



G·CONSULTING
COMPLIANCE

<https://gconsultingcompliance.com/>



Índice

01 Introducción

02 Funcionalidades

03 Informes

04 Razones de uso

05 Otros productos
Ámbito Ciberseguridad

06 Catálogo general
Producto propio



Introducción

GConsulting Compliance

01

Centraliza tu cumplimiento normativo y ciberseguridad en una única plataforma ágil que funciona como un vCISO.

Automatiza controles, mantiene actualizado tu plan maestro de ciberseguridad y se adapta a ISO 27001, HIPAA, NIS2 o NIST.

Desde una sola interfaz obtienes trazabilidad completa de vulnerabilidades, amenazas, riesgos, controles y acciones de remediación.

- **Gestión de cumplimiento simplificada, centralizada y automatizada para una toma de decisiones más efectiva.**
 - Cumple con estándares de privacidad como el GDPR, la Directiva NIS2 y otras regulaciones clave desde una única plataforma que guía todo el proceso, desde la identificación de obligaciones hasta la implementación de medidas.
- **Plan Maestro de Ciberseguridad automatizado para reducir los costos operativos.**
 - GConsulting genera y mantiene tu plan de ciberseguridad actualizado como lo haría un vCISO, con recomendaciones personalizadas, controles por sector y una hoja de ruta clara.
 - Evalúa los riesgos en tiempo real y adapta tus medidas a marcos como ISO 27001, NIST o NIS2.
- **Realiza un seguimiento de la seguridad de tu organización fácilmente con alertas automáticas en caso de desviaciones.**
 - Los dashboards te permiten tener una visión clara del estado de cumplimiento en cada área de la organización y estar preparado para cualquier auditoría.

Gestión de cumplimiento normativo

ENS - RGPD - ISO 27001 - NIS 2 - DORA

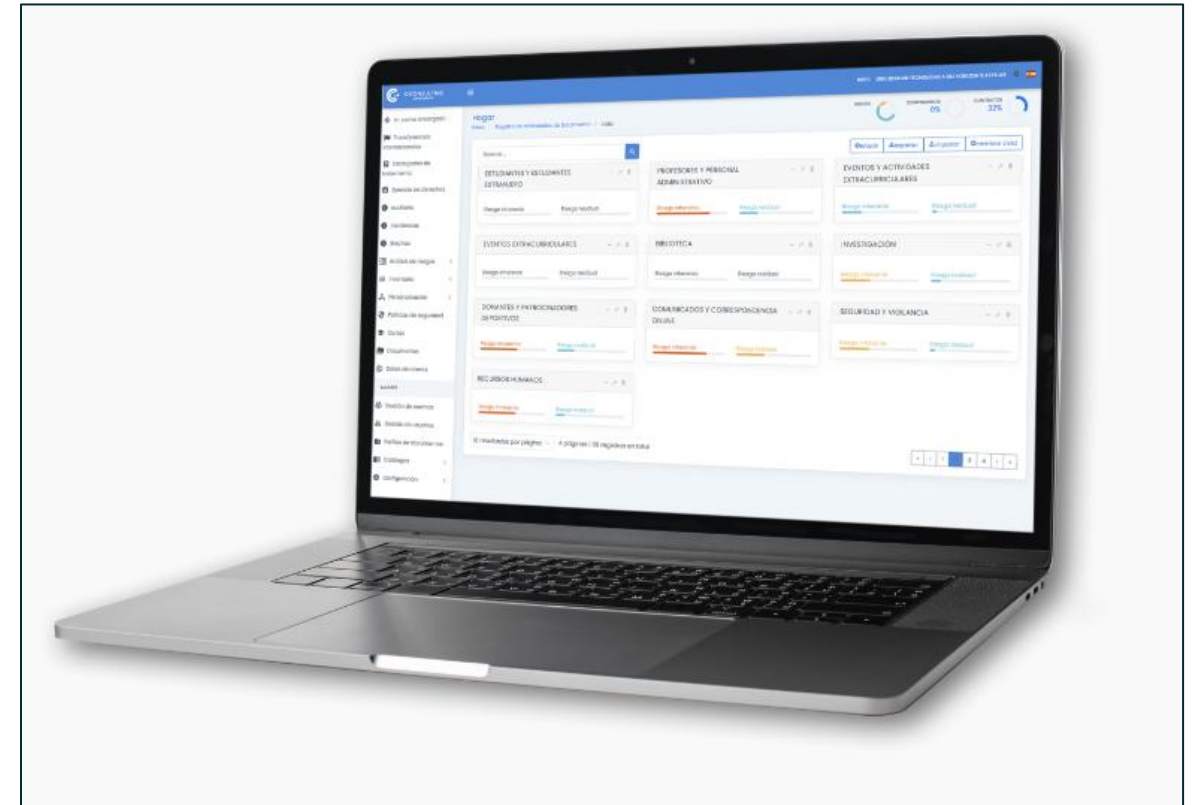
GConsulting proporciona una visión global y detallada de todos los aspectos relacionados con el gobierno, el riesgo y el cumplimiento de tu empresa presentando de forma centralizada la información más importante.

