SINGLAR
Innovación

Puente entre operaciones (CTO) y gestión (CISO)

Herramienta de contexto para el SOC

Difusión restringida externa

SIRENA

SIRENA es una Plataforma integral para la gestión de la Seguridad. Incluye una Plataforma GRC completa para cumplimiento y plan de tratamiento de riesgos, y simplifica y potencia cualquier SIEM, convirtiendo la información técnica compleja en datos comprensibles gracias a la incorporación de contexto semántico que relaciona los elementos técnicos con su relevancia para el negocio. El objetivo de SIRENA es unir de manera fluida la gestión y las operaciones de seguridad para proporcionar a tu SOC una visión más integral de la seguridad de tu empresa.

Los dashboards proporcionan visibilidad en tiempo real al agrupar datos operativos complejos, lo que facilita una respuesta rápida y apoya la toma de decisiones.

- Permite a los usuarios determinar rápidamente las prioridades al tener una visión clara de cómo y qué eventos de seguridad afectan a los activos críticos del negocio, facilitando la toma de decisiones informadas.
- Visualiza fácilmente todos tus activos junto con sus amenazas y vulnerabilidades.
- Identifica qué alertas y vulnerabilidades están asociadas a diferentes procesos y activos del negocio.
- Exporta informes profesionales con un solo clic.

Contexto semántico y empresarial: Sirena comprende el significado de la anomalía técnica y lo explica en lenguaje claro, añadiendo contexto directo de negocio, lo que permite tomar decisiones más rápidas.

- Ejemplo: La IP x.x.x.x corresponde a un equipo de radiología médica que está enviando información crítica con contraseña en texto plano en lugar de cifrada → Posible filtración de datos de pacientes.
- Ejemplo: Indica todos los activos y las amenazas actuales relacionadas con los gasómetros.

Plataforma GRC integral que supervisa y mitiga riesgos de manera dinámica para garantizar el cumplimiento de los objetivos normativos.

- Decide o supervisa cómo se están gestionando los riesgos detectados en tiempo real y quién asume la responsabilidad.

Difusión restringida externa

Descripción del producto

Funcionalidades

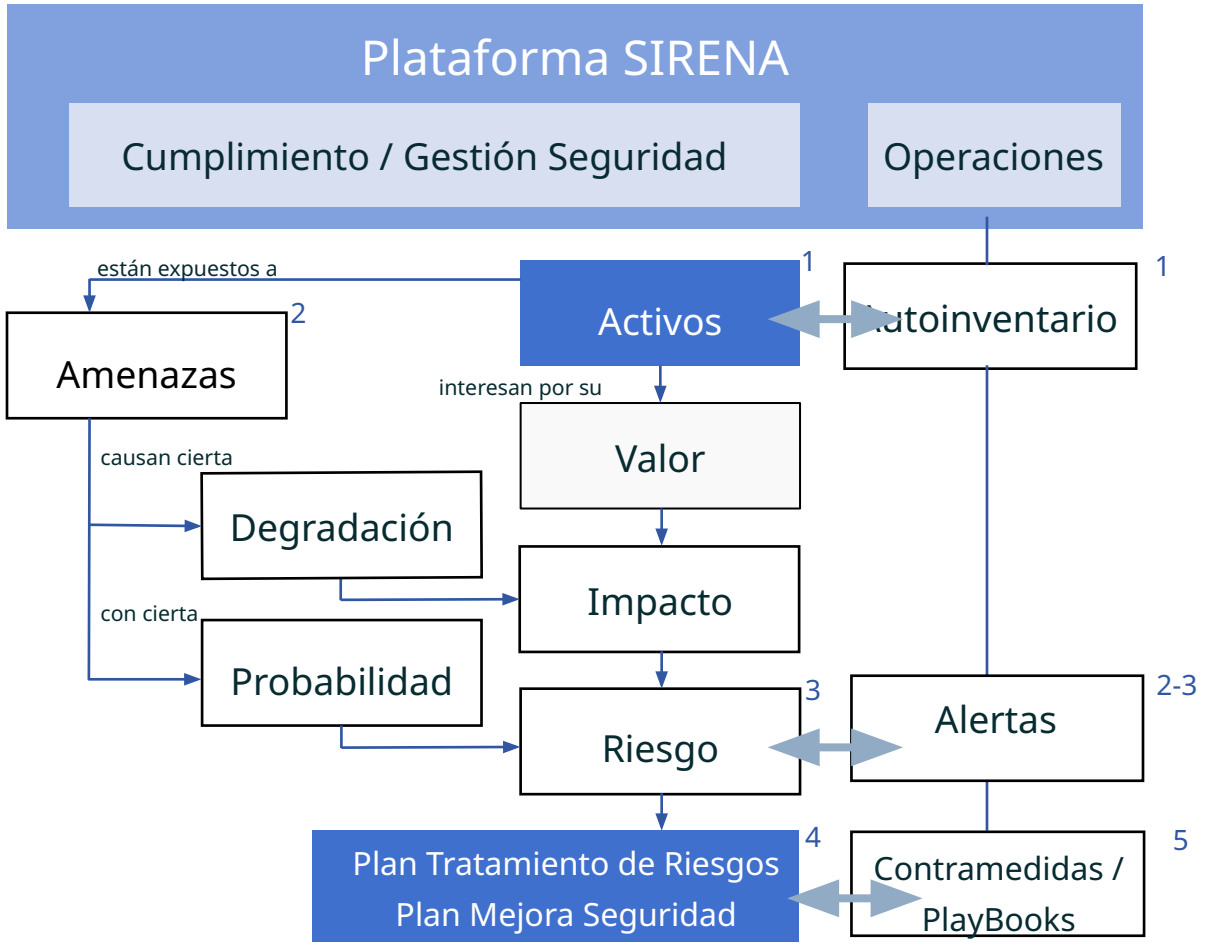
01

Difusión restringida externa

Cumplimiento y gestión de la Seguridad Dinámica

Información de negocio

- AARR (Dependencias de negocio)
- Ley PIC
- PDSI
- ENS
- NIS
- Sistemas SCADA existentes
- Inventarios en Excel (Plano)



Difusión restringida externa

Mejoras en Operaciones

Cada alerta va enriquecida con información del negocio (cumplimiento, gestión…)

SOC TRADICIONAL

Sin seguridad semántica Total 7t

- Clasificación (Basado en el tipo de alerta)
- Investigación
- Contexto
  - Llamadas
  - Información de infraestructura
  - Histórico
- Reclasificación
- Registro
- Conclusión y respuesta
- Informes manuales al CISO

SOC ENRIQUECIDO

Con seguridad semántica Total 3t

- Clasificación automática (Basado en negocios)
- Investigación automática de contexto
- Conclusión y respuesta (semiautomático)
- Informe al CISO y ajuste del plan de riesgos (automatizado)

- Los empleados de TI y los técnicos de CyberSOC necesitan conocer el contexto de cada incidente.
- Todo lo que viene en la propia alarma permite un proceso más rápido y eficiente.

