ANCORA INFORMA

COVID-19 Y RIESGOS CIBERNÉTICOS: AMENAZAS CRECIENTES

Por ANCORA Financial Lines

Durante las últimas semanas el mundo ha visto eventos que no tienen precedente en la historia contemporánea. Una pandemia originada por la propagación sin control del virus **SARS-Cov2** o mejor conocido como **Covid-19**, ha puesto prácticamente a todas las economías del mundo en jaque y tiene a prueba a distintos sectores de la economía; millones de colaboradores de empresas se han visto forzados a modificar sus rutinas de trabajo al famoso Home Office, mientras que muchos otros simplemente no tienen donde presentarse a trabajar.

En este entorno, otra clase de amenazas coyunturales y oportunistas se han hecho presentes, **otro tipo de virus**, el de la **delincuencia cibernética**. El entorno cibernético que permite mantener a flote la economía actual ante esta crisis, se ha vuelo al mismo tiempo, una de las principales amenazas para mantener la continuidad del negocio. De acuerdo con la firma de ciberseguridad CYE, **tan solo en Europa los ataques cibernéticos se han quintuplicado desde febrero a la fecha.**

Esta situación ha puesto a miles de compañías alrededor del mundo en una situación de alta exposición ante estos riesgos, según datos de The Economist, **para finales de abril habrá casi mil millones de personas laborando desde sus hogares en todo el mundo.** Algunos de los riesgos más palpables de esta nueva realidad son: interrupción del negocio ante ataques de cibercriminales que buscan dañar o robar datos, impedir el acceso al sistema **(DoS Attack)** y solicitar un rescate **(Ransomware)**, difundir información valiosa o incluso robar recursos de la compañía bajo la modalidad del famoso **Fraude de Ingeniería Social o Social Engineering.**

AUMENTO DE RIESGOS: FACTORES A CONSIDERAR

Millones de colaboradores de empresas alrededor del mundo se encuentran **laborando desde casa**. Lo anterior ha expuesto o saturado los sistemas digitales de muchas compañías, permitiendo a los hackers introducirse en los mismos y obtener información valiosa de todo tipo.

La fuerza laborar que se encuentra hoy en día trabajando desde casa ha tenido que adaptarse a procesos y programas digitales que posiblemente nunca antes había utilizado, incrementando el riesgo de abrir por error **archivos maliciosos** o permitir acceso a terceros malintencionados a sistemas seguros de la compañía.

La crisis sanitaria ha cambiado las prioridades y el enfoque de las empresas alrededor del mundo, provocando con ello una reducción en la difusión tanto interna (empleados) y externa (clientes), de **campañas contra "phishing" y ataques de "ransomware".**

La Ingeniería social ha sido foco de atención en los últimos meses. Esta consiste en hacerse pasar de forma fraudulenta por algún funcionario o directivo de la compañía, ya sea CEO, CFO o cualquier otro; utilizando mecanismos como correos electrónicos, documentos falsificados, llamadas y cualquier otro medio externo haciéndose pasar por cualquiera de estos directivos para engañar a colaboradores, solicitándoles el acceso a recursos de la empresa o a información valiosa como bases de datos de clientes. Incluso la Organización Mundial de la Salud (OMS) fue blanco de este tipo de modalidad criminal en semanas recientes.

Videoconferencias. Una de las herramientas más utilizadas en todo el mundo para mantener los niveles de servicio y atención de muchas empresas se ha visto altamente vulnerada. ZOOM, una de las aplicaciones de videoconferencia más famosas, ha sido vulnerada en distintos meetings donde ciberdelincuentes han mostrado contenido ajeno a la reunión, muchas veces de tipo pornográfico.

