D&O, Ciberrisc i Protecció de dades

Presentació formativa de riscos empresarials

6 de Febrer de 2018

ACRA
Associació Catalana de Recursos Assistencials

Ferrer&Ojeda

D&O

Responsabilitat d’Administradors i Directius

RESPONSABILITAT ADMINISTRADORS I DIRECTIUS

Els Consellers, Directius i càrrecs de direcció de les empreses han de respondre en front de la Societat, accionistes, creditors socials i qualsevol tercer perjudicat per les decisions que prenguin i gestió que realitzin en la Societat. **Responen de manera solidària amb el seu patrimoni personal.**

A més des de 2010 s'estableix la responsabilitat penal de les persones jurídiques i s'amplia encara més l'àmbit de responsabilitat d'aquests Administradors i Directius.

DEURES DEL BON ADMINISTRADOR (I)

- ✓ Desenvolupar el càrrec amb la diligència d'un ordenat empresari
- ✓ Representant lleial en defensa de l'interès de la Societat complint els deures imposats per la llei i els Estatuts
- ✓ No utilitzar el nom de la Societat ni aprofitar-se del seu càrrec per realitzar operacions per compte propi o a través de persones vinculades
- ✓ Informar els socis de qualsevol possible conflicte d'interessos amb la Societat

DEURES DEL BON ADMINISTRADOR (II)

- ✓ No dedicar-se a la mateixa activitat que la Societat per compte pròpia o aliena sense autorització expressa
- ✓ Deure de secret d'informació confidencial de l'empresa i vigilància de les dades
- ✓ Complir les obligacions en matèria de PRL
- ✓ Liquidar els impostos corresponents en temps i forma
- ✓ Sol·licitar concurs en els terminis previstos si la situació financera de la Societat així ho requereix

QUÈ ÉS UNA PÒLISSA DE D & O?

Assegurança que protegeix el patrimoni personal dels administradors i directius d'una entitat en front de reclamacions per la seva falta de diligència en l'exercici de les seves funcions, incloent errors i omissions no intencionats.

QUI ESTÀ ASSEGURAT?

Cada vegada s'està ampliant més el concepte de persona assegurada, també per donar cabuda a nous llocs de treball dins les empreses. Ex: *Compliance Officer*

Es considera D & O qualsevol conseller, delegat, president, administrador, gerent o càrrec equivalent i en general qualsevol persona amb poder de decisió en algun àmbit de l'empresa.

MÒDULS DE COBERTURA

MÒDUL I: RC ADMINISTRADORS I DIRECTIUS (PRINCIPAL)

Reclamacions presentades contra les persones assegurades (Administradors i Directius) per actes realitzats durant el desenvolupament de les seves funcions.

- ✓ Cobreix despeses de gestió de crisis, investigació, etc…
- ✓ Cobreix els costos de representació i defensa. Advocats de companyia són despatxos de reconegut prestigi. Possibilitat lliure elecció de defensa jurídica

MÒDULS DE COBERTURA

MÒDUL I: RC ADMINISTRADORS I DIRECTIUS (PRINCIPAL)

- ✓ Cobreix la constitució i/o despeses de constitució de les fiances judicials
- ✓ Cobreix la possible indemnització en cas de ser condemnat per negligència en el desenvolupament de les seves funcions

No cobreix actes dolosos, lesions corporals o danys materials ni circumstàncies anteriors

MÒDULS DE COBERTURA

MÒDUL II: PRÀCTIQUES DE TREBALL

Reclamacions derivades d'actes incorrectes en matèria de treball als Administradors, Directius i treballadors o a la Persona Jurídica

- ✓ Cobreix despeses de gestió de crisis, investigació, etc…
- ✓ Cobreix els costos de representació i defensa. Advocats de companyia són despatxos de reconegut prestigi. Possibilitat lliure elecció de defensa jurídica

