El cumplimiento del ENS como vehículo estratégico

Nueva Estrategia de Ciberseguridad del Sistema Nacional de Salud

SOCINFO DIGITAL

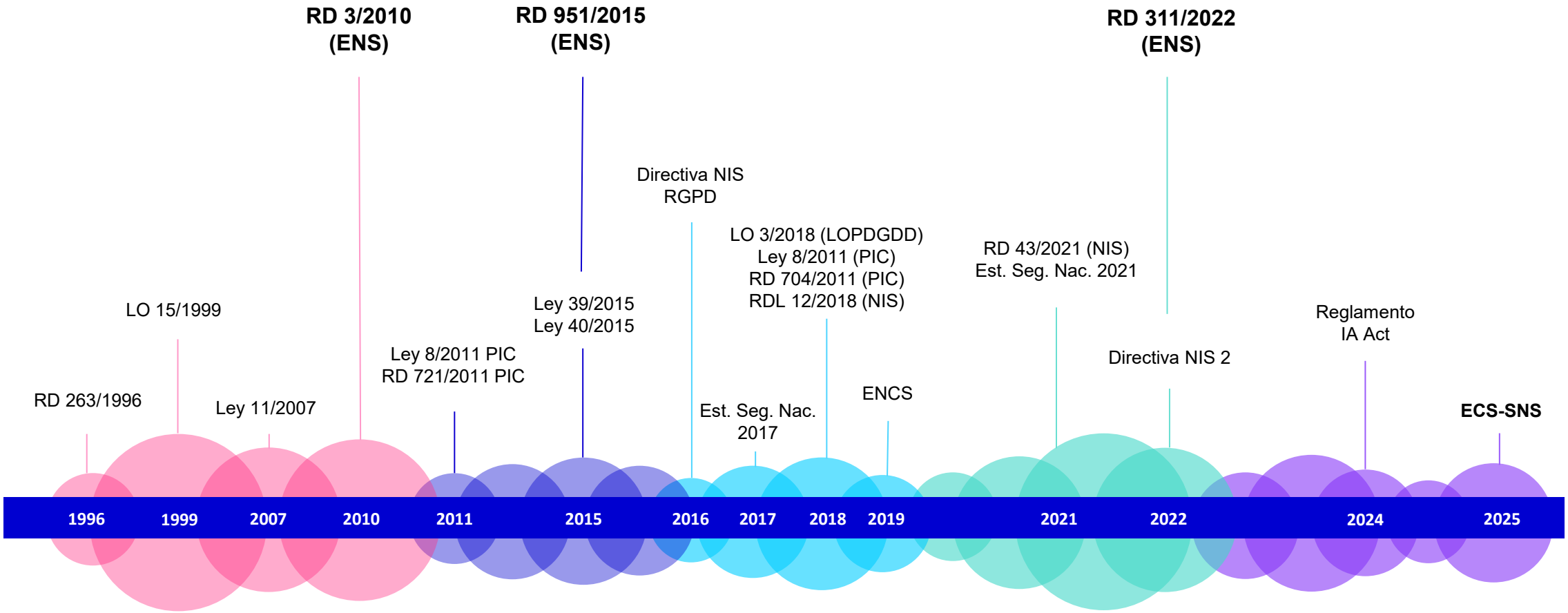
20 de enero de 2026

ayesa

SOCINFO sociedad de la información digital

[01] Cumplimiento normativo

Evolución Cumplimiento normativo relacionado con ciberseguridad



[02] Afectación sector salud

LA VERDAD 120 ANIVERSARIO

Javier Pérez Parra

Miércoles, 21 de septiembre 2022, 18:07

Salud sufre una estafa informática de 276.000 euros

Escudodigital

Home / Ciberseguridad /

CIBERSEGURIDAD

Investigan los motivos del ciberataque contra el Hospital Central de Asturias

Se da la circunstancia de que el ciberataque al centro hospitalario ha coincidido con el ingreso del presidente del principado, Adrián Barbón

Sara Olivo Redactora Jefe de Escudo Digital 20 de diciembre de 2021 (12:16 CET) Guardar

EL MUNDO

SANIDAD

La Policía investiga un ciberataque al servicio público de Salud de Baleares

EDUARDO COLOM
Palma

Actualizado Miércoles, 19 enero 2022 - 16:42

Comentar

El gobierno autonómico activó los servicios de alerta para proteger los datos de los pacientes

CyberSecuritynews

El Hospital de Vall d'Hebron bajo investigación por un posible ciberataque

Samuel Rodríguez 28/02/2022 Sin comentarios

Antonio M. Figueras
Periodista y escritor.
Publicado el 22 de mayo de 2025 a las 10:05

Escudodigital
Diario de seguridad y tecnología

CIBERSEGURIDAD

La Agencia Española de Medicamentos restablece su web tras el ciberataque del 14 de mayo

La entidad asegura que no se han producido daños estructurales ni fuga de datos por el ciberataque del 14 de mayo.

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

incibe-cert_

INICIO / INCIBE-CERT / Publicaciones / Bitácora de ciberseguridad / Ciberataque ransomware paraliza actividad del Hospital Clínic de Barcelona

Ciberataque ransomware paraliza actividad del Hospital Clínic de Barcelona

Fecha de publicación 13/03/2023
05/03/2023

Servicio Andaluz de Salud
Consejería de Sanidad, Presidencia y Emergencias

05 agosto 2024

El SAS informa de un incidente de seguridad en la provincia de Granada.