Difusión restringida ex

MEJORA SEGURIDAD MEDIO LARGO PLAZO

MEJORA SEGURIDAD CORTO PLAZO

Difusión restringida externa

Cuadros de mando

Estadísticas de activos y alertas personalizados a cada cliente

IOC's

Indicadores de compromiso

Alertas asociadas a

ACTIVOS

- Top 10 dispositivos con más alarmas
-Top de riesgos
-Número de anomalías por operación

Métricas

Medición de procesos por perfil

Alertas asociadas a

PROCESOS

- Alertas por tipología
-Top de vulnerabilidades
-Nivel de riesgos general
-Volumen de alertas por nivel de riesgo

Cuadro de mando

Afectación a negocio

Alertas asociadas a

NEGOCIO

- Alertas por Sistema de Información crítica
-Nivel de riesgo de cada sistema
-Alertas de negocio por zonas, etiquetas y procesos

El cuadro de mando permite ver las alertas, riesgos y anomalías agrupadas por Activo de negocio, pero también por servicios de alto nivel o por Negocio directamente, de modo que tengamos una foto completa de nuestro entorno de operaciones, y cada responsable pueda tener su propio cuadro de mando.

Los informes se pueden programar y enviar a cada responsable para analizar el estado de la seguridad, de las operaciones, y la tendencia de cada sistema

Difusión restringida externa

Arquitectura

Ecosistema de SIRENA

02

Difusión restringida externa

Plan De mejora de la Seguridad Asistido y Proactivo (SGSI)

Fuente de inteligencia de negocio para Respuesta a Incidentes

SIRENA® Seguridad semántica

GESTION

- Plan Director Seguridad
- Tratamiento de riesgos
- Seguimiento acciones mejora

GOBIERNO/CUMPLIMIENTO

- ISO 27001
- ISA/IEC 62443
- NIS2
- ENS

OPERACIÓN

- Detección temprana entornos IT/OT
- Autoinventario

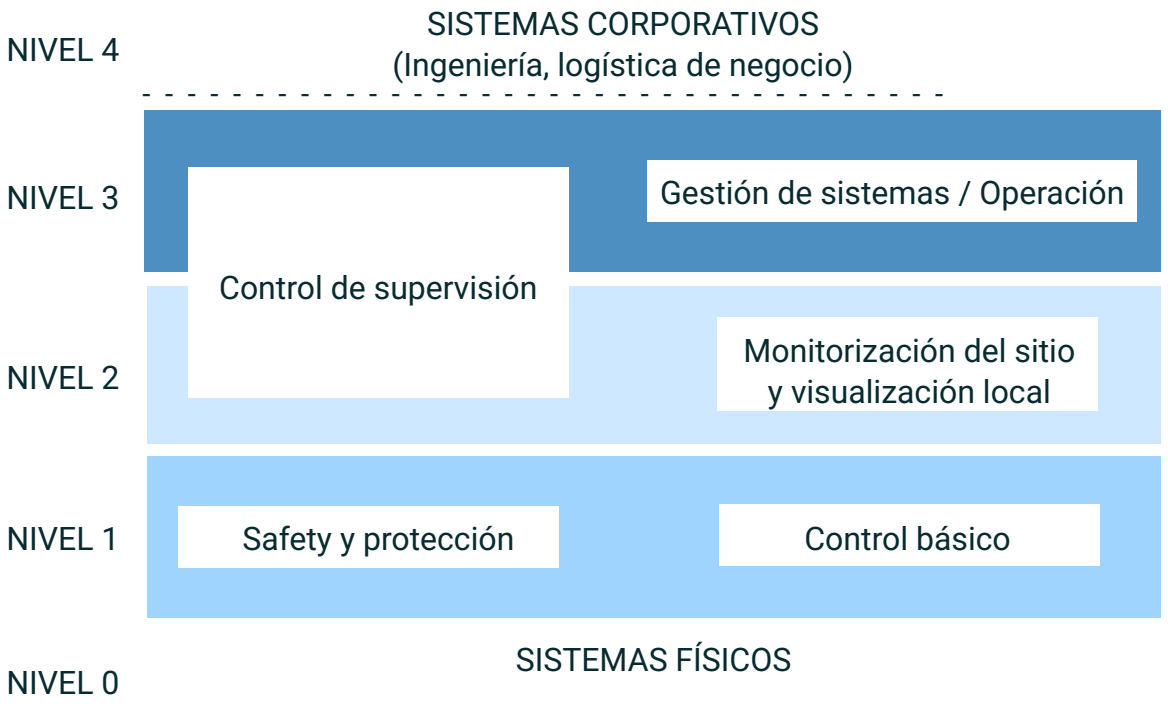
RGPD	Esquema Nacional de Seguridad	Sistema de Gestión de Seguridad de la Información	Plan Director de Seguridad: NIS2, DORA	Ciber Industrial
GDPR	ens Esquema Nacional de Seguridad	International Organization for Standardization ISO 27001		ISA

