Junta de Andalucía: **Centro de Operaciones de Ciberseguridad**

SOCINFO DIGITAL 2024

Junta de Andalucía

SIA
An Indra company

Ciberseguridad en la Junta de Andalucía

SOCINFO
DIGITAL
2024

Junta
de Andalucía

La Junta

81
organismos

~220.000
empleados conectados

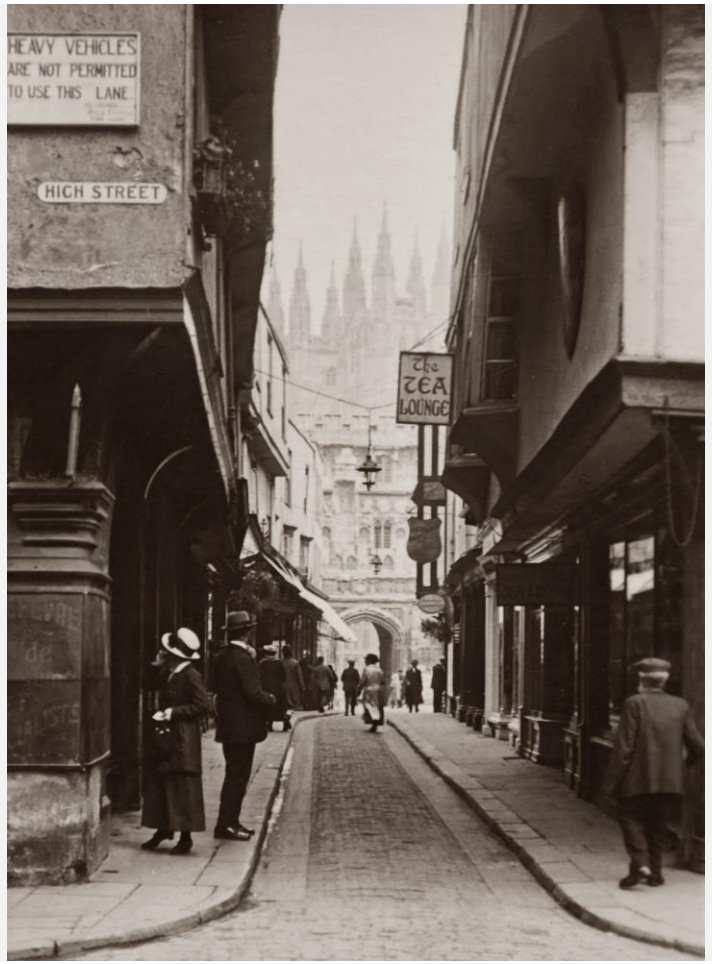
10.500 sedes
(1.500 centros de salud,
4.600 centros educativos,
700 juzgados)

120.000
teléfonos fijos

40.000
teléfonos móviles

+500 sistemas
de información

¡Peligro!



Fotografía antigua


Programa ALCAZABA
2008
Plan Director de Seguridad
2010
2011
Decreto 1/2011
Plan de Seguridad y Confianza Digital 2020 (2014-2016)
2014
2016
Orden junio 2016
Plan de Seguridad y Confianza Digital 2020 (2017-2020)
2017
Decreto 70/2017
03/21 Agencia Digital de Andalucía
Estrategia Andaluza de Ciberseguridad 2022-2025
Octubre 2022