[03] Objetivos

El cumplimiento del ENS es un vehículo facilitador para la implantación de la estrategia de ciberseguridad en el SNS.

ESTRATEGIA CIBERSEGURIDAD SNS

- Establecer una **red de colaboración** en ciberseguridad.
- Definir medidas para **asegurar [DICAT] datos sanitarios**.
- Posicionar al **SNS** como un **referente de ciberseguridad**.
- Fomentar el **cumplimiento normativo**.
- Establecer **indicadores**.
- Impulsar la investigación y el **análisis de riesgos**.
- Garantizar la **continuidad asistencial**.
- Promover la **capacitación** continua.

ENS

- Garantizar un **nivel adecuado de seguridad** para la **información** y **servicios**.
- **Asegurar [DICAT]** en la **información y servicios**.
- Homogeneizar criterios y requisitos sirviendo de **marco común** a todas las organizaciones.
- Aplicar **medidas proporcionales al riesgo** según la categorización del sistema.
- Facilitar la **cooperación e interoperabilidad** segura entre Administraciones.
- Impulsar la **mejora continua**.
- **Principios básicos**.
- **Requisitos mínimos**.

[04] Ejes estratégicos

Cumplimiento del articulado del ENS e implantación de medidas de seguridad del Anexo II facilita la adopción de la estrategia de ciberseguridad del SNS.

Gobernanza de la Ciberseguridad Sanitaria Roles y responsabilidades Estructura organizativa Capacitación	01	**ENS** Art.11 Diferenciación responsabilidades Art.12 Política de Seguridad y req. min. de seguridad Art.13 Organización e implantación seguridad
Intercambio de Información de Ciberseguridad Compartición información Estructura organizativa Capacitación	02	**ENS** [op.mon.2] Sistema de métricas [op.mon.3] Vigilancia Red Nacional de SOC
Cumplimiento regulatorio en ciberseguridad ENS, LPIC, NIS2, LOPDGDD, RGPD Definición de guías Directrices y procedimientos Línea base cumplimiento Incorporación nuevos proyectos en entornos certificados Análisis dispositivos médicos Análisis de riesgos	03	**ENS** [org.2] Normativas [org.3] Procedimientos Guía CCN-STIC-891 Perfil cumplimiento Guía CCN-STIC-857 Aplicaciones cibersalud Art.23 / [op.ext.4] Interconexión de sistemas [op.pl] Explotación / [mp.com] Protección comunicaciones [op.pl.1] Análisis de riesgos
Observatorio de madurez Ciber Porcentaje inversión TIC Nivel madurez TIC Cuadros de mando Alineamiento INES e informe SEIS	04	**ENS** Art.32 Informe del estado de seguridad [op.mon.2] Sistemas de métricas Guía CCN-STIC-824 Información del estado seguridad Modelo de madurez de capacidad (CMM) [L0-L5]

[04] Ejes estratégicos

Seguridad de la información del SNS
Categorización Sistemas de Información

05

ENS
Guía CCN-STIC-891 Perfil cumplimiento
[op.exp.1] Inventario de activos
Anexo I ENS / CCN-STIC-803 Valoración de los sistemas

05

Modelo de gestión de crisis
Roles, responsabilidades, flujos de comunicación
Guía CCN-STIC-817
Simulación, Ciberejercicios
Capacidades de resiliencia

06

ENS
Art.11 Diferenciación responsabilidades
Guía CCN-STIC-817 Gestión ciberincidentes
[op.cont] Continuidad del servicio

06

Gestión de la cadena de suministro
Inventario proveedores
Controles de seguridad para proveedores
Tipología de productos y servicios
Certificación de proveedores / servicios

07

ENS
[op.acc.5] Autenticación usuarios externos
[op.pl.3] Adquisición de nuevos componentes
[op.ext.3] Protección de la cadena de suministro
Art.19 Extensible no solo a productos o servicios seguridad

07

Mejora de la capacitación en ciberseguridad
Formación según perfiles profesionales
Itinerarios de formación
Realización de campañas de phishing/smishing, etc.

08

ENS
Art. 6 Seguridad como un proceso integral
Art.16 Profesionalidad
[mp.per] Gestión del personal

08

[04] Ejes estratégicos

Liderazgo de pensamiento en ciberseguridad
Grupos de Trabajo
Fuentes de información
Capacitación

09

ENS
Art.10 Vigilancia continua y reevaluación periódica
Art.14 Análisis y gestión de los riesgos
Art.27 Mejora continua del proceso de seguridad

09

Optimizar el proceso de contratación de productos y servicios de ciberseguridad
Requisitos de certificación
Repositorio de pliegos

10

ENS
Art.19. Adquisición de productos de seguridad y contratación de servicios de seguridad.
Guía CCN-STIC-105 CPSTIC

10

Búsqueda de líneas de financiación
Fondos europeos
Oportunidades de financiación

11

ENS
Cumplimiento ENS, LOPDGDD, RGPD, NIS2

11

Apoyo para la implantación de la Estrategia en los Servicios Públicos de Salud
Sensibilizar a la alta dirección
Medidas a desplegar según madurez
Plataforma gestión del conocimiento
Indicadores

