UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

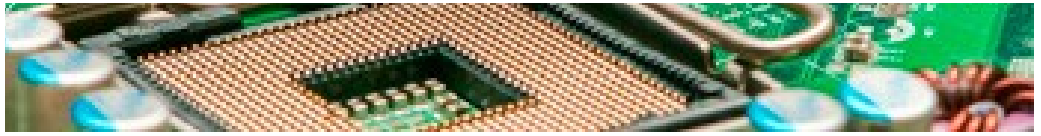
Máster Universitario en Ingeniería Informática

CyberSeguridad
Tema 7: Aspectos Legales

José Ismael Ripoll Ripoll

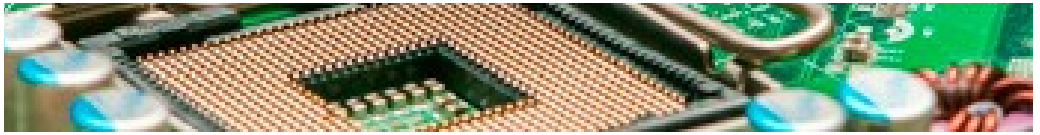
Máster Oficial Universitario en Ingeniería Informática
muiinf.webs.upv.es

MUIInf



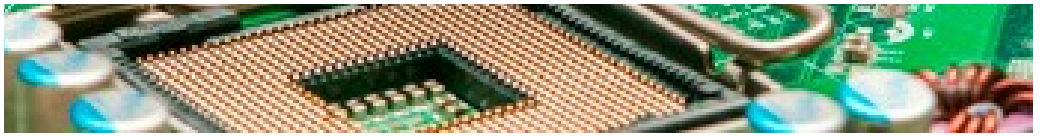
Contenido

- El valor de la Información.
- Reglamento General de Protección de Datos: RGPD
  - https://rgpd.es/
  - https://www.aepd.es
- Infraestructuras Críticas.
  - http://www.cnpic.es/



¿Ciberseguridad?

- Existen 3 motivos para aplicar políticas de seguridad en nuestra empresa:
  - Por concienciación propia de la necesidad de tener una continuidad del negocio.
  - Porque nos los exijan los clientes.
  - Porque lo exija la ley:
    - RGPD
    - Ley de Infraestructuras Críticas.
- La falta de seguridad es un lujo que pocos se pueden permitir.



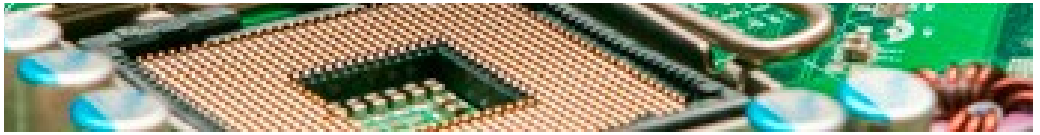
Caso reciente

§ *"La Caixa expidió cuatro millones de tarjetas 'vulnerables'"*

- http://www.economiadigital.es/es/notices/2015/11/caixabank-ha-distribuido-cuatro-millones-de-tarjetas-quevulneran-la-ley-de-proteccion-de-datos-78968.php

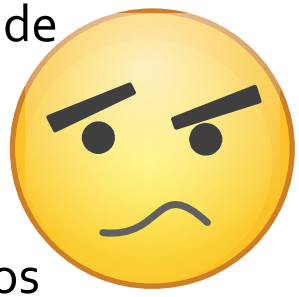
- Los dispositivos permiten la interceptación fraudulenta de datos suficientes para realizar compras en páginas web como Amazon (Noviembre 2015)
- La tecnología Contactless, en el punto de mira por infringir la **Ley Orgánica de Protección de Datos (LOPD)** y resultar vulnerable al fraude.
- La Caixa (ahora CaixaBank) emitió, a sabiendas, cuatro millones de tarjetas a las que, con sólo un teléfono móvil, se podía interceptar el nombre del usuario, el número y la fecha de caducidad porque la información no está encriptada. Datos suficientes para realizar compras en el portal Amazon.

