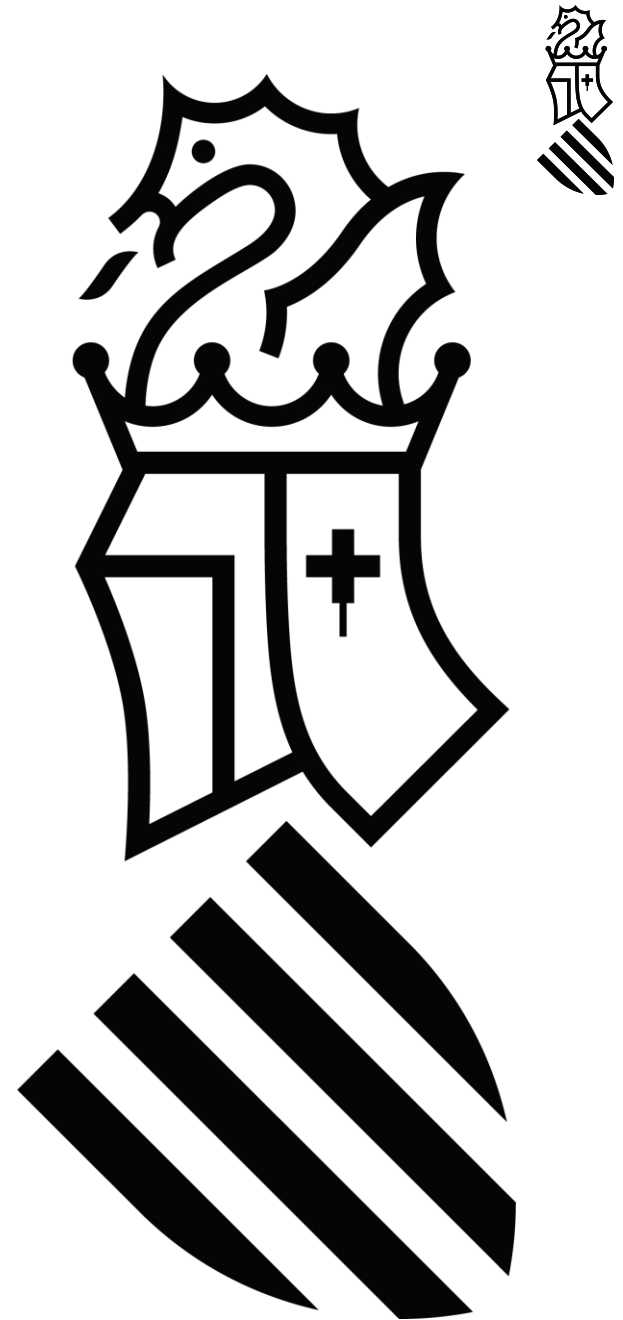
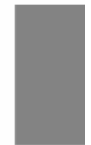