MÒDULS DE COBERTURA

MÒDUL II: PRÀCTIQUES DE TREBALL

- ✓ Cobreix la possible indemnització en cas de ser condemnat per negligència en el desenvolupament de les seves funcions

No cobreix acomiadaments múltiples, plans de pensions o circumstàncies i litigis anteriors

MÒDULS DE COBERTURA

MÒDUL III: RESPONSABILITAT CORPORATIVA (EXCEPCIONAL)

- ✓ Cobreix les reclamacions a la Persona Jurídica
- ✓ Cobreix pèrdues derivades de suplantació d'identitat, incompliment de Protecció de Dades
- ✓ No cobreix actes dolosos, lesions corporals o danys materials, etc…

EXEMPLE I: RECLAMACIÓ PERSONAL

El Consell d'Administració d'una empresa reclama contra el seu gerent per haver invertit negligentment (compra d'empreses, inversió immobiliària, valors) el líquid de l'empresa ocasionant-li quantioses pèrdues a aquesta.

60.000 euros de despeses de defensa

EXEMPLE II: TREBALLADORS

Un treballador interposa una demanda contra un Directiu per incompliment del deure de confidencialitat per haver divulgat dades dels seus expedients mèdics.

Sanció 1.500 euros + Despeses de defensa 9.000 euros

EXEMPLE III: CONCURS

S’interposa una demanda contra un directiu per no haver instat el concurs quan les pèrdues de la Societat provocaven que el Patrimoni Net fos inferior al 50 % del capital social.

Despeses de defensa 80.000 euros

QUÈ CAL PER CONTRACTAR UNA PÒLISSA DE D & O?

Respondre i signar un qüestionari amb preguntes com ara:

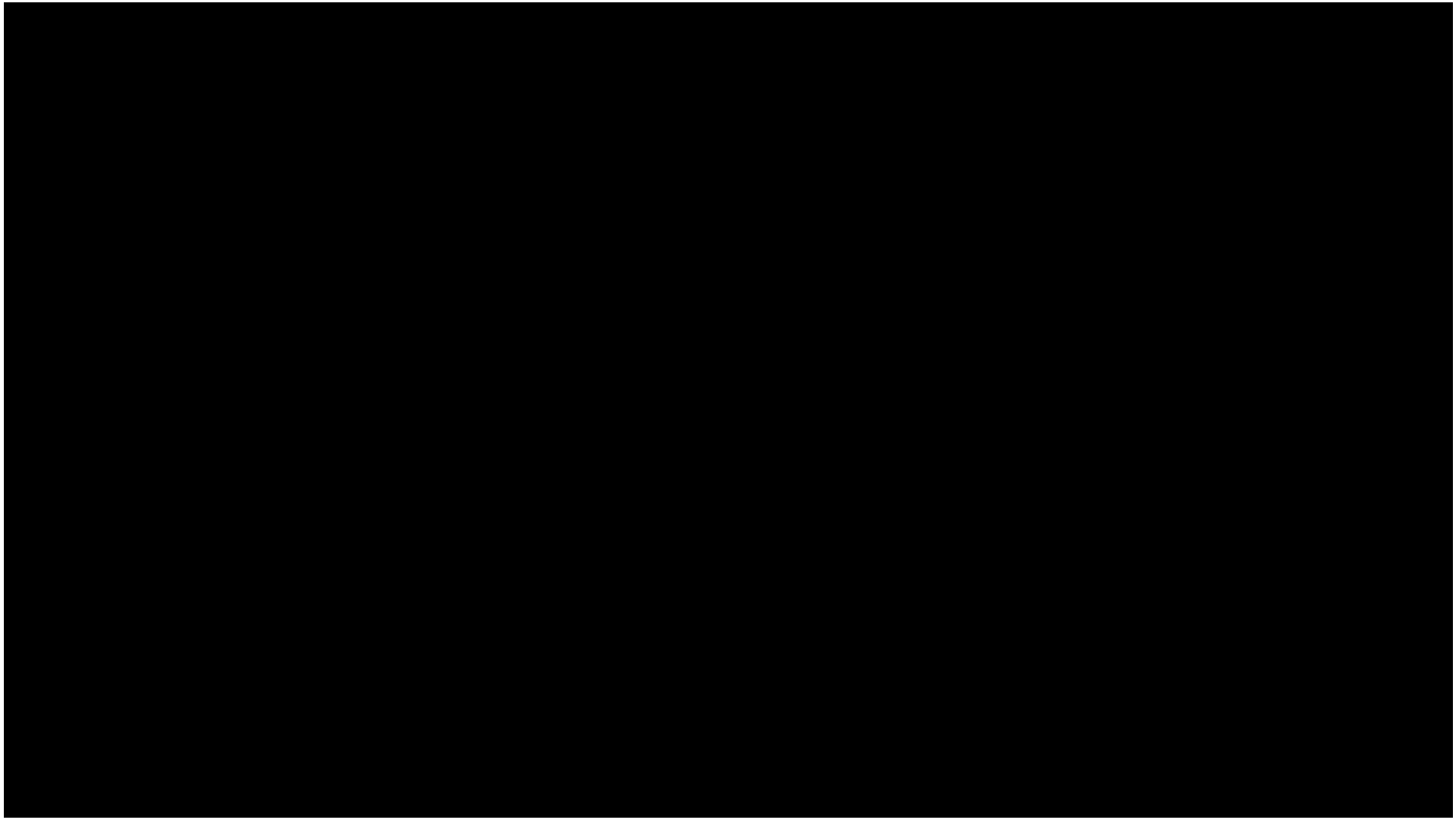
- ✓ Facturació i número de treballadors
- ✓ Activitat
- ✓ Estructura societària i composició de l'accionariat
- ✓ Situació financera (existència de beneficis)
- ✓ Límit a contractar

