



**XIII  
JORNADAS  
STIC  
CCN-CERT**



**Cumplimiento  
conjunto del RGPD y  
ENS en la Universidad  
de Sevilla**

**COMUNIDAD Y CONFIANZA,  
BASES DE NUESTRA CIBERSEGURIDAD**

**#XIIIJORNADASCCNCERT**



**Francisco de Asís Gómez,  
Responsable de Seguridad de la Información**



**Julia Cortés,  
Responsable de Seguridad Delegada**

**Universidad de Sevilla  
CRUE TIC Grupo de Trabajo de Seguridad y Auditoría TI**

**Contacto: [seguridadtic@us.es](mailto:seguridadtic@us.es)**

# Índice

## 1. Acerca de la Universidad de Sevilla

## 2. Gestión de datos personales dirigida por proyectos

- PARSUS
- PARGEUS

## 3. Adecuación al ENS por etapas/fases

- Etapa I: diseño del Plan de adecuación
- Etapa II: desarrollo del Plan de adecuación

## 4. Gestión conjunta de Protección de Datos y Seguridad de SI

## 5. Dificultades

## 6. Facilitadores

# Acerca de la Universidad de Sevilla

102

Grados  
ofertados

> 52.000 alumnos de grado

32

Programas  
de doctorado

> 3.100 alumnos  
de doctorado

95

Másteres  
Universitarios

> 5.100 Alumnos de máster

4.185 PDI  
2.672 PAS

Sevilla es tu Campus !



32 centros  
133 departamentos

551 grupos de investigación

600.000 m2 construidos en edificios repartidos en 8 campus

## Más acerca de la Universidad de Sevilla

160

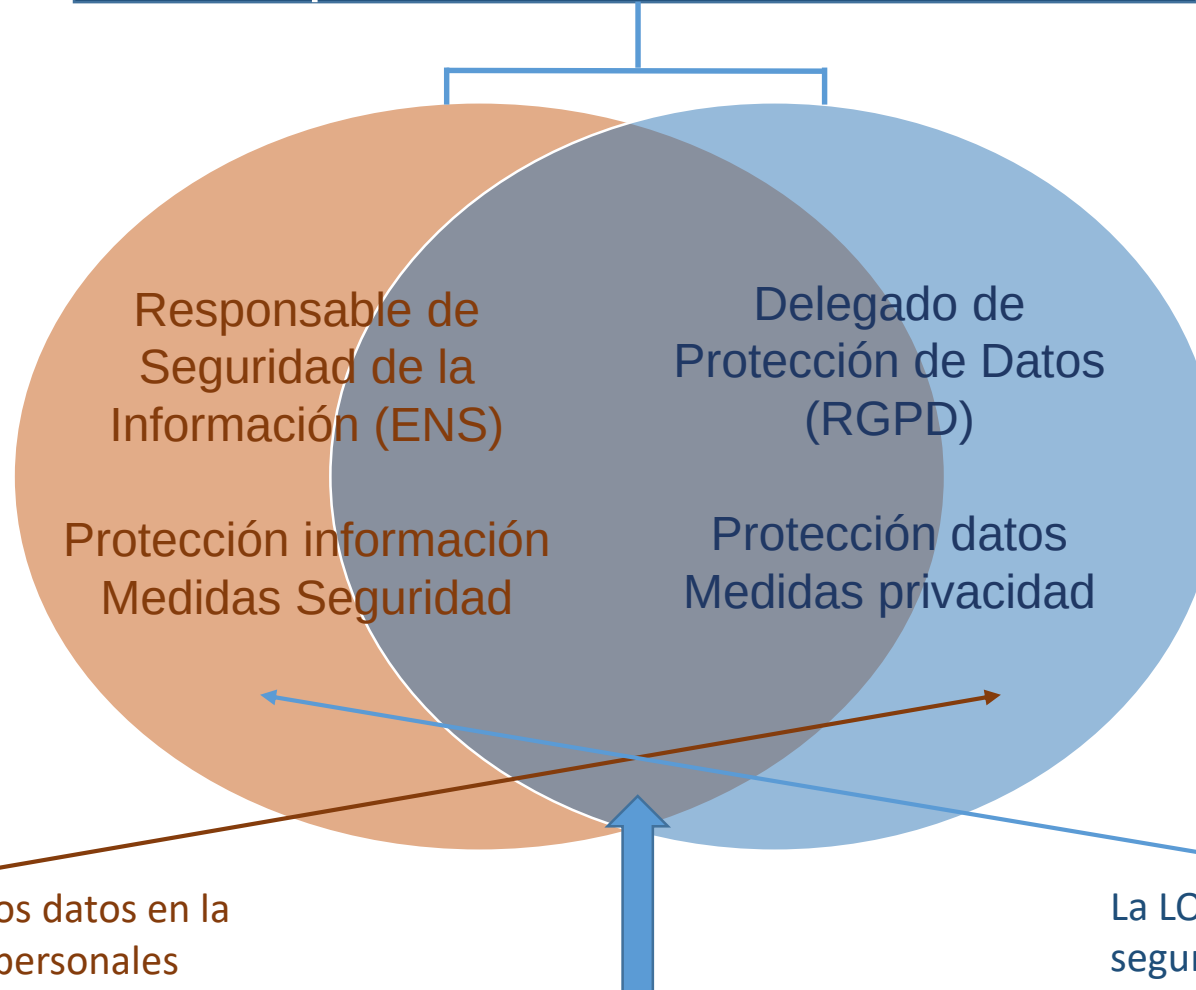
Servicios TI de la cartera  
de Servicios CRUE TIC