**PLAN  
ESTRATÉGICO DE  
CIBERSEGURIDAD  
DE LA  
CONSELLERIA DE  
SANIDAD  
(2025-2027)**



# ¿Qué vamos a hacer?

Ejes de actuación e iniciativas de la ESD-CV

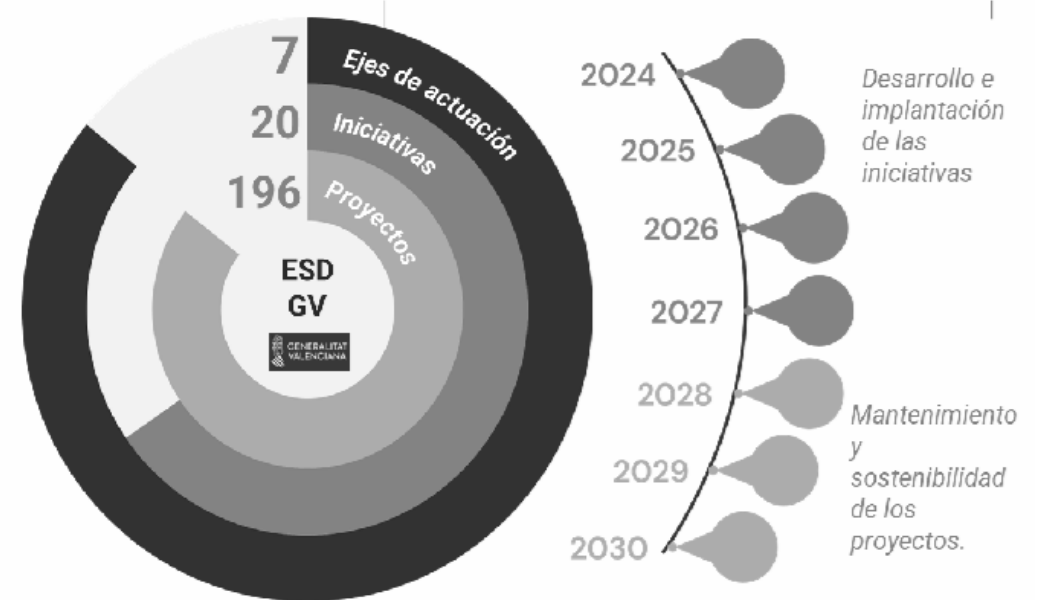


## Ejes de actuación

7 Ejes de actuación



## Marco temporal y proyectos



# Índice

- 01 Introducción
- 02 Modelo de red RedHos 2.0 y RedPrim 1.0
- 03 Seguridad desde el desarrollo
- 04 Endpoint seguro
- 05 Seguridad en el ciclo de vida de los sistemas operativos
- 06 Gestión de alertas de seguridad (SOC)
- 07 Proceso integral de copias de seguridad
- 08 Gestión de identidades
- 09 Capacitación del personal
- 10 Modelo de gobierno



# Introducción

## ¿Por qué un plan estratégico de ciberseguridad?



### Situación actual

La Conselleria de Sanidad impulsa la transformación digital garantizando la **seguridad de los sistemas** y datos que sostienen los servicios públicos.

**La ciberseguridad es un eje estratégico** dentro de la Estrategia de Salud Digital, con un plan desarrollado por GT7-Seguridad basado en el **Esquema Nacional de Seguridad (ENS)** y **centrado en 8 áreas clave para reforzar la resiliencia digital.**

### Esquema Nacional de Seguridad (ENS)



El Capítulo 2 del **Esquema Nacional de Seguridad (ENS)** proporciona los **principios básicos de seguridad** que todo sistema de información debe cumplir para **reducir los riesgos, proteger la información** pública y **fortalecer la confianza** en el servicio público.

Tal y como indica el “Artículo 5. Principios básicos del Esquema Nacional de Seguridad”, el objeto último de la seguridad de la información es garantizar que una **organización** podrá cumplir sus **objetivos**, desarrollar sus **funciones** y ejercer sus **competencias** utilizando sistemas de información.

# Introducción

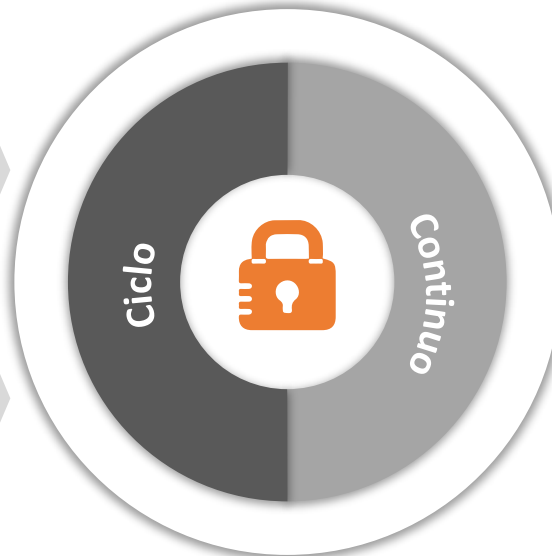
## Líneas de acción

RedHos 2.0 y RedPrim 1.0

Seguridad desde el desarrollo

Seguridad en el ciclo de vida del Sistema Operativo

Endpoint seguro



Gestión de alertas de seguridad - SOC

Proceso integral de copias de seguridad

Gestión de Identidades

Divulgación, formación y capacitación

# Modelo de red RedHos 2.0 y RedPrim 1.0

Una de las piezas clave de la **seguridad global** es la **seguridad en la red**. RedHos y RedPrim establecen un **modelo estandarizado de arquitectura de red** diseñado desde el punto de vista de la seguridad.

