VNIVERSITAT DE VALÈNCIA

Càtedra de privacitat i transformació digital
Microsoft-UV

# IMPLICACIONES LABORALES EN EL ÁMBITO UNIVERSITARIO DE LA NUEVA NORMATIVA EN PROTECCIÓN DE DATOS

Ricard Martínez Martínez.

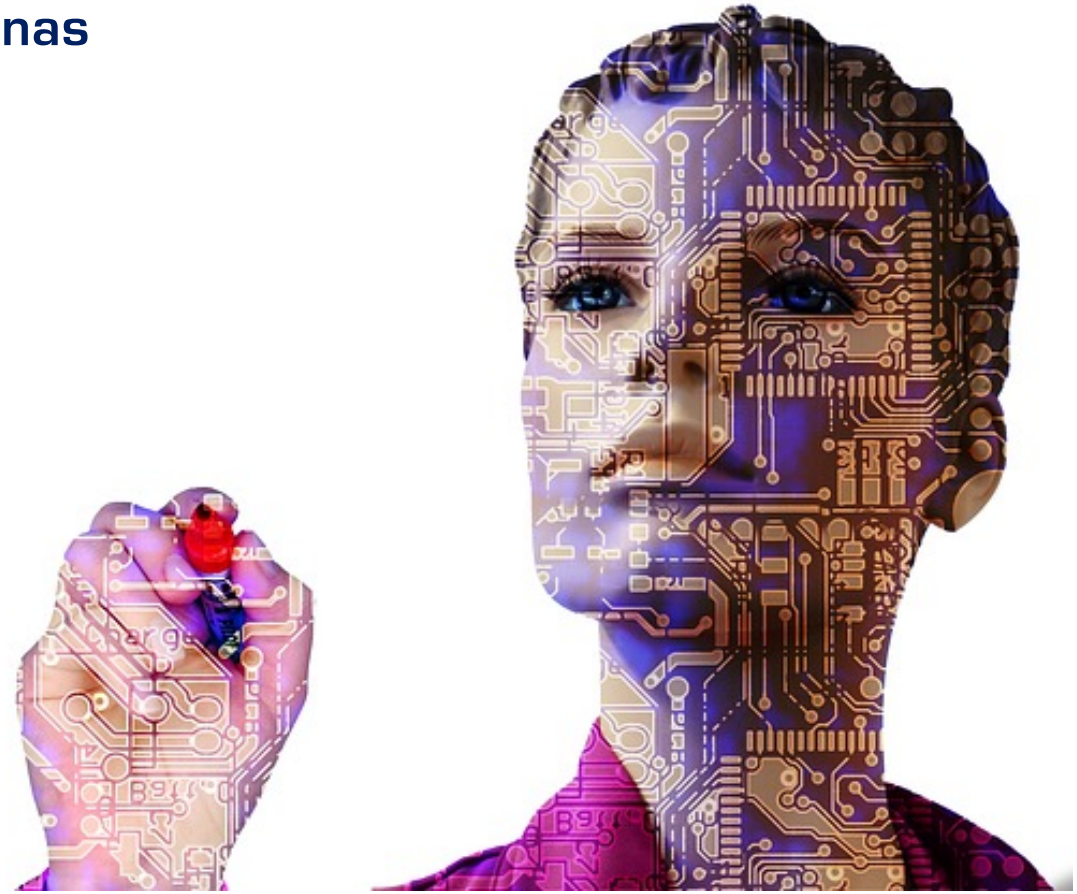
Càtedra Microsoft
Universitat de València
**Privacitat &**
**Transformació Digital**

VLC/CAMPUS
VALENCIA, INTERNATIONAL CAMPUS OF EXCELLENCE

CAMPUSHABITAT5U

## Tratamos datos:

## Protegemos personas



# Derechos digitales del trabajador

**Disposición final decimotercera. Modificación del texto refundido de la Ley del Estatuto de los Trabajadores.**

Se añade un nuevo artículo 20 bis al texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre, con el siguiente contenido:

**«Artículo 20 bis. Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.**

Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.»

**Disposición final decimocuarta. Modificación del texto refundido de la Ley del Estatuto Básico del Empleado Público.**

Se añade una nueva letra j bis) en el artículo 14 del texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, que quedará redactada como sigue:

«j bis) A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.»