ESTADÍSTIQUES ASSEGURANCES D & O

- ✓ Una de cada tres empreses amb assegurança de D & O ha rebut almenys una reclamació
- ✓ La sinistralitat és del 43,2 %
- ✓ Les despeses de defensa jurídica suposen el 74 % del cost dels sinistres

Ciberriesgos

Un riesgo empresarial más allá de la tecnología



Datos para dimensionar el problema

- Coste del cibercrimen en la economía global:
  - En 2015 $3 trillones (AIG)
  - Se estima que esta cifra se doblará en 2021.(Fuente Thiber)
  - $325 mil recaudados en los 3 últimos años mediante Cryptowall
  - $30 millones recaudados por Cyptolocker en 2015
  - Ataque Ddos disponibles a 5-10 € la hora.
  - Valor medio “Fraude CEO” 160.000 $

Situación en España

- España ocupa el tercer lugar en el ranking de países más atacados por los ciber-delincuentes, según han analizado los expertos en seguridad informática de la Universidad Pontificia Comillas.
- En España se producen más de 4.000 ataques al día.
- La motivación de los ataques es, sobre todo, económica: "el ciber-crimen mueve más dinero que la droga".
- El 73% de las empresas son vulnerables por que sus equipos han superado su ciclo de vida natural.

- En el país se dedica cada año 3,8 millones de euros en ciber-seguridad, lo que representa un incremento del 18% en los últimos años, las empresas españolas dedican tan solo un 3% de su inversión tecnológica en ciber-seguridad.