33

Tratamientos de datos  
personales registrados

- > 12.000 IPs públicas
- > 200.000 cuentas de usuario (UVUS)
- > 100.000 buzones de correo electrónico
- > 2.000 alojamientos de páginas webs
- > 200 certificados digitales de servidor
- > 790 listas de distribución

## Responsable de la Información

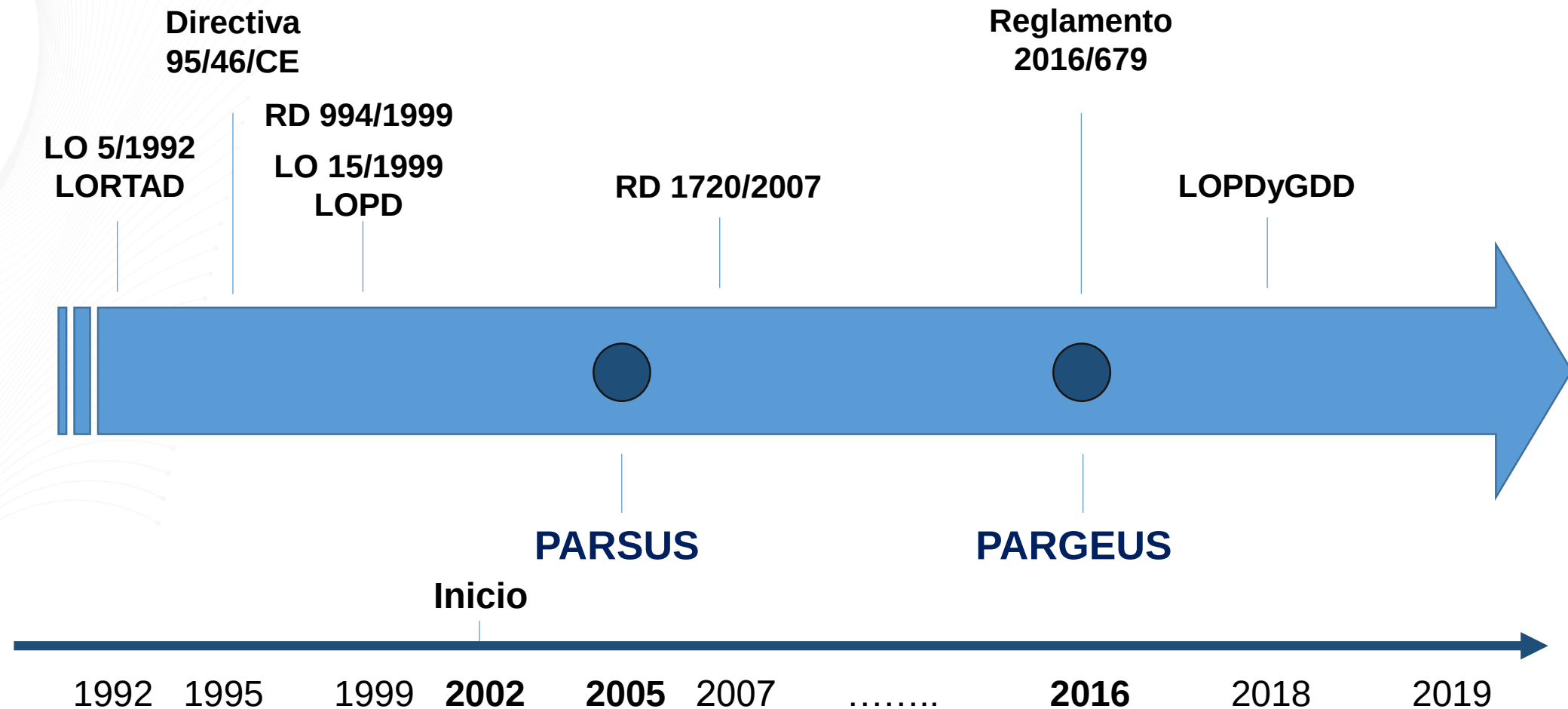


El ENS delega la protección de los datos en la legislación vigente sobre datos personales

La LOPDyGDD remite a las medidas de seguridad del ENS

**Seguridad basada en análisis de riesgos y en la auditoría continua**

# Gestión de datos personales dirigida por proyectos



# Roles y responsabilidades LOPD (hasta 2018)

## Responsable de los ficheros: Universidad de Sevilla

### Grupo gestión de la protección de datos (subcomisión desde 2016)

- ✓ Gerente
- ✓ Responsable de Seguridad de la Información (desde 2016)
- ✓ Responsable de la Seguridad de la LOPD a efectos jurídicos
- ✓ Responsable de Seguridad de la LOPD a efectos técnicos
- ✓ Asesor experto en protección de datos y tecnologías de la información