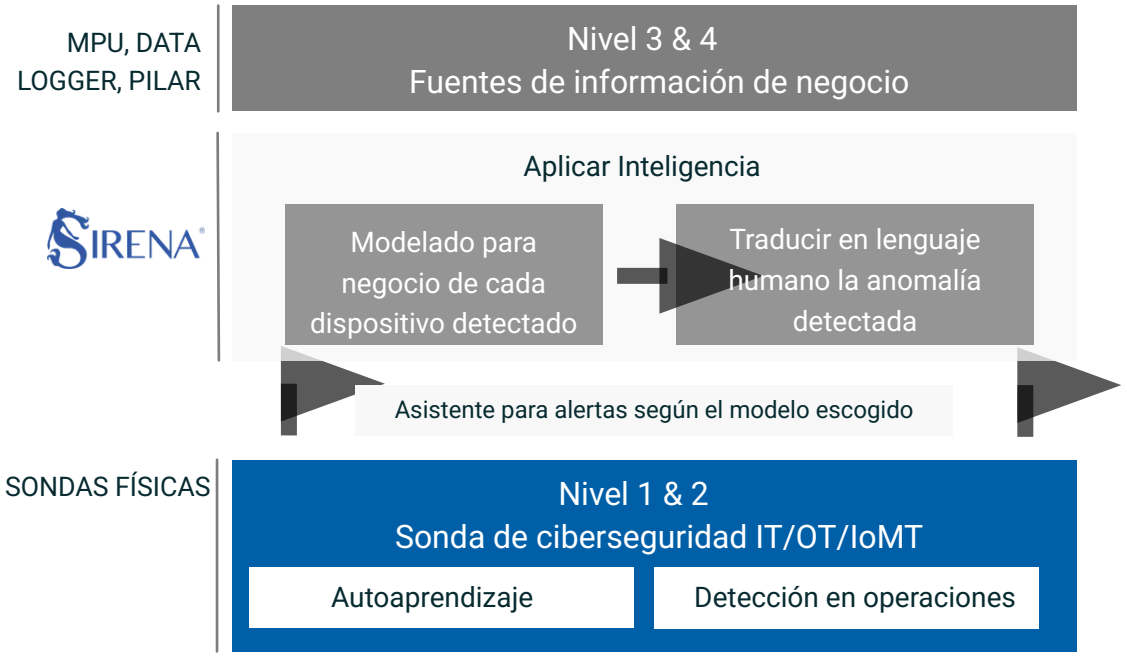
NIDS / SIEM IT/OT/IoT/IoMT

Difusión restringida externa

Arquitectura y ecosistema

Niveles





SIRENA es capaz de asociar cada activo de bajo nivel con un activo o servicio de negocio.

Difusión restringida externa

Funcionalidades

Demostración técnica entorno Salud

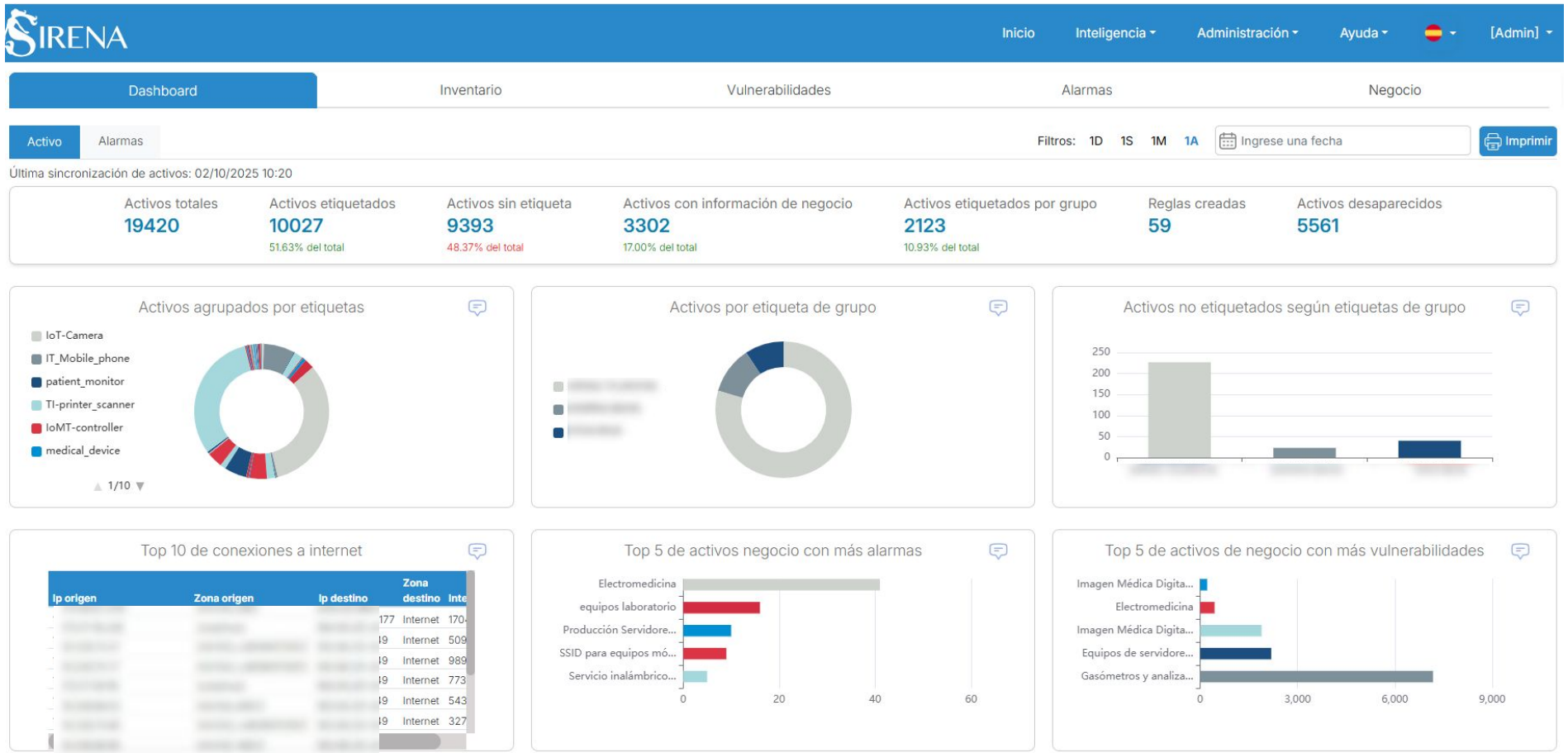
03

Difusión restringida externa

Operaciones de Seguridad

1 – Autoinventario mejorado

- Al autoinventario de las sondas NIDS/SIEM se suma el contexto de negocio basado en Machine Learning e IA que permite asociar activos físicos con activos de negocio y su contexto