## Artículo 88. Derecho a la desconexión digital en el ámbito laboral.



- Base legal:
  - Estatuto de los Trabajadores, legislación sobre función pública.
  - ¿única base legal?
    - ✓ Prevención de riesgos laborales (ejemplo decretos e instrucciones sobre agentes químicos y cancerígenos)
    - ✓ Responsabilidad en el cuidado de los pacientes.
- No afectación a la intimidad personal y familiar.
- Respeto del espacio vital fuera del tiempo de trabajo legal o convencionalmente establecido.
- Respeto de su tiempo de descanso, permisos y vacaciones.
- Debe tener en cuenta.
  - la naturaleza y objeto de la relación laboral
    - ✓ Tareas con dedicaciones específicas, guardias localizadas…
  - la negociación colectiva o lo acordado entre la empresa y los representantes de los trabajadores

# ¿Qué hacer?

- Elabora una política interna dirigida a trabajadores, previa audiencia de los representantes de los trabajadores, incluidos los que ocupen puestos directivos.
- Contenidos:
  - modalidades de ejercicio del derecho a la desconexión
  - acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática.
  - preservar el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

- Consideración previa:
  - principio de proporcionalidad, e intervención mínima (STC Casino de la Toja)
- El uso de videocámaras se basa en la legitimación del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.
- Condiciones y prohibiciones.
  - informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida
  - No se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos

- No se limita a videocámaras:
  - La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores.

# Una interpretación integrada

- Artículo 22. Tratamientos con fines de videovigilancia.
- Supresión de las imágenes:
  - plazo máximo de un mes desde su captación,
  - conservadas para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones y puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.
  - No existe la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.

# Artículo 90 Geolocalización



- Base legal:
  - Estatuto de los Trabajadores, legislación sobre función pública.
  - ¿única base legal?
    - ✓ Prevención de riesgos laborales (ejemplo decretos e instrucciones sobre agentes químicos y cancerígenos)
    - ✓ Responsabilidad en el cuidado de los pacientes.
- Condiciones y prohibiciones.
  - informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida

**Artículo 91. Derechos digitales en la negociación colectiva.**

Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral

# Cuestiones sobre protección de datos

- En el plano de los derechos fundamentales:
  - JUICIO DE PROPORCIONALIDAD
  - EXPECTATIVA DE PRIVACIDAD
    - ✓ STC 98/2000 (Casino la Toja). Vida privada en el puesto. Proporcionalidad: no grabar sonidos.
    - ✓ STC 186/2000, (caso Ensidesa): proporcionalidad, las cámaras únicamente grababan el ámbito físico estrictamente imprescindible (las cajas registradoras y la zona del mostrador de paso de las mercancías más próxima a los cajeros).
    - ✓ STC 29/2013 (caso Universidad de Sevilla): Ausencia de información previa).
    - ✓ STC 39/2016, (asunto Bershka): Se admite una información genérica (cartel).
    - ✓ STDH 9-1-2018, López Ribalda: Falta de información previa.

# ¿Y CÓMO.....?

- **Paso 1.-Defino el tratamiento.**
  - Finalidad.
  - Alcance.
  - Tecnología.
  - Sujetos concernidos.
- **Paso 2.-Análisis de riesgos.**
  - Impacto en los derechos.
  - Cumplimiento normativo.
  - Seguridad de la información.
  - Aspectos reputacionales.
  - Terceros concernidos (empresas de seguridad, proveedores)

- **Paso 3 . ¿Me hace falta una evaluación de impacto en la protección de datos?**
  - Criterios GDPR
    - ✓ Tratamiento a gran escala de las categorías especiales de datos).
    - ✓ Observación sistemática a gran escala de una zona de acceso público.
- Criterios AEPD
  - ✓ 1.- Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sobre sus hábitos.
  - ✓ 3.-Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.

- ✓ 7.-Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 "Directrices sobre los delegados de protección de datos (DPD)" del Grupo de Trabajo del Artículo 29.
- ✓ 5.-Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.
- ✓ 7.-Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 "Directrices sobre los delegados de protección de datos (DPD)" del Grupo de Trabajo del Artículo 29.

  el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;