EconomíaDigital Nov, 2015

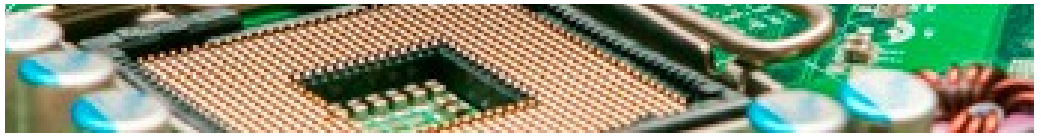


EL TEDH DECLARA QUE EL USO DE CÁMARAS OCULTAS VULNERA EL DERECHO A LA INTIMIDAD DEL TRABAJADOR

- El 9 de enero de 2018 el Tribunal Europeo de Derechos Humanos dictó sentencia en el caso "Ribalda y otros", en la que ha declarado que la empresa vulneró el **derecho fundamental a la intimidad** de los cinco trabajadores despedidos por haberse valido de **cámaras ocultas**, para denunciar la **sustracción de productos** en el supermercado en el que trabajaban.
- De acuerdo con la sentencia, el tribunal considera que el **dueño del supermercado violó el artículo 5 de la Ley Orgánica de Protección de Datos** y con ello, también el artículo 8 del Convenio Europeo de Protección de los Derechos Humanos sobre el derecho al respeto de la vida privada ya que las trabajadores deberían de haber sido informadas de la colocación de estas cámaras ocultas y no fue así.



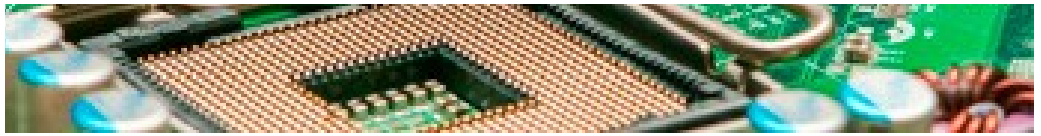
- Por ello, y pese a que la jurisdicción social española validó los despidos disciplinarios declarándolos procedentes, el **TEDH impone al empresario el pago de 4.000 euros** de indemnización a cada empleada en concepto de daños y perjuicios, además de 500 euros a una de las demandantes por los costes del procedimiento.



Errores sobre la seguridad

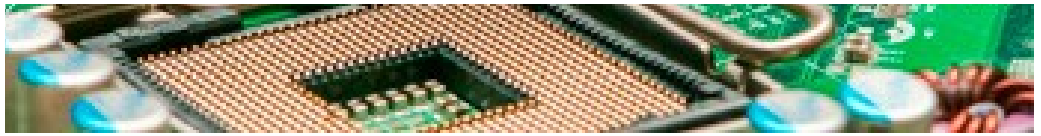
- Pensar que su información o sus sistemas no interesan a nadie.
- Creer que la seguridad es sólo técnica y por tanto sólo compete a los informáticos.
- Creer que un antivirus y un firewall son suficientes.
- Pensar que la seguridad es un producto y no un proceso.
- La confidencialidad es algo de espías y grandes multinacionales.
- No contemplar la seguridad en los contratos corporativos.
- Mirar hacia fuera pensando que las amenazas siempre son externas.
- Ofrecer servicios a través de Internet sin tener en cuenta seguridad.
- Descuidar la gestión de la red y los sistema

http://www.securityartwork.es



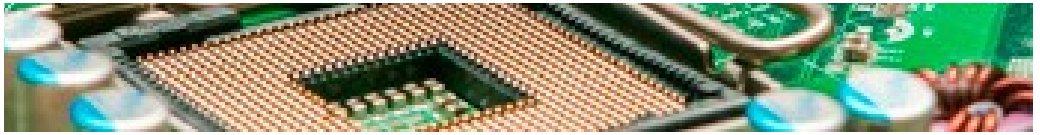
Política de seguridad en las PIMES

- Errores frecuentes en las PIMES:
  - Creer que por ser pequeña, no interesa a nadie.
  - Creer que la seguridad es sólo asunto de los informáticos.
  - Pensar que un antivirus y un firewall son suficientes.
  - Considerar que la seguridad es un producto y no un proceso.
  - La confidencialidad es algo de espías y grandes multinacionales.
  - No contemplar la seguridad en los contratos corporativos.
  - Mirar sólo hacia fuera.
  - Ofrecer servicios a través de Internet sin tener en cuenta su seguridad.
  - Descuidar la gestión de la red y los sistemas.

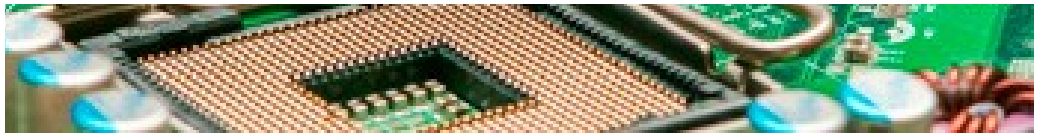


Concienciación

- Los elementos más importantes de la ciberseguridad son las personas.
- El primer paso a dar es concienciar a los responsables.
  - Es necesario que los responsables sean conocedores de los problemas y las soluciones.
  - Debe existir concincia del problema lo antes posible.
- Concienciar al resto de la organización de la necesidad de trabajar siguiendo protocolos seguros.
- Hoy en día, es quizás ,más necesario invertir esfuerzos en concienciar a los ciudadanos en los riesgos del cibercrimen que en perseguirlo.

