# Riesgos Cibernéticos.

Una amenaza creciente para nuestra industria.

# Tendencias.

- Se prevé que la industria del seguro cibernético alcance los US$ 20 mil millones en primas para el 2025.

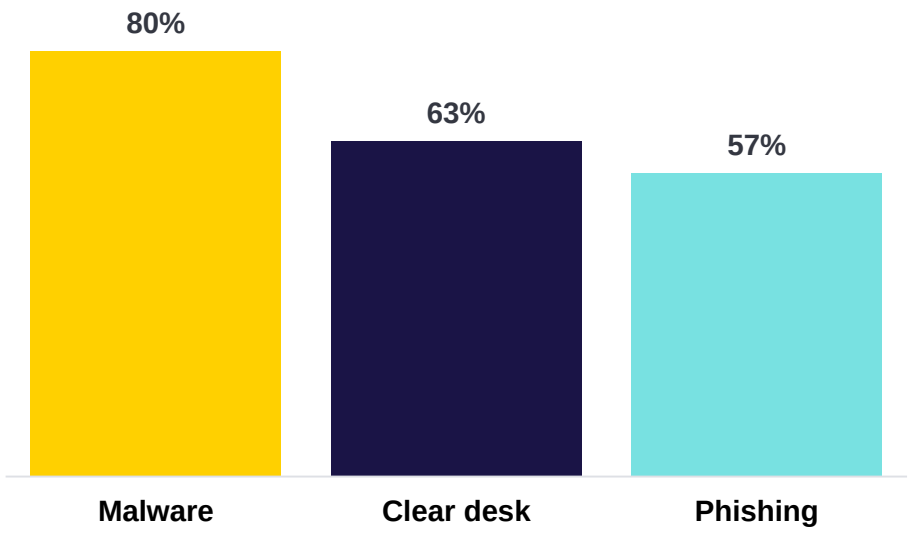
- Pérdidas relacionadas a delincuentes cibernéticos esta proyectada en $6 trillones anuales para el 2021. (Cybersecurity ventures)

# América Latina / Reporte OEA.

- En LatAm 9 de cada 10 bancos sufren ataques cibernéticos.
- 92% de las entidades bancarias de América Latina fue víctima de algún ataque cibernético en el 2018 y un 37% de las entidades sufrió un ataque en el que los piratas informáticos tuvieron éxito en su asalto.
- 49% de las entidades financieras carece de herramientas o controles usando tecnologías digitales emergentes.
- Convencer a la alta dirección de invertir en soluciones de seguridad digital es medianamente complejo.

# América Latina / Reporte OEA.

Los eventos más identificados durante el año 2017 fueron:



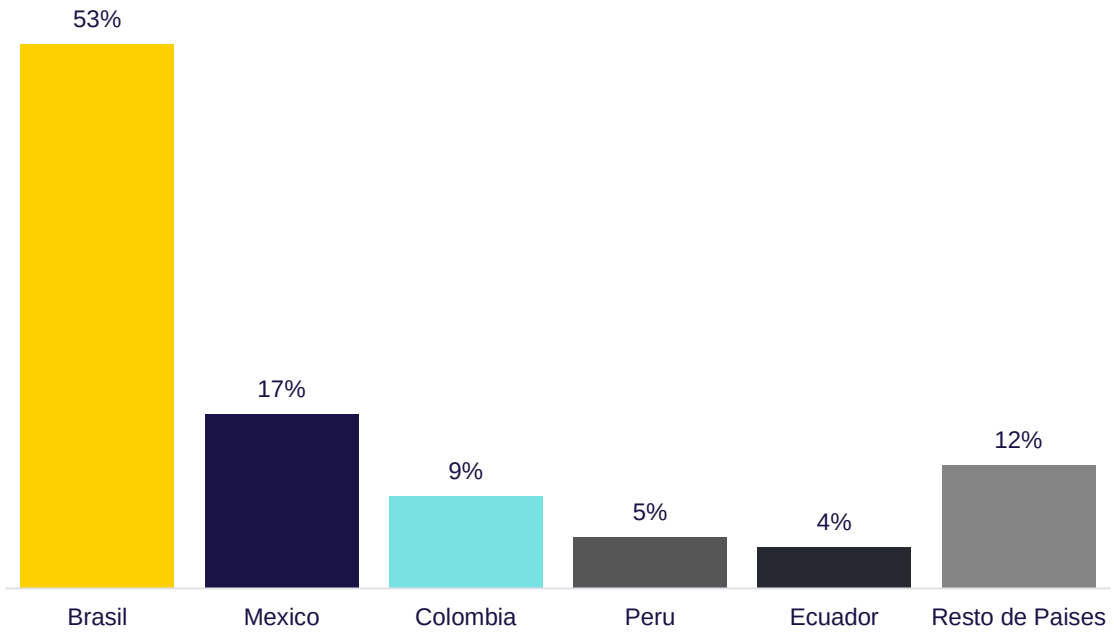

Costos estimados anuales por respuestas y recuperación ante incidentes de seguridad digital de las entidades bancarias en LatAm para 2017:

# Incidentes por victimas y tamaño de organización

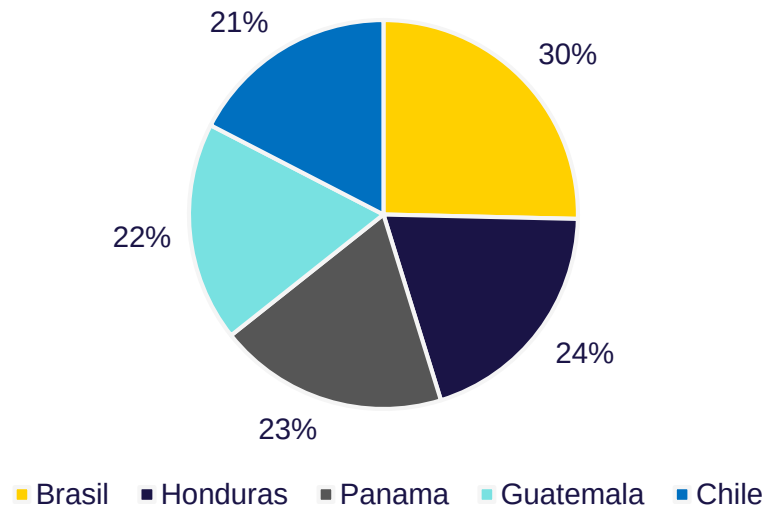
| Industry | Incidents Large | Small | Unknown | Total | Breaches Large | Small | Unknown | Total |
|---|---|---|---|---|---|---|---|---|
| Accommodation (72) | 40 | 296 | 32 | 368 | 31 | 292 | 15 | 338 |
| Administrative (56) | 7 | 15 | 11 | 33 | 5 | 12 | 1 | 18 |
| Agriculture (11) | 1 | 0 | 4 | 5 | 0 | 0 | 0 | 0 |
| Construction (23) | 2 | 11 | 10 | 23 | 0 | 5 | 5 | 10 |
| Education (61) | 42 | 26 | 224 | 292 | 30 | 15 | 56 | 101 |
| Entertainment (71) | 6 | 19 | 7,163 | 7,188 | 5 | 17 | 11 | 33 |
| Financial (52) | 74 | 74 | 450 | 598 | 39 | 52 | 55 | 146 |
| Healthcare (62) | 165 | 152 | 433 | 750 | 99 | 112 | 325 | 536 |
| Information (51) | 54 | 76 | 910 | 1,040 | 29 | 50 | 30 | 109 |
| Management (55) | 1 | 0 | 1 | 2 | 0 | 0 | 0 | 0 |
| Manufacturing (31–33) | 375 | 21 | 140 | 536 | 28 | 15 | 28 | 71 |
| Mining (21) | 3 | 3 | 20 | 26 | 3 | 3 | 0 | 6 |
| Other Services (81) | 5 | 11 | 46 | 62 | 2 | 7 | 26 | 35 |
| Professional (54) | 158 | 59 | 323 | 540 | 24 | 39 | 69 | 132 |
| Public (92) | 22,429 | 51 | 308 | 22,788 | 111 | 31 | 162 | 304 |
| Real Estate (53) | 2 | 5 | 24 | 31 | 2 | 4 | 14 | 20 |
| Retail (44–45) | 56 | 111 | 150 | 317 | 38 | 86 | 45 | 169 |
| Trade (42) | 13 | 5 | 13 | 31 | 6 | 4 | 2 | 12 |
| Transportation (48–49) | 15 | 9 | 35 | 59 | 7 | 6 | 5 | 18 |
| Utilities (22) | 14 | 8 | 24 | 46 | 4 | 3 | 11 | 18 |
| Unknown | 1,043 | 9 | 17,521 | 18,573 | 82 | 3 | 55 | 140 |
| Total | 24,505 | 961 | 27,842 | 53,308 | 545 | 756 | 915 | 2,216 |

