La responsabilidad legal frente al ciberataque

GARRIGUES

Montse Mas Llull
Clara Blanc López
Palma, 17 de mayo 2018

Entorno globalizado: riesgos en la era digital

GARRIGUES

Introducción

Ciberataques: a la orden del día

ATAQUES RANSOMWARE ›

Un potente ciberataque afecta a grandes empresas de todo el mundo

EL PAÍS Madrid - 28 JUN 2017 - 18:30 CEST

Cómo surgió y se propagó **WannaCry**, uno de los **ciberataques** más ...
Infobae.com - 12 may. 2018
Hoy se cumple un año de **WannaCry**, el mayor ataque de ransomware ... por el ataque a Telefónica y Alemania, donde la **empresa** ferroviaria ...
Se cumple un año del **ciberataque WannaCry** pero el riesgo todavía ...

Miles de empresas (y sus clientes), en peligro tras un ataque masivo de 'ransomware'

MongoDB es un sistema de base de datos omnipresente. Ahora, una serie de ataques ha robado la información de estas compañías

10 ENERO, 2017

Un nuevo ciberataque masivo afecta a empresas en todo el mundo

EL MUNDO ERO 27 JUN. 2017 | 19:14

Hackers 'secuestran' el servicio informático de un hotel en Los Alpes

Un grupo criminal se infiltró en el sistema informático del edificio y exigió cobrar 1.500 euros

Hackers bloquean la actividad de empresas en todo el mundo con un nuevo ataque de ransomware

elEconomista.es

Londres acusa a Rusia del ciberataque global NotPetya que secuestró 300.000 ordenadores

PATRICIA TUBELLA | 15/02/2018 - 10:31 CET
El Ejecutivo británico señala a las fuerzas armadas rusas como autoras del asalto informático

Presunto 'hackeo' al sistema de pagos de Banxico pega a operación
El Financiero - 30 abr. 2018
Tras el intento de **ciberataque** a 3 bancos mexicanos, los bancos operan el SPEI con el programa de contingencia, lo que vuelve más lentas las transacciones.

Varios ciberataques masivos inutilizan las webs de grandes compañías

Son los más graves de la última década. Los primeros indicios descartan a un país extranjero

GARRIGUES

Datos relevantes

Ciberamenazas

España: **tercer país más atacado del mundo** por los ciberdelincuentes

Ciberamenazas: **tercer riesgo** a nivel internacional, después de los conflictos armados y el terrorismo

72% de las empresas **ya han sido atacadas**; y un **85%** todavía **no cuentan con un plan de seguridad**

Pérdidas empresariales superiores al 20%

GARRIGUES

Datos relevantes

Ejemplos prácticos

White Lodging

Víctima de un ataque en 2013 y otro posterior en 2015. 24 hoteles afectados. Robaron datos de tarjetas de crédito, incluyendo nombres y códigos de seguridad.

Mandarin Oriental

Un malware infectó los terminales de punto de venta de algunos hoteles en marzo de 2015. Miles de tarjetas resultaron comprometidas

Trump Hotels

Siete establecimientos de la cadena sufrieron un ciberataque entre mayo de 2014 y junio de 2015. Afectó a terminales de venta de tiendas de regalos y restaurantes.

Hard Rock Las Vegas

Fueron robados datos de 173.000 tarjetas de crédito usadas en sus tiendas, restaurantes y bares durante siete meses, entre 2014 y 2015.

Hilton Worldwide

La compañía informó en noviembre de 2015 que había sufrido un ciberataque en sus terminales de venta. Robaron nombres y códigos de tarjetas.

Starwood

Un malware infectó sus terminales de venta en 105 hoteles, robando información de tarjetas de crédito de sus clientes.

Hyatt

249 hoteles de 54 países resultaron infectados por un ciberataque entre julio y septiembre de 2015. Robaron datos de tarjetas de crédito desde las terminales de venta.

Rosen Hotels & Resorts

Aunque no se han facilitado cifras del robo, se supo que la empresa estuvo infectada por malware durante un año y medio sin percatarse.

Fuente: Informe "El ciberexpolio hotelero", Panda Security.

Consecuencias legales: ¿es responsable la empresa ante un ciberataque?