El objetivo es **estandarizar la arquitectura de red** y los controles de seguridad en todos los centros con CPD propio. Este modelo incluye una **segmentación estándar de redes**, **políticas de firewall** homogéneas y un **sistema de prevención de intrusos unificado**.

Se implementará una **segmentación** diferenciada en las redes de acceso y CPD, **políticas** de firewall con **FortiGate**, control de acceso a la red (NAC) con **FortiNAC**, y sistemas de detección de intrusiones (**IPS**) tanto para IT como para IoMT.

## Segmentación de redes

Diferenciación en redes de acceso y CPD basada en **servicios prestados**.

1

## Control de acceso a la red (NAC)

Refuerzo de configuraciones de FortiNAC para una mayor seguridad de accesos y automatización de procesos.

2

3

4

## Políticas de firewall

Implementación de reglas y políticas en FortiGate para la protección y control del tráfico de red.

## Detección de intrusiones

IPS para IT con FortiGate y soluciones específicas para IoMT.

# Seguridad desde el desarrollo (DevSecOps)

El objetivo es integrar controles de seguridad en todas las etapas del desarrollo de software, desde el diseño hasta el despliegue. Esto minimizará vulnerabilidades y garantizará que las aplicaciones cumplan con los principios del ENS desde su concepción.



Se implementarán evaluaciones de riesgos en la fase de diseño, pruebas de seguridad durante el desarrollo utilizando herramientas como SonarQube y Veracode, gestión de dependencias con Snyk, y automatización en CI/CD con Jenkins o GitLab CI

## Evaluación de riesgos

Análisis de amenazas en fase de diseño.

## Pruebas de seguridad

Evaluación del software para identificar y corregir vulnerabilidades.

## Gestión de dependencias

Control y supervisión de las bibliotecas y componentes de terceros.

## Automatización CI/CD

Automatización de las fases de integración continua (CI) y entrega continua (CD) en el desarrollo de software.

# Seguridad den el ciclo de vida de los sistemas operativos

El objetivo es mantener la seguridad y soporte de los sistemas operativos durante todo su ciclo de vida, asegurando su actualización y salvaguardando las dependencias de las aplicaciones .



Se implementará un **parqueo y actualización** automatizados, **bastionado** de sistemas siguiendo **guías CCN, inventario** y gestión de obsolescencia con Lansweeper o SCCM, y monitorización continua.

1

## Sistema operativo actualizado

Se mantendrá el sistema operativo actualizado y se implementarán soluciones de gestión de actualizaciones aplicables.

2

## Bastionado de sistemas

Se implementarán configuraciones de hardening según las guías CCN publicada.

3

## Inventario y obsolescencia

Se implementarán procedimientos planificados de migración tecnológica.

4

## Monitorización continua

Se mantendrá una monitorización continua y su integración con los sistemas de seguridad.



# Endpoint seguro

El objetivo es asegurar que todos los dispositivos de punto final estén protegidos frente a amenazas y ataques, alineándose con los requisitos del ENS.

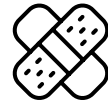


Se han implementado **soluciones avanzadas** de **antivirus** y **EDR** como **Cytopic**, complementadas con microCLAUDIA. Se establecerán **políticas** de actualización de **parches** de seguridad, bloqueo de **sesión**, e inicio de sesión seguro con **dobles** factor de autenticación.



## Antivirus y EDR

Implementación de Cytopic y microCLAUDIA.



## Actualización de parches

Política de actualización constante.



## Bloqueo de sesión

Prevención de accesos no autorizados.



## Inicio de sesión seguro

Doble factor de autenticación.



# Endpoint

# Gestión de alertas de seguridad

El objetivo es identificar y responder de manera rápida y eficiente ante amenazas de seguridad para minimizar el impacto en la organización. Para este punto estratégico se creará un SOC sanitario que gestionará los eventos de seguridad y realizarán simulacros periódicos de respuesta a incidentes.



Se implementará un SIEM (Security Information and Event Management) para centralizar eventos de seguridad y correlacionar alertas. Además, se utilizarán herramientas para automatizar respuestas ante incidentes.

## SIEM

Integración y centralización de eventos de red, sistemas y aplicaciones.

1

## Auditorías

Realización periódica de auditorías de hacking ético (pentest) a todos los niveles y servicios.

2

3

4

## SOAR

Respuestas automatizadas y playbooks

## Simulacros

Realización de ejercicios programados de ciberseguridad.