lajunta.es/estrategiaciberseguridad

LA1 - Estructuras organizativas

LA2 - Capacidades de prevención, detección y respuesta

LA3 – Cooperación y colaboración

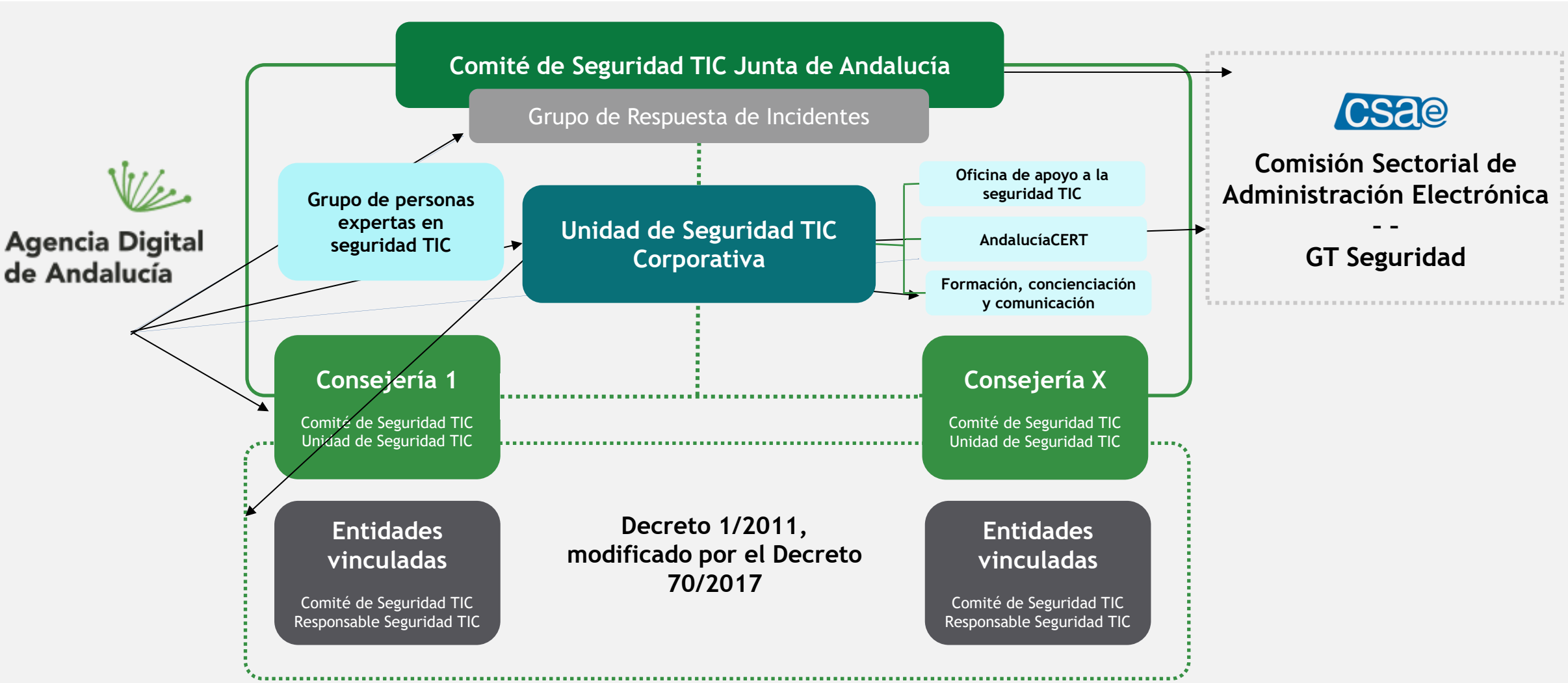
LA4 – Promoción de Andalucía

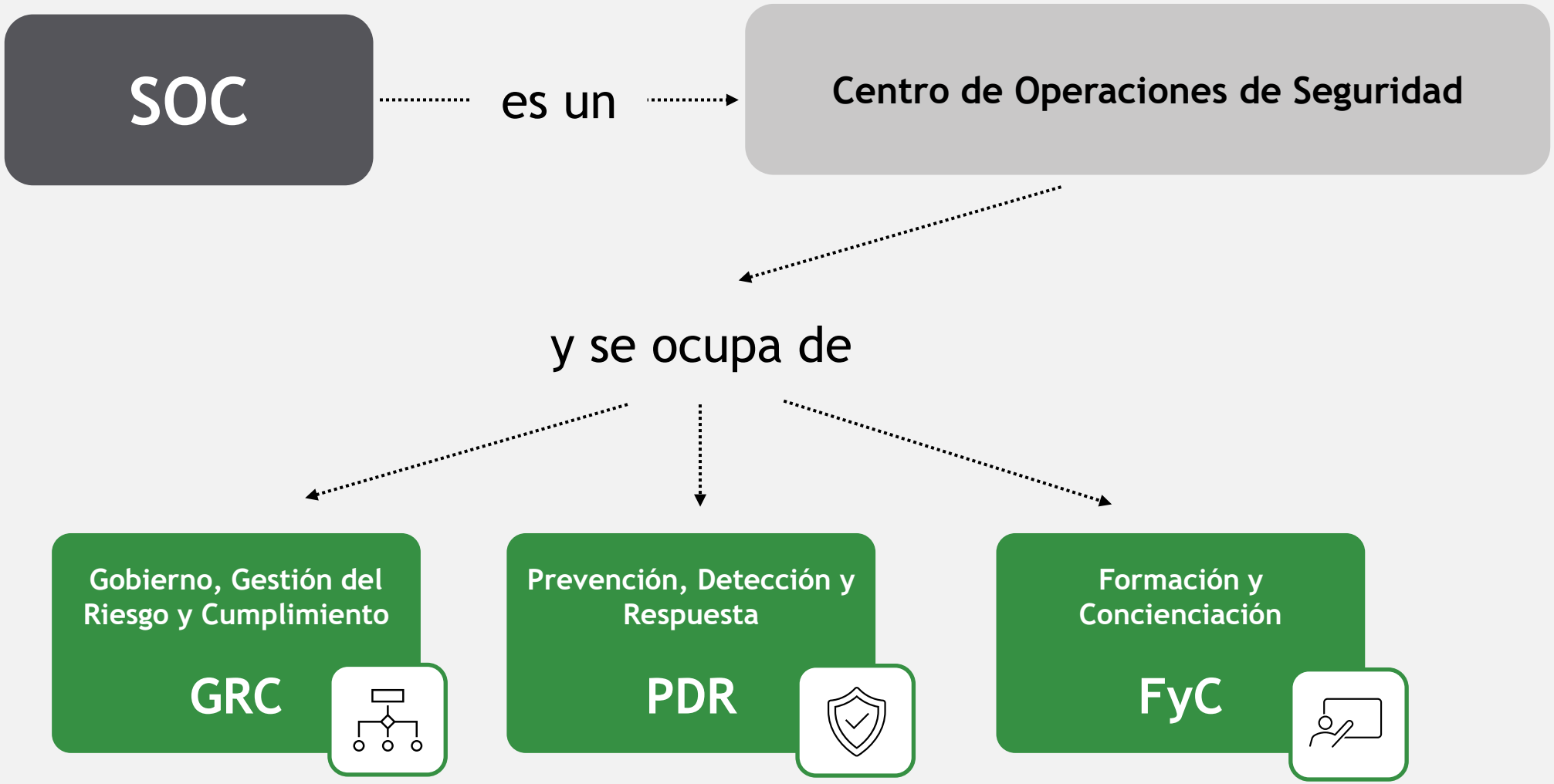
LA5 – Ciberseguridad en el sector empresarial

LA6 – Industria especializada

LA7 – Programas formativos

LA8 – Concienciación y sensibilización en ciberseguridad


Comité de Seguridad TIC Junta de Andalucía
Grupo de Respuesta de Incidentes
Agencia Digital de Andalucía
Grupo de personas expertas en seguridad TIC
Unidad de Seguridad TIC Corporativa
Oficina de apoyo a la seguridad TIC
AndalucíaCERT
Formación, concienciación y comunicación
csae
Comisión Sectorial de Administración Electrónica
- -
GT Seguridad
Consejería 1
Comité de Seguridad TIC
Unidad de Seguridad TIC
Consejería X
Comité de Seguridad TIC
Unidad de Seguridad TIC
Entidades vinculadas
Comité de Seguridad TIC
Responsable Seguridad TIC
Decreto 1/2011, modificado por el Decreto 70/2017
Entidades vinculadas
Comité de Seguridad TIC
Responsable Seguridad TIC


SOC
es un
Centro de Operaciones de Seguridad
y se ocupa de
Gobierno, Gestión del Riesgo y Cumplimiento
GRC
Prevención, Detección y Respuesta
PDR
Formación y Concienciación
FyC

SOC Junta Andalucía

Incremento en anchura, altura y profundidad // Equipo, herramientas, servicios

- **AndalucíaCERT (2010)**
  - 2023: 7.800 incidentes
  - 2024: 11.203 incidentes
  - Desde 2010: 73.106
- **OASTIC (2017)**
  - 2024: 260 casos. 75 organismos.
- **OFyC (2019)**
  - 2024: >30 actuaciones, >6.000 participantes