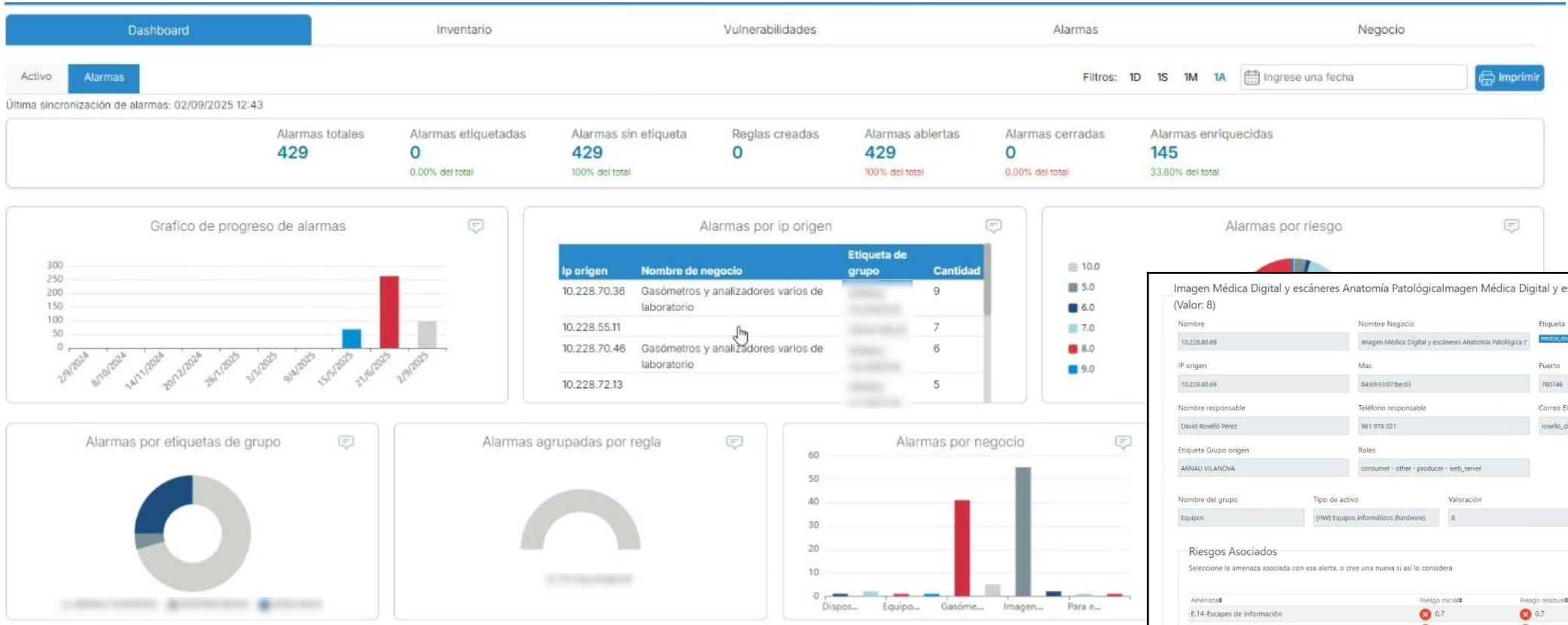


Difusión restringida externa

Operaciones de Seguridad

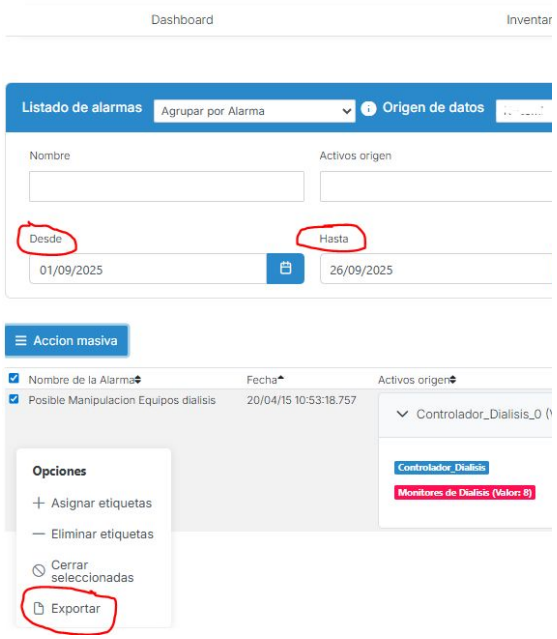
2 – Alertas clasificadas por negocio y fácilmente entendibles