# Proceso integral de copias de seguridad

El objetivo es garantizar la **disponibilidad y recuperación de la información crítica** en caso de incidentes, alineado con la disponibilidad y confidencialidad del ENS.



Se aplicará **cifrado a las copias de seguridad almacenadas**, se implementará **almacenamiento redundante** con replicación en ubicaciones físicas **separadas**, y se realizarán **pruebas** periódicas de restauración para asegurar la **eficacia** de los procesos de **backup**.

## Soluciones de backup

Revisión de los procedimientos para su adaptación a los requisitos ENS.

## Protección antiransomware

Revisión de los procedimientos para su adaptación a los requisitos ENS.

## Pruebas de restauración

Simulaciones periódicas para la optimización y aseguramiento de la eficacia en la restauración de los sistemas respaldados.

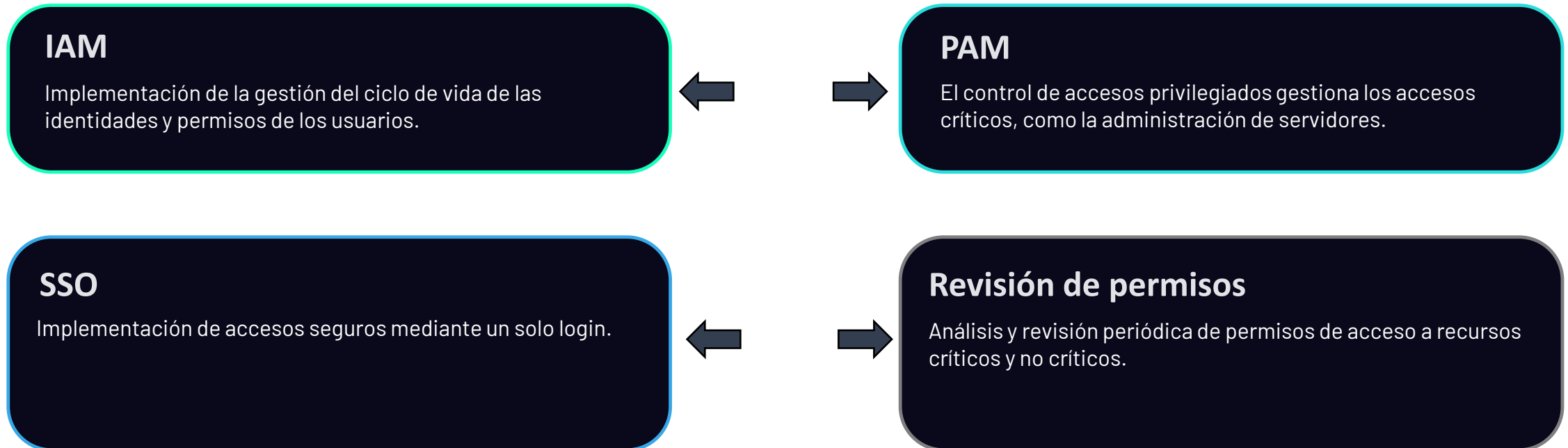


# Gestión de identidades **Identidad Digital del Empleado**

El **objetivo** es proporcionar un **control seguro de accesos y permisos** en función del rol y responsabilidad de cada usuario. Se implementará un sistema de **IAM (Identity Access Management)** utilizando herramientas como NetIQ y OAM de Oracle para garantizar que solo las **personas autorizadas** tengan acceso a los recursos necesarios.



Además, se utilizará PAM (Privileged Access Management) con Wallix para controlar accesos privilegiados, se implementará Single Sign-On (SSO) para facilitar accesos y reducir riesgos, y se realizarán revisiones periódicas de permisos.



# Capacitación del personal

El **objetivo** es fortalecer la **cultura de seguridad en la organización**, aumentando la conciencia y las habilidades de los empleados para prevenir, detectar y responder ante amenazas.



Se realizarán simulaciones de phishing y campañas de concienciación en colaboración con el CSIRT-CV, y se distribuirán boletines y campañas internas para reforzar las buenas prácticas.



## Formación continua

Se realizarán campañas de formación para todos los DDSS y SSCC: formaciones presenciales y online, píldoras formativas y cuestionarios.



## Simulación de phishing

Uso de herramientas como PhishMe para la evaluación y mejora de respuesta de los trabajadores sanitarios.