Red Nacional de SOC

CSIRT.es

TF-CSIRT Trusted Introducer

Relaciones


SOC Junta Andalucía
123 organismos
Grupo Atendido
("ámbito 81")
GA Extendido:
(Sector Público local, Universidades...)
CENTRO CIBERSEGURIDAD ANDALUCÍA
Ciudadanía y empresa
Red corporativa
Sistemas horizontales
Infraestructuras comunes
...
IESPA
IAAP
CCN
INCIBE
Otras CCAA
FCSE / UPA
ENISE
DSN

Servicios

SOC Junta Andalucía

GRC

- Relaciones
- Consejo
- Seguimiento y reporte
- Criterios comunes y normalización

FyC

- Concienciación
- Comunicación
- Formación

PDR

- Gestión de eventos
- Detección / recepción de incidentes
- EDR
- Respuesta (coordinación + in situ)
- Alerta temprana
- Gestión y difusión de CTI / IoCs
- Auditoría técnica
- Forense / gestión evidencias
- Vigilancia digital
- Superficie de exposición

Inversión

IOSSOC
9,6M€ + 1,9M€

EDR
18M€

CARMEN
370K€

AMGRC
1,5M€

AMCIBER
2,5M€

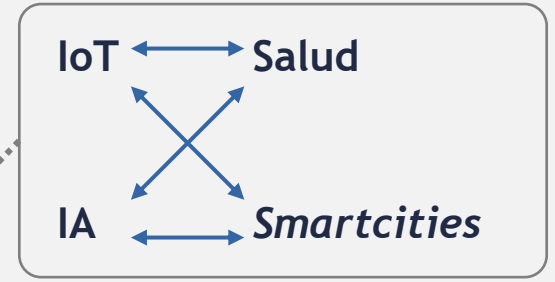
Retech - Red Argos
14M€

Inversión - Retech

Retech - Red Argos
14M€

INCIBE
JCYL / PV / AND

Centro de Excelencia
CIAN



Estado:
- Mapa
- Auditorías

Dirección:
- Guías conf. segura
- Marcos certificación

Impulso:
- Aceleradora
- Laboratorio
- Formación

El futuro

GRC

- Nueva política de ciberseguridad
- Consolidación y homogeneización
- Apoyos y servicios comunes
- Profesionalización

PDR

- Nueva infraestructura
- Nuevos servicios
- Crecimiento
  - Altura: puesto...nube
  - Anchura: extensión
  - Profundidad: no sólo perímetro
- Automatización

FyC

- Nuevos métodos
- Crecimiento
  - Altura: personal…altos cargos
  - Anchura: exterior
  - Profundidad: formación especializada
- Automatización

ACA


SIA responde
sia
An Indra company

Qué solicitaba la Junta de Andalucía

Junta de Andalucía

Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa
Agencia Digital de Andalucía

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Suministro y servicios asociados de plataforma de monitorización, y de servicios recurrentes y bajo demanda, para apoyo al Centro de Operaciones de Seguridad de la Junta de Andalucía (AndalucíaCERT)

Expte. CONTR 2023 642838

LOTE 1 - SUMINISTRO Y SERVICIOS ASOCIADOS DE PLATAFORMA DE MONITORIZACIÓN PARA APOYO AL CENTRO DE OPERACIONES DE SEGURIDAD DE LA JUNTA DE ANDALUCÍA (ANDALUCÍACERT)

LOTE 2 – SERVICIOS RECURRENTES Y BAJO DEMANDA PARA APOYO AL CENTRO DE OPERACIONES DE SEGURIDAD DE LA JUNTA DE ANDALUCÍA (ANDALUCÍACERT)

Cofinanciado por la Unión Europea

ELOY RAFAEL SANZ TAPIA		30/05/2023	PÁGINA 1 / 160
VERIFICACIÓN	NJyGwfg81745g8vN7HKqTVBa69hQ3E	https://ws050.juntadeandalucia.es/verificarFirma	