Asimismo, últimamente ha circulado en redes que el Directorio de **ZOOM, supuestamente** adhiere de forma automática personas distintas a las listas de contacto de empresas o personas físicas, si es que el email registrado comparte el mismo dominio. Lo anterior ha ocasionado que distintos usuarios desconocidos tengan acceso a correos electrónicos, nombres y fotografías de perfiles privados que no debieran conocer. Las consecuencias de lo anterior son graves; el lunes se presentó una Class Action en contra de ZOOM por la transferencia de datos sin autorización de los usuarios. El mismo día, el Procurador General de Nueva York envió una carta a ZOOM preguntando qué medidas de seguridad se han puesto en marcha ahora que la app se ha catapultado a la fama.

Interrupción de las actividades comerciales. Pareciera el peor momento para que un ataque cibernético obligue a una compañía a suspender su actividad, ya sea una fábrica de alimentos o una tienda departamental en línea, ambas pueden ser objeto de ataques que impidan la realización de su actividad productiva y comercial con el subsecuente costo para la entidad afectada.

¡ES TIEMPO DE PROTEGERSE!

01 CONCIENTIZAR A LOS COLABORADORES Y CLIENTES

Mantener vigentes las campañas de concientización ahora más que nunca, reforzar las políticas digitales y asegurarse de que tanto nuestros colaboradores desde casa, hasta nuestros clientes y usuarios de plataformas, conozcan los procesos y eviten caer en engaños de ingeniería social y/o acceder por error a sitios o programas que comprometan los sistemas de la empresa.

02 CONEXIONES SEGURAS

Las áreas de IT deben de mantener un control completo sobre los usuarios en los sistemas y asegurarse de que estos, vía remota, accedan desde conexiones y equipos seguros.

03 DISPOSITIVOS MÓVILES CONTROLADOS

Un tema que con frecuencia se queda fuera de la discusión; sin embargo, la experiencia dicta que **2 de cada 5 ataques cibernéticos a empresas ocurre desde o hacia un dispositivo móvil** y que la compañía afectada con frecuencia no tiene control o registro. Es importante tener un inventario y control de estos dispositivos en posesión de los empleados.

04 VIGENCIA DE LAS LÍNEAS DE DENUNCIA Y MECANISMOS DE CONTROL INTERNO

Difundir o en caso de no que no exista, establecer una línea de denuncia anónima a disposición de los empleados, con el fin de conocer lo antes posible potenciales actividades ilícitas como tráfico de información y datos personales, cometidas por colaboradores desde dentro de la entidad. Asimismo, establecer protocolos de control interno de conocimiento general.

05 CUMPLIMIENTO NORMATIVO

Tanto la **Ley Federal de Protección de Datos personales en Posesión de Particulares** como ciertas regulaciones especificas en ciertas industrias como el sector financiero, son marcos legales a los cuales cualquier entidad que posea datos de terceros debe sujetarse. El asegurarse que los requerimientos normativos en materia de protección de información se cumplan, es clave para aminorar el riesgo de sufrir pérdidas financieras derivadas del mal manejo de información.

06 DISPERSIÓN DEL RIESGO

Si bien, el mantener un control general sobre los sistemas de la empresa y poseer políticas claras y actualizadas es fundamental, **el riesgo de una vulneración o error interno,** aún más en la coyuntura actual es grande, por ello **es clave contar con una cobertura robusta de Riesgos Cibernéticos que proteja la continuidad del negocio de la compañía, así como proteja sus recursos ante posibles eventualidades de esta naturaleza.**

CONCLUSIÓN: UN NUEVO ENTORNO DE NEGOCIOS

Sin duda, una vez que hayamos transitado por la actual crisis sanitaria, el mundo y el entorno de negocios no volverán a ser igual. Muchas reglas cambiaran y procesos que antes requerían de la interacción humana, documentos y mecanismos físicos, se automatizarán. Es por ello que nuestra dependencia a los sistemas y medios electrónicos crecerá y con ello el riesgo de dependencia de dichos sistemas. Conceptos como ciberdelincuentes serán cada vez más comunes y pérdidas relacionadas con este riesgo aumentarán considerablemente.

Es vital que toda organización cuente con protección ante eventos de este tipo, por lo que ponemos a su disposición la experiencia que tenemos en la elaboración de programas a la medida para todo tipo de empresas e industrias con riesgos de esta naturaleza.