Estándares de buenas prácticas

Un estándar ISO es una estructura probada para la gestión y mejora continua de la calidad, respeto al entorno, seguridad, fiabilidad, eficiencia e interoperabilidad en una organización”



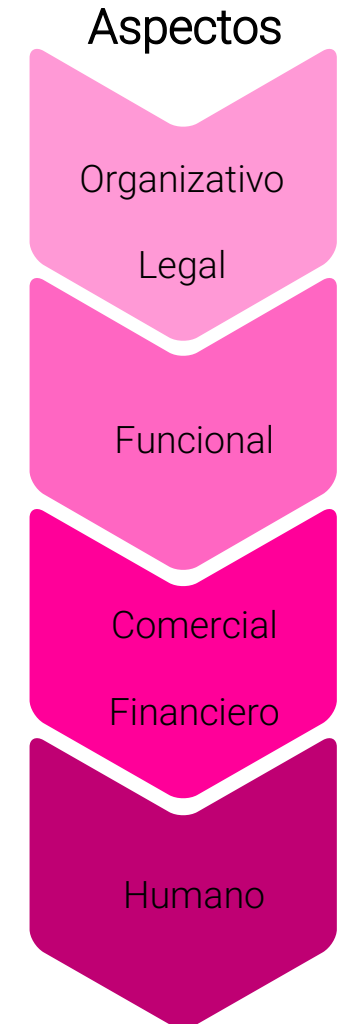
International
Organization for
Standardization



Herramienta de apoyo a la consultoría

Sistemas de Gestión: Beneficios para la empresa

- Metodología de gestión de seguridad clara y estructurada.
- Seguridad garantizada en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Integración de los diversos sistemas de gestión (ISO 19600, ISO 27001, RGPD, ENS...).
- Continuidad de las operaciones.
- Conformidad con la legislación vigente.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Reduce costes y mejora los procesos y servicios.
- Proporciona confianza y reglas claras al personal de la organización.
- Aumenta la motivación y satisfacción del personal.

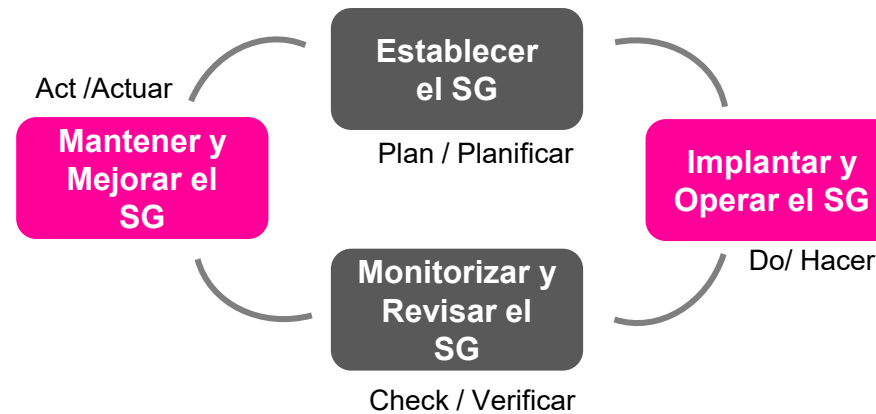


Modelo PDCA (Plan, Do, Check, Act)