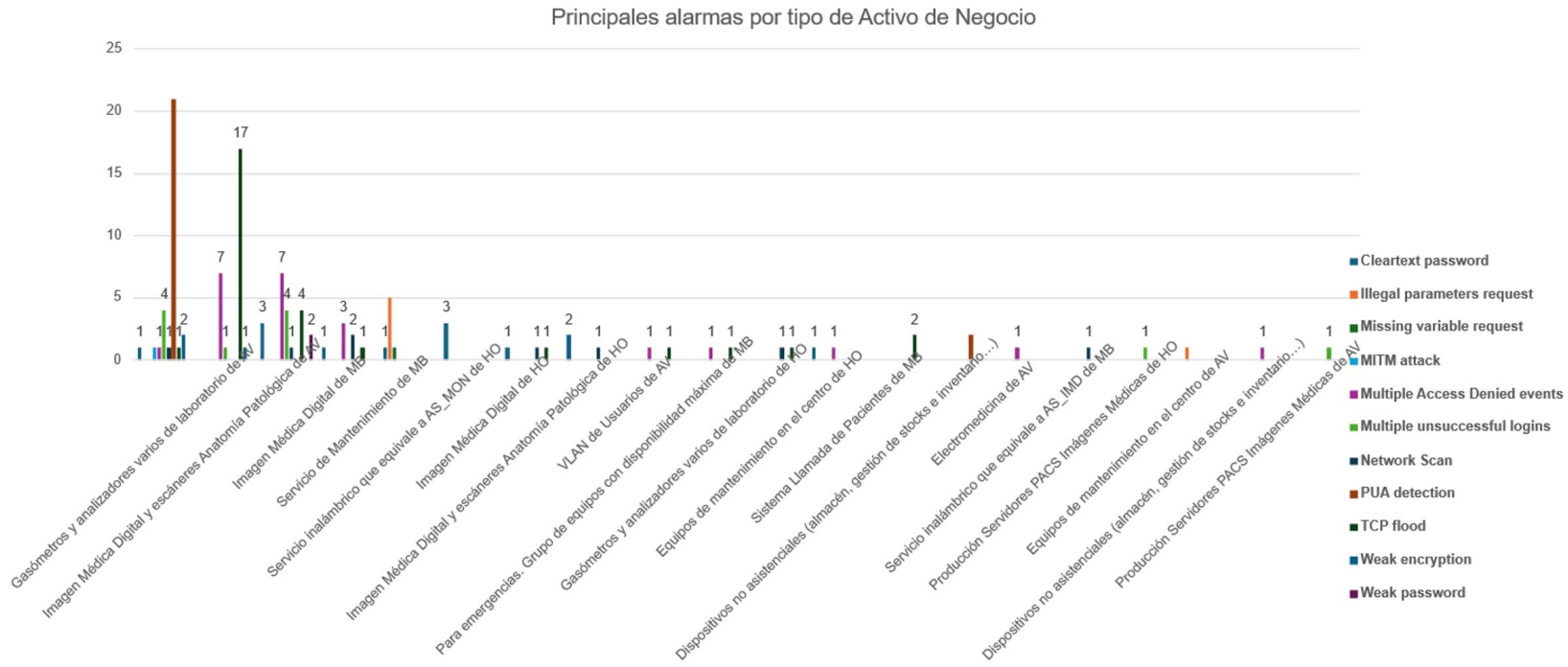
- Cuadros de mando e informes a golpe de click organizados por activo de negocio y por criticidad para la organización



Operaciones de Seguridad

3 - Incidencia en un entorno enriquecido





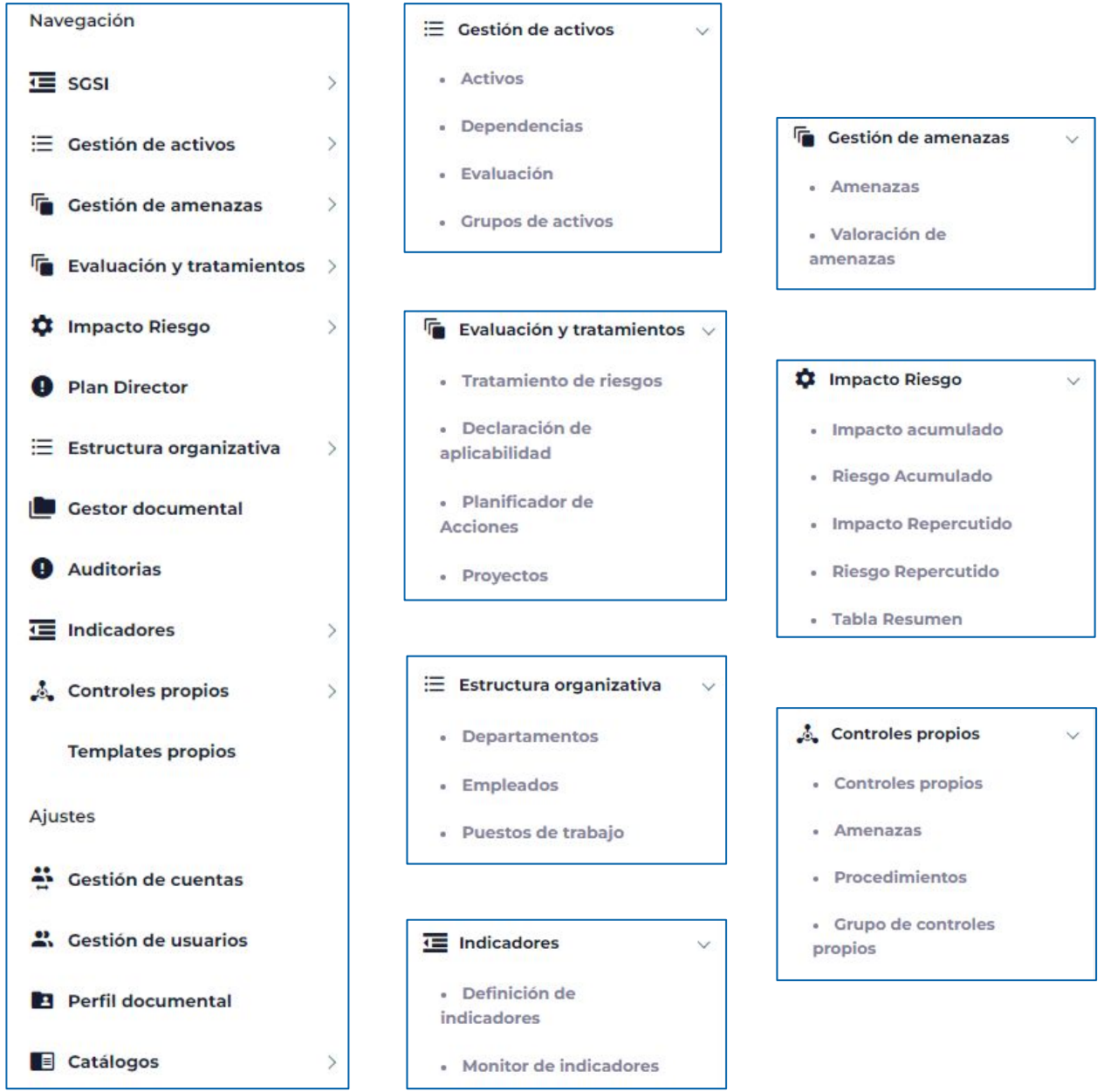
La alarma viene enriquecida con información de negocio (Equipos de imagen digital, anatomía patológica) y los riesgos previamente identificados (acceso no autorizado, posible fuga de información), así como acciones previstas y responsables (control “Gestión de la Configuración” pendiente en dicho equipo por Responsable1 en la fecha DD/MM/AA). Los informes salen personalizados por cliente y negocio (permite cargar plantillas).