RAUL JIMENEZ JIMENEZ		25/09/2023 12:16:19	PÁGINA: 1 / 160
VERIFICACIÓN	NJyGweZEzRG66ellRrO3pGpg9Gq83D	https://ws050.juntadeandalucia.es/verificarFirma/	

LOTE 1 - SUMINISTRO Y SERVICIOS ASOCIADOS DE PLATAFORMA DE MONITORIZACIÓN PARA APOYO AL CENTRO DE OPERACIONES DE SEGURIDAD DE LA JUNTA DE ANDALUCÍA (AndalucíaCERT)

Plataforma de monitorización de eventos y detección de incidentes

- Capturar y analizar tráfico de red
- Recoger y normalizar eventos de seguridad y flujos de distintas fuentes
- Realizar correlación y generar alarmas que se pueden gestionar a través de una consola de operación integrada con capacidad para generar informes.

Equipos para la actualización de sondas del Sistema de Alerta Temprana (SAT) de CCN-CERT

Servicio de gestión y respuesta a incidentes de seguridad y de incidencias, peticiones y consultas de AndalucíaCERT

SIA responde

El servicio de gestión y respuesta a incidentes de seguridad y de incidencias, peticiones y consultas de AndalucíaCERT incluye diversas actividades:

Despliegue inicial de la plataforma

- Instalación del hardware
- Instalación del software
- Configuración y puesta en marcha de la plataforma

Servicio de mantenimiento de la plataforma

- Soporte hardware y software
- Administración de la plataforma de monitorización
- Atención a las incidencias de indisponibilidad de la plataforma
- Monitorización de la disponibilidad de la plataforma

Monitorización

- Identificación y reporte al servicio avanzado
- Monitorización de otras consolas en la Junta de Andalucía
- Atención a las detecciones y alarmas en sistemas auxiliares
- Notificación de los incidentes de seguridad en la plataforma Lucía de AndalucíaCERT
- Detección de incidentes de seguridad
- Interlocución con el servicio de soporte y mantenimiento de la plataforma de monitorización, fabricantes de los productos y los proveedores de servicios
- Atención de consultas técnicas

Transición del servicio

En los últimos tres meses del contrato (o de sus posibles prórrogas) se iniciará un periodo de transición del servicio

Servicio avanzado de la plataforma de monitorización

- Ajuste fino continuo en la detección de incidentes de seguridad de la plataforma y corrección de posibles falsos positivos
- Asesoramiento en los procesos de nuevos despliegues de la plataforma de monitorización
- Definición y documentación sobre casos de uso incluyendo runbooks/playbooks para la detección y respuesta
- Monitorización de incidentes de seguridad
- Diseño de cuadros de mandos y reporte periódico de situación
- Identificación y propuesta de mejoras del servicio y de la funcionalidad de la plataforma
- Informe singular de actividad y hallazgos
- Identificación y diseño de automatizaciones y optimizaciones
- Gestión de los IOC/IOA del fabricante y de terceros
- Búsqueda proactiva de amenazas (Threat Hunting)
- Integración de nuevas fuentes de eventos

Formación y Capacitación

- Capacitación inicial
- Capacitación adicional/de refuerzo

Nuevos despliegues

- Diseño del Plan Técnico de Despliegue
- Recepción del equipamiento necesario para el despliegue de la solución propuesta
- Despliegue de la solución propuesta y optimización de la misma

Respuesta a incidentes

Gestión de incidentes de seguridad de Nivel 1 (TN1) y Nivel 2 (TN2)