## Portal OSI

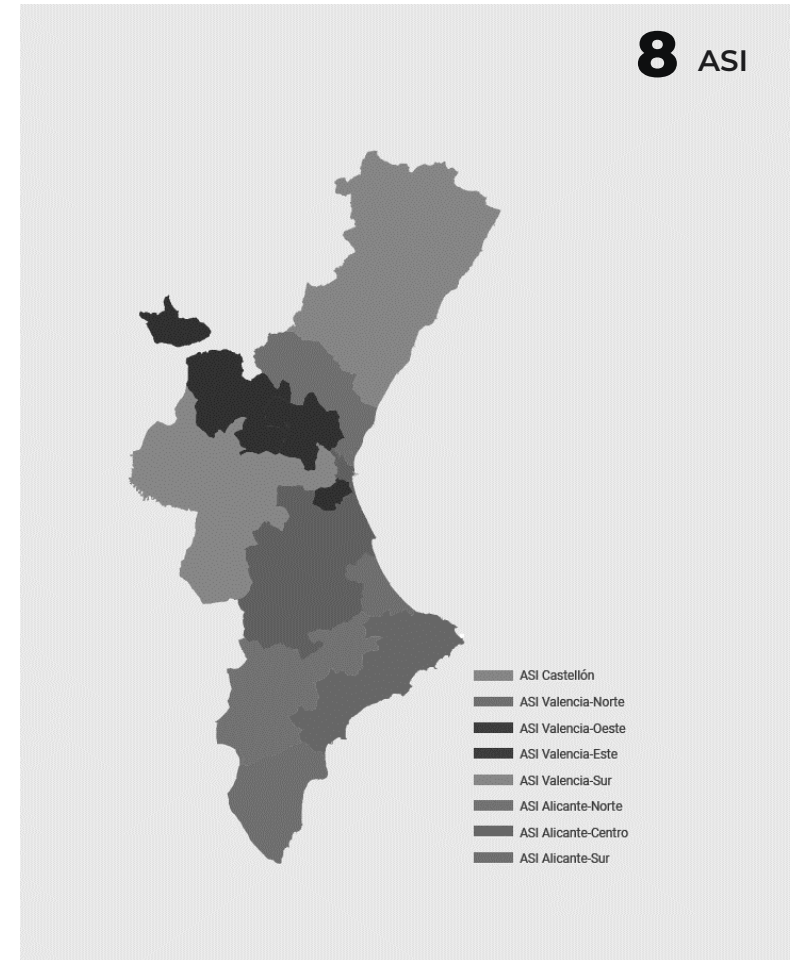
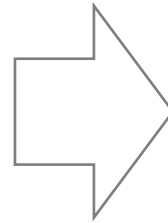
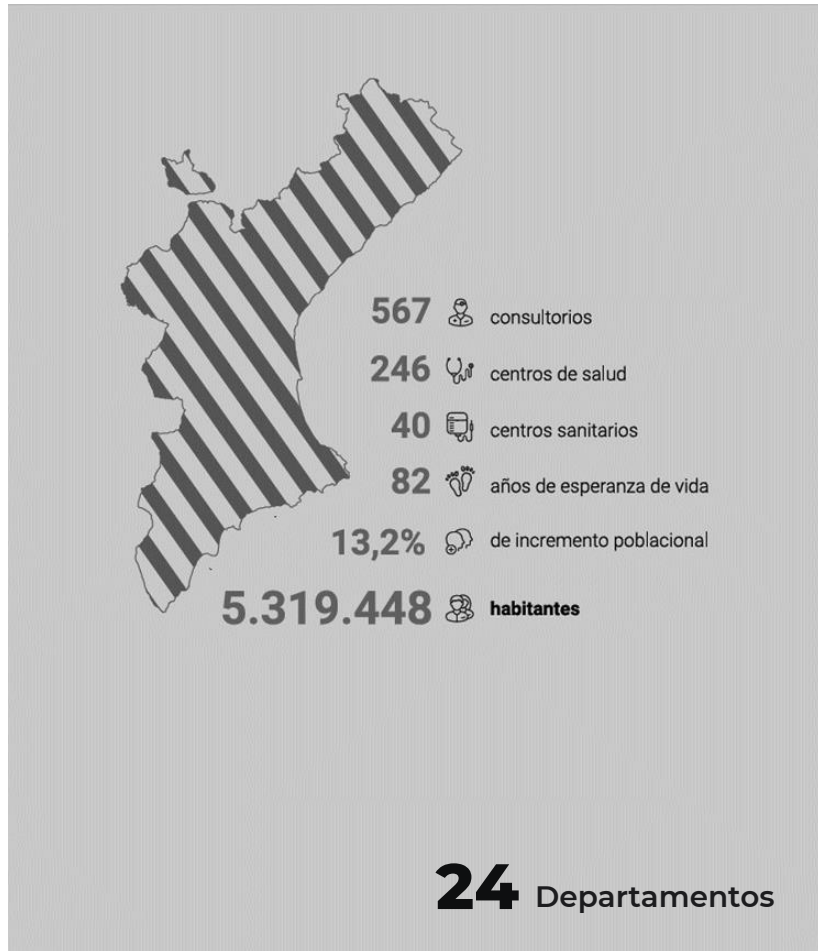
Se impulsará un portal de la OSI para la divulgación de la ciberseguridad y la seguridad de la información.