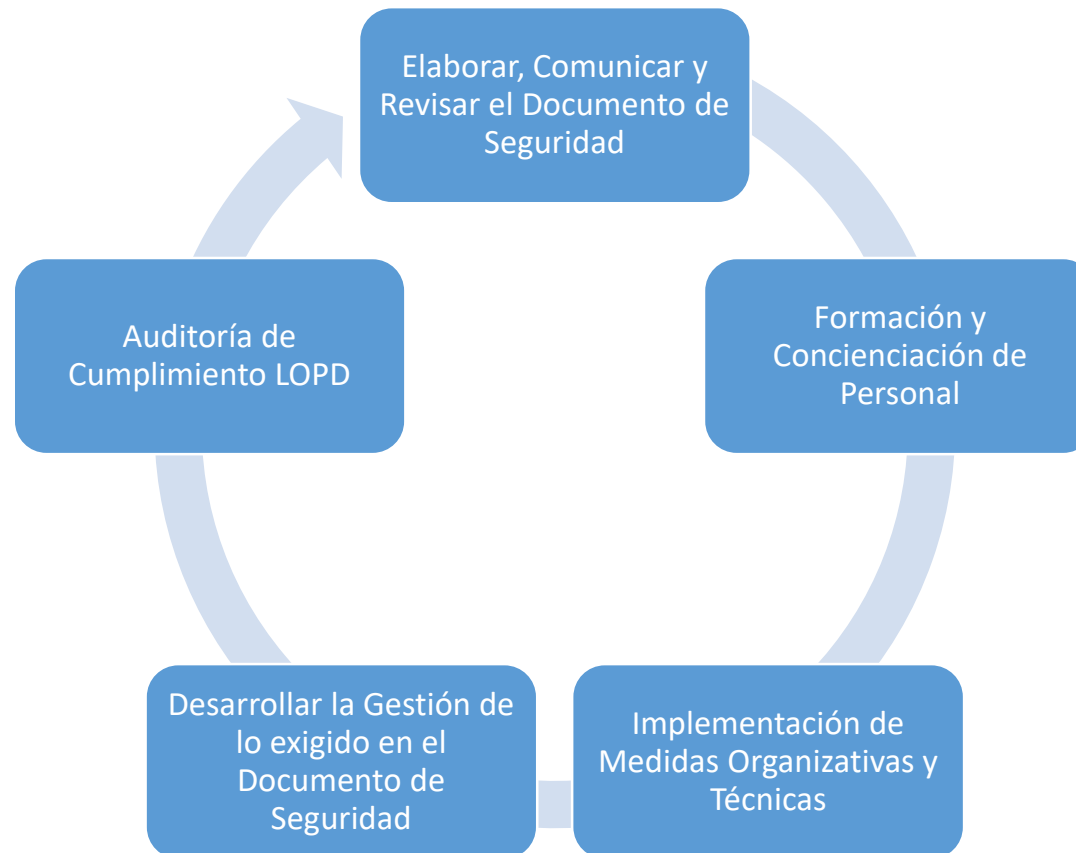
### Responsables propietarios de los ficheros

- ✓ Responsable funcional (aspectos lógicos)
- ✓ Responsable tecnológico (aspectos técnicos)

### Delegados de los responsables propietarios

# Proyecto PARSUS

## Plan de Adaptación al Reglamento de Medidas de Seguridad



# Proyecto PARGEUS

Plan de Adaptación al Reglamento General Europeo en la US

- Adaptación de los procesos del PARSUS a la nueva normativa e inclusión de nuevos procesos y procedimientos
- Se basa en las directrices emitidas en Diciembre de 2016 por el Grupo de Trabajo del Artículo 29 (GP29) de Protección de Datos Personales de la Unión Europea
- Se inician líneas de trabajo relacionadas con cambios que impone el RGPD siguiendo recomendaciones de la Agencia Española de Protección de Datos.