Cuestiones previas

Obligaciones derivadas de la era digital

- **Directiva (UE)** núm. 2016/1148, del Parlamento Europeo y del Consejo, de 6 de julio del 2016, **relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión** (Directiva RSI, o, por sus siglas en inglés, Directiva NIS -*Network and Information Systems*-)

  - Pieza clave de la estrategia de ciberseguridad de la Unión Europea
    - **impone a las empresas nuevas obligaciones para proteger la información de sus clientes.**
    - **de probarse que no han obrado con la diligencia necesaria, existirían riesgos legales de diversa naturaleza: contractual, extracontractual, administrativos e incluso penal.**
  - Entrada en vigor: 8 de agosto de 2016
  - Obligatoriedad: 9 de mayo de 2017

- **Convenio del Consejo de Europa sobre Cibercriminalidad** de 23 de noviembre de 2001 (ratificado por España el 3 de junio de 2010)

Riesgos legales

Responsabilidad Penal

Responsabilidad penal de la persona jurídica

- Art. 264 CP: Daños informáticos
- Art. 197 al 200 CP: Revelación de secretos

Responsabilidad civil subsidiaria de la persona jurídica

- Art. 120.4 CP

Riesgos legales
Responsabilidad Penal

- **Ciberataques de relevancia penal:**
  - aquellos que, por su gravedad, son capaces de integrar los **delitos de descubrimiento y revelación de secretos por medios informáticos y los de daños**, contenidos en nuestro Código Penal, **artículos 197 al 200**.
  - Se trata de delitos que castigan:
    - el acceso ilícito a los sistemas informáticos,
    - la permanencia y la interceptación de transmisiones no públicas de datos informáticos,
    - conductas de sabotaje tendentes a la destrucción o deterioro de los datos y programas informáticos;
    - obstaculización del funcionamiento de un sistema informático.
  - Además, en un intento no ya de castigar el ciberataque sino de evitarlo, se **adelanta la barrera punitiva**, castigando el facilitar de programas informáticos para la comisión de cualquiera de los antedichos delitos.

Riesgos legales

Empresa y protección de datos

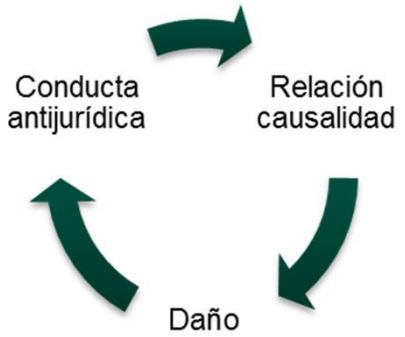
Al margen de los delitos penales, **que consecuencias tendría para una empresa ser victima de un ciberataque careciendo de las necesarias medidas de seguridad?**

- **Administrativas**

Infracción	Causa	Sanción
Leves	No atender las solicitudes de rectificación o cancelación. No proporcionar la información requerida por la AEPD No inscribir ficheros en el Registro General de Protección de Datos	**entre 600 € y 60 000 €**
Graves	No recabar el consentimiento de los titulares Mantener datos inexactos No aplicar las medidas de seguridad correspondientes Obstrucción de la inspección	**entre 60 000 € y 300 000 €**
Muy graves	Recolección de información de forma engañosa Comunicación de datos sin requisitos legales Tratar datos de alto nivel sin consentimiento expreso y escrito	**entre 300 000 € y 600 00 €**

GARRIGUES

Riesgos legales
Empresa y protección de datos



- **Reclamación en vía civil**
  - Las **responsabilidades contractuales** (art. 1.101 y siguientes CC) **y extracontractuales** responden al **deber general de no dañar a los terceros** *(alterum non laedere art.1.902 y 1.089 CC):* el daño se produce por violación de deberes generales de conducta.
    - Exoneración de responsabilidad: Artículo 1.105 y 1.107 del Código Civil
    - *Especial protección al **cliente consumidor:*** Artículo 128 y 147 del TRLGDCyU
  - **artículo 19 de la LOPD**, expresamente reconoce el derecho a indemnización de aquellos interesados *"que, como consecuencia del incumplimiento de lo dispuesto en la presente ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos"*.
    - No es preceptivo acudir a la AEPD con carácter previo a la interposición de esta acción.
    - Este **derecho a la indemnizació**n no es automático, debe probarse el incumplimiento de la ley, y acreditarse que efectivamente se han producido daños o perjuicios que, además, deben ser susceptibles de valoración.
    - No existe un baremo prefijado para determinar el **alcance de estas indemnizaciones**
    - Posibilidad de incluirse en esta reclamación la **indemnización de los daños morales** sufridos. Problema de la prueba: consecuencias objetivas que puedan ser verificadas

GARRIGUES

Riesgos legales

Empresa y protección de datos

Nuevo Reglamento Europeo General de Protección de Datos (RGPD):

- Régimen de responsabilidad más exigente para las empresas
  - "*accountability*": el hecho de garantizar la seguridad de los datos personales pasa de ser una **obligación de medios a convertirse en una obligación de resultados**, donde **no incumplir ya no será suficiente**.
  - obligación de establecer políticas de prevención y realizar evaluaciones de impacto ("*Privacy Impact Assessment*"); así como la obligatoriedad de denunciar, sin dilación indebida, las violaciones o brechas de seguridad ("*Data Breach Notification*") tanto a la Agencia Española de Protección de Datos (AEPD), como a los propios interesados.