Verizon 2018 report - Security Incidents and breaches by victim industry and organization size

# Ataques cibernéticos en LatAm.




**Volumen Geográfico de los ataques en Latinoamérica en el 2017**




**Países mas propensos a ataques cibernéticos (cantidad de usuarios por internet per cápita)**

# Costos e impactos de la industria.

| Brechas de Seguridad entre Enero 2015 y Abril 2018. | Costo Promedio por un ataque de código malicioso. | Costo promedio en tiempo por un ataque de código malicioso. | Costo de Ransonware. | Costo promedio por robo de dato por individuo. |
|---|---|---|---|---|
| 8.854 | $ 2.4 M | 50 días | $ 5 Bn | $ 141 |
| Fuente: Cisco | Fuente: Accenture | Fuente: Accenture | Fuente: CSO | Fuente: Ponemon Institute |

# Famosos Malwares

**Tipos de Malware (Programa Malicioso)**

- Virus informáticos.
- Gusanos.
- Adware.
- Spyware.
- Ransomware.
- Bots.
- Rootkits.
- Caballos de Troya.
- Errores.

**Famosos Malwares en el 2018**

- Teslacrypt (Ransomware).
- Industroyer (Virus informático).
- Crysis (Ransomware).
- Wannacry (Ransomware).
- Petya (Not Ransomware / Destructive Wiper).
- “Se regala el nuevo iphone a los ciudadanos  latinoamericanos por $1 dólar (Troyano).
- Houdrat (Troyano) – Criptominería.

# Caso reales de Ransomware en Latam

**Empresa retail de equipos electrónicos.**

- El aplicativo de ventas no funciona! Error en el servidor?
- Base de datos con la información logística secuestrada y encriptada.
- Pago bitcoin solicitado 1.5 bitcoins ($15,000).
- Operación comercial paralizada por horas.
- Deciden no pagar el monto, formatean los servidores, actualizan el software y restauran base de datos con información de 24 horas atrás.
- Gran problema…stock se actualiza en tiempo real.
- Decenas de ventas canceladas.
- 1 día y medio el servidor retoma operación, 1 semana actualizar inventario.

**Consultora.**

- En menos de 1 hora, 25 computadoras infectadas.
- “Your files have been encrypted”.
- Solicitaban el pago de un bitcoin.
- Deciden formatear el equipo.
- Fallas - no actualizar el sistema operativo de las computadoras. Vulnerabilidades.
- No plan de contingencia, no actuaron con rapidez.

# Tendencias de Reclamaciones

# Tendencias de Riesgo Cibernético.

- La seguridad informática ya no es un lujo, es una necesidad.
- Mientras todo funcione bien, no lo notamos. No tenemos conciencia del peligro y extensión del daño. (Un riesgo invisible).
- Las computadoras son parte de nuestra vida cotidiana.
- Es hora de tomar medidas concretas contra la amenaza del delito informático. La infraestructura critica de la región esta en peligro.
- La ciberseguridad debe ser considerada por los gobiernos como elemento clave para la estabilidad económica de la región.

# ¿Qué nos espera en el 2019?

A continuación, los pronósticos de Karspersky Lab. sobre amenazas para en el 2018-19.

- Adopción y uso de técnicas de ataques dirigidos (APTs “Amenaza Persistente Avanzada”).
- Ataques a la cadena de suministros.
- Mas malware de alta gama en móviles.
- La identidad en el comercio electrónico entrara en crisis.
- Mas ataques a módems y enrutadores.

# Predicciones sobre industria y tecnología

- La industria automotriz.
- Las instituciones medicas y la salud individual.
- Servicios financieros.
- Seguridad industrial.
- Criptomonedas.
- Infraestructura Publica.
- Ciberguerra entre países.

# Coberturas de Seguro Cibernético. Liberty Cyber Risk

# Pólizas tradicionales – La mayoría tienen exclusiones de riesgos cibernéticos.

**Property & RC.**

- Solo cubre daños tangibles a la propiedad.
- No cubre daños informáticos o pérdida de datos.

**Infidelidad de Empleados (BBB, Crimen).**

- Como la información electrónica no es tangible, las pólizas no ofrecen la cobertura adecuada.
- No cubre el coste de restauración y recuperación de información dañada.

**RC Profesional.**

- Solo cubre reclamaciones por errores profesionales en la realización de servicios definidos.
- No cubre actos intencionales de empleados.
- No cubre gastos de notificación y/o de investigación.