# Proyecto PARGEUS

## Líneas de trabajo

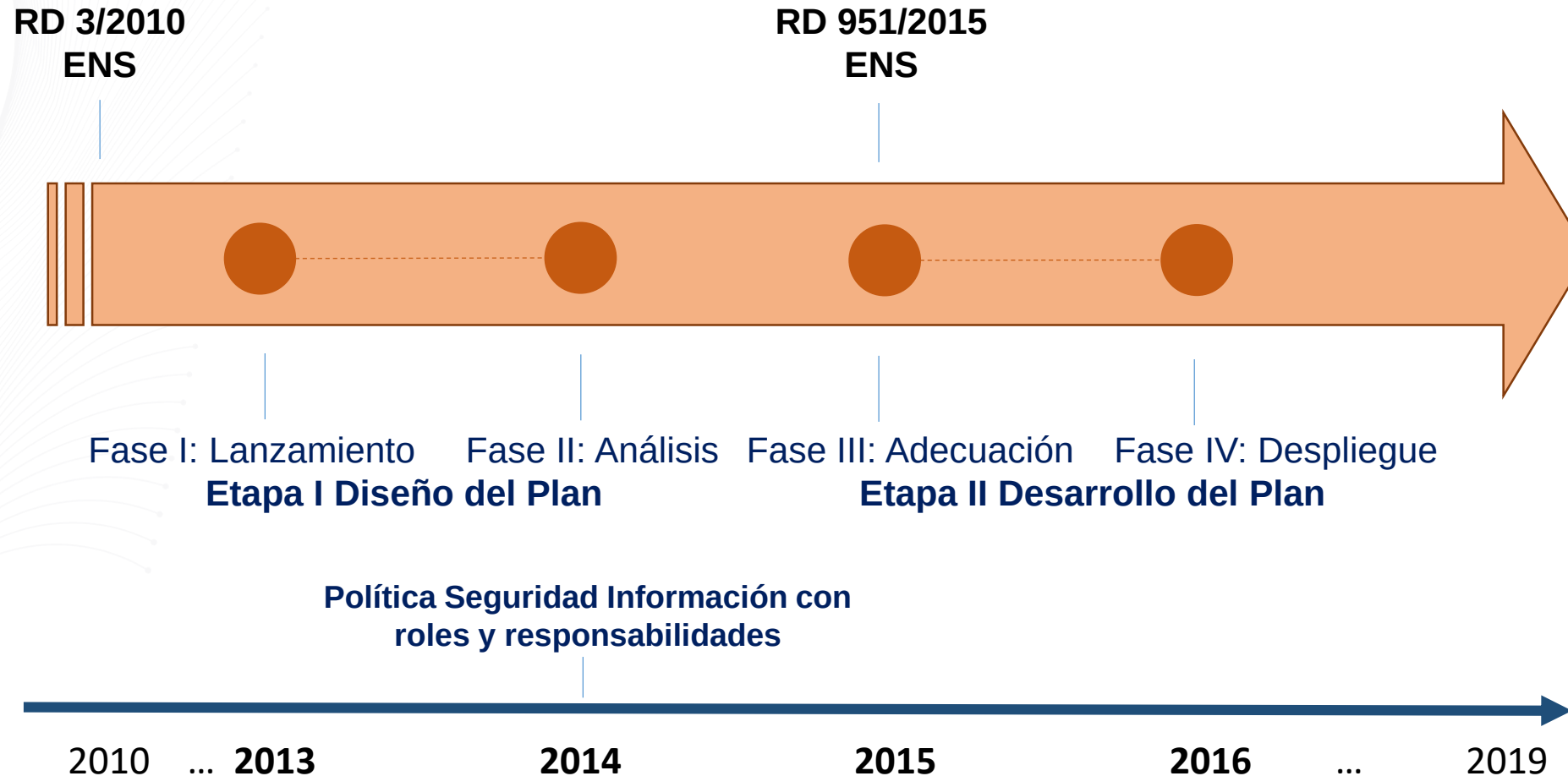
- Registro de tratamientos: se modifica procedimiento de alta de ficheros en AEPD por procedimiento de registro de tratamientos.
- Consentimiento: estudio de la licitud y adecuación de la recogida de datos.
- Transparencia: deber de informar por capas. Se elabora un documento de ayuda para los responsables delegados de tratamiento que empiezan a modificar las aplicaciones.
- Nuevos derechos: se añaden a los existentes la portabilidad, derecho al olvido, restricción del tratamiento, objeción, etc.
- Privacidad desde el diseño y por defecto: EIPD, medidas organizativas y técnicas necesarias previas a la recogida de datos y durante el tratamiento.