**¿Cómo lo vamos a hacer ?**  
Modelo de Gobernanza



# ¿Cómo lo vamos a hacer?

Gobierno federado de las TIC



# Modelo de gobierno

El plan de ciberseguridad engloba un conjunto de proyectos que tienen como objetivo la protección de los **activos críticos**, la **confidencialidad e integridad de la información**, el aseguramiento de la **disponibilidad** de los sistemas, el control y verificación de las **identidades** de usuarios y sistemas, el control de **acceso** a los recursos y servicios, la gestión, el registro, la **auditoría** y monitorización de las actividades de usuarios y el cumplimiento normativo.

	Responsable del plan global										GT- Seguridad	
	Coordinadores de Seguridad de las ASIs											
	Proyectos del plan de Ciberseguridad											
Responsables	SSCC ASI		SSCC ASI		SSCC ASI		SSCC ASI		SSCC ASI			SSCC ASI
	Modelo de red y RedPrim 2.0 y RedPrim 1.0	Seguridad desde el desarrollo	Seguridad en el ciclo de vida de los SO	Endpoint seguro	Gestión de alertas de seguridad	Proceso integral de copias de seguridad	Gestión de identidades	Divulgación, formación y capacitación del personal				
Servicios de Informática Departamental (SID)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Centro de Gestión de la Red Arterias (CGRA)	✓				✓							✓
Gestión de Sistemas del Centro de Informática (GSCI)		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Gestión de Sistemas de Infraestructuras Distribuidas (GSID)			✓		✓		✓	✓	✓	✓	✓	✓
Gestión de la Entrega y Evaluación del Software (GEES)		✓										✓
Gestión del Puesto de Trabajo (GPT)			✓	✓	✓			✓	✓	✓	✓	✓
Coordinadores técnicos de aplicaciones			✓					✓				✓
Empresas desarrolladoras SW o implantadoras			✓									✓