12

ENS
Art.14 Análisis y gestión de los riesgos / [op.pl.1]
Art.31 Auditoría de seguridad
Art.32 Informe del estado de seguridad
Art.37 Mecanismos de control cumplimiento ENS

12

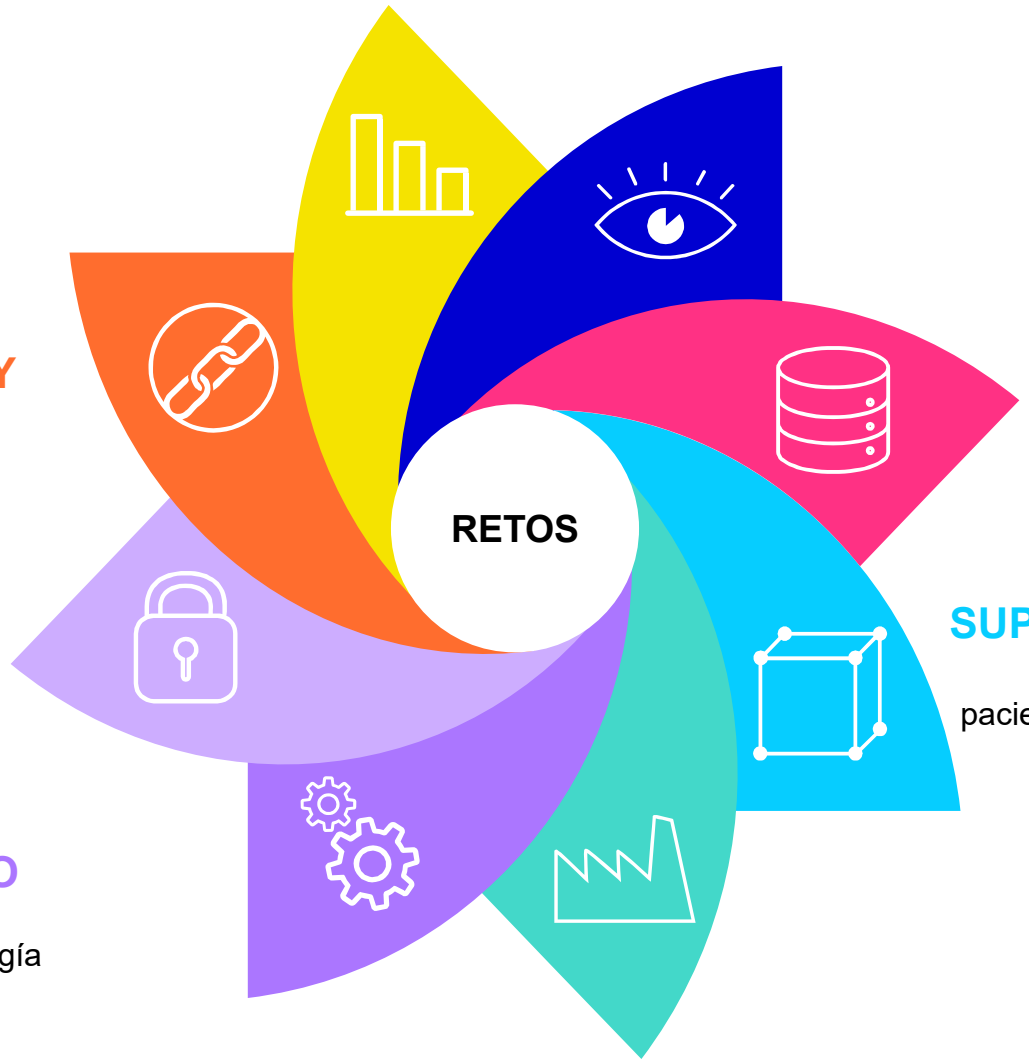
[05] Retos

CONCIENCIACIÓN
Concienciación alta dirección y profesionales sanitarios.

EQUIPOS IoMT y LEGACY
Identificación y protección a nivel de red.

ENS
Implantación y conformidad con el ENS.

CADENA DE SUMINISTRO
Protección de la cadena suministro, especialmente empresas de tecnología sanitaria.



CIBERDELINCUENTES
Sector salud en el punto de mira por sus datos sanitarios.

GESTIÓN DE ACTIVOS
Necesidad de identificar cualquier equipo conectado a la red sanitaria.

SUPERFICIE DE EXPOSICIÓN
Dispositivos médicos en hospitales y pacientes, teletrabajo, adopción cloud, IA.

INVERSIÓN
Ciberseguridad no es un gasto, es una inversión.

[06] Conclusiones

Debilidades

- ✓ Complejidad de la adecuación por descentralización.
- ✓ Sistemas legacy.
- ✓ Baja visibilidad y control de activos.
- ✓ Prioridad asistencial sobre seguridad.
- ✓ Falta de cultura seguridad y protección del dato sanitario.