# Proyecto PARGEUS

## Líneas de trabajo

- Contratos de prestación de servicio: directrices para la elaboración de contratos con encargados de tratamientos y prestadores de servicios
- Revisión de los modelos de acuerdos de confidencialidad para cumplir con los requerimientos del RGPD
- Código de conducta: en tanto no exista un Código de Conducta para el sector Enseñanza al que adherirnos, nos planteamos adecuar el Documento de Seguridad al RGPD y que sirva como código tipo interno
- Notificación de brechas de seguridad: procedimiento de gestión, registro y comunicación de incidentes (ITS de Notificación al CCN-Cert y comunicación a la AEPD en 72 horas si hay DP)

# Adecuación al ENS por etapas/fases



# Roles y responsabilidades ENS hasta 2018

## COMISIÓN DE SEGURIDAD DE LA INFORMACIÓN

### N1: Especificación

Máximo responsable con competencias en materia de TI

Gerente

Secretaria General

Máximo responsable de los Servicios Jurídicos

Máximo responsable de Recursos Humanos

### N2: Supervisión

Responsable de la Seguridad de la Información

### N3: Operación

Responsables del Sistema (Directores de Área de SIC)

Subcomisión de gestión de protección de datos (desde 2016)

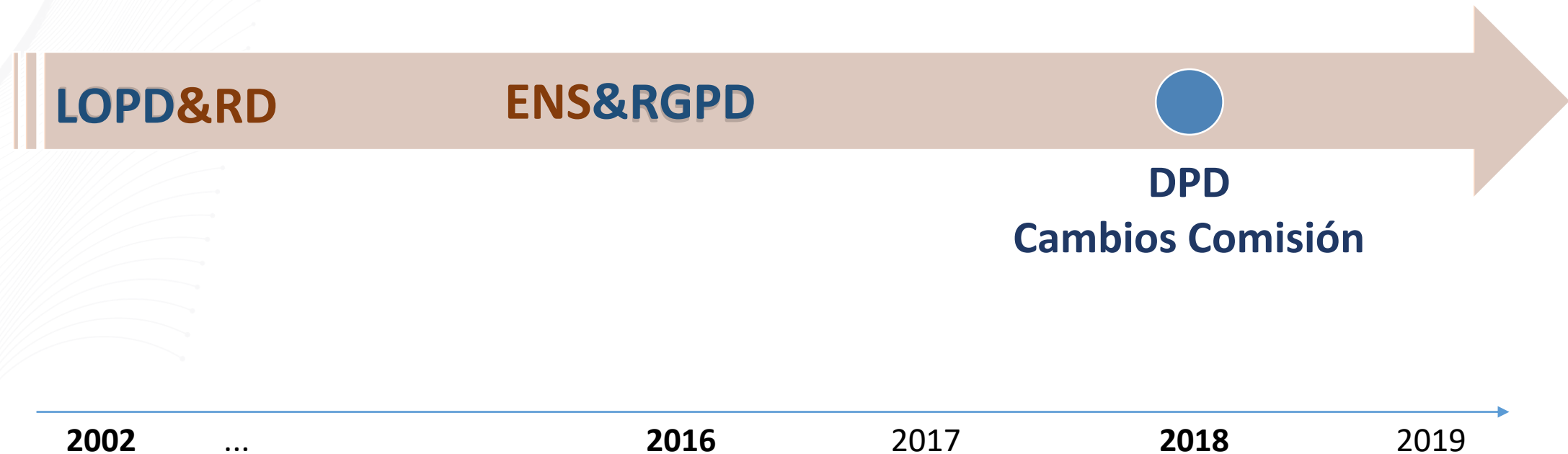
## Etapas y Fases del Proyecto de Adecuación al ENS

