

# Agencia de Transformación Digital de Castilla-La Mancha.

## Dirección General de Salud Digital.

Área de Infraestructuras Tecnológicas.  
Unidad de Ciberseguridad.

## Estrategia Ciberseguridad DGSD



# Agencia de Transformación Digital de Castilla-La Mancha.

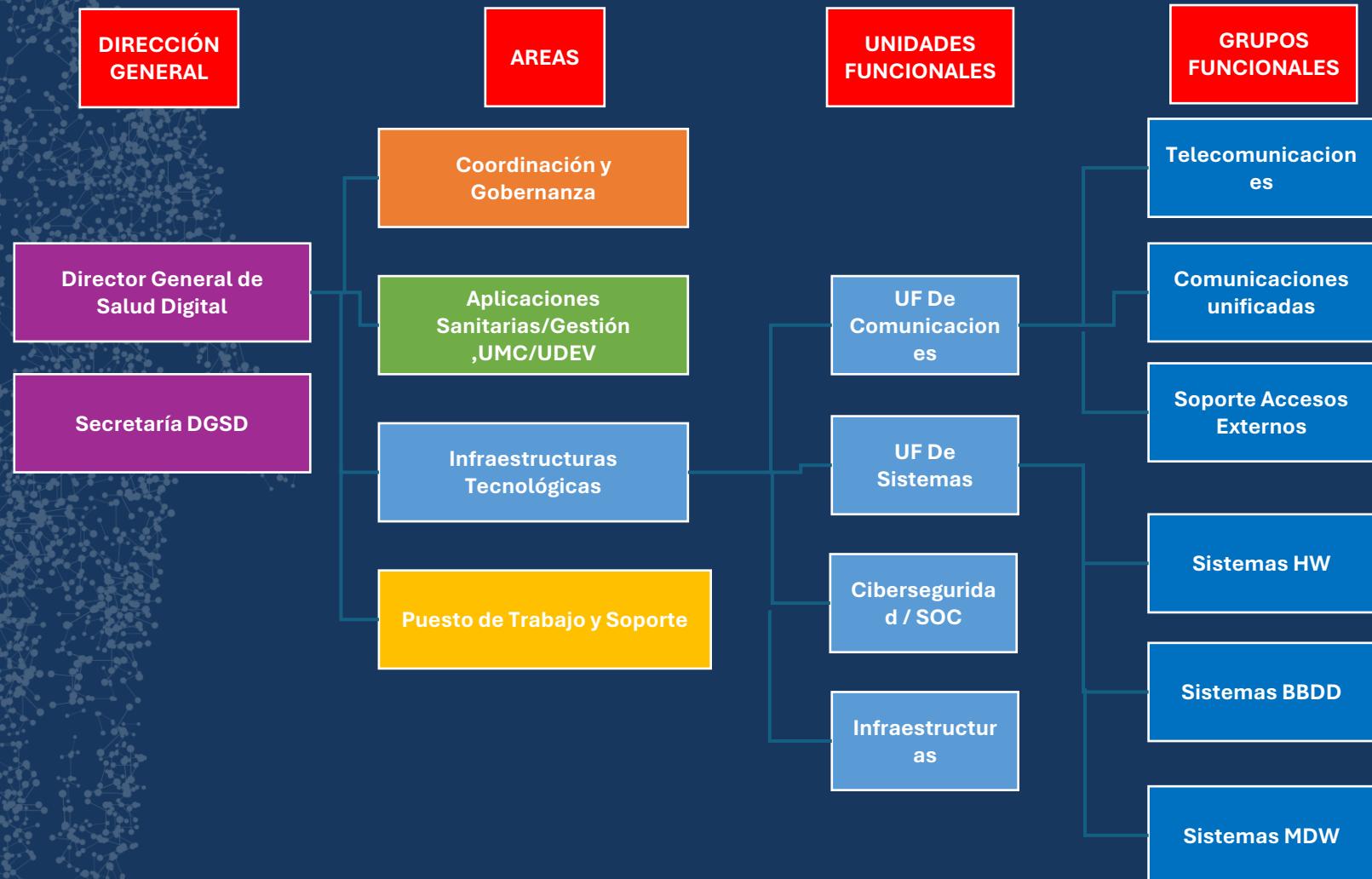
## Dirección General de Salud Digital.

Área de Infraestructuras Tecnológicas.