Riesgos legales

Empresa y protección de datos

- **Nuevo mapa de responsabilidades: frente a los perjudicados (a quienes el RGPD les reconoce el derecho a exigir una indemnización por daños materiales e inmateriales) y, por otro, frente a la administración competente**
  - **Administrativas**: Se agrava el régimen sancionador contra los responsables y encargados del tratamiento. En caso de incumplimiento, el importe de las sanciones se establecerán en función a la infracción de que se trate (art. 83.2):

Norma aplicable	Sanciones		
	Leve	Grave	Muy grave
LOPD/RLOPD	900€ - 40.000€	40.001€ - 300.000€	300.001€ - 600.000€
RGPD	No se establece un rango mínimo de cuantía	Multa administrativa de hasta 10.000.000€ o, en el caso de empresas, de cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, lo que resulte mayor en cuantía.	Multa administrativa de hasta 20.000.000€ o, en el caso de empresas, de cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, lo que resulte mayor en cuantía.

Riesgos legales

Empresa y protección de datos

- **Civil:**
  - ✓ Derecho específico del titular de datos personales a exigir la indemnización por los daños y perjuicios que se le causen por tratamientos de sus datos realizados con incumplimiento de la ley **(Art. 82 RGPD)**
  - ✓ Mención expresa a los **daños inmateriales (¿morales?):**
    - *Artículo 82 Derecho a indemnización y responsabilidad: 1. Toda persona que haya sufrido* ***daños y perjuicios materiales o inmateriales*** *como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos."*
- **Penal:**
  - ✓ **posibilidad de que los Estados miembro puedan instaurar sanciones penales por el incumplimiento del RGPD,** trascendiendo la vía administrativa

Riesgos legales

Empresa y protección de datos

Algunos casos (notables) recientes

- ✓ FACEBOOK (septiembre 2017)
  - sanción de 1.200.000 € impuestas a Facebook por tratar datos, incluso de categoría especial, sin el consentimiento de sus titulares
- ✓ GOOGLE (noviembre 2017)
  - sanción de 300.000 euros a Google, por recoger datos de redes wifi con sus vehículos de Street View, sin el consentimiento de los titulares.
- ✓ Whatsapp y Facebook (marzo de 2018)
  - dos infracciones graves de la LOPD, sancionadas cada una con 300.000 euros: una de ellas a Whatsapp por comunicar datos a Facebook sin haber obtenido un consentimiento válido de los usuarios y otra a Facebook por tratar esos datos para sus propios fines sin consentimiento.

MAR GALTÉS, Barcelona
22/03/2018 01:40 | Actualizado a 22/03/2018 20:30

Facebook podría enfrentarse a una **sanción de 2 billones de dólares** si finalmente se demuestra que los **datos de 50 millones de sus usuarios** fueron utilizados de forma irregular por la empresa **Cambridge Analytica** para apoyar la **campaña de Donald Trump** en el 2016. La Federal Trade Comission (FTC), autoridad de competencia de Estados Unidos, investiga si Facebook ha incumplido el **acuerdo sobre la privacidad de los datos de los usuarios** que firmaron en el 2011; Facebook asegura que no ha violado el acuerdo, pero si la investigación lo demuestra, la multa podría ascender a 40.000 dólares por usuario. El caso afecta a 50 millones de usuarios.

GARRIGUES

Riesgos legales
Aplicación del nuevo régimen sancionador del RGPD

FACEBOOK

Conductas imputadas		
— Tratar datos sensibles sin consentimiento de sus titulares		
	Sanción conforme a la LOPD	**Sanción estimada conforme al RGPD**
	1.200.000 € (600.000 +300.000 +300.000)	1.075,4 millones de dólares (aproximadamente 872,07 millones de euros) (4% del volumen de negocio total anual global del ejercicio financiero anterior) (1) (2)
Calificación de la infracción y normativa aplicada	**Infracción muy grave**: Arts. 44.4 a) y 45 . 3 y 4 LOPD **Infracciones graves**: Arts. 44.3.b) y 45.2 y 4 LOPD RD 1720/2007 , en relación con el artículo 5 de la LOPD	**Tres infracciones de los principios básicos para el tratamiento de datos:** Art. 83 5, letras a) y b) del RGPD, en relación con sus arts. 5, 6, 7 y 9 y 12 a 22. **Infracciones muy graves** según los arts. 72.1, letras a), b), c), d) y e) y 76 PLOPD
Circunstancias concurrentes	Tratamiento sin consentimiento de datos especialmente protegidos	Tratamiento sin consentimiento de Categorías especiales de datos