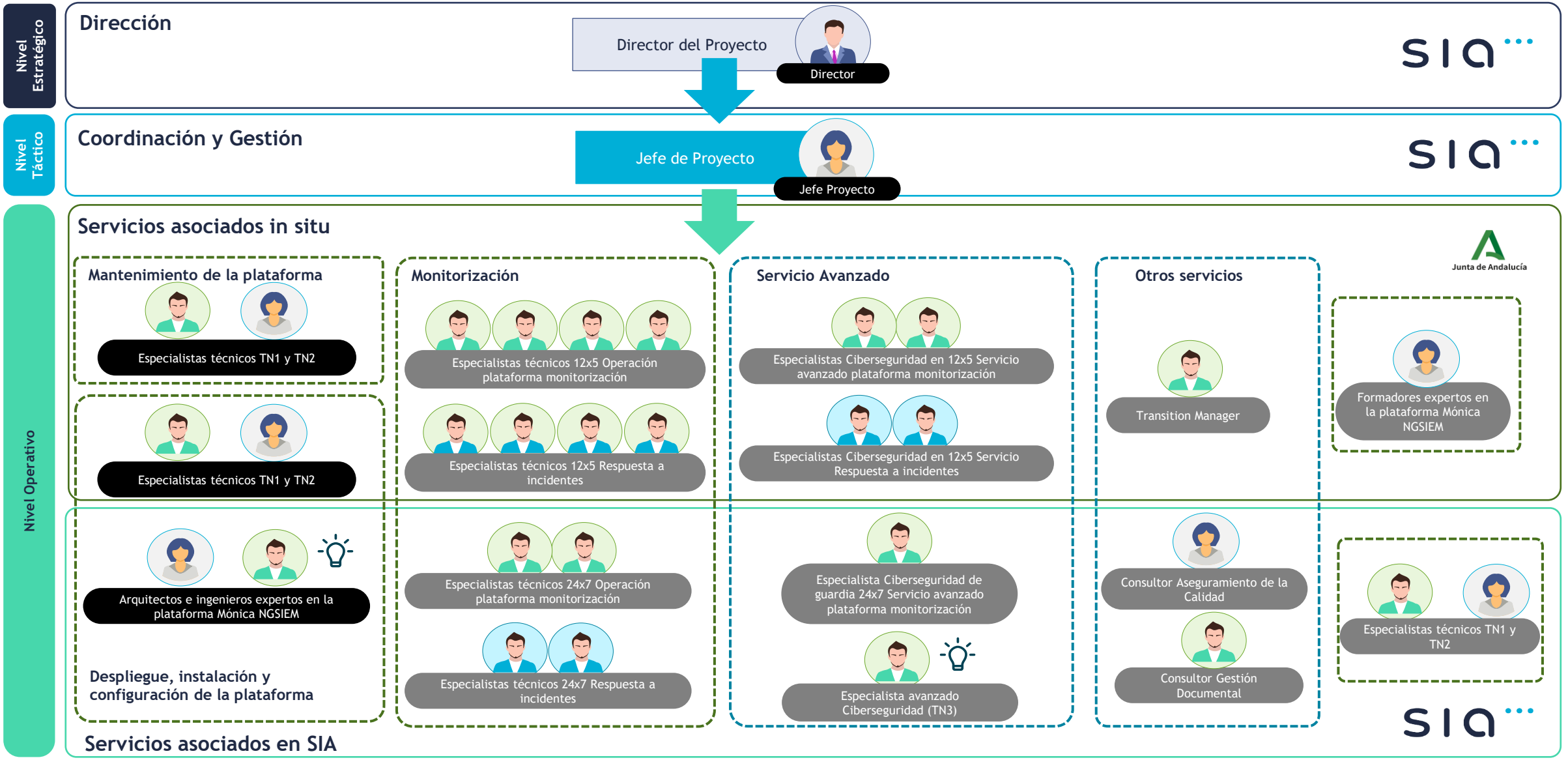
- Atención a los canales de recepción de solicitudes de servicio y notificaciones
- Atención de los incidentes de seguridad recibidos o detectados
- Atención de las consultas, peticiones e incidencias que lleguen a AndalucíaCERT.
- Escalado de incidentes de seguridad al nivel 2 (caso TN1) o a Respuesta rápida (Caso TN2)
- Tareas de apoyo a la gestión interna y a los sistemas de calidad
- Generación de informes de servicio
- Identificación y propuesta de mejoras del servicio y de la funcionalidad de la plataforma

Respuesta rápida in situ para soporte a la recuperación

Prestación de apoyo técnico y organizativo para atender incidentes de seguridad de especial gravedad o complejidad

SIA responde

… que ejecuta un equipo multidisciplinar in situ (Málaga) y en remoto



SIA responde

Plataforma de monitorización de eventos y detección de incidentes

Producto 100% español alineado con la Estrategia Nacional de Ciberseguridad

- Nace Lógica en 2008 , en 2020 el CCN la integra como producto cualificado dentro de su ecosistema de herramientas y es publicada en el catálogo del CCN como producto cualificado.
- Inversión y soporte de SIA y el Grupo Indra para evolución del producto y para garantizar su futuro
- Roadmap coordinado con CCN y posibilidad de incorporar necesidades de clientes.