# Estructura de la Póliza.

## Responsabilidad frente a terceros:

- Responsabilidad Civil por violación de normativa de privacidad, datos personales, confidencialidad y medidas de seguridad.
- Responsabilidad Civil por actividades multimedia.
- Gastos de defensa en procedimientos regulatorios.

## Daños propios:

- Pérdida de activos digitales.
- Interrupción de negocios.
- Extorsión.

## Protección del cliente y gastos reputacionales:

- Gastos de notificación.
- Gastos legales en material de privacidad.
- Gastos de gestión de crisis.
- Gastos de investigación forense.

# Cobertura de Daño Propio.

***Ocasionadas por:***

Secuestro de Información


Delitos Informáticos

Cyber extorsión

- Costos de contratación de expertos en gestión de crisis/ extorsión

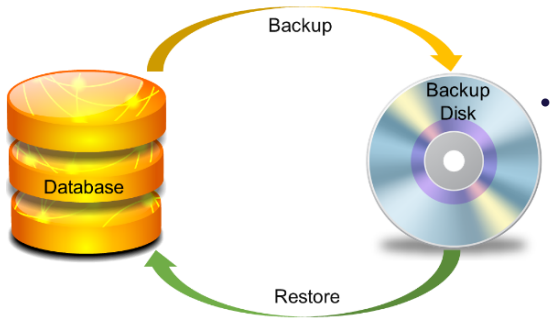

Errores operativos y administrativos

Lucro Cesante: Disminución de las ventas.

Gastos Forenses :

- Costos para determinar el alcance y la causa de la intrusión

Pérdida de la Información




- Restauración, recogida y recreación de activos digitales:

# Cobertura de Responsabilidad de Terceros y Gestión de Crisis.

***Gestión de Crisis :***

- Armar Equipo de Gestión de Crisis

- Preparación /
- Entrenamiento y Ejecución del Plan de Gestión de Crisis

- Desenvolvimiento de la Gerencia en situación de Crisis

- Soporte Legal


- Comunicación y gestión de imagen pública

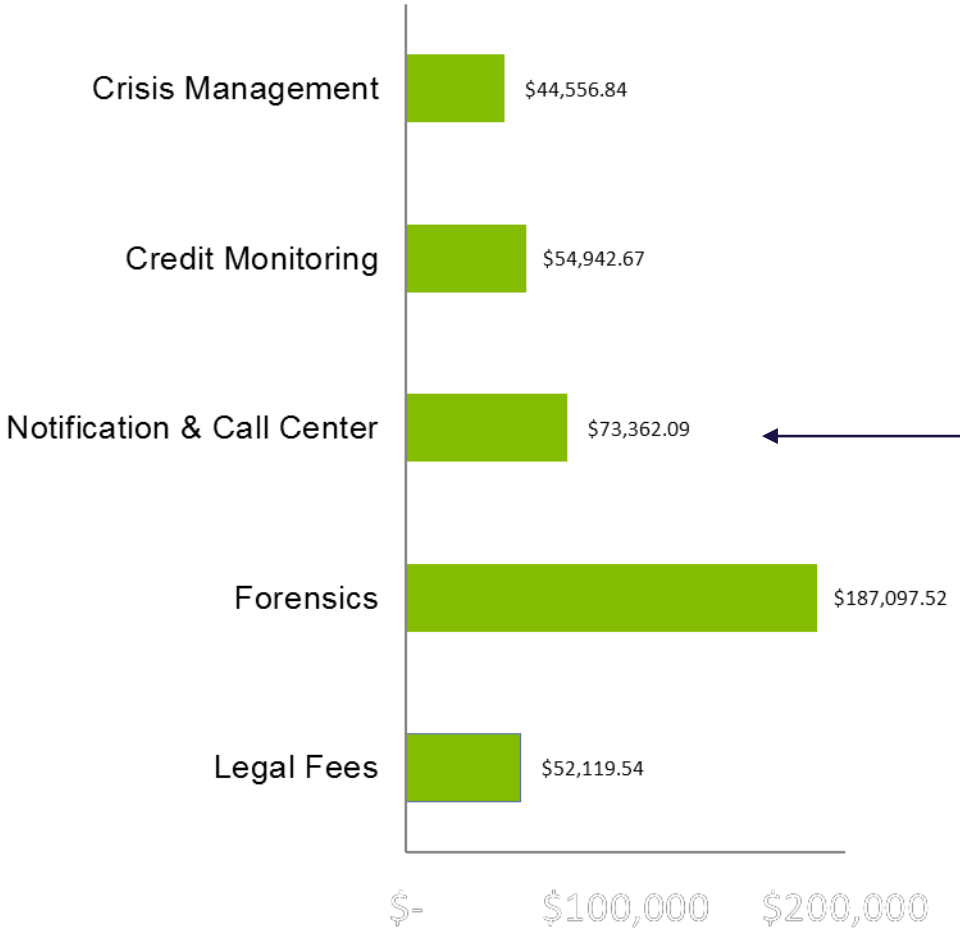
***Gastos para Terceros:***

- Gastos para notificar a los clientes que hubo una intrusión de información

- Costos para monitorear estados de cuenta de clientes afectados

# Análisis de Reclamos.

Promedio de Costos de Daño propio *




**El Manejo de cada Intrusión es único**

## Rangos de Costo de cada servicio:

- **Gastos Legales:**
  USD $5,000 hasta USD $400,000
- **Gastos Forenses:**
  USD$10,000 hasta millones de USD
- **Notificación y Call Center:**
  Aproximadamente USD $3 por record (persona)
- **Monitoreo de Crédito:**
  USD $15 a $30 Costo por inscribir a cada persona en el servicio
- **Costo minimo de manejo de crisis**
  USD 5,000 hasta USD 85,000

**Objetivo: Proteger la IMAGEN y MARCA**

# Puntos a considerar en un riesgo cibernético.

| | |
|---|---|
| Identificación | • ¿Cuáles son sus activos digitales mas críticos?(datos, infraestructura y aplicaciones)<br>• ¿Dónde se encuentran localizados y quien tiene acceso a ellos? |
| Protección | • ¿Cómo los están protegiendo<br>• Control técnico y entrenamiento<br>• Control humano (Interno y externo) |
| Detección | • ¿Cómo detectarían cualquier problema?<br>• Registros (logs) |
| Respuesta | • ¿Cómo responderían a un incidente?<br>• Plan de recuperación de desastre (DRP) y Plan de Continuidad del Negocio (BCP). |
| Cuantificación | • ¿Cómo se cuantificaría el impacto? |

# ¿Porqué debo contratar un seguro?

- Por mas que invierta en seguridad informática, siempre existirá un riesgo.
- Se trata de un riesgo invisible.
- Información de clientes comprometida.
- Interrupción de sus negocios.
- Pérdida de ingresos comerciales.
- Una empresa puede quedar insolvente y quebrar.
- Daños a la reputación de su empresa.
- Notificación a afectados.
- Altos costos de investigación.
- Sanciones legales.

# Riesgos Cibernéticos – Flujo de Respuesta de Incidentes.

**USTED ESTA AQUI:**

Su organización ha sufrido una violación de datos o ataque de seguridad de la red.

Determine si el evento es un incidente real. Si es así, reúna a las partes internas interesadas y revise el plan de respuesta de incidentes sin demora.

Inmediatamente envíe un correo electrónico a **Liberty** al **LatamNewClaim@LibertyMutual.com.** El área de reclamos de **Liberty** monitorea el buzón de correo siete (7) días a la semana.

O marque nuestras líneas gratuitas:

- Argentina: 0800-666-0084
- Chile: 800-914-495
- Colombia: 01800-518-5276
- San Salvador: +503-21367213
- Guatemala City: +502-23753956
- México: 01-800-099-0446
- Panamá: 800-0330
- Perú: 0800-78358

**Liberty** acusará recibo de su Notificación y confirmara el número de reclamo del incidente.

Un profesional de Cyber Forensic responderá su llamada y discutirá:

- La (s) fecha (s) del incidente,
- La naturaleza del incidente,
- Detección de hechos y recopilación de pruebas, si las hay, por parte del equipo interno de TI

Un profesional cibernético lo ayudará de inmediato a contener o detener la violación de datos o el ataque cibernético.

Un profesional de reclamos de Liberty Cyber lo ayudará a coordinar con interesados externos.

- Abogado especialista en violación de datos.
- Abogado defensor.
- Clientes, Accionistas, Reguladores.
- Cumplimiento de la ley de relaciones públicas.
- Centro de llamadas o monitoreo de crédito.

**EJECUTAR** su plan de respuesta a incidentes

# Contáctanos

Raul Muller
Raul.Muller@LibertyMutual.com
Tel: +(51) 942 469-146

Frency Guillen
Frency.Guillen@LibertyMutual.com
Tel: +(51) 961 876-289

Francisco Padilla
Francisco.Padilla@LibertyMutual.com
+(51) 942 436 039

**www.libertyseguros.com.pe**


Liberty
Seguros