CONTACTO

JORGE SALAS
DIRECTOR NACIONAL DE VENTAS
jsalasb@ancora.com.mx

MARTHA VEGA
LÍNEAS FINANCIERAS
mvega@ancora.com.mx

MARIO ANDRADE
LÍNEAS FINANCIERAS
mandrade@ancora.com.mx

ANCORA. COBERTURA TÍPICA DE UN SEGURO CYBER

1 PÉRDIDAS PROPIAS

Extorsión Cibernética

Difundir Información Confidencial o Personal en el Sistema

Dañar o Borrar los Datos

Atacar el Sistema con Malware

Secuestrar los Datos

Impedir el Acceso al Sistema

Reembolso del pago de la extorsión

Si es asegurable y permitido localmente

Gastos relacionados con el Evento

- Consultores IT
- Consultores Legales
- Negociadores de Crisis
- Relaciones Públicas

Pérdida de Activos Digitales e Interrupción del Negocio

Acto Malicioso de Cómputo → Hackeo → Malware → Ataque de Denegación de Servicios → Uso o Acceso no Autorizado

Error Humano → Error de Programación Oculto → Falla de Energía bajo el control del Asegurado

Pérdida de Activos Digitales

- Costos de Reconstruir los Activos Digitales

Interrupción del Negocio

- Utilidad dejada de Percibir
- Gastos Adicionales para terminar la interrupción

2 PÉRDIDA DE TERCEROS

Gastos de Defensa

Acciones Regulatorias

Multas Regulatorias

Perjuicios

Tarjetas de Pago

Fondo de Compensación

Contenidos Electrónicos

- Derechos de Autor, Piratería , Plagio
- Difamación, Injuria, Calumnia
- Infracciónes a una marca o nombre comercial
- Negligencia en la creación de contenido Electrónico

GASTOS PARA MITIGAR UN INCIDENTE

Forenses IT

Cumplir Regulaciones

Asesoría Legal Regulatoria

Manejo de Crisis Reputación

Monitoreo de Créditos

Restauración de Identidad

Servicios de Notificación

USD 250,000

COSTO PROMEDIO DE UNA RECLAMACIÓN

FUENTE: CHUBB Cyber 2018. Capacitación Comerciales Mex.

ANEXO 1
RIESGOS CIBERNÉTICOS - PRINCIPALES INDICADORES

Allianz RISK BAROMETER

2,415 EXPERTOS EN RIESGO DE 86 PAÍSES
- CEO's
- Directores Ejecutivos
- Suscriptores
- Brokers
- Administradores de Riesgo
- Ajustadores