Datos para comprender el riesgo

- Los ataques están en los sistemas de media 256 días hasta que son detectados.
- El 90% de ataques de suplantación de identidad (phishing) tienen éxito con el envío de 10 e-mails. (Verizon DBIR-2014)
- El 95% de todos los incidentes el factor humano es uno de los factores desencadenantes.
- El 80% de los ataques podría evitarse con la aplicación de políticas de higiene y seguridad en las redes, los sistemas y los dispositivos, que incluyese claves de acceso y configuración segura, así como la recertificación de accesos.
- Un 85% de incidentes de ciber espionaje son descubiertas por terceros.
- El 96% de las vulnerabilidades que afectan a Windows se podría mitigar quitando el perfil de administrador a los usuarios (Avecto 2013 Microsoft vulnerability study)
- En el 100% de las brechas de datos se detecta un robo de credenciales (Mandiant)

¿Quién está detrás de un ataque?

- **Estados Soberanos**

  Objetivo: Ventaja política y militar. En algunos casos económica.

- **Crimen Organizado**

  Objetivo: Ganancia económica.

- **Terrorismo**

  Objetivo: Ganar adeptos, ganancia económica, instalaciones críticas.

- **Hacktivistas**

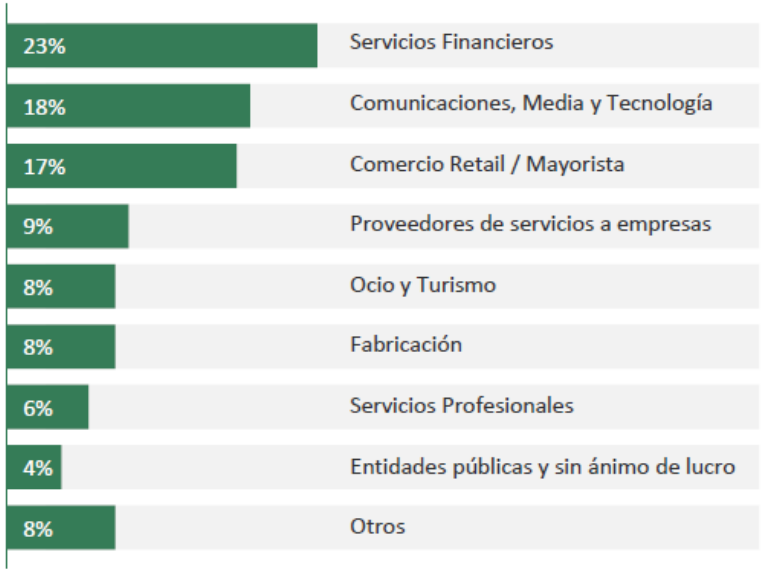
  Objetivo: Cambiar la sociedad a través de exponer modelos de negocio, transparencia, poner en relieve deficiencias en seguridad.

- **Script Kiddies**

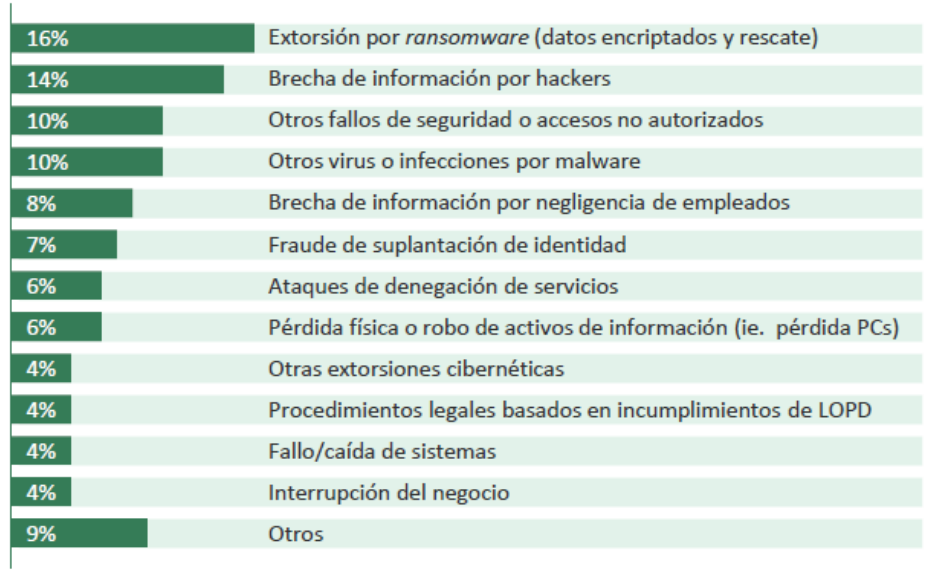
  Objetivo: Reconocimiento.

