Contáctenos

Chubb Seguros Chile S.A.
Miraflores 222, Piso 11
Santiago Centro
Chile
T +562.2549.8300

www.chubb.com/cl

Con fecha 14 de enero de 2016, ACE Limited adquirió Chubb Corporation. La adquisición no tiene un efecto inmediato sobre ACE Seguros de Vida S.A., ACE Seguros S.A., Chubb de Chile Compañía de Seguros Generales S.A.
Las pólizas de seguros suscritas con estas empresas permanecerán vigentes, respetándose la totalidad de sus términos y condiciones, y continuarán siendo celebradas con la empresa filial hasta nuevo aviso.

Chubb. Insured.℠

Para consultar la totalidad de los términos y condiciones por favor remitirse a la póliza de cada producto o consultar a Chubb Seguros.

CHUBB®

Chubb Cyber Riesgos

Póliza para la gestión de riesgos cibernéticos

Chubb en Chile, a través de ACE Seguros S.A. ofrece el producto Chubb Cyber Riesgos

Contenido

Administración de Riesgos Cibernéticos

En el conectado entorno de hoy en día, la seguridad cibernética se ha convertido en una preocupación común. Sin embargo, los analistas temen que en muchos sectores industriales, algunas de las empresas no estén tomando en serio su responsabilidad. Frecuentemente, las empresas no entienden los riesgos de privacidad de datos y cibernéticos en su organización hasta que sucede una situación de este tipo.

Cualquier empresa podría verse afectada por incumplimiento relacionado con el manejo de la información sensible de sus clientes o empleados. Incluso, el extravío de un equipo portátil, si no se gestiona adecuadamente, puede convertirse en un desastre en las relaciones públicas de la empresa, destruyendo no sólo la marca, sino también sus finanzas. Como líder mundial en seguros cibernéticos, Chubb entiende el negocio de la protección.

A través de nuestra experiencia y capacidades en todo el mundo, junto con la experiencia en Chile en seguros y gestión de riesgos, trabajamos para ayudar a las empresas en su crecimiento de manera confiable.

Una solución completa en riesgos

Más de 15 años de experiencia en riesgos cibernéticos

Nuestro equipo Global dedicado a la cibernética, cuenta con una experiencia de más de 15 años en suscripción y siniestros.

Con esta experiencia internacional, estamos preparados para entender y responder a los retos actuales y futuros en riesgos cibernéticos de nuestros clientes.

Nuestros suscriptores y especialistas en riesgos, apoyan a nuestros clientes ayudándoles a identificar y prevenir las posibles situaciones que pudieran ocasionar incidentes cibernéticos

Pasando de los seguros a la gestión de riesgos empresariales

Nuestros suscriptores y especialistas en riesgos, apoyan a nuestros clientes ayudándoles a identificar y prevenir las posibles situaciones que pudieran ocasionar incidentes cibernéticos, previo a la contratación de una póliza. Estamos orgullosos de ayudar a convertir el mercado de seguros de una simple póliza, a una solución integral de control de pérdidas y gestión de riesgos.

La respuesta al incidente es la clave

En Chubb sabemos que cuando se trata de un evento cibernético, las primeras horas son cruciales por lo que contamos con la disponibilidad de un gerente dedicado a la atención de incidentes; una de las características importantes de Chubb. Con disponibilidad los 365 días del año, las 24 horas al día, un experto evalúa la situación, atiende las situaciones urgentes y toma las medidas apropiadas en el momento indicado cuando se requiera de la atención de expertos en cualquier lugar del mundo, dependiendo de las circunstancias enfocadas en las necesidades del cliente.

La mejor oferta del mercado

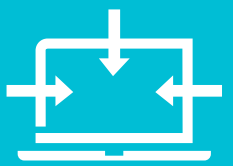
- Equipo de atención a siniestros disponible 24/7, brindando atención ante cualquier situación de riesgo cibernético
- Asistencia de proveedores que proporcionan una avanzada administración de riesgos durante la vigencia de la póliza
- **Sencillez de la póliza y estructura de soluciones integrales con el respaldo de un asegurador global de clasificaciones de solidez financiera AA de Standard & Poor's y A++ de A.M. Best.**

Principal riesgo emergente: Riesgo tecnológico

De acuerdo a nuestro Barómetro de Riesgos Emergentes 2015, con respuesta de 500 encuestados en 25 países, mostró que el 43% de los expertos expresaron el riesgo tecnológico como su principal preocupación. También indicaron que es el riesgo que consume la mayor cantidad de tiempo y recursos entre los riesgos emergentes y en consecuencia el mayor impacto financiero en sus negocios.