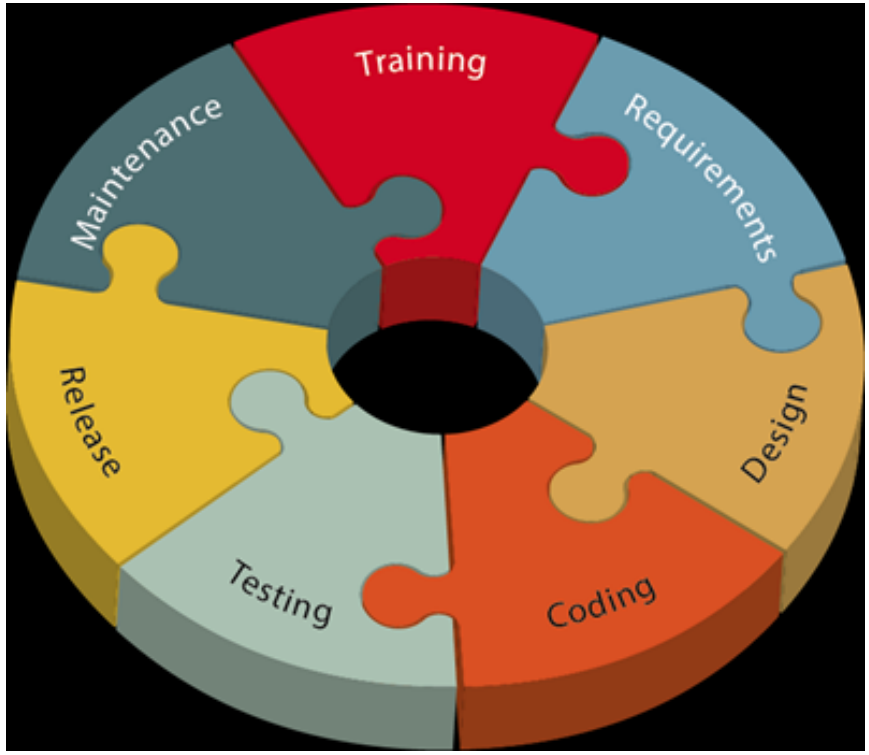
  el volumen de datos o la variedad de elementos de datos que son objeto de tratamiento

  la duración, o permanencia, de la actividad de tratamiento de datos;

  el alcance geográfico de la actividad de tratamiento.

# Paso 4. Protección de datos desde el diseño y por defecto.

Datatilsynet




The Norwegian Data Protection Authority has developed these guidelines to help organisations understand and comply with the requirement of data protection by design and by default in article 25 of the General Data Protection Regulation. We have cooperated with security professionals and software developers in public and private sector among others.

- Formar no es el punto de llegada.
  - Formación al equipo político.
  - Formación general.
  - Formación de cuadros directivos.
  - Formación al equipo IT.

## Training

During this activity, the specific types of training that should be given are determined. To ensure that everyone in the organisation understands both the need for, and the risks associated with, data protection and security, the training needs to be structured.


# ¿Qué necesitamos?



- Preguntas de ir por casa:
  - ¿Qué datos?
  - ¿Para qué?
  - ¿De quién?
  - ¿Cómo?
  - ¿Dónde?
  - ¿Desarrollado por quién?
  - ¿Alojado dónde?
- Procesos:
  - ¿Legalmente puedo?
  - Análisis de riesgos.
  - SbD
  - Evaluación de impacto relativa a la protección de datos.
- Juicios complementarios:
  - Legalidad y GDPR
  - Seguridad
  - Capacidad (recursos)
  - Oportunidad


**Requirements**

This activity revolves around setting requirements for data protection and information security for the final product. These requirements must reflect the need for data protection and information security, and should be included as part of the project plan.


**The target group comprises everyone involved in development, or with ownership of the software, including those responsible for defining the requirements, the product owners, customers/purchasers, project leaders, developers, architects, and testers. The Data Protection Officer and security advisor should also be involved in this activity.**

# Vamos a Iterar, y a Iterar...



## Design

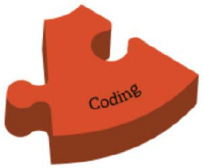
During this activity, you must ensure that requirements for data protection and information security are reflected in the design. The requirements identified during the requirements activity must be met, and requirements for the design must be defined.


It is important to take into account the existence of threat actors that may attempt to obtain and gain access to personal data. To reduce the attack surface, it must be analysed, and the software modelled and designed to ensure a robust end product.

**The target group for this activity is primarily architects, secondarily data protection officers, security advisors, and developers.**

## Coding

This activity will enable developers to write secure code by implementing the requirements for data protection and security.