Principales amenazas

Ciberataques recibidos: por industria



Ciberataques recibidos: por tipología



Fuente: AIG EMEA, periodo 2013-2016

Legislación que regula la seguridad de la informática

- Ley Orgánica 15/1999, de 13 de diciembre de Protección de datos de carácter personal – LOPD.
  - Seguridad de la información y confidencialidad de los datos.
- Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal – RLOPD.
  - Medidas de seguridad y protección de los datos.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos derogando la Directiva 95/46/CE . - RGPD aplicable a partir del 25 de mayo de 2018.
  - Evaluación de riesgos y medidas de seguridad.
  - Obligación de notificación 72 horas a la entidad de control y si hay riesgo a los afectados.
  - Sanciones hasta de 20 millones € o el 4% del volumen de negocio.

Gestión del Riesgo

Prevención – Decálogo para la Pyme segura

1.- Política y normativa: Desarrollar normativas y procedimientos para usuarios,

2.- Control de acceso: Política de contraseñas, niveles de acceso, etc..

3.- Copias de seguridad: Disponibilidad, actualización, situación, cifrado, etc..

4.- Protección antimalware: Utilizar antivirus y analizar todos los dispositivos.

5.- Actualizaciones: Mantener los sistemas actualizados con la última versión.

6.- Seguridad de la red: Controlar un uso de la red corporativa segura.

7.- Información en transito: Control de los medios móviles y su conexión.

8.- Gestión de soportes: Tipos de soportes e idoneidad de estos.

9.- Registro de actividad: Monitorizar los procesos.

10.- Continuidad de negocio. Crear un plan de continuidad y recuperación.

Gestión del Riesgo

Asesoría y Formación

- Educar a la organización sobre los riesgos actuales y emergentes.
- Valoración de los riesgos y las amenazas dentro del marco operacional de la organización.
- Auditoría por expertos en seguridad de los sistemas y protocolos.
- Plan de actuación:
  - Gestión de incidentes
  - Revisiones periódicas
  - Plan de contingencias

Gestión del Riesgo: El seguro - Coberturas

1

Servicios y gastos

- Gestión de incidentes

2

Responsabilidad por Protección de Datos

- Responsabilidad en protección de datos.

3

Indemnización por Daños y Pérdidas Económicas a Terceros

- Responsabilidad por la seguridad y el tratamiento de la información.
- Responsabilidad en medios digitales (redes sociales, web, etc.)

4

Indemnización por Daños y Pérdidas Económicas Propias

- Extorsión cibernética.
- Pérdida de beneficios por la interrupción de la actividad.
- Daños materiales.
- Transferencias fraudulentas.

Gestión del Riesgo: El seguro - Coberturas

1 Servicios y Gastos

› Gestión de incidentes:

- Teléfono 24 h de atención al usuario de urgencia.
- Asesoría legal.
- Asesoría en RRPP.
- Asesoría tecnológica – informática forense.
- Recuperación de datos y los sistemas.
- Gastos de notificación.
- Servicios de control de identidad y crédito.

2 Responsabilidad en protección de datos

- Sanciones LOPD.
- Asesoría legal y gastos de defensa.

Gestión del Riesgo: El seguro - Coberturas

3 Indemnización por Daños y Pérdidas Económicas a Terceros (R.C.)

- Responsabilidad por la seguridad y el tratamiento de la información:
  - Responsabilidad por la custodia de los datos.
  - Fallos de seguridad.
  - Divulgación no autorizada de datos.
  - Falta de diligencia en la notificación.
  - La alteración, corrupción o alteración de los datos de una red.
  - Incumplimiento en las regulaciones de privacidad.
  - Pérdida de la información de los empleados.