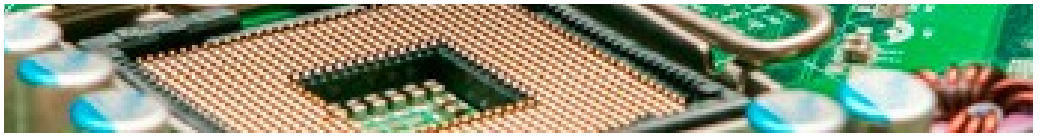


- El Reglamento General de Protección de datos substituye a la antigua LOPD.
- Es una ley Europea de aplicación directa. Por tanto, reemplaza las locales.
- Agencia Española de Protección de Datos:
  - http://www.agpd.es/



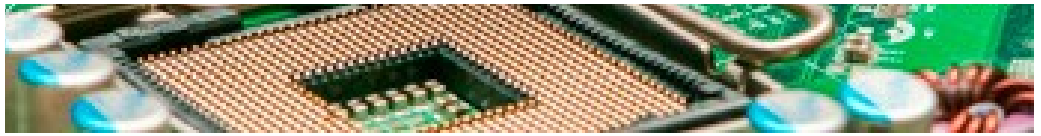
RGPD vs LOPD

- Aparte de otras consideraciones, la principal diferencia con la LOPD reside en el objeto que se protege o legisla:
  - LOPD: Se centra en los datos.
  - RGPD: Se centra en el tratamiento de los datos.
- En la LOPD, el DNI de una persona ES un dato sensible y definía tres grados según el tipo de información:
  - Alto: ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, etc.
  - Medio: sanciones administrativas, créditos, tráfico, etc.
  - Bajo: resto de datos.
- En la RGPD, el uso que se le de al DNI será lo que se regule.
- La LOPD era más "garantista" y con penas más duras que la RGPD.
- LOPD obligaba a registrar cualquier fichero de nivel Alto o Medio.



§ Responsabilidad:

- Habrá que implementar mecanismos que permitan acreditar que se han adoptado todas las medidas necesarias para tratar los datos personales como exige la norma. Es una responsabilidad **pro-activa**. Las organizaciones deben ser capaces de **demostrar** que cumplen dichas exigencias, lo cual obligará a desarrollas políticas, procedimientos, controles, etc.
- Por ejemplo, los propietarios de los datos deben dar su consentimiento "inequívoco".

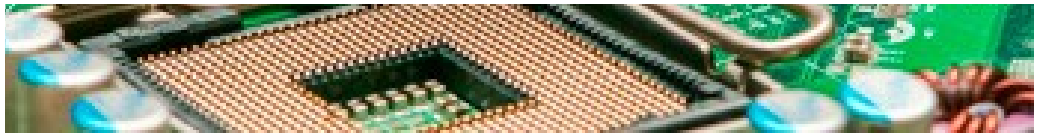


§ Protección de datos desde el diseño:

- Se deberán adoptar medidas que garanticen el cumplimiento de la norma desde el mismo momento en que se diseñe una empresa, producto, servicio o actividad que implique tratamiento de datos, como regla y desde el origen.

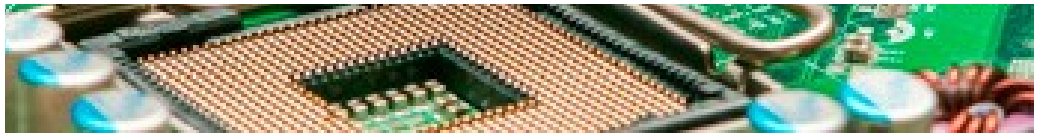
  Construir sistemas que sean seguros…

  Y no al revés: "asegurar los sistemas"



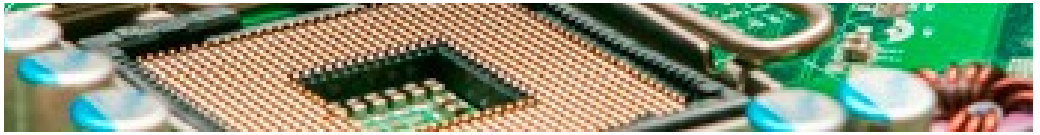
§ Transparencia:

- Los avisos legales y las políticas de privacidad deberán ser más simples e inteligibles, facilitando su comprensión, además de más completas. Incluso se prevé que, con el fin de informar sobre el tratamiento de los datos, puedan utilizarse iconos normalizados.
- Se deben **registrar y notificar** las brechas de seguridad que afecten a los tratamientos de datos personales en un plazo no superior a 72 horas a la autoridad de control competente (CCN-CERT, CSIRT, …).
- Cuando la brecha de seguridad pueda entrañar un alto riesgo para los derechos y libertades de los titulares de los datos, el responsable del tratamiento deberá **comunicar a los afectados**, sin dilación indebida, la brecha de seguridad.