Máximas certificaciones de seguridad

Common Criteria ®

Funcionalidades de Mónica NGSIEM

Arquitectura flexible

- Funcionalidad Multitenant
- Escalabilidad. Crecimiento horizontal y vertical de manera transparente

Motor centralizado de correlación

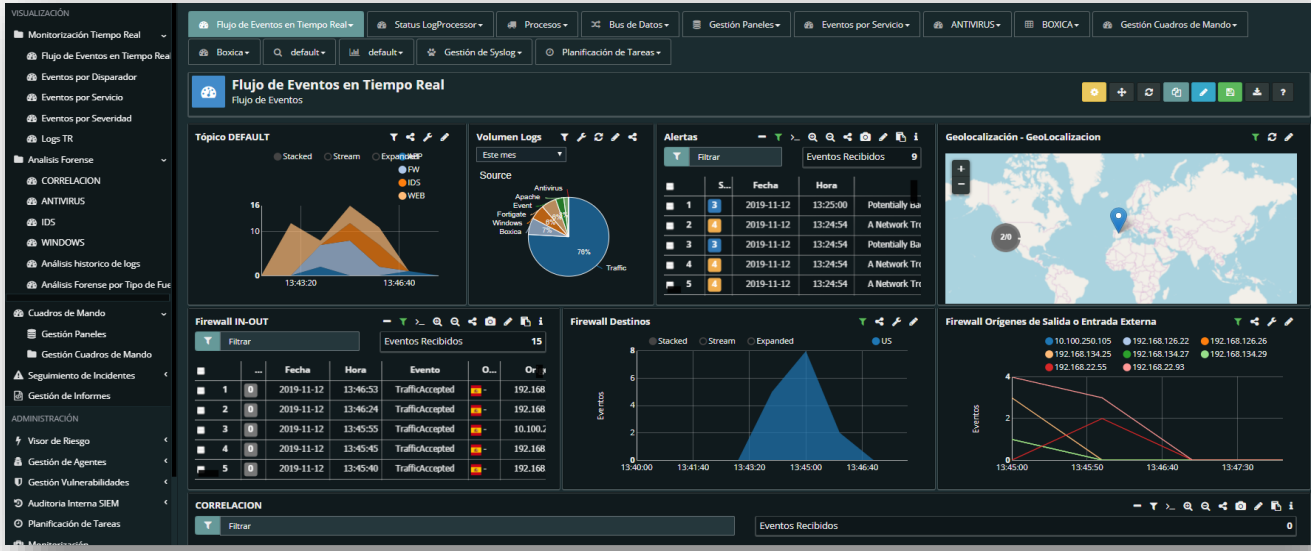
- UCs out of the box y generación e identificación de nuevos UCs
- Correlación: eventos/anomalías/ IOC/entidades
- Gestión de reglas de correlación

Recolección de logs

- Múltiples protocolos
- Agentes de monitorización (multitecnología, multifabricante…)

Threat Intelligence

- Feeds, reputacional y APTs
- IOCs externos e IOCs de CCN
- Dark web, Deep web, RRSS, hacktivistas



Repositorio centralizado de Logs

- Integridad del repositorio de logs
- Búsqueda cruzada eventos – logs

Visibilidad

- Cuadros de mando en tiempo real
- Tablas y gráficos personalizables
- Geolocalización de incidentes

Analítica avanzada (UEBA)

- Tendencias y evolución de comportamientos en la red
- Gestión de incidentes
- Análisis estadístico de eventos de seguridad
- Análisis forense

SOAR

- Orquestación y automatización de gestión de incidentes con TheHive/Cortex/MISP
- Integración por API con

Red Nacional de SOC

¿Preguntas?

An Indra company

Muchas gracias
por tu atención

BEYOND CYBERSECURITY