Unidad de Ciberseguridad.

## Contexto de la unidad de Ciberseguridad de la DGSD

# Dirección General de Salud Digital.



# Área de Infraestructuras Tecnológicas

Coordinador

Unidades  
Funcionales

Grupos  
Funcionales

Telecomunicaciones

Coms Unificadas

Telecommunicacion  
es

Accesos Externos

Sistemas

Sistemas HW

Sistemas BBDD

Sistemas  
Middleware

Cibersegurida  
d

Ingeniería e  
instalaciones.

+1,5K Sedes

38k profesionales

24 x7x365

4 CPDs

Corporativos

- 13 Gerencias de Área Integrada
- 1 Gerencia de Atención Especializada
- 1 Gerencia de Atención Primaria
- 2 Gerencias Generalistas
- 1 Hospital Nacional de Parapléjicos
- IDISCAM
- Servicios Centrales del SESCAM
- 20 Hospitales
- 12 CEDT
- 204 Centros de Salud
- 183 PACS
- 1.144 Consultorios Locales
- 7 SS.PP. Coord. e Inspección



equipos de LAN

controladoras Wi-Fi

Firewalls de Hospitales

Firewalls de CPD.

Firewalls de acceso a internet.

servers físicos

Cabinas de Almacenamiento

SIEM

Máquina virtuales.

equipos de agregación

SAIS Gestionados

VDI

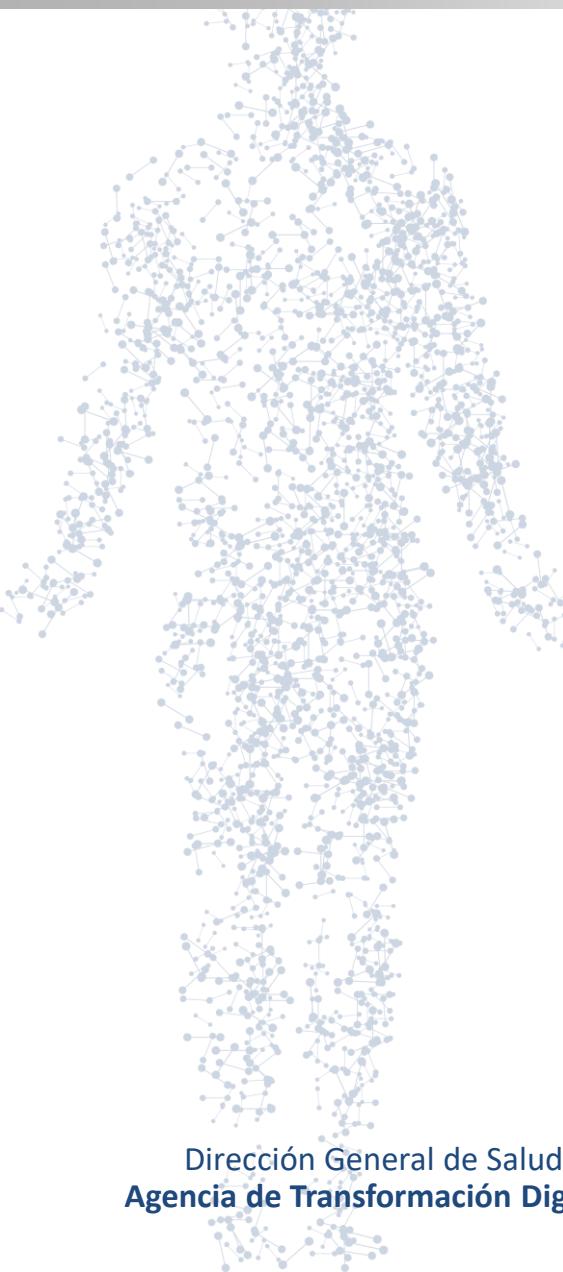
equipos Proxy.