RISK BAROMETER
TOP BUSINESS RISKS FOR 2019

10 DISMINUCIÓN DE MANO DE OBRA CALIFICADA

09 PÉRDIDA DE REPUTACIÓN O VALOR DE MARCA

08 CAMBIO CLIMÁTICO

07 NUEVAS TECNOLOGÍAS

06 INCENDIO Y EXPLOSIÓN

05 EVOLUCIÓN DE LOS MERCADOS

04 CAMBIOS EN LEGISLACIÓN Y REGULACIÓN

03 CATÁSTROFES NATURALES

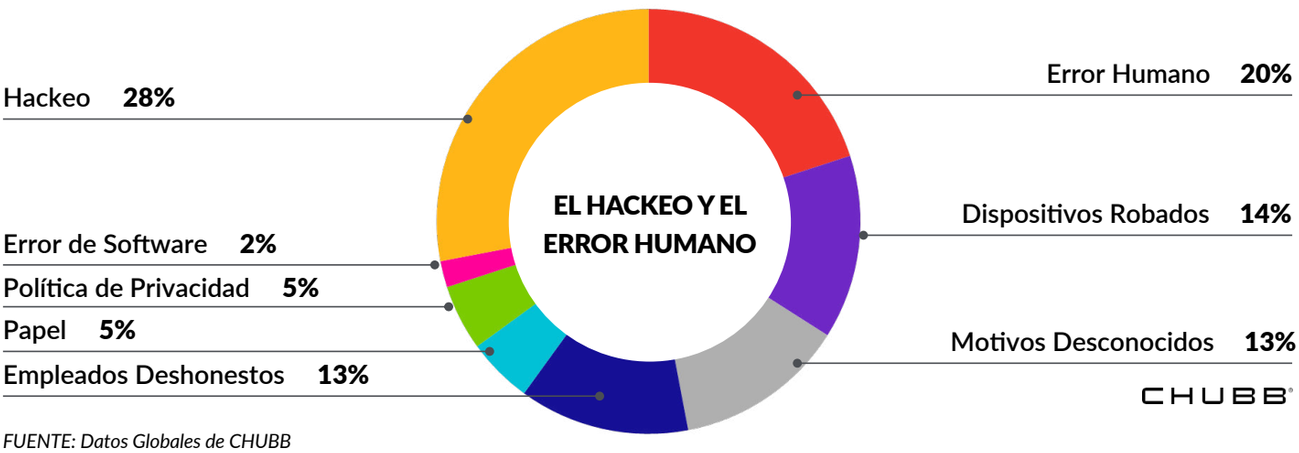
02 INCIDENTES CIBERNÉTICOS

CYBER INCIDENTS #2=2018
1. *Cyber Crime*
2. *Falla de Sistemas*
3. *Data Breach*
4. *Multas y Sanciones*