- Responsabilidad en medios digitales (redes sociales, web, etc.):
  - Intromisión en la intimidad o daño reputacional.
  - Infracción de derechos de autor, titulo, eslogan, marca.
  - Plagio, piratería, robo de ideas.
  - Injurias, calumnias.

Gestión del Riesgo: El seguro - Coberturas

4 Indemnización por Daños y Pérdidas Económicas Propias

› Extorsión cibernética :

- Los gastos derivados de solucionar el problema.
- El importe pagado a los ciberdelincuentes para salvaguardar la información con el consentimiento de la aseguradora.

› Pérdida de beneficios por la interrupción de la actividad:

- Los gastos relacionados con la recuperación de la actividad.
- Las pérdidas sufridas debido a la paralización.

› Daños materiales:

- Los gastos incurridos para la recuperación de los datos debido a un siniestro de daños materiales: Incendio, fenómenos meteorológicos, daños eléctricos, daños por agua.

› Transferencias fraudulentas:

- Dentro de la póliza CIBER como cobertura incluida o a través de un apéndice de extensión de cobertura.

Ver siguiente pág....

Gestión del Riesgo: El seguro - Coberturas

Transferencias fraudulentas :

- A través de una póliza de CRIME, donde se da cobertura a la infidelidad de empleados y a los actos fraudulentos de terceros.

El Internet de las cosas (IoT)

- Actualmente en alguna aseguradora es posible asegurar la Pérdida de Beneficios y la recuperación de datos derivados de un error humano, de un fallo del sistema o de un fallo de seguridad.

Casos reales de siniestros por ciberriesgos

Extorsión cibernética

Varios empleados de una empresa manufacturera reciben un mail de una empresa telefónica indicando que tienen una deuda pendiente de 900 €. En el mail se invita a acceder a un link para obtener mayor información y detalle.

La mayor parte de los empleados destruyen dicho correo electrónico dado que ni tan siquiera son clientes de la operadora telefónica. No obstante uno de ellos, que concretamente es el responsable de Administración, cliente de la operadora telefónica, hace click en el link y automáticamente salta un pop-up informando que todos sus archivos han sido encriptados y pidiendo un rescate en bitcoins. Además del rescate, los delincuentes informáticos detectan información sensible con lo que incrementan su demanda. La amenaza es clara: o hacen frente al pago o destruyen la información.

Solución aseguradora

Mediante la cobertura de extorsión cibernética, se daría cobertura a los Gastos de Informática Forense, Asesoramiento Legal y Consultoría sobre el proceso adecuado para pagar el rescate, además del reembolso de dicho rescate.

Empleado negligente

En un bufete de abogados que asesora en operaciones de fusiones y adquisiciones, uno de sus socios olvida un pendrive con información sensible de una operación, en el puente aéreo Madrid - Barcelona.

En ese mismo vuelo otra persona, que dio la casualidad era periodista de un medio local, encuentra dicho pendrive y comprueba que la información es tremendamente interesante para publicarla en prensa.

Al aparecer la noticia en los medios, el bufete de abogados, único conocedor del proceso de compra-venta y que había firmado una clausula de confidencialidad, tiene que asumir el error. La compra-venta no se realiza por injerencias externas, y ambas partes reclaman al bufete daños y perjuicios.

Solución aseguradora

Mediante la cobertura de responsabilidad civil por el uso indebido de información corporativa se otorga cobertura a los gastos de defensa, los gastos de restitución de imagen, sanciones ADP y posibles indemnizaciones.

Suplantación de identidad

El Director Financiero de una cadena de *retail* entra desde su ordenador corporativo en un mail de LinkedIn para aceptar una solicitud de amistad. Lo que no sabe es que dicho mail es falso.