Amenazas

- ✓ Falta de cultura y formación en seguridad y protección de datos del personal sanitario.
- ✓ Exfiltración de datos de salud.
- ✓ Ataques a la cadena de suministro.
- ✓ Ransomware y su impacto en la actividad asistencial.
- ✓ Aumento superficie exposición (IoMT/OT)

Fortalezas

- ✓ Marco sólido normativo para la gestión de la seguridad.
- ✓ Colaboración entre distintos servicios de salud y colaboración público-privada.
- ✓ Estrategia sectorial.
- ✓ Concienciación criticidad servicio asistencial.
- ✓ Fondos UE para mejora resiliencia.

Oportunidades

- ✓ ENS como marco operativo estándar.
- ✓ NIS2 como palanca de madurez.
- ✓ Mejora la confianza de los ciudadanos en el sistema sanitario.
- ✓ Estandarizar prácticas de seguridad y mejorar la interoperabilidad nacional y europea.
- ✓ Fomentar una cultura de seguridad en los servicios de salud.

Servicios de Ciberseguridad

ayesa

[07] Ayesa

Somos un proveedor global de servicios tecnológicos y de ingeniería.

Top 5
de los servicios TI en España

Top 50
mayores ingenierías del mundo

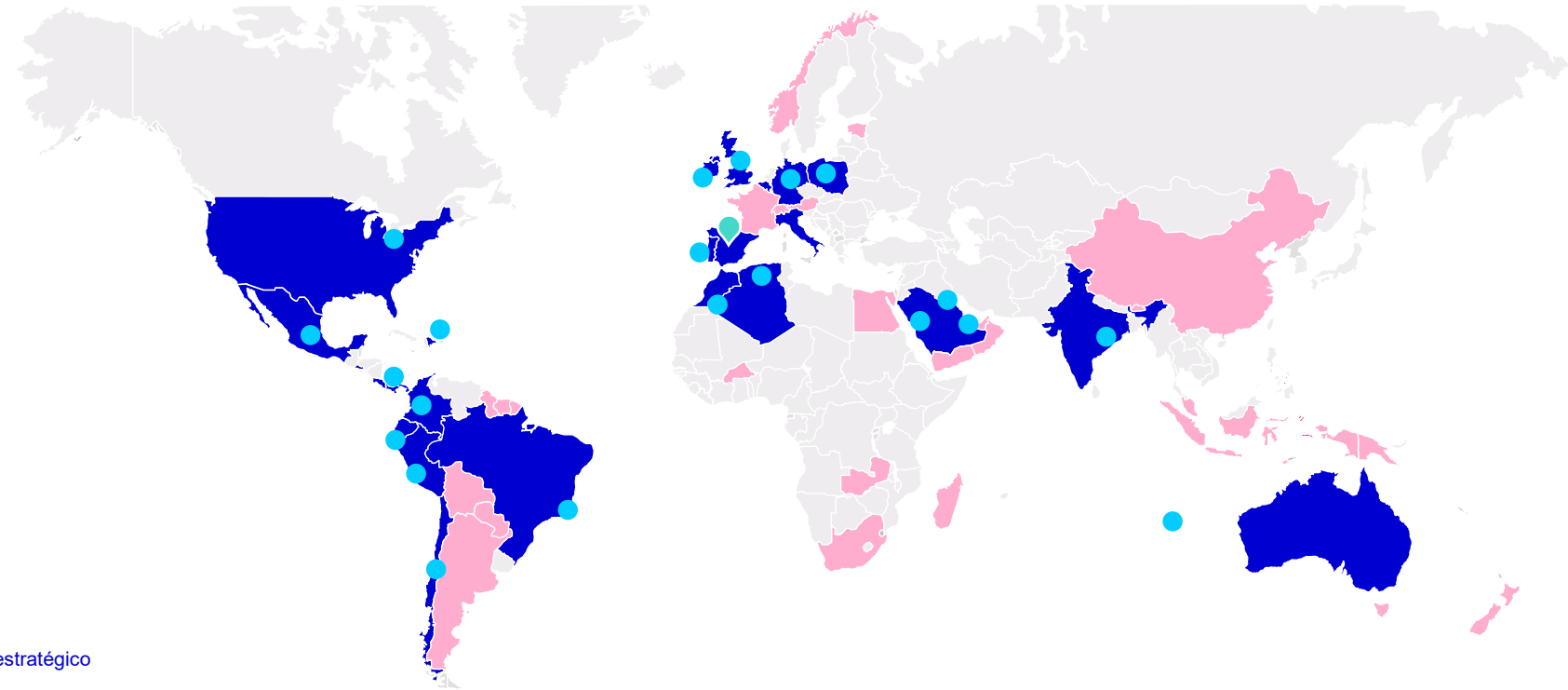
+900 M€
cifra de negocio

15.000
profesionales

24
sedes en todo el mundo

71
nacionalidades

+70
disciplinas

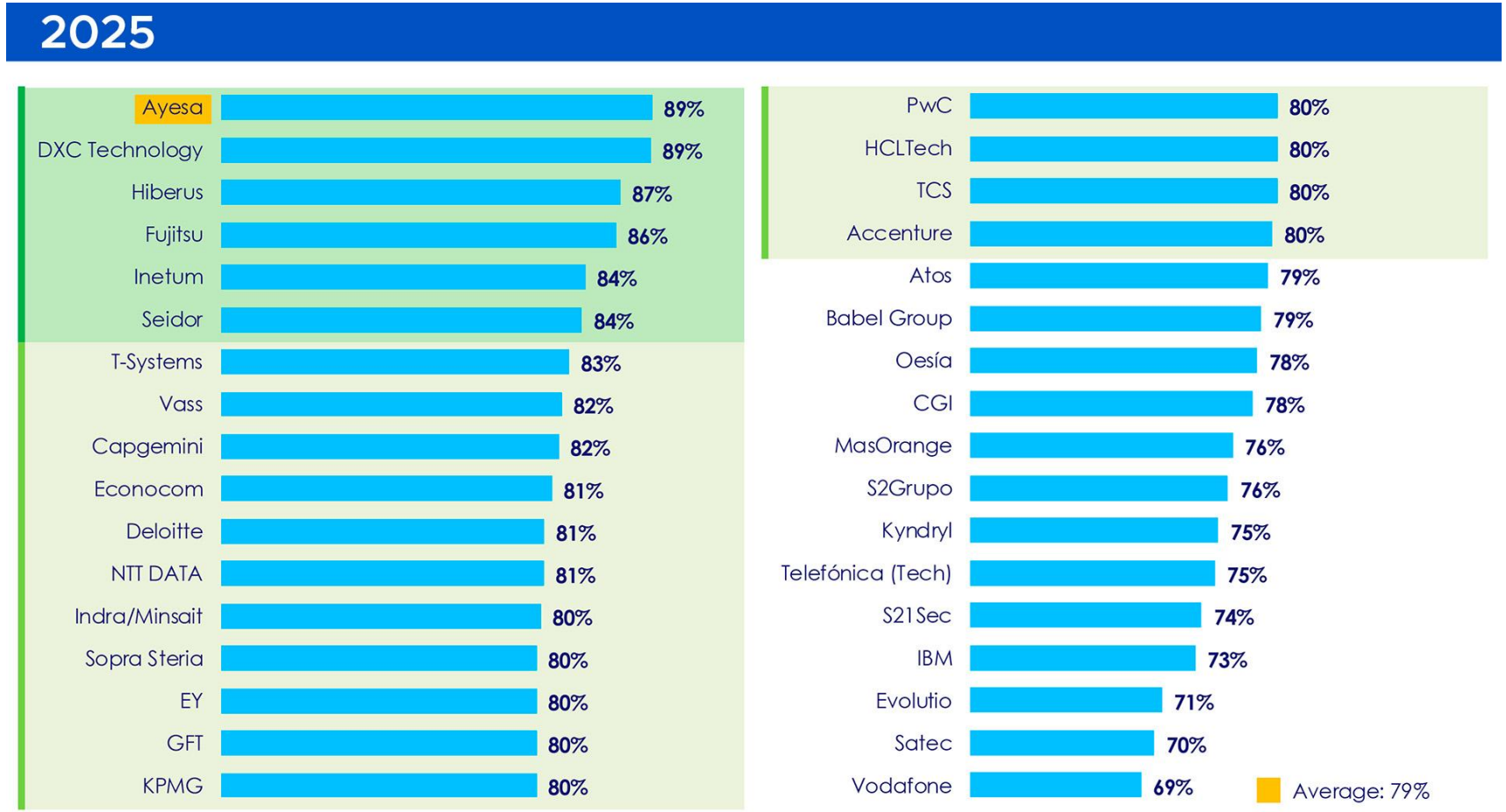


Satisfacción de nuestros clientes

Ayesa se consolida como el **mejor proveedor de servicios tecnológicos** de los últimos años en el **mercado español**. El prestigioso 'Estudio sobre Sourcing de Servicios de TI' elaborado por las consultoras Eraneos y Whitelane Research, con las opiniones proporcionadas por más de 300 clientes del sector público y privado, le vuelven a situar en lo más alto de su ranking.