Cyber Crime cuesta a la Economía Global
US 600 BN anuales

01 INTERRUPCIÓN DE NEGOCIO

PRINCIPALES TRIGGERS DE EXPOSICIÓN DE LA ÚLTIMA DÉCADA



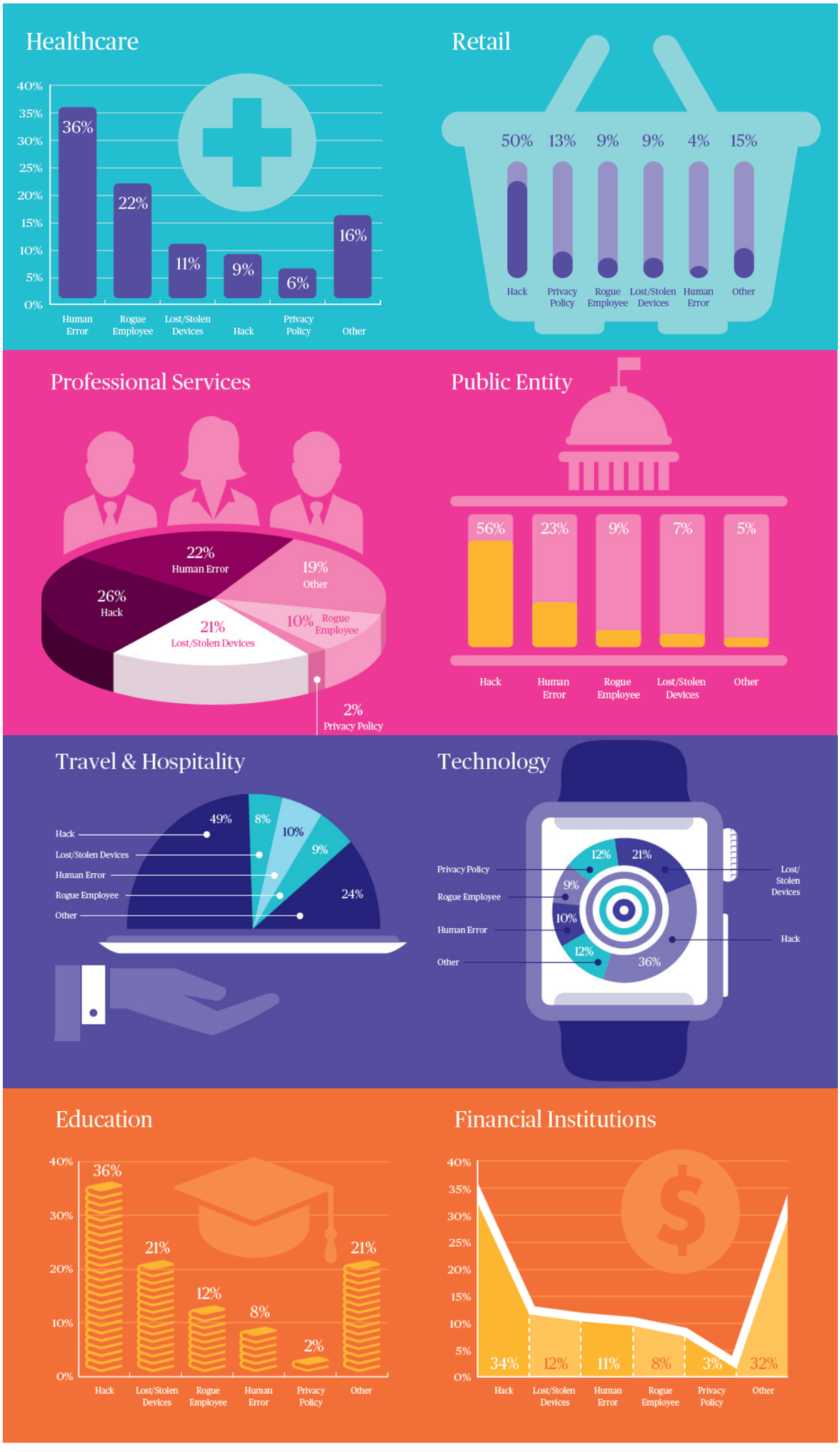
FUENTE: Datos Globales de CHUBB

MAYORES IMPACTOS DE LOS INCIDENTES CIBERNÉTICOS EN ORGANIZACIONES

FUENTE: The future of cyber survey 2019. Deloitte

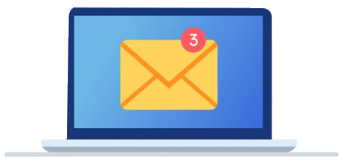
ANEXO 2

TRIGGERS DE EXPOSICIÓN POR INDUSTRIA EN LA ÚLTIMA DÉCADA



FUENTE: Datos Globales de Chubb (10 años de datos hasta Dic 2017)

ANEXO 3
EJEMPLOS DE SINIESTROS CYBER

ESCENARIO 1: ERROR HUMANO	IMPACTO POTENCIAL	
Un encargado de selección de personal para una organización de salud adjuntó accidentalmente el archivo equivocado al enviar un correo electrónico a cuatro solicitantes de empleo. El archivo incluía datos demográficos de recursos humanos de 43,000 nombres, direcciones y documentos de identificación de exempleados. El asegurado llamó a la Línea de Respuesta de Incidentes de la aseguradora para asistencia y se asignó un Gerente de Respuesta de Incidentes. Se gestionaron servicios legales para manejar implicaciones normativas. 	**Responsabilidad de Privacidad** Manejo inadecuado de información personal y/o corporativa confidencial, violación de la política de privacidad de la compañía. • Gastos de defensa resultantes de investigación normativa. • Costos de defensa y conciliación por demandas de empleados cuya identidad fue hurtada. **Gastos de Respuesta a Incidentes** • Honorarios del Gerente de Respuesta a Incidentes. • Notificación a individuos afectados. • Servicios de monitoreo de hurto de identidad para individuos afectados. • Honorarios de asesoría legal.	**USD 78,571** **USD 142,857** **USD 7,143** **USD 4,286** **USD 19,643** **USD 14,286**
Para Considerar Tan inocente como puede parecer, el error humano puede ser muy costoso y ocurre con más frecuencia de lo esperado. Es importante entender que eventos de cyber no se relaciona solo con incidentes tecnológicos. Muchas de las reclamaciones que vemos radican en errores muy simples.		**USD 266,786** COSTO TOTAL