Difusión restringida externa

Gestión de Seguridad

1 - Implantación un Sistema de Gestión

- Se debe implantar un **SGCI** que asegure la mejora continua de la ciberseguridad
- Con **SIRENA**, al consultor de apoyo, al **CISO** y al **CTO** le es muy fácil seguir punto por punto la norma y asegurar una correcta implantación en cada una de sus fases **PLAN-DO-CHECK-ACT** gracias a Nozomi
- El interfaz está personalizado para **ISO 27001/NIS2/ENS/IEC62443** y para Operaciones con **SIEMs** y **Cyber-physical systems protection-CPS** .



Difusión restringida externa

Gestión de Seguridad y Cumplimiento

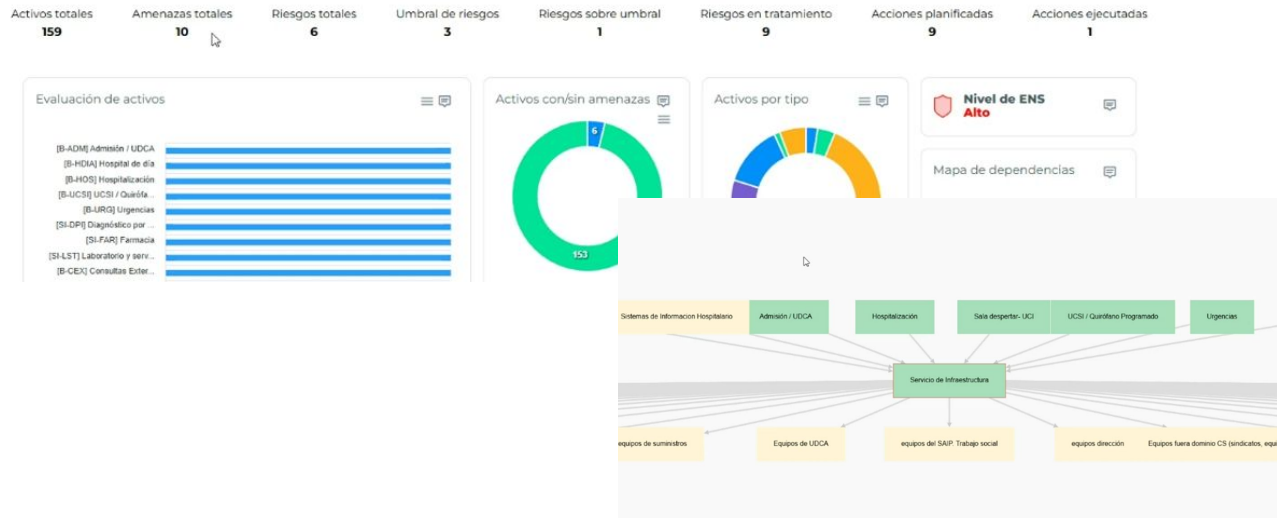
2 - Análisis y Gestión de Riesgos

En las normas y esquemas que requieren un análisis de riesgos, este módulo permite siguiendo el análisis cualitativo de MAGERIT:

1. Identificación de activos.
2. Identificación dependencias entre activos.
3. Valoración del activo en cada una de sus dimensiones y categorización de Sistemas
4. Selección conjunta de amenazas que pueden afectar a cada activo.
5. Valoración de las amenazas.
6. Aplicar un Plan de tratamiento de Riesgos
7. Controles automáticos según compliance.
8. Seguimiento

Integrable con PILAR, comparte metodología y catálogos

EAR / PILAR

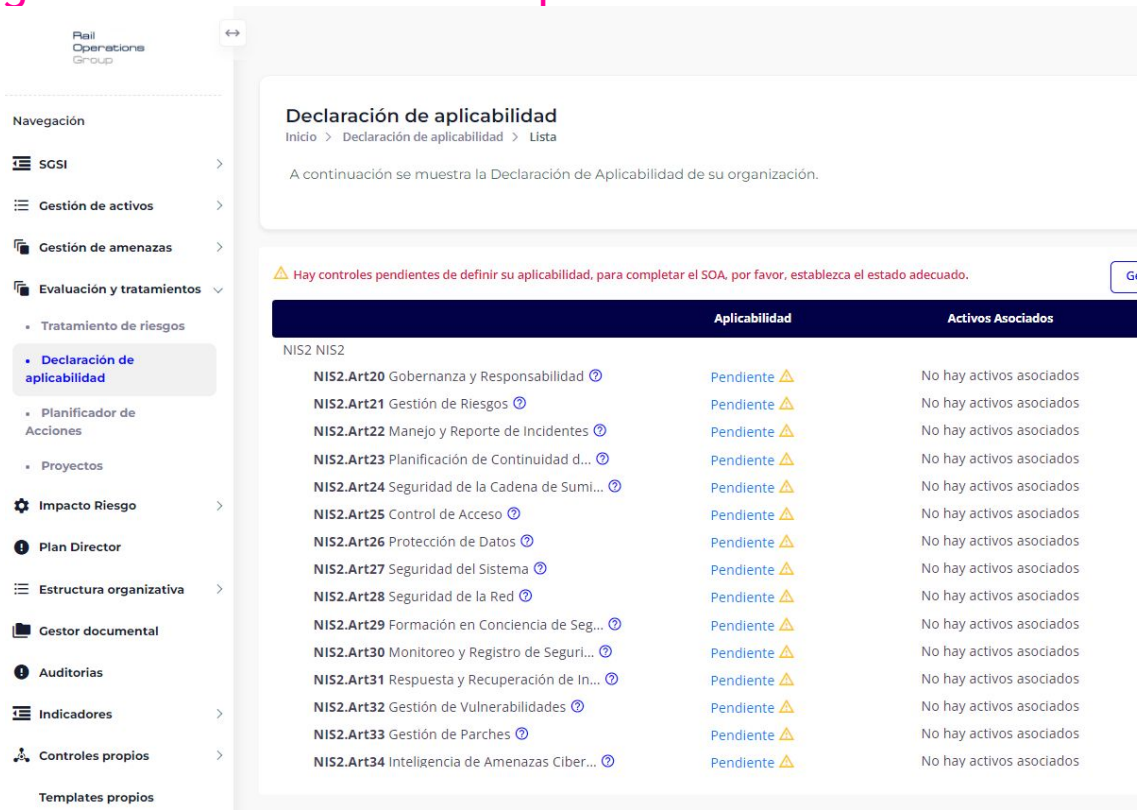


3 - Implantación de marcos normativos (NIS2, ENS…), en definitiva de controles de seguridad, basados en el riesgo REAL del entorno de operaciones