Dispositivos IoT/IoMT

Puntos de Acceso Wi-Fi/1600 en servicio



# Estrategia de la unidad de Ciberseguridad de la DGSD.



## Proteger entorno Sanitari o.

*Proteger y asegurar la infraestructura de información sanitaria y administrativa de la DGSD mediante la implementación de medidas de ciberseguridad que garanticen la prestación asistencial, protección de los datos sanitarios, la seguridad en la interoperabilidad de los sistemas de información y aumentar el nivel de madurez en ciberseguridad.*

# Estrategia

La estrategia de ciberseguridad para el Sescam se basa principalmente en 3 pilares fundamentales



**PROCESOS**



**PERSONAS**



**TECNOLOGÍA**

# Estrategia de la unidad de Ciberseguridad de la DGSD.

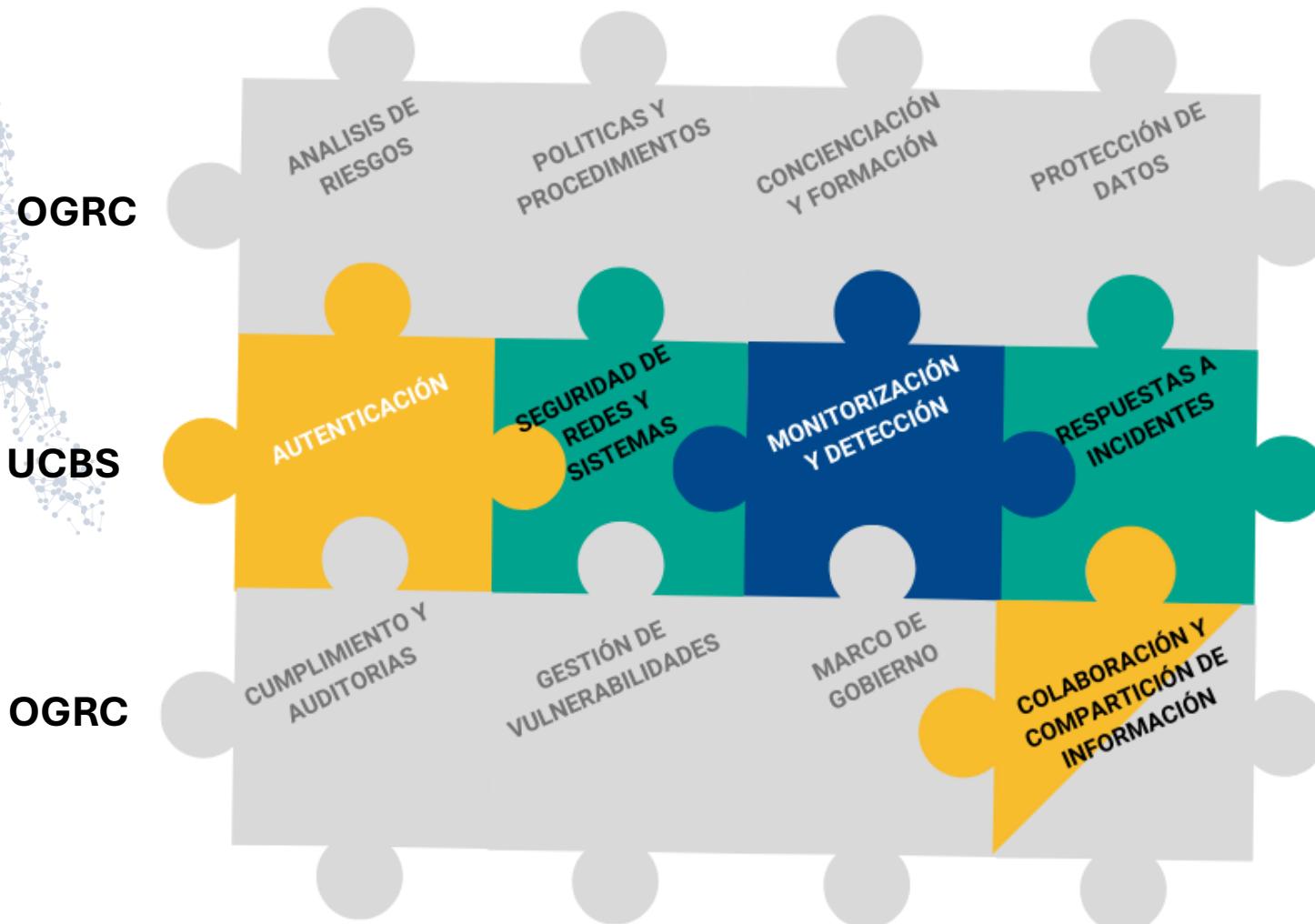
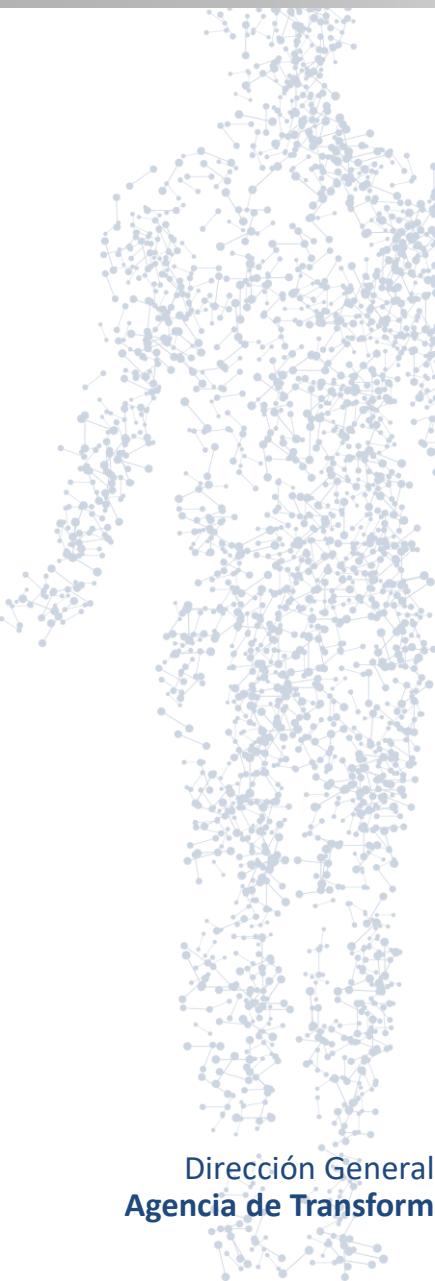
Aspectos identificados antes de crear la Estrategia de Ciberseguridad:

- Carencias en Formación y Concienciación de Ciberseguridad.
- Ausencia de un Sistema de Control de Identidades unificado.
- Infraestructura TI algo obsoleta.
- Procesos de comunicación y Gobernanza difusos.

# Ejes Estratégicos desarrollados



# Principios de la estrategia



# Líneas de acción y proyectos

## Línea de Acción

Gestión de crisis en entorno sanitario.

## Seguridad en servicios Cloud

Protección del dato Sanitario

## Cumplimiento del ENS en salud

## SOC centralizado para el ámbito sanitario

## Formación y capacitación en ciberseguridad

Seguridad en la cadena de suministro

## Seguridad en IoMT / IoT

Mejorar la seguridad en la red corporativa de salud.

## Proyecto

**CiberCrisis:** Avanzar en materia de gestión de crisis y desarrollar indicadores.

**Cloud Security:** Securización en servicios cloud, IA y correo electrónico.

**Sanidata Protect:** Establecer medidas de ciberseguridad para proteger el dato sanitario.

**ENS-Salud:** Diagnóstico y adecuación normativa.

**SOC-SALUD:** Centro de operaciones de seguridad regional de la DGSD.

**CiberEduca:** Capacitar al personal de la DGSD en materia de ciberseguridad.

**SupplySecure:** Reforzar medidas de ciberseguridad en los proveedores externos.

**IoMT Shield:** Gestión y protección de dispositivos conectados IoT/IoMT.

**InfraCiber:** Incrementar la seguridad en la red corporativa de la DGSD y reducir la superficie de ataque.



# Servicios prestados

## Proteger

- Servicios de seguridad perimetral
- Servicios de navegación Segura
- Servicio de correo seguro
- Acceso remoto seguro
- Protección Endpoints