ESCENARIO 2: ATAQUE DE DENEGACIÓN DE SERVICIO	IMPACTO POTENCIAL	
El centro de datos que alojaba la página web de una compañía de ventas en línea al detalle se convirtió en objetivo de un ataque distribuido de denegación de servicio (DDoS), que utilizaba dispositivos hackeados conectados a Internet de las cosas, inundó la red del centro de datos con tanto tráfico que su red colapsó. Esto hizo que la página web de la compañía de ventas en línea al detalle estuviera sin acceso durante seis horas antes que los sistemas de respaldo pudieran restaurar la funcionalidad al 100%. El asegurado en este caso es la Compañía de ventas en línea. Después de llamar a la Línea de Respuesta a Incidentes de la aseguradora, se asignó un Gerente de Respuesta a Incidentes. 	**Costos de Recuperación** • Aumento de Costos, debido al trabajo requerido para tener la página web operando apropiadamente. • Costos por subcontratar con un proveedor de servicios externo. **Reducción de la Utilidad** • Ventas y ganancias perdidas por el tiempo muerto de la página web. **Gastos de Respuesta a Incidentes** • Firma de TI forense. • Honorarios de asesoría legal. • Honorarios de Gerente de Respuesta a Incidentes.	**USD 13,214** **USD 17,857** **USD 136,071** **USD 17,857** **USD 14,286** **USD 8,571**
Para Considerar Los ataques distribuidos de denegación del servicio (DDoS) se hacen más potentes a medida que aumenta el uso de dispositivos hackeados, conectados al Internet de las Cosas. Para minimizar el impacto de un escenario como este, es importante construir un plan de continuidad del negocio que asegure que las aplicaciones, sistemas y actividades críticas del negocio no se apoyen en un solo proveedor crítico de TI. Los gerentes de respuesta a incidentes y proveedores que hacen parte del equipo de respuesta de la aseguradora, tienen experiencia en el manejo de ataques de DDoS y le asistirán en poner su negocio nuevamente en marcha tan pronto como sea posible.		**USD 207,857** COSTO TOTAL

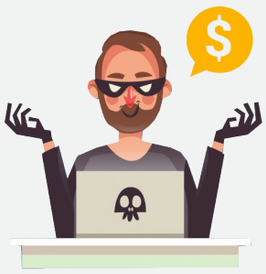
FUENTE: Datos Globales de Chubb (10 años de datos hasta Dic 2017)

ANEXO 4
FLUJOGRAMA DE UN SINIESTRO CYBER

Antes del Incidente...

Comunícate al centro de respuesta de incidentes en caso de algún incidente.

Al ocurrir un incidente...



01

Llama al número del Centro de Respuesta de Incidentes de la aseguradora 24/7 manejado por First Responder.

El contacto con la Línea de Respuesta a Incidentes será reportado al departamento de indemnizaciones de la aseguradora y constituirá automáticamente un aviso de circunstancia bajo la póliza. En caso de que usted quiera realizar la notificación directamente a la aseguradora de forma separada, por favor indíquelo a First Responder.

02

Asignamos a un supervisor de respuesta de incidentes. Ellos emitirán un plan de acción dentro de las primeras 5 horas de la llamada y te guiarán a través de cada paso.

Te pedirán acordar un convenio con la compañía First Responder para los Servicios de Respuesta de Incidentes en caso de no haberlo hecho anteriormente.

El equipo de reclamaciones de la aseguradora te contactará para discutir la manera en que tu póliza responderá al incidente.

03

El supervisor de respuesta de incidentes movilizará a las personas de nuestro panel dentro de las primeras 24 horas. Esto puede incluir Forenses de TI, expertos de RP, equipos legales, especialistas en fraudes, contadores forenses y otras asistencias necesarias.

04

Una vez que el incidente esté bajo control, los especialistas de panel asignados te guiarán para regresar a la normalidad a tu negocio.

05

El panel de especialistas la asguradora te proporcionará análisis, remedios futuros, un resumen de lecciones aprendidas y consejos para mitigar riesgos.