La tecnología juega un papel importante en casi toda planeación estratégica de las empresas, ya sea en el diseño de nuevos servicios o productos, hasta el desarrollo de mejoras operativas. Sin embargo, cuando se trata de la administración de riesgos tecnológicos, las investigaciones sugieren que las compañías pueden no estar enfocándose en las áreas correctas ante las probables fuentes de amenazas debido a la falta de conocimiento.

Actualmente, los siguientes aspectos de riesgo tecnológico crean preocupación en los expertos en riesgos:



33 %
Hackeo/Ataques de denegación de servicio

30 %
Fallas del sistema

29 %
Amenazas de los avances tecnológicos en el modelo de negocio existente

Nuestro equipo de Chubb

En Chubb sabemos que los riesgos cibernéticos no respetan fronteras y pueden atacar desde cualquier lugar y en cualquier momento a cualquier organización con consecuencias globales. Por ello, hemos establecido las Prácticas Globales Cibernéticas de Chubb.

Esta es una red de especialistas de Chubb en riesgos cibernéticos alrededor del mundo. Juntos, se aseguran de tener una consistente e inmediata respuesta a riesgos cibernéticos y a las necesidades del mercado de forma global.

En Chile, nuestros especialistas forman parte integral de esta red.

Un equipo de suscripción local en Chile y Latinoamérica, trabajan en conjunto para entregar soluciones de Administración de Riesgos Cibernéticos.

Este equipo de especialistas, entiende los retos que las instituciones enfrentan hoy día y quienes en conjunto con nuestros ingenieros en riesgos de IT, se especializan en desarrollar soluciones personalizadas para cubrir las necesidades específicas de las compañías con operaciones en México y en otras partes del mundo.

Chubb Cyber Riesgos
Escenarios

Considere los siguientes escenarios con base en experiencias actuales de siniestros y pregúntese si cuenta con un seguro adecuado:

Violación al Gobierno Corporativo de parte de los empleados

Causa de la acción:
Negligencia y violaciones que derive en la interrupción de operaciones

Detonante de la cobertura:
Interrupción del negocio, responsabilidad por privacidad, costos de recuperación, gastos por reparación de daño

Tipo de empresa:
Comercio

Número de empleados:
20

Ingreso anual:
$5 millones USD

Descripción de la situación:
Un empleado de una tienda de computadores ignoró las políticas y procedimientos internos y abrió un aparentemente inofensivo archivo dentro de un email. Al día siguiente, los sistemas de pedidos y las cajas registradoras comenzaron a fallar y el sistema estaba deficiente a consecuencia de fallas en la red.

Resultado:
La tienda de computadores incurrió en $100,000 USD en gastos de investigación y recuperación. También se incrementaron los gastos de operación en $20,000 USD y se perdieron ingresos por $50,000 USD derivado de las operaciones deficientes.

Gastos totales asociados al evento:
$170,000 USD

Invasión de la privacidad a consecuencia de robo de laptop

Causa de la acción:
Negligencia por robo de laptop que llevó a la invasión de la privacidad

Detonante de la cobertura:
Gastos por reparación del daño, responsabilidad por privacidad, interrupción del negocio, costos de recuperación, multas, extravío de tarjetas

Tipo de empresa:
Empresa de Energía

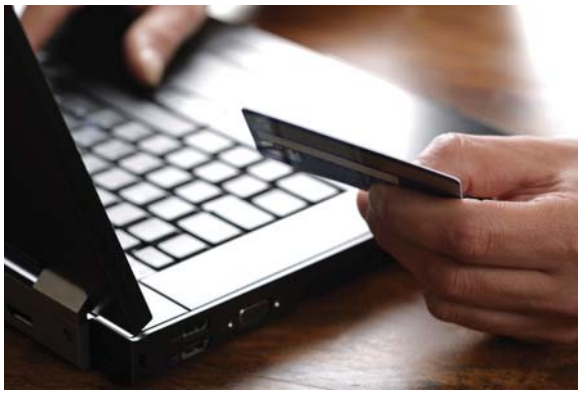
Número de empleados:
100

Ingreso anual:
$20 millones USD

Descripción de la situación:
La laptop de un ejecutivo de una empresa de energía fue robada de un auto de la empresa. La laptop contenía información importante de clientes y empleados. A pesar de que el archivo estaba encriptado, la contraseña de acceso al equipo era sencilla y el NIP del archivo estaba comprometido.