## Detectar

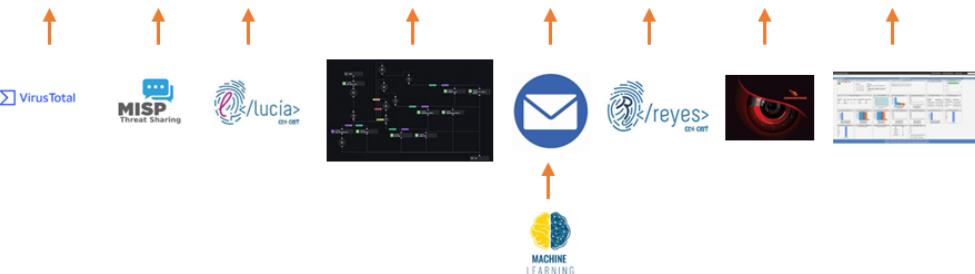
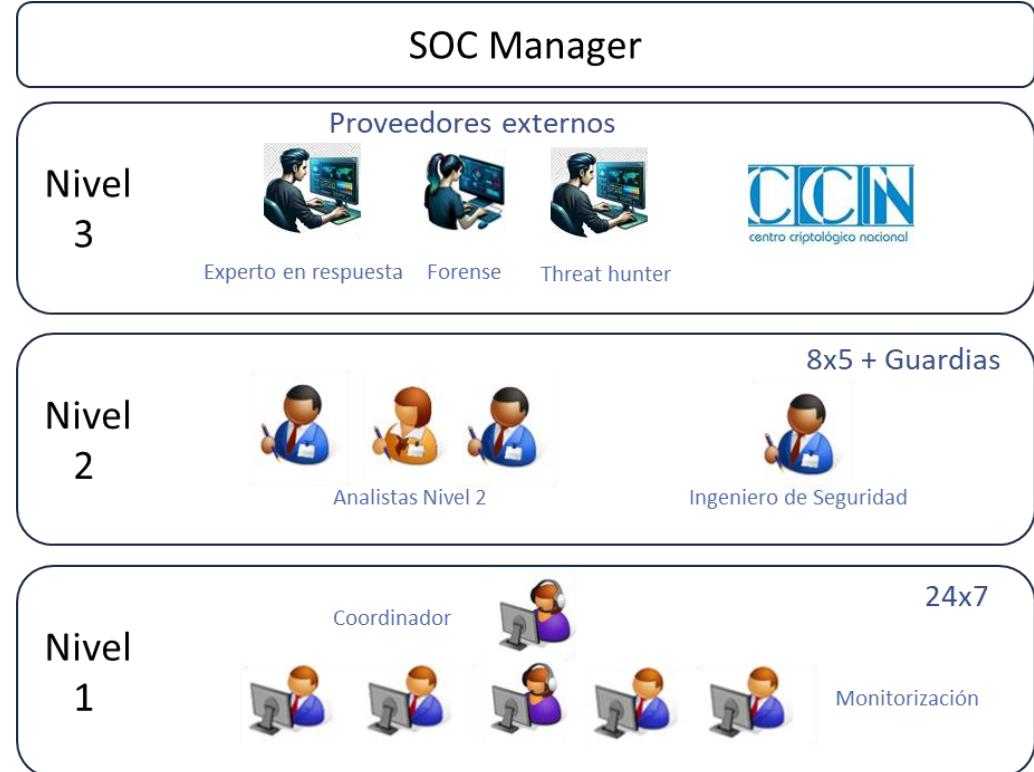
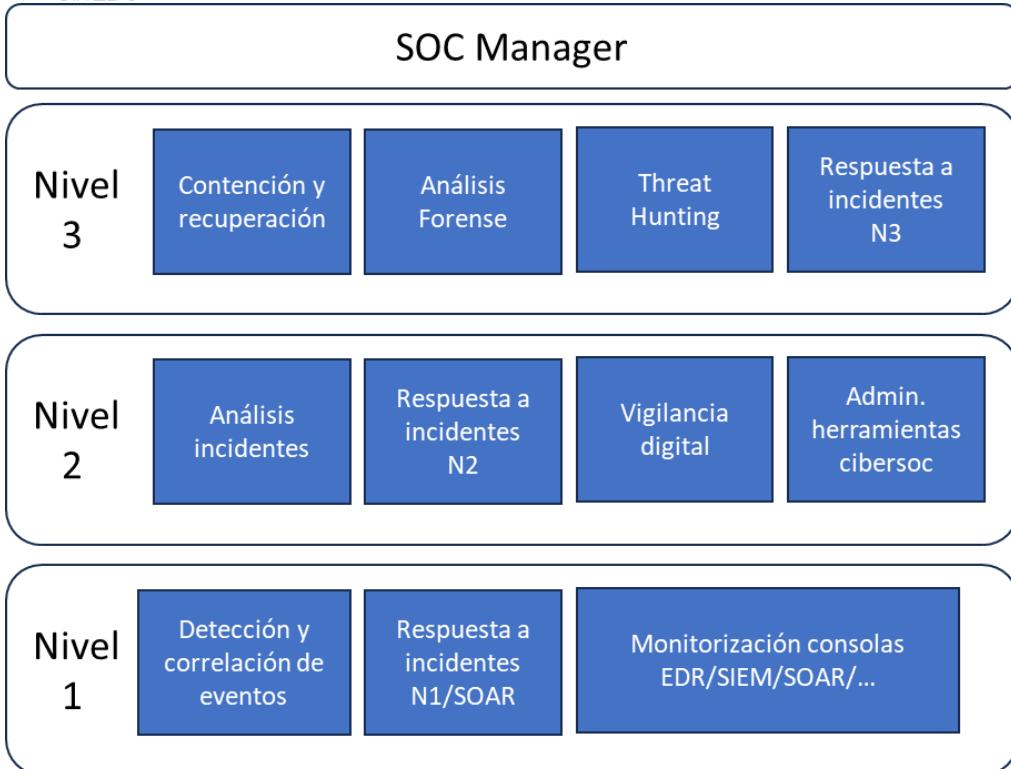
- Distribución de herramientas de protección. EDR, Microclaudia...
- Monitorización de eventos de seguridad
- Detección de incidentes.
- Threat Hunting proactivo.
- Vigilancia de la superficie de ataque.

