
WATCH&ACT
be smart, being human

Cómo evitar el pago en el próximo Black Friday Cibernético

Javier Huergo
Responsable de Aseguramiento.
Watch&Act Protection Services (WAPS)

Congreso CSTIC 2017

Be Agile, Be digital, Be Secure

Organiza

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

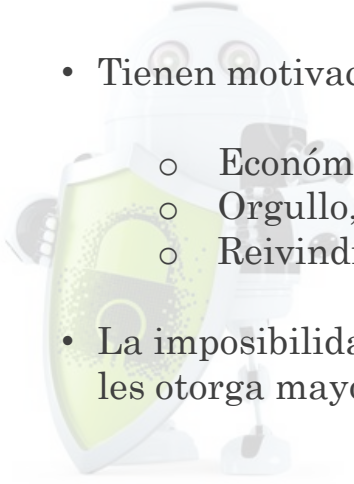
30 mayo 2017

WATCH&ACT
Protection Services

El cáncer cibernético de nuestro siglo

- En España se producen más de 200.000.- Ciber ataques diarios a las empresas.
- Se estima que en el 2020 estarán conectados por internet más 20.8 billones de aparatos.
- Generarán más de 20 ZETABYTES de datos. (Fuente: Gartner)
- Las empresas españolas pierden, de media cada una, más de 1,3 millones de euros (1,4 millones de dólares al cambio actual) anuales como consecuencia de ciberataques o incidentes de seguridad.
- No es sólo la información lo que interesa a los ciber delincuentes sino también y más importante las consecuencias derivadas de la **imposibilidad de acceder a la información**.

El cáncer cibernético de nuestro siglo



- Los Ciber delincuentes de una forma sencilla y con unos conocimientos básicos, pueden acceder a toda la información que se encuentre en la red de internet.

- Tienen motivaciones muy distintas:

  - Económicas.
  - Orgullo, autoestima.
  - Reivindicativas: políticas, sociales o incluso personales.

- La imposibilidad de trazabilidad de los pagos efectuados mediante el uso de Bitcoins les otorga mayor impunidad.

¿A quién afecta?

- **A todas las empresas**. No sólo a aquellas que almacenen, manipulen o transmitan datos.

- **No importa el tamaño de empresa**.

- Hay empresas más sensibles por su impacto en los medios, en sus accionistas o por la información que manejan:
  - Empresas de Comunicación.
  - Empresas de Tecnología.
  - Empresas de gestión de infraestructuras. (Luz, gas, etc).
  - Empresas de servicios. (Despacho de Abogados, Consultoras, Gestorías, etc.)
  - Instituciones financieras. (Bancos, Aseguradoras, EAFI, etc.).
  - Sanidad.
  - Comercio.
  - Hoteles y Ocio.
  - Etc.

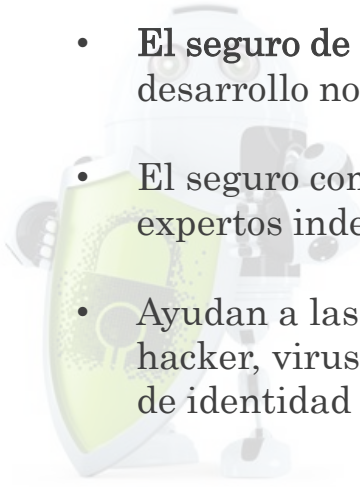
¿Por qué protegerse?

- **No existe protección total** por mucho que inviertas en tecnología.
- Siempre encontrarán alguna vulnerabilidad para acceder a la información de la empresa.
- Ausencia de servicios expertos en respuestas técnicas , legal y comunicación.
- **La empresa y la marca son los activos más importantes** y por ello hay obligación de protegerlos para dar seguridad a:
  - Clientes.
  - Proveedores.
  - Empleados.
- La **responsabilidad implícita del órgano de control y dirección de la empresa que ha de velar por:**

- La cuenta de resultados. (Interrupción del negocio).
- La reputación de accionistas, consejeros, directivos y empleados.
- El clima laboral de la organización.