Resultado:
Después de evaluar la naturaleza de la información de la laptop con un experto en investigación forense y un consejero de cumplimiento externo con un costo de $50,000 USD, la compañía decidió voluntariamente notificar a los clientes importantes y empleados. También instaló un call center, monitoreo y restablecimiento de servicios. Los costos extras ascendieron a $100,000 USD y la compañía incurrió en gastos por $75,000 USD correspondientes a la investigación regulatoria en varios estados. Finalmente, la compañía fue multada con $100,000 USD por apartarse de su política de privacidad de datos.

Costo total:
$325,000 USD



Extorsión cibernética, interrupción del negocio y gastos extras a consecuencia de robo de información

Causa de la acción:
Violación del contrato y negligencia

Detonante de la cobertura:
Extorsión cibernética, gastos por reparación del daño, responsabilidad por privacidad, interrupción del negocio, costos de recuperación

Tipo de empresa:
Firma de abogados

Número de empleados:
55

Ingreso anual:
$20 millones USD

Descripción de la situación:
Una organización desconocida vulneró la red de una firma de abogados y obtuvo acceso a la información sensible de los clientes, incluyendo la propuesta de adquisición de una compañía pública, información de una empresa pública de patentes de tecnología, el prospecto de un inversionista y una considerable lista de acciones legales con información personal identificable de los demandantes. Un investigador forense de tecnología determinó que un malware fue instalado en la red. Poco tiempo después recibieron una llamada del delincuente pidiendo 10 millones USD para no subir la información a internet.

Resultado:
La firma de abogados incurrió en gastos por $2 millones USD por la investigación, negociación, reembolso del dinero pagado por el asegurado para terminar la extorsión de acuerdo con lo permitido por la ley, notificaciones, monitoreo de créditos y robo de identidad, servicios de recuperación y honorarios de consultores independientes. Igualmente tuvo pérdidas por $600,000 USD debido a la interrupción del negocio y gastos adicionales asociados a la desconexión del sistema.

Costo total:
$2.6 millones USD

Un empleado con acceso al sitio de Recursos Humanos, vende información personal de empleados

Causa de la acción:
Negligencia y responsabilidad por privacidad

Detonante de la cobertura:
Gastos por reparación del daño y pérdida de datos

Tipo de empresa:
Firma de servicios profesionales

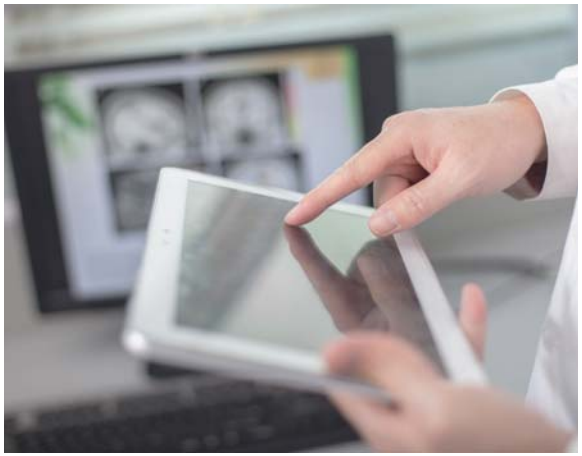
Número de empleados:
25

Ingreso anual:
$7.5 millones USD

Descripción de la situación:
Un empleado deshonesto accedió a la plataforma de Recursos Humanos de un proveedor de servicios profesionales. El empleado extrajo información y la vendió al mercado negro antes de ser aprehendido. Por consiguiente, varios casos de robo de identidad fueron realizados en contra de empleados de la firma.

Resultado:
El proveedor de servicios profesionales contrató un investigador forense y un consultor de cumplimiento externo. También comunicó a los empleados sobre la violación, estableció un call center y proporcionó monitoreo y reparación del daño a los empleados afectados.

Costo total:
$75,000 USD



Un fabricante paga por invasión a la privacidad perpetrada por un intermediario

Causa de la acción:
Un intermediario roba información personal derivando en negligencia e invasión a la privacidad

Detonante de la cobertura:
Gastos por reparación del daño, pérdida de datos y responsabilidad por privacidad

Tipo de empresa:
Fabricante

Número de empleados:
50

Ingreso anual:
$10 millones USD

Descripción de la situación:
Un fabricante arrendó una copiadora por dos años. Durante ese periodo la compañía realizó copias de información personal identificable propiedad de clientes y empleados, incluyendo números de cuentas de pensión, número de licencia de conducir y otra información que facilitaba la identificación personal. Al finalizar el plazo de arrendamiento el fabricante devolvió la copiadora al arrendador a través de un intermediario. Previo a la devolución de la copiadora, un empleado deshonesto del intermediario, accedió a la información de la copiadora con fines maliciosos.