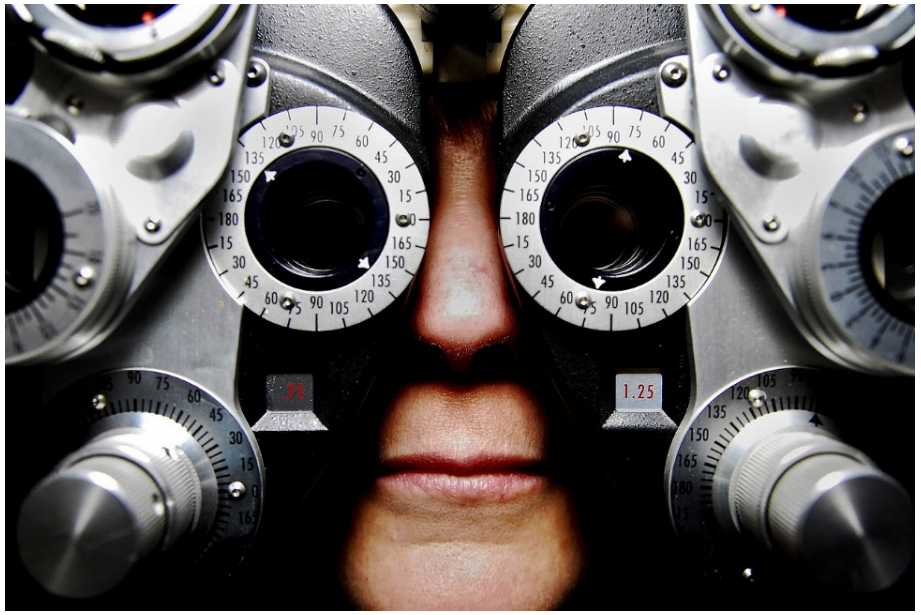



It is important that the company choose a secure and common methodology, both for coding and for enabling the developers to detect and remove vulnerabilities from the code. Automated code analysis tools should be introduced, and the company must have established procedures for static code analysis and code review.

**The target group for this activity is primarily developers, secondarily data protection officers, security advisors, and testers.**

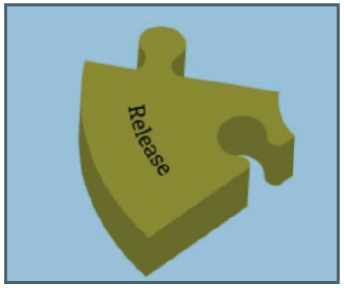
## Testing

During this activity, testers check that the requirements for data protection and information security defined during the Requirements and Design activities have been implemented as planned, as well as verify that the requirements have been properly met.

## Release

During this activity, the software is prepared for release. This includes planning for how the organisation effectively can handle incidents that may arise after release, as well as procedures for updating the software. A comprehensive and final security review should be done before the software is released.





In organisations where software releases are frequent, an incident response plan should be established before the initial release, while security reviews should be carried out upon each release. It is important to archive all relevant data from the development process.

**The target group for this activity is primarily project leaders, security advisors, and data protection officers. When preparing an incident response plan, those responsible for incident response handling should contribute, while testers should contribute to the security review.**

## Maintenance

The most important element of this activity is that the organisation has implemented a plan for incident response handling (prepared during the release activity) and follows it.



The organisation must be prepared to handle incidents, security breaches, and attacks that can result in breaches of confidentiality, integrity, or availability relating to personal data. It should have a response centre that can handle incidents and deliver updates, guidelines, and information to users and data subjects.

**The target group for this activity is primarily the response incident team, security advisors, and data protection officers, as well as maintenance, service, and operation staff.**

- Paso 6. Aspectos estratégicos a considerar para “cumplir”
  - Protocolizar.
  - Escoger bien la herramienta de control.
  - Asegurar transparencia.
  - Implicar a destinatarios y representación sindical.
  - Garantizar la proporcionalidad.
  - Garantizar la seguridad.

**Artículo 96. Derecho al testamento digital.**

1. El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas:

a) Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión.

Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto.

b) El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones.

c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

2. Las personas legitimadas en el apartado anterior podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones.

El responsable del servicio al que se le comunique, con arreglo al párrafo anterior, la solicitud de eliminación del perfil, deberá proceder sin dilación a la misma.

3. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones y, en su caso, el registro de los mismos, que podrá coincidir con el previsto en el artículo 3 de esta ley orgánica.

4. Lo establecido en este artículo en relación con las personas fallecidas en las comunidades autónomas con derecho civil, foral o especial, propio se regirá por lo establecido por estas dentro de su ámbito de aplicación.

# Una reflexión final



- El problema entre lo público y lo privado en la universidad.

GR@CIAS

ricard.martinez@uv.es ;

@catedramuv1


VNIVERSITAT DE VALÈNCIA