¿Cómo protegerse? El Seguro de Ciber Riesgo

- La mejor forma de protegerse ante los Ciber ataques es **la prevención**.
- Es la solución aseguradora completa de gestión de estos riesgos cibernéticos.
- **El seguro de Ciber Riesgo** responde en la gestión y control del impacto que ello supone el desarrollo normal de la actividad empresarial.
- El seguro combina protección aseguradora con servicios de gestión de riesgo con acceso a expertos independientes.
- Ayudan a las entidades a proteger su patrimonio ante posibles fugas de seguridad, ataques hacker, virus informáticos, empleados deshonestos o negligentes, fuga de información y robo de identidad entre otros.



Principales coberturas

Responsabilidad civil:

- Por fallos en el sistema de seguridad
- Por fugas, pérdida de datos
- Accesos ilegales. No autorizados
- Plagios, piratería multimedia

Defensa jurídica y fianzas:

- Gastos legales y/o profesionales.
- Gastos de investigación, peritaje.
- Gastos de representación.
- Fianzas judiciales.

Sanciones administrativas:

- Por violación de la seguridad
- Por violación de la privacidad

Gastos y coberturas complementarias

- Gastos de comunicación.
- Gastos por notificación a terceros.
- Gastos de gestión de crisis.
- Gastos de apoyo al cliente y supervisión

Otras

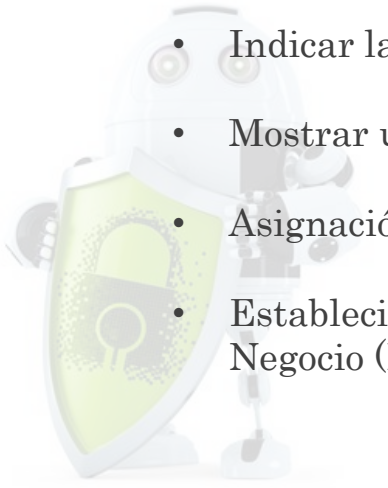
- Extorsión por datos.
- Responsabilidad multimedia.
- Restablecimiento de datos.
- Pérdida de ingresos comerciales

Cómo conseguir mejores primas, franquicias y coberturas

Información del riesgo a asegurar. Amplia y detallada

De una forma especial para los seguros de ciber riesgo:

- Indicar las medidas de prevención aplicadas.
- Mostrar una cultura de seguridad informática y buenas prácticas.
- Asignación de personal dedicado al cumplimiento de las normas básicas de seguridad.
- Establecimiento de Plan Director de Seguridad que incluya: Plan de Continuidad del Negocio (BCP) y Plan de Recuperación de Desastres. (DRP).



Aspectos clave de la propuesta

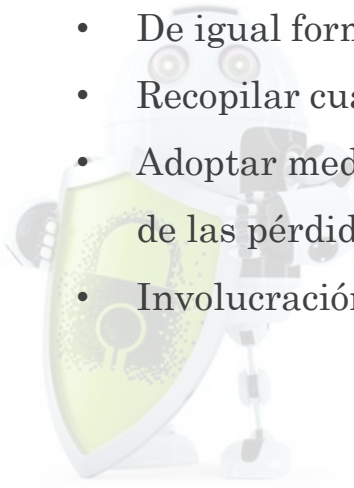
- La industria o sector de actividad.
- Evaluación del riesgo en los datos:
  - Tipo de datos, cantidades.
  - Procedimientos de protección de los datos. Documentos, contraseñas, etc.
  - Acceso a los datos, seguridad de las redes y recuperación. Firewalls, antivirus, etc.
  - Datos en dispositivos móviles y portátiles. Nivel de seguridad.
- Servicios de externalización. Outsourcing de servicios.
- Gestión de brechas de seguridad. Planes de respuesta, recuperación y de continuidad.
- Reclamaciones previas o pre-existentes.
- Cumplimiento de normativa legal.
- Identificar claramente **las inquietudes del negocio** que se desea a asegurar.