RGPD: Roles

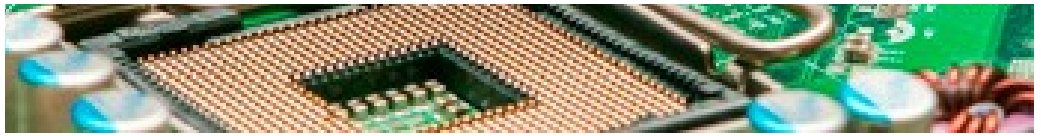
- **Responsable** del tratamiento:
  - Responsable legal.
- **Encargado** del tratamiento:
  - Responsable técnico.
- Delegado de Protección de Datos (**DPD**)
  - Asesor legal.



RGPD "responsable"

- **Responsable** del tratamiento:
  - Legitimar la necesidad y proporcionalidad del tratamiento.
  - Informar a los usuarios de sus derechos.
  - Contratar al **encargado** de la seguridad.
  - Contratar a un **Delegado de Protección de Datos**.
  - Definir/crear el registro de incidentes de seguridad.
  - Evaluación del riesgo.
  - Definir el plan de contingencias.
  - Identificar las medidas de seguridad necesarias.

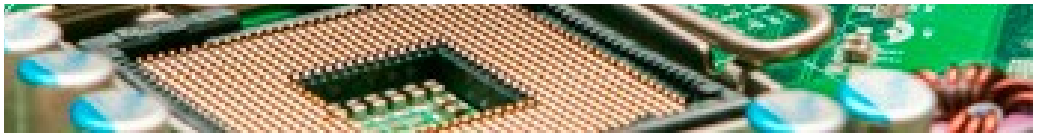
Demostrar una actitud pro-activa



RGPD "Encargado"

- **Encargado** de tratamiento:
  - Mantener un registro de actividades de tratamiento.
  - Determinar las medidas de seguridad aplicables a los tratamientos que se realicen.
  - Debe designar un Delegado de Protección de Datos en los casos previstos por el RGPD.

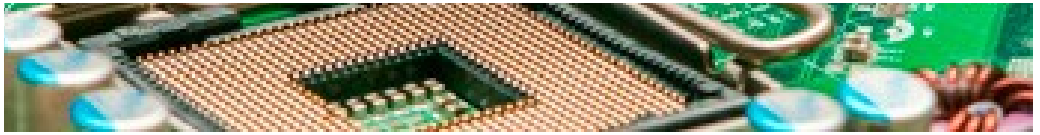
Puede ser una
empresa de ciberseguridad



§ Delegado de protección de datos

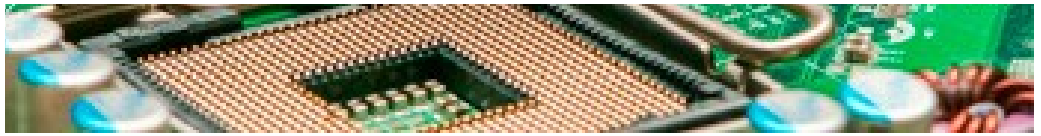
- Informar al responsable de sus obligaciones en el tratamiento.
- Supervisar el correcto cumplimiento de la normativa.
- Asesorar sobre la evaluación de impacto relativa a la protección de datos.
- Colaborar con la autoridad de control comunitaria y nacional.

Persona con conocimiento especializado en Derecho y la práctica en materia de protección de datos.



Y las grabaciones de vídeo

- En Rusia es costumbre grabar la circulación como prueba en casos de accidente.
- Hasta la llegada de la RGPD, en España estaba prohibido.
- Ahora (guia-videovigilancia.pdf), estarían permitidas:
  - Finalidad domestica: Cascos de un ciclista o motorista, que fuesen tomando imágenes paisajísticas.
  - Grabaciones con la finalidad de obtener pruebas para determinar responsabilidades asociadas a la producción de un suceso.
  - Drones: ?!?!
- Se pueden hacer fotos de una playa?



Conclusiones

- RTFM
- Las leyes las interpretan los jueces.
- Lo lógico y lo legal no siempre van de la mano.
- Yo de mayor quiero ser DPD.