(1) La facturación de Facebook en 2016 fue de 26.885 millones de dólares. Fuente: Expansión

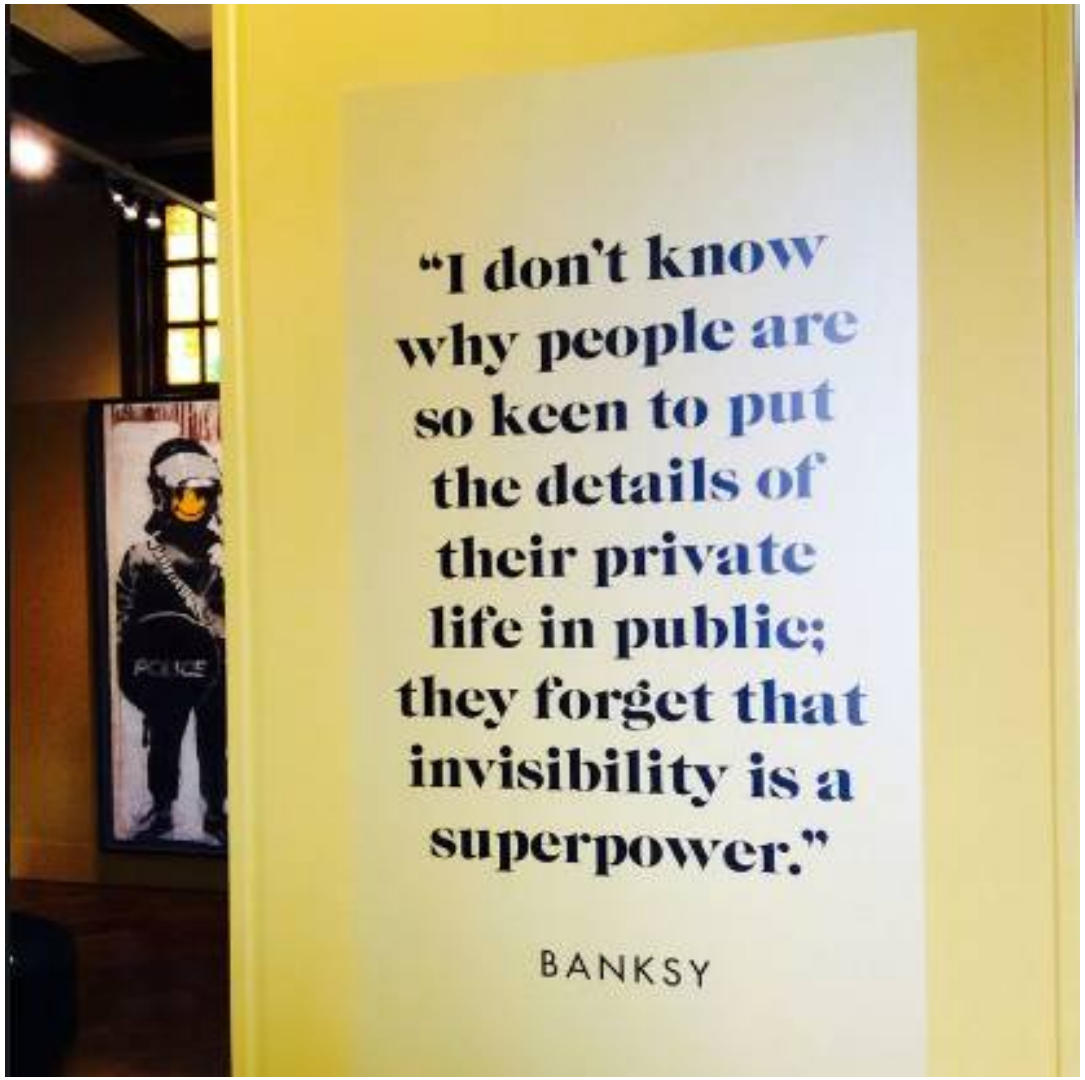
(2) El tipo de cambio Euro-dólar considerado del mes de abril es de 1.233

Fuente: Noticias.jurídicas.com

Medidas para reducir / eliminar la responsabilidad

Ámbitos de protección

GARRIGUES


"I don't know
why people are
so keen to put
the details of
their private
life in public;
they forget that
invisibility is a
superpower."
BANKSY

GARRIGUES

GARRIGUES

www.garrigues.com

MONTSE
MAS LLULL

SOCIO

montse.mas@garrigues.com Palma de Mallorca

CLARA
BLANC LÓPEZ

ASOCIADO PRINCIPAL

clara.blanc.lopez@garrigues.com Barcelona
Palma de Mallorca