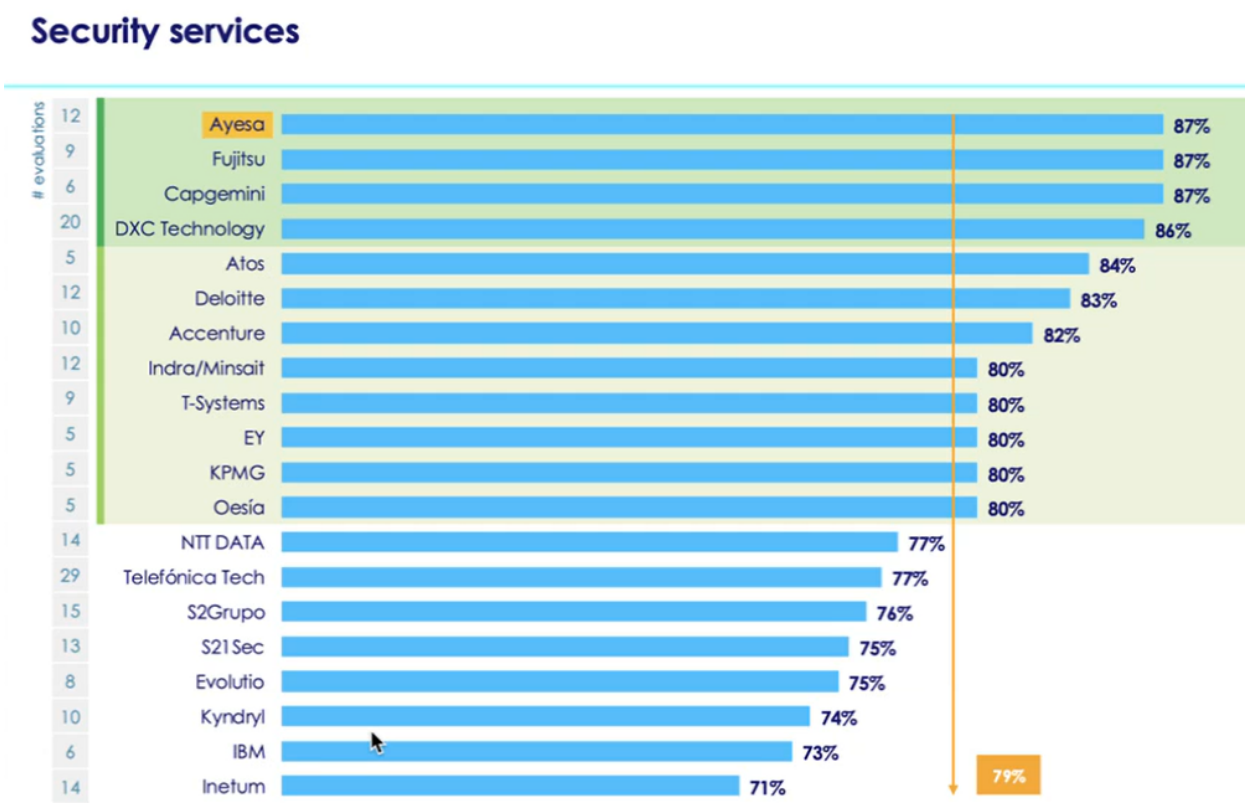
Bate todos los registros y alcanza por primera vez los **89 puntos** de satisfacción general de sus clientes, tres puntos por encima de la máxima puntuación lograda antes por ningún otro proveedor.

Ha ocupado la **primera posición** en 8 de los 13 informes independientes que elaboran con carácter anual desde 2013 las consultoras Eraneos y Whitelane Research, sin abandonar nunca los puestos de cabeza.



[07] Ayesa

Satisfacción en servicios de seguridad.

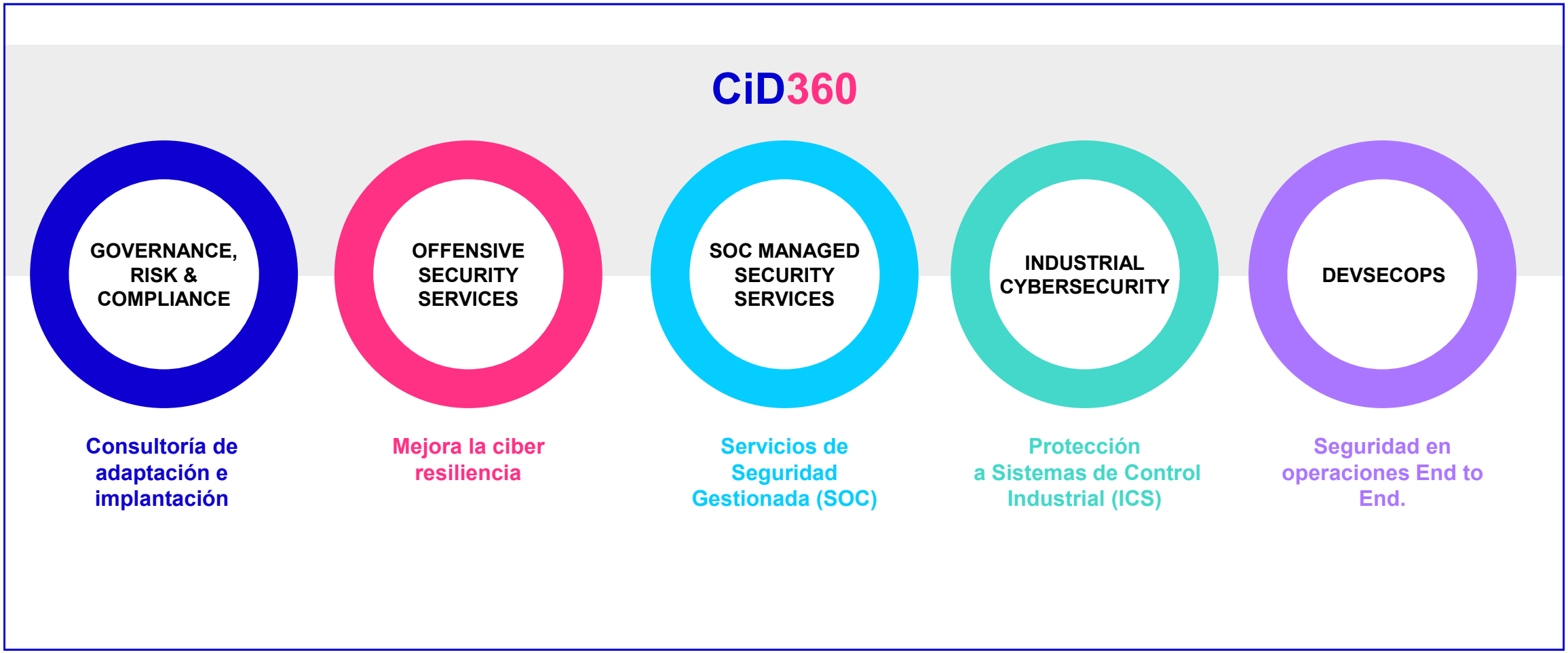


Lideramos el ranking de servicios de Ciberseguridad con una puntuación del 87%.