**Gracias !**



# ¿Cómo lo vamos a hacer?

Gobierno federado de las TIC



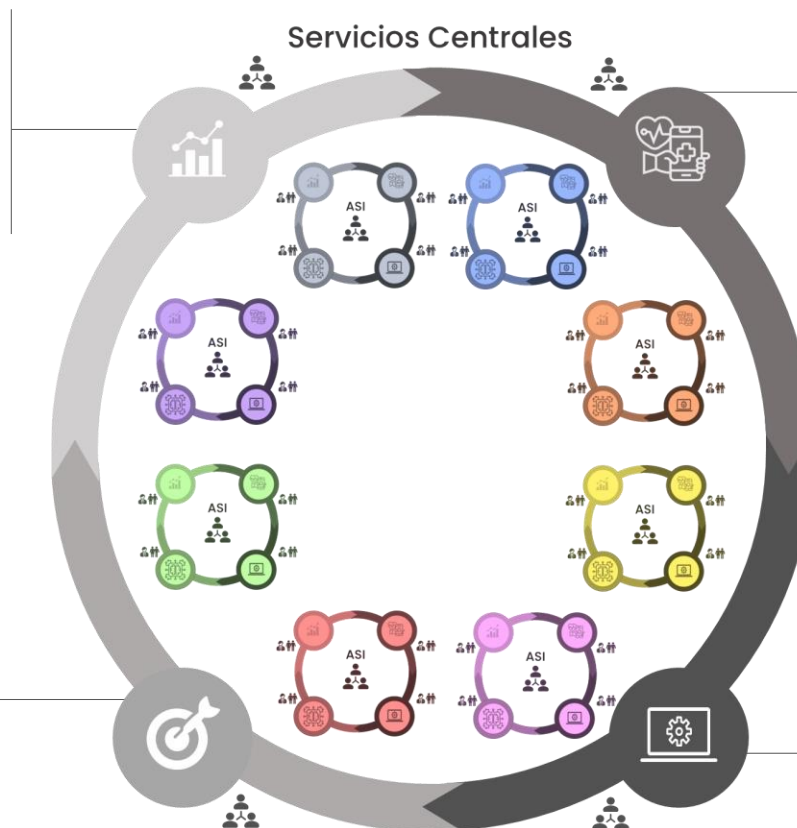
## Oficina del Dato

Su función es la centralización de los trabajos relacionados con ámbitos asistenciales de datos.

La Oficina del Dato actuará como el "cerebro" de la gestión de la información clínica, asegurando que los datos sean de alta calidad, estén estandarizados y sean accesibles para todos los usuarios autorizados, facilitando así la toma de decisiones clínicas, la gestión sanitaria y la investigación.

## Oficina de la IA

Su función principal será la de impulsar la adopción de la IA en el sistema sanitario, fomentar la innovación y la investigación en IA aplicada a la salud, asesorar a los profesionales y a las instituciones en la implementación de soluciones de IA, y velar por el uso ético y responsable de la IA en el ámbito sanitario.



## Oficina para la Transformación Digital

Su función principal es la de realizar todos los trabajos relacionados con catalogación de procesos actuales, normalización, homogeneización de procesos y diseño de procesos adecuándolos a las posibilidades de la tecnología desplegada en la organización. Los procesos contemplarán soluciones tecnológicas que permitan automatizar de forma progresiva procesos y tareas complejas.

## Oficina para el Gobierno de las Aplicaciones

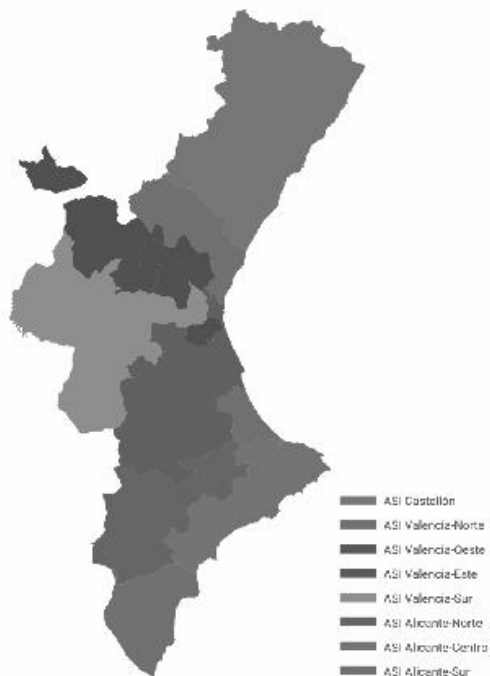
Su función es poner gobierno al contenido de las aplicaciones y futuros desarrollos que de hacerse han de serlo en el contexto de versión única vamos para todos.

Se encargará de la evaluación de los sistemas distribuidos y heterogéneos existentes, con el fin de detectar convergencias y sinergias entre ellos. Se diseñarán y supervisarán las políticas de convergencia de aplicaciones y sistemas con el objetivo de maximizar los recursos, desarrollar procesos más eficientes y optimizar su gobernanza.