Afinidad de la propuesta

- La ciber delincuencia es un sector emergente y por lo tanto hay gran desconocimiento asegurador.
- En constante evolución.
- Disparidad de ofertas por parte de las compañías de seguros en función de:
  - "Apetito al riesgo".
  - Sector estratégico.
  - Conocimiento técnico en seguridad informática.
  - Capacidad de asumir individualmente la cobertura.
- Los condicionados no son homogéneos con coberturas no estándar y sub limitadas a discreción del asegurador.
- Las primas pueden variar entre compañías en más de un 100% y con franquicias dispares.
- La necesidad de entender bien el riesgo es básico para el asegurador, cliente y siempre contando con el asesoramiento de un experto

Actuación en caso de siniestro

- Comunicar en el momento del **"descubrimiento" y a la mayor brevedad posible por escrito** al asegurador y/o corredor de seguros.
- De igual forma para las **reclamaciones** derivadas de un siniestro.
- Recopilar cuantas más **pruebas, circunstancias, evidencias y consecuencias del siniestro**.
- Adoptar medidas y emplear medios razonables para reducir o aminorar las consecuencias de las pérdidas.
- Involucración de todas las áreas afectadas.



El mercado asegurador de Ciber riesgos

- El mercado asegurador americano, pionero en el aseguramiento de estos riesgos, prevé superar la cifra de negocio de 12.700 millones de euros en los próximos 5 años. Es decir multiplicar por 10 su cifra actual.
- En Europa se estiman cifras de 18.000€ para el 2025.
- No todas las aseguradoras cuentan con el ramo de Ciber Riesgo pues:
  - Han de contar con experiencia y formación en servicios de ciber riesgo.
  - Llegar a acuerdos con empresas de servicios que den soporte a los siniestros.
  - Falta de información de siniestralidad que permita el establecimiento de una prima adecuada con una correcta atención a los siniestros.
- El mercado asegurador de Ciber Riesgos en España crece ante las posibilidades reales de sufrir ataques.
- La ley Europea de Protección de Datos (GDPR) que entrará en vigor el próximo 25 de mayo de 2018 conllevará probables incrementos de prima por la obligatoriedad de comunicación de las brechas de seguridad en las empresas.

Casos reales. Algunos ejemplos

Ataque de Ransomware en un hospital

Respuesta aseguradora:

- Se activa gestión del incidente:
  - Clonación disco duro. Búsqueda de evidencias: copias, Dropbox, etc.
  - Intento de recuperación.
  - Valorar potencial reclamación de terceros.
  - Potencial procedimiento administrativo

Perjuicios financieros:

- Gastos de investigación. (18.000€)
- Costes de recuperación de datos. (15.000€)
- Asesoramiento y defensa legal. (15.000€)
- Pago de perjuicios e indemnizaciones. (50.000€)
- Gastos de notificación. (15.000€)

Indemnización aproximada: 113.000€

Error humano. Vulneración de privacidad

Respuesta aseguradora:

- Análisis de responsabilidades.
- Gastos de defensa por procedimiento normativo.
- Gastos de defensa por reclamaciones de terceros.
- Gastos de gestión de incidente:
  - Gastos de investigación.
  - Gastos de notificación a los afectados.
  - Asesores legales.
  - Servicios de monitorización de las consecuencias para los afectados.

Indemnización aproximada: 200.000€

¿Usurpación de identidad?

https://www.youtube.com/watch?v=_IuIBfuPdt0

Seguro de Ciber Riesgos
Muchas gracias

;)

Javier Huergo
Responsable de Aseguramiento
+34 91 159 17 87 // +34 616 67 61 38
C/ Puerto Rico 8B,28016 Madrid

javier.huergo@watchandact.eu
watchandact.eu

WATCH&ACT
Protection Services