Resultado:
El fabricante incurrió en gastos por $75,000 USD para la contratación de una investigación forense, notificaciones, monitoreo de la identidad, reparación del daño y honorarios de un consultor independiente. También incurrió en gastos por $100,000 USD en defensa legal.

Costo total:
$175,000 USD

Acerca de Chubb

Chubb es la compañía de seguros de propiedad y daños que cotiza en bolsa más grande del mundo. Con operaciones en 54 países ofrece seguros comerciales y personales en daños y bienes, accidentes personales, seguros complementarios de salud, reaseguro y vida a un diverso grupo de clientes.

La compañía se distingue por un extenso portafolio de productos y servicios, capacidad global de distribución, una excepcional fortaleza financiera, excelencia en suscripción, gran habilidad en la gestión de reclamaciones y operaciones locales globalmente.

Las aseguradoras de Chubb atienden a corporaciones multinacionales, pequeñas y medianas empresas a las que ofrecen servicios y seguros de propiedad y daños; clientes patrimoniales y de alto valor que requieren de protección a sus apreciables bienes; personas que adquieren seguros de vida, accidentes personales, salud complementaria, hogar y otras coberturas especializadas; compañías y grupos de afinidad que ofrecen o proveen programas de accidentes y salud y seguros de vida a sus empleados o miembros y a aseguradoras que administran el riesgo con coberturas de reaseguro.

Para más información visite www.chubb.com/cl

Riesgos Cibernéticos
Definiciones

Los riesgos cibernéticos cada vez más forman parte del diálogo entre nuestros agentes y sus clientes, ofrecemos una guía corta con la terminología asociada con términos y definiciones de uso común con fines informativos. Para más información sobre este u otros temas, por favor contacte a su agente.

- **Ataque DoS (Denial of Service Attack).** Tipo de ataque en un servidor que es diseñado para inundarlo de información sin valor.
- **Ataque DDos (Distributed Denial of Service).** La información de entrada que inunda al network de la víctima se origina de diferentes fuentes, haciendo difícil la detección de usuarios/tráfico legítimos de los falsos y casi imposible de detener dado que el origen está en muchos puntos.
- **Ataque Waterhole.** Ataque donde los usuarios son llevados a un sitio comprometedor en donde el atacante planta malware en los visitantes del sitio.

- **Botnet.** Se refiere a una red de computadoras "robot" que automáticamente transmiten spam, malware, o virus sin el conocimiento del usuario. También son llamadas "zombies" dado que usalmente son inyectados por un troyano y controladas por el creador del botnet y no por el dueño de la computadora.
- **CERT (Equipo de respuesta a Emergencias de Computadora).** Equipo de expertos que manejan incidentes de seguridad cibernética.
- **Cyber.** Frefijo usado en numerosos términos que describen cualquier cosa relacionada con el internet. El ciberespacio es un terreno no físico creado por sistemas computacionales.
- **Hacker White Hat.** Hacker que usa sus habilidades para exponer vulnerabilidades del sistema antes de que hackers maliciosos (conocidos como Black Hat Hackers) las exploten. Típicamente son contratados por las organizaciones para mejorar los sistemas de seguridad.
- **IDS (Sistema de Detección de Intrusión).** Sistema pasivo de monitoreo diseñado para alertar sobre actividades sospechosas que pueden resultar en virus, worms (gusanos) o hackeo. IDS no es un firewall ya que unicamente señala alertas y no las previene o detiene.
- **IPS (Sistema de Prevención de Intrusión).** Combinación de un IDS y una aplicación firewall para protección. El IPS es generalmente considerado como la próxima generación del IDS.
- **Inyección SQL (Lenguaje Estandar Query).** Forma de ataque a un sitio con base de datos en donde el atacante "inyecta" comandos SQL no autorizados para atravesar firewalls. Esta es una forma muy común de intrusión en el crimen cibernético.
- **Malware.** Abreviación de software malicioso, generalmente diseñado para accesar secretamente a un sistema sin el consentimiento del dueño y roba información con fines ilegales. Malware incluye virus, caballo de troya, crimeware, rootkits y worms (gusanos).