Nuestros servicios son excepcionales, según la opinión de nuestros clientes.

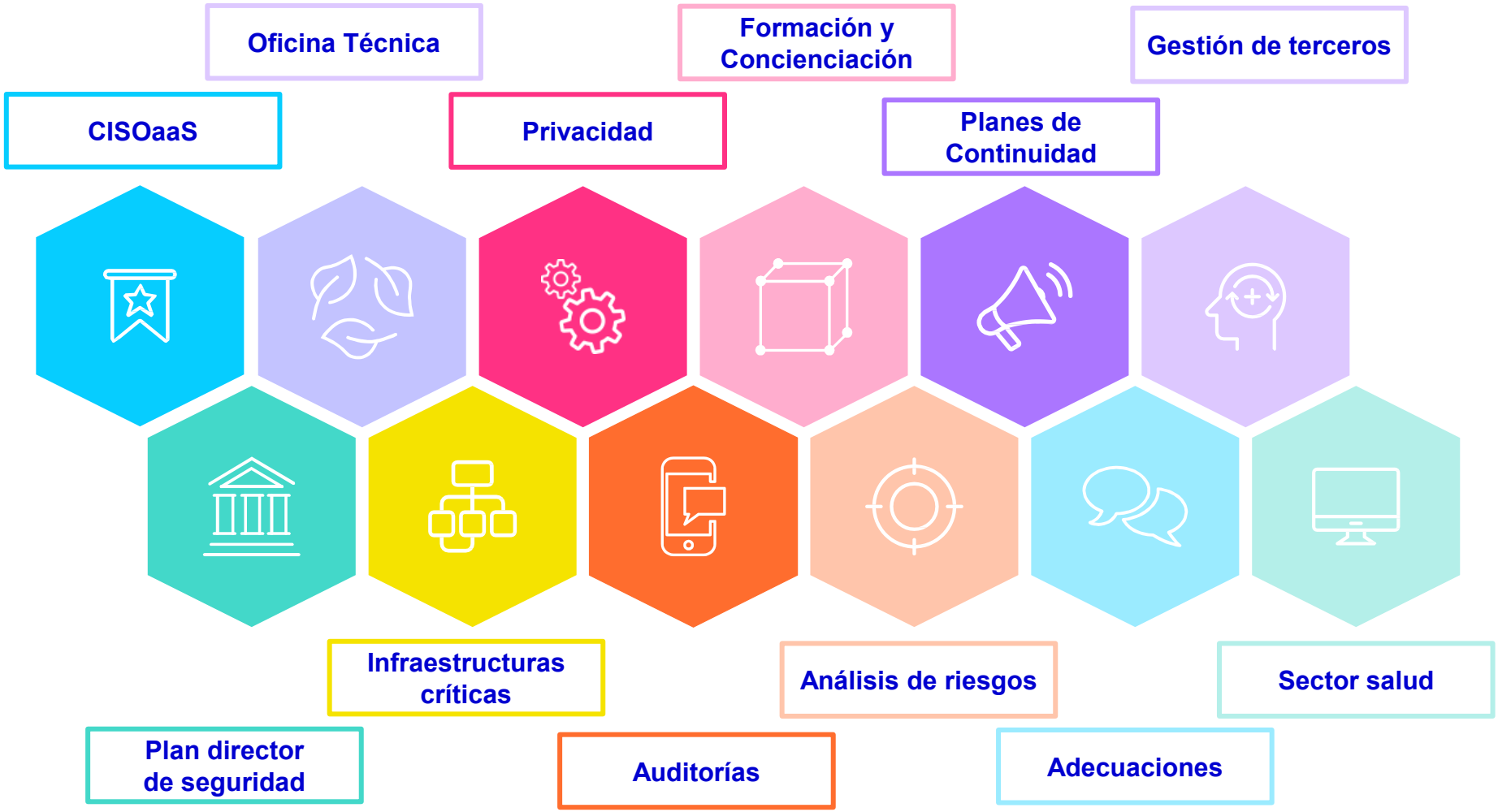
[08] Servicios de Ciberseguridad

Portfolio de servicios de ciberseguridad



[08] Servicios de Ciberseguridad

Servicios GRC Ciberseguridad



[08] Servicios de Ciberseguridad

Servicios de seguridad ofensiva

SERVICIOS DE TEST DE INTRUSIÓN

- TEST DE INTRUSIÓN EXTERNO
- TEST DE INTRUSIÓN INTERNO
- TEST DE INTRUSIÓN WIFI
- TEST DE INTRUSIÓN APLICATIVO WEB O API WEB
- TEST DE INTRUSIÓN APLICACIÓN MÓVIL
- INGENIERÍA SOCIAL
- TEST DE INTRUSIÓN PCI-DSS
- TEST DE INTRUSIÓN IoT