Al hacer click en el link un delincuente informático se conecta en remoto a su ordenador, y roba sus credenciales como Director Financiero. Empieza a ordenar que ciertas transferencias de consolidación de cuentas en lugar de acabar en una cuenta de la empresa acaben en cuentas domiciliadas en Rusia y China. Al cabo de cinco días el Director Financiero se da cuenta de que el ratón del ordenador se mueve solo…

Solución aseguradora

Mediante la cobertura de primera respuesta se daría cobertura inmediata a la informática forense y asistencia de un equipo asesor especializado, que hubiese detenido las transferencias y analizado de donde venía la amenaza, además de saber si había algún archivo comprometido. Además con la cobertura adicional de fraude informático se hubiera dado cobertura al dinero robado.

Protecció de dades

LOPD i Nou Reglament

ON ESTÀ REGULADA LA PROTECCIÓ DE DADES?

Actualment a la LOPD, però el passat 25 de maig de 2016 va entrar en vigor el Nou Reglament General de Protecció de Dades (Reglament UE 2016/679) i s'aplicarà a partir del 25 de maig de 2018.

CANVIS IMPORTANTS

L'aplicació del nou Reglament implica una sèrie de canvis importants respecte de l'actual LOPD.

L'objectiu d'aquest nou Reglament és donar més seguretat jurídica i control als interessats sobre la seva informació privada, simplificar la regulació actual i harmonitzar la regulació existent entre els diferents països de la UE.

CONSENTIMENT EXPRÉS

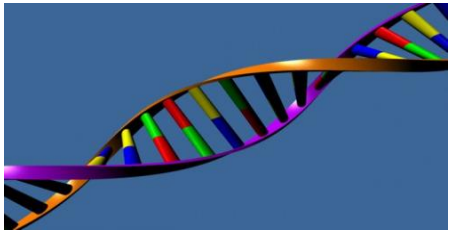
Fins ara era válid el consentiment tàcit per al tractament de dades de caràcter personal. A partir d'ara el consentiment haurà de ser un acte afirmatiu clar (exprés).

NOVES CATEGORIES DE DADES SENSIBLES

S'introdueixen categories especials de dades com ara:

Dades Biomètriques: Permeten identificació única de persones, p.e. imatges facials o dades dactiloscòpiques.

Dades Genètiques: Proporcionen informació sobre la fisiologia o salut de les persones obtinguts per l'anàlisi de mostres biològiques.



REFORÇ I FLEXIBILITZACIÓ DEL RÈGIM SANCIONADOR

Increment molt important de les sancions.

Les multes seran proporcionals a cada cas particular podent arribar al límit de fins a 20 milions d'euros o el 4% de la facturació global de l'empresa infractora.

OBLIGACIÓ DE NOTIFICACIÓ DELS TRENCAMENTS DE SEGURETAT

S'haurà de notificar a l'Autoritat de Protecció de Dades (a Catalunya APD) en cas de trencament/fuga de seguretat amb un termini de 72 hores i en sùpòsits d'alt risc caldrà notificar també les persones interessades que puguin veure els seus drets afectats.

EXTENSIÓ ÀMBIT TERRITORIAL D'APLICACIÓ

El Reglament s'aplicarà no només com fins ara als responsables encarregats de tractament de dades establerts a la UE, sinó que s'amplia a tots aquells no establerts a la UE sempre que es realitzin tractaments derivats d'una oferta de béns o serveis destinats a ciutadans de la UE.

POSSIBILITATS DE COBERTURA

1) Possibilitat de cobertura addicional de sancions LOPD dins la pòlissa de D & O

2) Algunes pòlisses de RC Professional ofereixen una extensió de cobertura per a cobrir sancions LOPD

3) Dins de la pòlissa de Ciber Risc

Seguridad.
Confianza.
Futuro