- **Metatags.** Código oculto insertado en páginas web que permiten a los buscadores a agrupar rápidamente la información a cerca de las páginas.
- **PCI DSS (Sistema de Seguridad de la Industria de Pago con Tarjeta, a veces denominado PCI).** Estándar de seguridad de propiedad de información desarrollado por MasterCard, Visa, American Express, Discover y JCB International usado para asistir comercios en la prevención de fraudes con tarjeta y mejorar la seguridad en torno en el procesamiento y almacenamiento de información de tarjetas. PCI direcciona los requerimientos mínimos de seguridad como firewalls, encriptamiento y antivirus.
- **Phishing.** Una estafa y/o timo en internet que recopila información personal. Spear phishing está más dirigido a recolectar información de usuarios específicos o confidencial.
- **PII (Información Personal Identificable).** Información única que establece una identidad individual.
- **PKI (Infraestructura de Llave Pública).** Sistema de certificados digitales, autenticaciones y otras autoridades de registro que verifican y autentican la validez de cada parte involucrada en una transacción de Internet. PKIs están evolucionando y no hay un estándar para configurarlos.

- **Rootkits.** Software malicioso que es activado cada vez que el sistema empieza a funcionar. Son difíciles de detectar porque son activados antes de que el sistema operativo ha empezado a funcionar por completo. Los Rootkits pueden interceptar información de terminales, conexiones a red y del teclado.
- **Servicios en la Nube.** Un tipo de recursos de computación que se basan en compartir y usar recursos vía internet en lugar de servidores locales o equipos personales para manejar aplicaciones.
- **Software de aplicaciones (a veces llamados programas para end-user).** Incluyen programas de bases de datos, procesadores de palabras, hojas de cálculo. Estas no se pueden usar si no se tiene un sistema operativo y utilidades de sistema.
- **Sniffer.** Programa o equipo que monitorea el viaje de información en un servidor. Estos programas pueden ser usados tanto para fines legítimos e ilegítimos.
- **Troyano Caballo de Trojano.** Programa destructivo que se distingue a él mismo como una aplicación benigna pero que está diseñada para destruir y borrar archivos. usualmente no son detectados por software antivirus.

- **Worms (Gusanos).** Es un tipo especial de virus que se puede autoreplicar y usar memoria. Pero a diferencia de un virus, los worms (gusanos) no pueden atacar a otros programas.
- **Virus.** Programa que es cargado en una computadora y que inicia sin el conocimiento del usuario. Todos los virus de computadoras son hechos por el hombre e incluso autoreplicables . Es peligroso porque rápidamente usan la memoria disponible y llevan al sistema a detenerse. Otros tipos mas peligrosos de virus son capaces de transmitirse a ellos mismos a lo largo de redes sobrepasando los sistemas de seguridad.
- **Vulnerabilidades Día cero.** Vulnerabilidad en un código fuente que es desconocida por el desarrollador cuando es tomado por hackers para lanzar un “ataque día cero”.

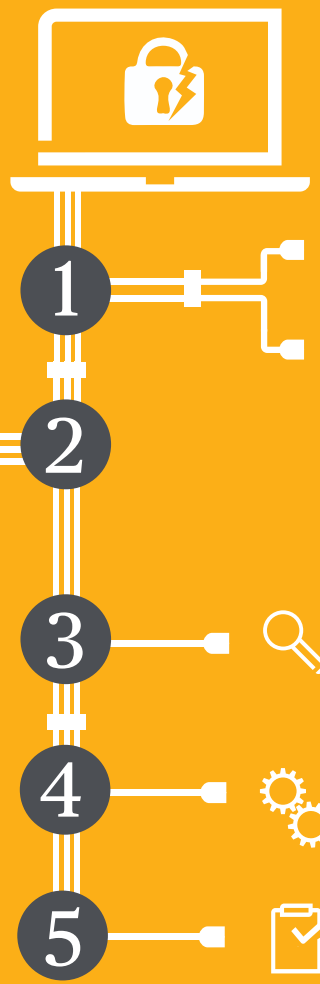
Chubb Cyber Riesgos

Diagrama de Flujo de Incidentes

Antes del incidente...

Decide si serás tú o tu agente quien se comunique al centro de respuesta de incidentes en caso de algún incidente.

Al ocurrir un incidente



1. Llama al Centro de Respuesta de Incidentes Chubb Cyber 24/7 manejado por Crawford.

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

2. 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 Crawford & Company para los Servicios de Respuesta de Incidentes en caso de no haberlo hecho anteriormente.

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

3. 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.

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

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