## Responder

- Gestión y respuesta ante incidentes de seguridad.
- Notificación de incidentes de seguridad.
- Análisis forense.

# Proyectos de interés

# SOC y DFIR



# Solución IoT/IoMT



162,327

Total Images Scanned

4,344

Total Case Studies



## Imaging Scan Analysis



17371

Head & Neck

289

Upper Extremity

42673

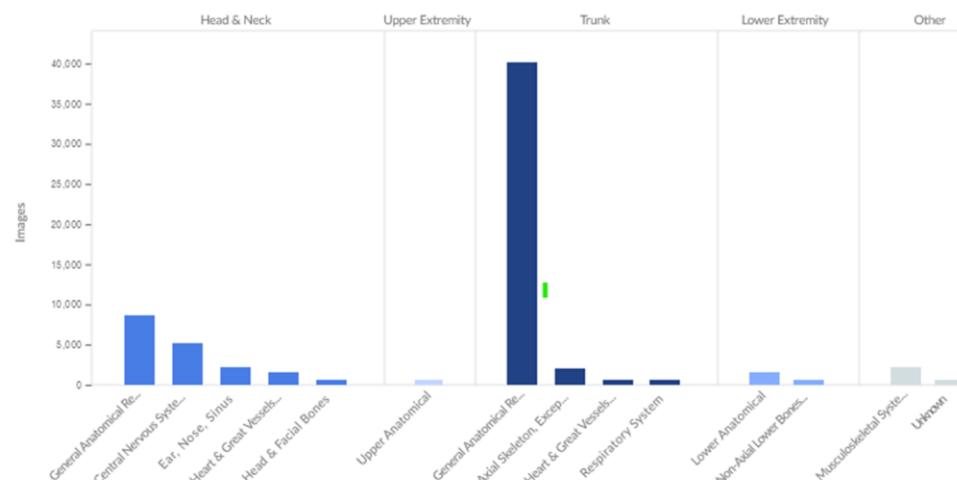
Trunk

1474

Lower Extremity

2194

Other



# Mejora en las capacidades de seguridad

- Proyecto que se encarga de :
  - Proveer características de detección y respuesta extendida a la herramienta corporativa EDR.
  - Permitirá la agregación, correlación , orquestación y respuesta de la telemetría de elementos de seguridad y de Sistemas de la DGSD
  - A partir de motores de detección y prevención locales y la correlación en cloud de esta telemetría, la plataforma permite identificar y bloquear ciberataques sofisticados.
  - IA como asistente del analista.
  - Reduce significativamente los **tiempos de detección y respuesta.**

# GRACIAS

Alvaro Espinosa Muñoz.

[aespinosa@sescam.jccm.es](mailto:aespinosa@sescam.jccm.es)

Coordinador Regional de Infraestructuras Tecnológicas.

Dirección General de Salud Digital de la Agencia de Transformación Digital de CLM



Financiado por  
la Unión Europea  
NextGenerationEU



MINISTERIO  
DE SANIDAD



Plan de Recuperación,  
Transformación  
y Resiliencia



Castilla-La Mancha