Difusión restringida externa

Gestión de Seguridad y Cumplimiento

3 - Implantación de marcos normativos (NIS2, ENS…), en definitiva de controles de seguridad, basados en el riesgo REAL del entorno de operaciones



Difusión restringida externa

Gestión de Seguridad y Cumplimiento

4 - Trazabilidad entre activo – vulnerabilidad – amenaza – alertas - tratamiento – control NIS2/ENS/ISO27001/ISA-IEC 62443

Activo	Amenaza	Riesgo repercutido	Riesgo residual actual	Acciones	Riesgo residual esperado	Estado	
[E-PC-LAB] equipos laboratorio	[A.14] Interceptación de información (escucha)	9.6	9.6	0/1	0.9		Tratar el Riesgo
[SI-SDI] Servicio de Infraestructura	[E.20] Vulnerabilidades de los programas (software)	8.2	8.2	0/1	4.1		Tratar el Riesgo
[SI-SDI] Servicio de Infraestructura	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3.1	3.1	0/1	1.1		Tratar el Riesgo
[E-AS_IMD2] Imagen Médica Digital y escáneres Anatomía Patológica	[A.11] Acceso no autorizado	2.1	2.1	0/1	2.1		Tratar el Riesgo
[E-AS_IMD2] Imagen Médica Digital y escáneres Anatomía Patológica	[A.8] Difusión de software dañino	2	2	0/1	0.7		Tratar el Riesgo
[COM-HAV-WMANT] Servicio inalámbrico para empresas de mantenimiento	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1.7	1.7	-	1.7		Tratar el Riesgo
[COM-HAV-WMANT] Servicio inalámbrico para empresas de mantenimiento	[A.11] Acceso no autorizado	1.6	1.6	0/1	0.4		Tratar el Riesgo
[E-AS_ELECTROMEDICINA] Electromedicina	[A.11] Acceso no autorizado	1.1	1.1	0/1	0.4		Tratar el Riesgo
[E-AS_IMD2] Imagen Médica Digital y escáneres Anatomía Patológica	[E.14] Escapes de información	0.7	0.7	0/1	0.7		Tratar el Riesgo
[E-CPD-OTR] Firewall, gestor ancho de banda	[A.11] Acceso no autorizado	0.2	0.2	0/1	0.1		Tratar el Riesgo

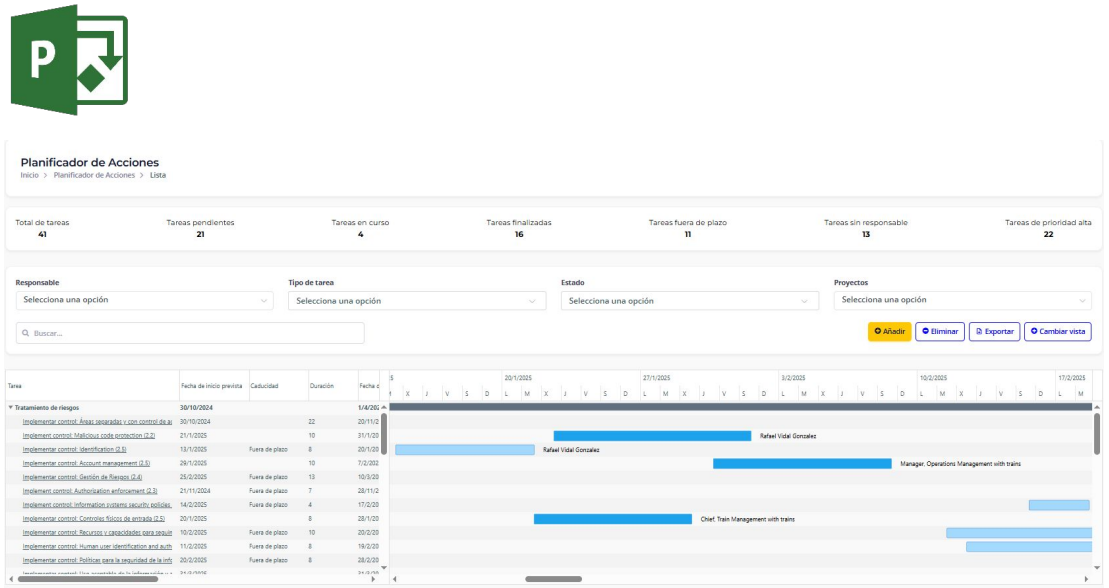
Difusión restringida externa

Estrategia de Seguridad

5 - Plan de Mejora de la Seguridad basado en incidencias detectadas en Operaciones (SOC)

Plan de acciones

- Plan de acciones asociado a resolución de incidencias OT
- Controles de seguridad a implantar para cumplimiento normativo
- Plan de acciones asociado a las No Conformidades de auditorías