|                                                     |                                  |                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Etapa I – Diseño del Plan de Adecuación</b>      | <b>Fase I – Lanzamiento</b>      | <ul style="list-style-type: none"> <li>• Equipo de trabajo</li> <li>• Roles y responsabilidades</li> <li>• Alcance</li> <li>• Plan de trabajo</li> </ul>                                                                                                                                                                                                                                      |
|                                                     | <b>Fase II – Análisis</b>        | <ul style="list-style-type: none"> <li>• Diagnóstico: AR preliminar</li> <li>• Plan de adecuación</li> </ul>                                                                                                                                                                                                                                                                                  |
| <b>Etapa II – Desarrollo del Plan de Adecuación</b> | <b>Fase III – Implementación</b> | <ul style="list-style-type: none"> <li>• Activos, SI y categorización</li> <li>• Actualización del AR</li> <li>• Plan de tratamiento de riesgos</li> <li>• Elaboración de documentación</li> <li>• Auditoría externa del ENS</li> </ul>                                                                                                                                                       |
|                                                     | <b>Fase IV – Despliegue</b>      | <ul style="list-style-type: none"> <li>• SGSI basado en 27001 (PDCA)</li> <li>• AR y Plan de seguridad anual</li> <li>• Organización de la Seguridad</li> <li>• Arquitectura de Seguridad</li> <li>• Procedimiento de autorizaciones</li> <li>• Gestión y notificación de incidentes</li> <li>• Plan de Formación y concienciación</li> <li>• Implantación del plan de tratamiento</li> </ul> |

Gestión del cambio

Difusión  
Formación

# Gestión conjunta de Protección de Datos y Seguridad de SI



# Organización Seguridad Información

**Responsable de los tratamientos: Universidad de Sevilla**

## COMISIÓN DE SEGURIDAD DE LA INFORMACIÓN

### N1: Especificación

**Máximo responsable con competencias en materia de TI**  
**Responsable de la Información (Secretario General)**  
**Responsable del Servicio (Gerente)**  
**Máximo responsable de los Servicios Jurídicos**  
**Máximo responsable de Recursos Humanos**

### N2: Supervisión

**Responsable de la Seguridad de la Información**  
**Delegado de Protección de Datos**

### N3: Operación

**Responsable del Sistema**

## GRUPO DE GESTIÓN DE PROTECCIÓN DE DATOS Y SEGURIDAD DE SI

### Responsables delegados de los tratamientos para cumplimiento

**Responsable/s delegado/s (aspectos organizativos)**  
**Responsable/s tecnológico/s (aspectos tecnológicos)**  
**Gestores (seguimiento en la plataforma de gestión)**

# Gestión conjunta protección de datos y seguridad de SI

## Roles y responsabilidades

- La **Comisión de Seguridad** dirige, gestiona, coordina, establece y aprueba las actuaciones en materia de protección de datos y seguridad de SI
- **DPD y RSEG** asesoran y supervisan a los responsables delegados y tecnológicos de los tratamientos y SI
- **Grupo de gestión de protección de datos y seguridad de SI** da soporte a DPD y RSEG. Elabora documentación y hace seguimiento de la implantación.
- **Responsables delegados y tecnológicos** implantan las medidas de cumplimiento de protección de datos y de seguridad en los SI (dimensiones privacidad y ACIDT)
- **Gestores** mantienen la plataforma de gestión de proyectos.

# Gestión conjunta protección de datos y seguridad de SI

## Tareas coordinadas

- Privacidad y seguridad desde el diseño y por defecto previo a la recogida de datos y puesta en producción de los sistemas
  - Categoría de datos y sistemas acorde al RGPD y ENS
  - AR de SI corporativos y tratamientos asociados con PILAR. Estudio de necesidad de EIPD.
  - Medidas de organizativas y medidas técnicas
- Gestión y notificación de incidentes de seguridad (LUCIA)
- Plan bienal de formación y difusión único
- ¿Auditorías conjuntas? Ya veremos si esto se puede llegar a hacer

# Gestión conjunta protección de datos y seguridad de SI

Herramienta de gestión

- Plataforma [gestionlopd.us.es](https://gestionlopd.us.es): *Redmine* (sw libre gestión proyectos)
  - Los responsables delegado y tecnológico de cada tratamiento y los gestores en quienes deleguen tienen un proyecto asignado
  - Seguimiento del cumplimiento mediante actualización de registros
  - Proyectos transversales con información de interés general para todos los responsables y gestores
  - Proyectos privados para la gestión interna de PARSUS (histórico) y PARGEUS