# ¿Cómo lo vamos a hacer?

Gobierno federado de las TIC

## Agrupaciones Sanitarias Interdepartamentales



## Gobierno TI federado



Eficiencia en la gestión TIC



Sinergias entre ASI y centros en la Conselleria



Impulso de la especialización técnica

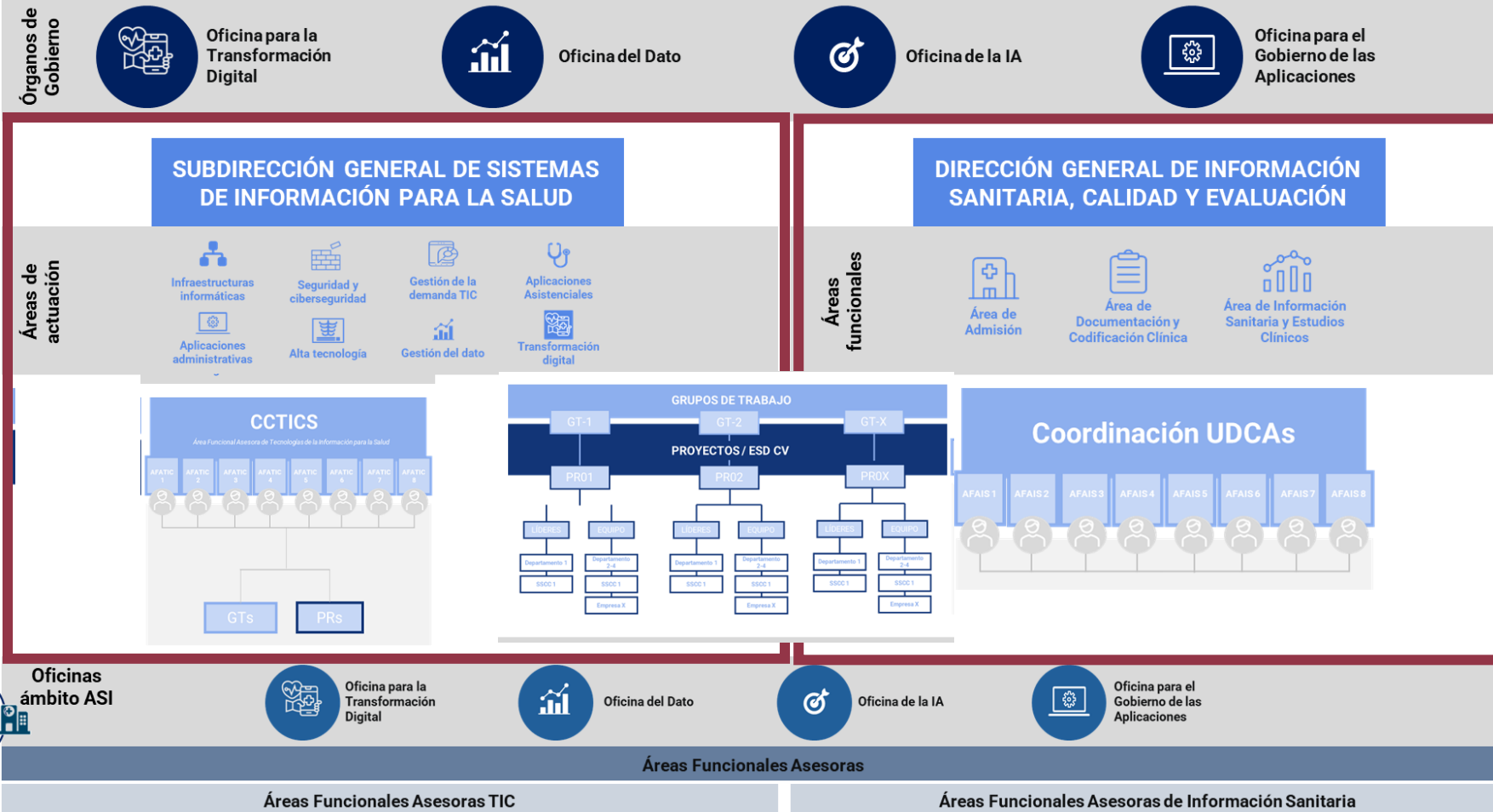


Medición de resultados

# Modelo organizativo

Liderazgo, gobernanza estratégica, coordinación global, definición políticas y evaluación resultados

## PLANIFICACIÓN, INFORMACIÓN Y TRANSFORMACIÓN DIGITAL



## Propósito del gobierno federado

- ✓ **Visión global** y foco en una única dirección
- ✓ **Trabajar juntos** de manera **coordinada** y sentimiento de pertenencia
- ✓ **Maximizar** el conocimiento técnico y operativo de cada ASI e identificar carencias para trabajar en ellas
- ✓ **Optimizar** la toma de **decisiones** y la implementación de soluciones
- ✓ **Estandarización** de procesos y tecnologías
- ✓ **Desarrollo** de competencias **“especialización”**