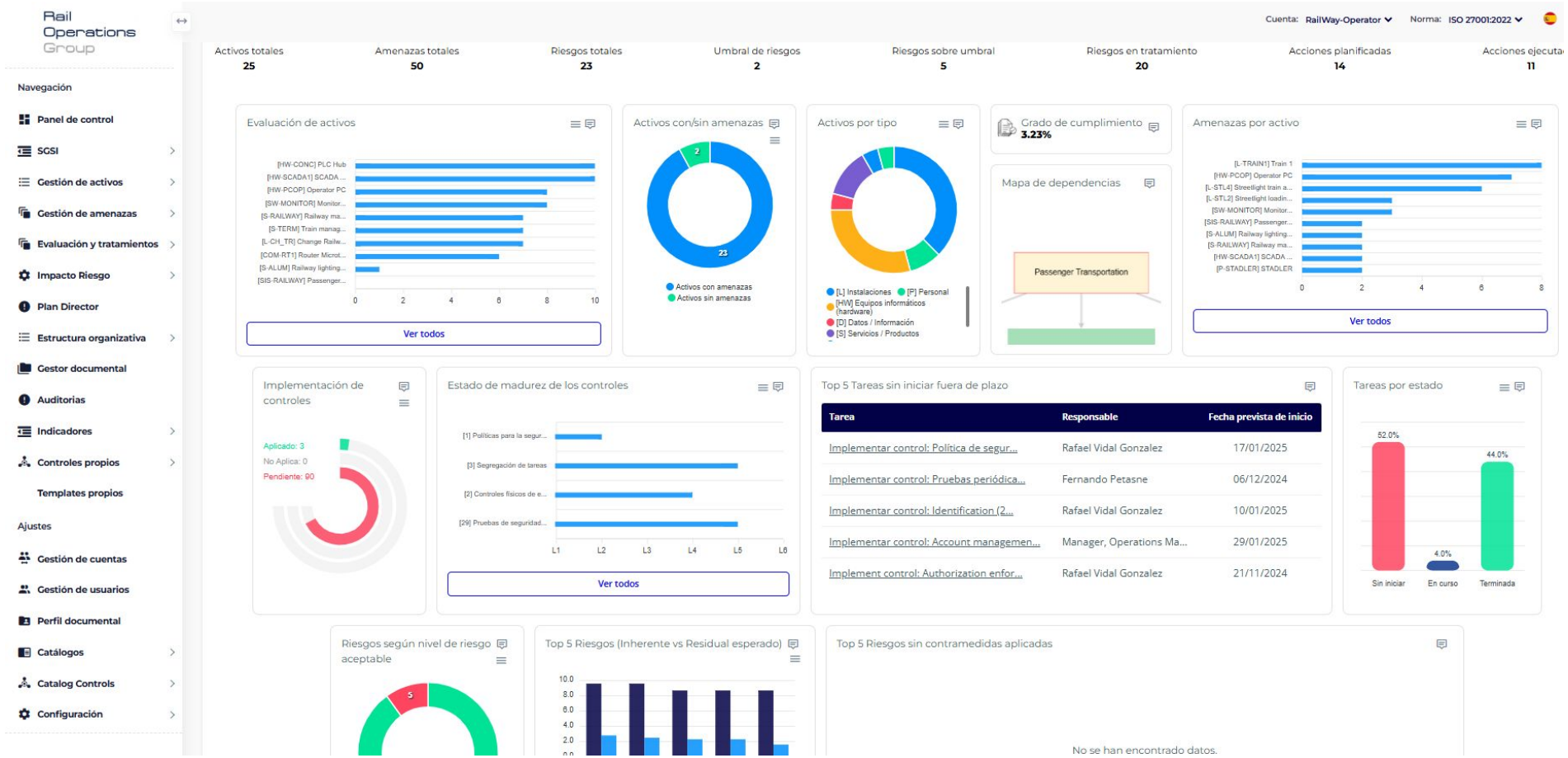
Seguimiento de acciones

- Notificaciones automáticas a los responsables de acciones.
- Cierre automático de acciones desde el correo
- Notificación al consultor de las acciones de sus clientes

Difusión restringida externa

Cuadros de mando

6 – Cuadro de mando de Gestión y Cumplimiento con trazabilidad de operaciones /Alertas



Difusión restringida externa

Modelo de negocio

Valor para partners y clientes finales

04

Difusión restringida externa

Enriquecimiento de servicios

Servicios para un partner

Proyecto de integración

Poder ofrecer un Servicio integrado de cumplimiento, gestión y operación (Oficinas técnicas).

Servicio de operación de incidencias de entorno IT/OT

- Servicio de atención a incidencias enriquecidas con datos de negocio

- Mejor entendimiento de la incidencia y mejora en el tiempo de resolución

Servicio de gestion de la seguridad y mejora continua

-Eficiencia en elaboración e informes (Ahorro de costes). Seguimiento del Plan Director de Seguridad

- Seguimiento del Plan de Tratamiento de Riesgos dinámico basado en alertas. Maximizar conocimiento de los activos.

Nuestro objetivo

-Facilitar la labor al integrador y enriquecer su oportunidad de servicios al cliente

Difusión restringida externa

Propuesta económica para Partners/Integradores

Licencias SIRENA: Integradores de Valor Añadido (VAR)

- La plataforma SIRENA se licencia por activos gestionados (los potenciales activos a enriquecer de las sondas de bajo nivel con las que sincroniza)
- Sin límite de usuarios accediendo a la plataforma (CTO, CISO, cualquiera con activos y acciones asignadas)
- Descuentos para compañías por encima de 5.000 activos
- Se facilita una OVA para on premise, o una instancia para SasS
- Licencia personalizada para demandas especiales (p.e. desarrollos o integraciones a medida)

Descuento para integradores de 20 a 40%

Difusión restringida externa

Propuesta económica para Integradores

Precio por cliente:

Organización	Activos	Importe cliente final
SME	< 5.000	1 €/activo/mes
Grandes cuentas	> 5.000	0.7 €/activo/mes
Demandas especiales	Bajo presupuesto	

Descuento para Distribuidor de Valor añadido:

Licencias para cliente final	Descuento por licencias
1er cliente	20%
1<5 clientes	25%
5<10 clientes	30%
> 10 clientes	40%

Difusión restringida externa

Más información

Enlaces

Puedes consultar el webinar y una demo en el entorno Sirena en los siguientes enlaces además de consultar a través de nuestra página web:

https://youtu.be/BYaXAs9asZQ

https://singlarinnovacion.com/productos/sirena/

Difusión restringida externa

SINGLAR
Innovación

SIRENA®

¡Gracias!

Difusión restringida externa