# Dificultades

# Tamaño y dispersión de la Universidad

102

Grados ofertados > **52.000 alumnos de grado**

96

Másteres Universitarios > **5.100 Alumnos de máster**

32

Programas de doctorado > **3.100 alumnos de doctorado****8 campus, 32 centros**> **12.000 IPs públicas****133 departamentos**> **200.000 cuentas de usuario (UVUS)****551 grupos de investigación**> **100.000 cuentas de correo electrónico****4.185 PDI y 2.672 PAS**> **790 listas de distribución****160 servicios TI corporativos**> **2.000 alojamientos de páginas webs**

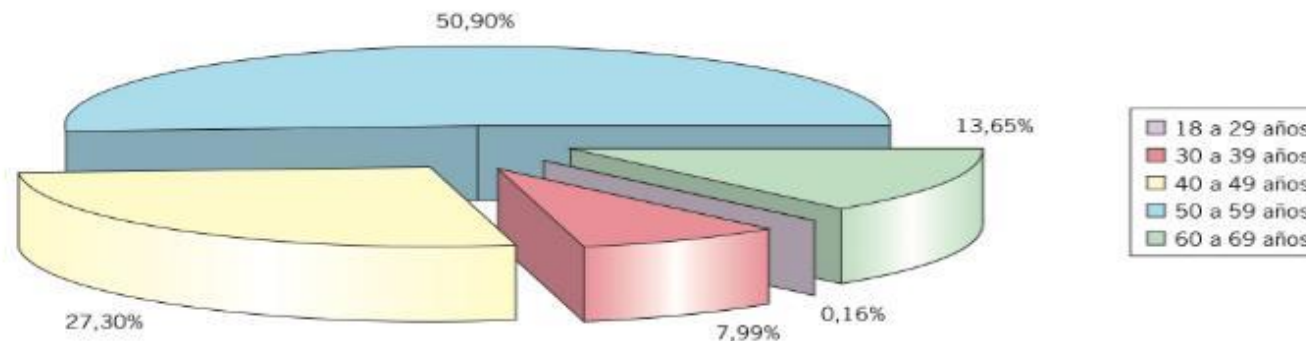
# Organización

- Es necesaria una estructura que permita:
  - Canalizar cualquier iniciativa, proyecto, servicio que trate datos personales y/o conlleve uso de tecnologías para asegurar la visibilidad completa de tratamientos y SI
  - Aplicar privacidad y seguridad desde el diseño y por defecto antes de la puesta en producción de los servicios
  - Vigilar la protección de datos y la seguridad de la información
  - Realizar auditorías internas
- Una estructura cuyo alcance sea toda la Universidad

## Factores económicos y humanos

- La Seguridad es cara
- La concienciación y la formación es un proceso lento
- El entendimiento entre técnicos y funcionales es difícil a veces
- La edad media del personal de la Universidad es alta

Rangos de edades del PAS funcionario de la Universidad de Sevilla



Fuente: Anuario estadístico 2018-2019

# Facilitadores en la US

# Estrategia, organización, tecnología y formación continua

- Equipo directivo de **personas muy implicadas** que creyeron y se esforzaron para que la protección de datos y la seguridad de SI fuera una realidad en la Universidad
- Integración de **personas del ámbito jurídico y tecnológico** en el equipo
- Organización adecuada de **roles y responsabilidades**
- Definición de **procesos y procedimientos**
- Apuesta por la **automatización** de la gestión de la seguridad
- **Observatorio** para adaptación a los cambios legislativos
- Actividades de **concienciación y formación** para TODOS

**Gracias por la atención**

**COMUNIDAD Y CONFIANZA,**  
BASES DE NUESTRA CIBERSEGURIDAD

**#XIIIJORNADASCCNCERT**

**OC.CCN.CNI.ES**

**WWW.CCN.CNI.ES**

**WWW.CCN-CERT.CNI.ES**

**XIII  
JORNADAS  
STIC  
CCN-CERT**

**ccn-cert**  
centro criptológico nacional