. Así se distribuyen los ataques por sectores económicos:

- **El sector financiero:** 214.600 ataques por día (39,56%).
- **Telecomunicaciones:** 138.329 ataques por día (25,5%).
- **El sector Gobierno:** 83.756 ataques por día (15,44%)
- **Sector energético:** 19.583 ataques por día (3,61%)
- **Industria:** 51.263 ataques por día (9,45%).
- **Retail:** 34.934 (6,44%).

Frente a este elevado número de ataques, los expertos hicieron un llamado a los Gobiernos para que creen mecanismos y espacios de investigación para fortalecer la educación en seguridad informática.

Del mismo modo, los invitaron a tomar medidas a tiempo para hacer frente a la evolución de los ataques informáticos a partir de computación en la nube, **Blockchain**, apps, **IoT**, machine learning, entre otras tecnologías.

Otros de los datos relevantes publicados en el informe es que el impacto económico del cibercrimen podría ser de US$8 trillones en los próximos 5 años a nivel mundial, así mismo se expuso que 8 meses es el promedio de tiempo que una amenaza avanzada de

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

ciberseguridad pasa desapercibida en la red de una víctima y que US$3,62 millones es el costo promedio anual de un incidente de seguridad de una compañía.

En el marco de este evento, el experto en seguridad informática de Digiware, Andrés Galindo, comentó que ataques informáticos como **Petya** y **Wannacry** (wiper malware y ransomware) se deben principalmente a los avances tecnológicos y al crecimiento acelerado de la interconectividad.

*"Según nuestros datos en Colombia, Petya llegó a afectar a 16 empresas y, en la medida en que la tecnología avance, ataques como estos se convertirán en armas **cibernéticas** mucho más letales. La interconexión, por parte de las compañías filiales, el bajo control y medidas de seguridad ayudarán a propagarlos y las empresas colombianas en esta ecuación son un blanco ideal en América Latina"*, añadió.

Finalmente y con el propósito de brindar confidencialidad sobre la información aquí expuesta, invitamos a nuestros lectores a explorar el documento **TENDENCIAS CIBERCRIMEN COLOMBIA 2019 – 2020**, presentado por POLICIA NACIONAL, DIJIN, CCIT, TICTAC, SAFE y el patrocinio de otras marcas involucradas en temas de Seguridad Informática.

Este documento está disponible en la WEB:
https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Juan Carlos Lancheros Rueda
Cert CILA, BC´s Mech Eng, BC´s B.A, M.I.A, P.M.S, F.M.S.
C.E.O.