METODOLOGÍA

Alineada con los principales marcos de Red Team existentes: TIBER-EU, ASE, CBEST

[08] Servicios de Ciberseguridad

Servicios SOC

SOC / CERT

MONITORIZACIÓN

- Monitorización entornos industriales
- Monitorización Seguridad

GESTIÓN DE VULNERABILIDADES

- Gestión vulnerabilidades extendida
- Gestión vulnerabilidades

RESPUESTA A INCIDENTES Y ANÁLISIS FORENSE

- Forense digital
- Respuesta a incidentes
- Asesoramiento

CIBER INTELIGENCIA

- Vigilancia Deep / Dark Web
- Alerta temprana y vigilancia tecnológica
- Listas IOC

Plataforma CiD360

- Gestión y seguimiento
- Portal Web
- Alerting tiempo real
- Reporting

[08] Servicios de Ciberseguridad

Servicios de ciberseguridad industrial

La columna vertebral y el talón de Aquiles de todos los sectores de la industria y de infraestructuras críticas.

DIAGNÓSTICO OT ANÁLISIS GAP

Evalúa el nivel de madurez de las redes industriales de tu organización. Conoce el grado de vulnerabilidad de tu red de operación.

SEGMENTACIÓN OT RED IT / OT

A través de la definición de zonas y conductos, que permita reducir la superficie de ataque y mejorar el nivel de riesgo.

TEST DE INTRUSIÓN IoT / IIoT / ICS

Servicios de simulación de ataque. Realizamos pruebas de penetración en profundidad y evaluaciones de seguridad para sistemas ICS y entornos IoT, IIoT, **IoMT**.

NAC OT Control de acceso a red

Reducir el ciberriesgo, estableciendo y reforzando las políticas de seguridad que regulan los usuarios/dispositivos que pueden acceder a tu red.

NUKLEA 360 Monitorización OT

Monitorización y detección de ciberamenazas, junto con inventario y análisis, en entornos industriales OT.

[08] Servicios de Ciberseguridad

DevSecOps: End-to-end coverage

Gestión de Identidades

- Principio mínimo privilegio
- Autenticación multifactor
- Gestión de roles
- Auditoría de accesos

Inventario y Gestión de Activos

- Visibilidad y control
- Unificación multi-CSP
- Automatización de inventarios
- Etiquetados y clasificación
- Control de la superficie de ataque

Arquitectura Segura y Plataformas de Seguridad

- Principios Zero Trust
- Protección perimetral y API (WAF, FW, API GW, etc.)
- Protección Endpoint (EDR/XDR)
- Protección del dato (DLPs, Gestión de claves, etc.)

Cumplimiento Normativo y Auditoría

- Implementación de Frameworks (DORA, NIS2, ISO27k1, GDPR, etc.)
- Automatización y cumplimiento

Gestión de Vulnerabilidades y Parches

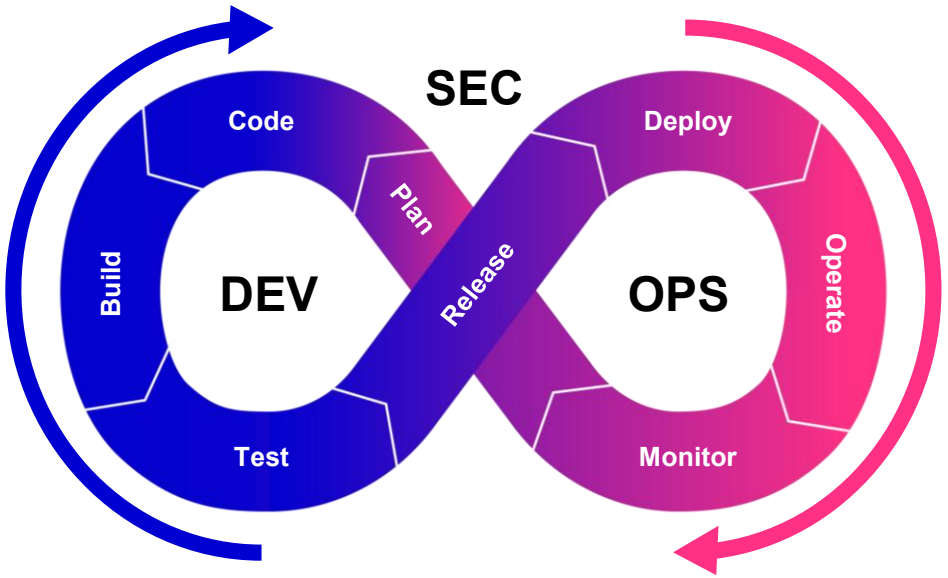
- Escaneo de Infraestructura y contenedores (tecnologías, malas configuraciones, etc.)
- Priorización de riesgos
- Automatización y gestión de remediaciones

Monitorización y Respuesta

- Monitorización y correlación de eventos.
- Integración e implementación SIEM/SOAR
- Respuesta automatizada o gestionada de incidentes

Código y Despliegue Seguro

- Seguridad en pipelines CI/CD
- Escaneo de código IaC (Terraform, Pulumi, etc.)
- Escaneo de imágenes y orquestadores (Docker, Kubernetes)



Gracias.

Javier Balongo Sánchez

Consultor Ciberseguridad

jbalongo@ayesa.com