Sistemas de Gestión

Definir el alcance del SG
 Definir la política del SG
 Análisis y gestión del riesgo
 Declaración de Aplicabilidad

Adoptar acciones preventivas y correctivas
 Implantar las mejoras propuestas
 Comunicar las mejoras
 Verificar que las mejoras cumplen su objetivo



Implantar controles seleccionados
 Implantar el Sistema de Gestión
 Indicadores y métricas
 Formación y concienciación

Establecimiento de registros
 Revisar regularmente el SG
 Auditar internamente el SG

Dificultades de Implantación

Apoyo a la consultoría

- Complejidad técnica y organizativa de las normas.
- Elevado volumen de documentación y necesidades de estructuras documentales específicas
- Se requieren conocimientos avanzados en múltiples materias
- No existe un modelo de implementación claramente establecido
- Requisitos específicos según la norma de referencia (Ej: la RGPD o ENS exige la aplicación de una metodología de Análisis y Gestión de Riesgos que es compleja y difícil de implementar)
- Mantenimiento de los registros complejo
- Gestión de indicadores compleja
- Burocracia excesiva
- Necesidad de automatizar la Gestión de los Sistemas

NECESIDAD DE UNA HERRAMIENTA QUE GUIE AL CONSULTOR Y A LA ORGANIZACIÓN DURANTE TODO EL PROCESO

Herramienta de implantación

Solución integral

GConsulting proporciona una solución integral para consultores y empresas a la hora de implementar y gestionar un Sistema de Gestión, facilitando las dificultades anteriormente expuestas.

GConsulting es una herramienta para la implantación y el seguimiento del Ciclo Completo de Sistemas de Gestión en la que destacan las siguientes características:

- Implantación de normas.
- Gestión documental.
- Análisis de Riesgos.
- Integración con el entorno



Módulos de cumplimiento principales

Integraciones

Plan Director de Seguridad Asistido y Proactivo

Sistemas de Gestión para el Cumplimiento



RGPD



Esquema Nacional de Seguridad



Sistema de Gestión de Seguridad de la Información



Plan Director de Seguridad: NIS2, DORA



Ciber Industrial



INTEGRACIONES

Sistema de Gestión de la Privacidad

RGPD y Herramientas integradas

GConsulting RGPD Incluye:



- Gestión de consultores y clientes
- Gestor documental
- Ciclo de revisión de los Sistemas
- Asistente en implantación de normas (RGPD y controles)
- Análisis diferencial (Con respecto a controles del reglamento)
- Recursos Humanos y Responsabilidades
- Módulo de Auditorías
- Gestor de Proyectos (Plan Implantación de Controles y Plan del Tratamiento del Riesgo)

Módulos específicos del Sistema de Gestión de la Privacidad

- PIA (Plan Impact Assesment)
- Integración con Análisis y Gestión de Riesgos PILAR
- Plan del Tratamiento del Riesgo inteligente
- Documentación asociada (cláusulas, contratos, tratamientos...)
- Controles de privacidad a implantar
- Seguimiento de acciones y métricas, sistema de alertas

Gestor de proyectos avanzado



Inventario de activos y tratamientos



Gestor documental



Gobierno, Riesgo y Cumplimiento (GRC)



Help Desk o gestor de Incidencias



Cuadros de Mando (servidor de informes)



INTEGRACIONES

Gestión Avanzada de Seguridad de la Información

ISO 27001 y Herramientas integradas

GConsulting SGSI incluye:

- Gestión de consultores y clientes
- Gestor documental
- Ciclo de revisión de los Sistemas
- Asistente en implantación de normas (SGSI y controles)
- Análisis diferencial (Con respecto a controles de la norma)
- Recursos Humanos y Responsabilidades
- Módulo de Auditorías
- Gestor de Proyectos (Plan Implantación de Controles y Plan del Tratamiento del Riesgo)



Módulos específicos del Sistema de Gestión de Seguridad de la Información

- Análisis de Riesgos
- Integración con Análisis y Gestión de Riesgos PILAR
- Plan del Tratamiento del Riesgo inteligente
- Declaración de Aplicabilidad (Controles ISO27002, CobIT)

Gestor de proyectos avanzados



CMDB automática y manual



Gestor documental



Gobierno, Riesgo y Cumplimiento (GRC)



Help Desk o gestor de Incidencias



Gestión de los SLAs Monitorización



Gestión logs



Cuadros de Mando Servidor informes



Autentica Certificado CAS



INTEGRACIONES

Adaptación al Esquema Nacional de Seguridad al completo

ENS, SGSI y Herramientas integradas de gestión

GConsulting ENS incluye:



- Gestión de consultores y clientes
- Gestor documental
- Ciclo de revisión de los Sistemas
- Asistente en implantación de normas (SGSI Asociado al ENS)
- Análisis diferencial (Guía CCN-STIC 808)
- Recursos Humanos y Responsabilidades (Guías CCN-STIC 801 y 805)
- Módulo de Auditorías (Guía CCN-STIC 802 y Guía CCN-STIC 809)
- Gestor de Proyectos (Plan de implantación de las Medidas de Seguridad y del Plan del Tratamiento del Riesgo)

Módulos específicos del Esquema Nacional de Seguridad

- Categorización de Sistemas (Guía CCN-STIC 803)
- Integración Análisis y Gestión de Riesgos PILAR
- Plan del Tratamiento del Riesgo inteligente
- Medidas de Seguridad (Guía CCN-STIC 804)
- Plan de Adecuación al ENS (Guía CCN-STIC 806)

Seguridad de la Información

- Análisis de Riesgos
- Declaración de Aplicabilidad (Controles Anexo II, CobIT)
- Nivel de aceptación del Riesgo

Gestor de proyectos avanzados



CMDB automática y manual



Gestor documental



Gobierno, Riesgo y Cumplimiento (GRC)



Help Desk o gestor de Incidencias



Gestión de los SLAs Monitorización



Gestión logs



Cuadros de Mando Servidor informes



Autentica Certificado CAS



INTEGRACIONES

Sistemas de Gestión de Ciberseguridad Industrial

ISA 62443 y SGCI

GConsulting SGCI Incluye:

- Gestión de consultores y clientes
- Gestor documental
- Ciclo de revisión de los Sistemas
- Asistente en implantación de normas (SGCI, 62443-3-2)
- Análisis diferencial (Con respecto a todos los aspectos de la norma)
- Recursos Humanos y Responsabilidades
- Módulo de Auditorías
- Gestor de Proyectos (Plan Implantación de la norma)



Módulos específicos del Sistema de Gestión de Ciberseguridad Industrial

- Análisis de Riesgos industriales
- Plan del Tratamiento del Riesgo inteligente
- Declaración de Aplicabilidad (Controles 62443-3-3)

Help Desk o gestor de Incidencias

Gestor documental

Gestión de los indicadores

Cuadros de Mando (servidor de informes)

INTEGRACIONES





Funcionalidades

G-Consulting

02

Descripción General

G-Consulting

- Lugar de encuentro entre consultores, empresa, y los equipos de trabajo que se relacionan con los Sistemas de Gestión.
- Gestión a través de Web para acceso desde cualquier lugar por cualquier perfil.
- Portal personalizado según el perfil de acceso.

La autenticación se puede integrar con Sistemas Abiertos (CAS) o con Certificados de Usuario como el DNle

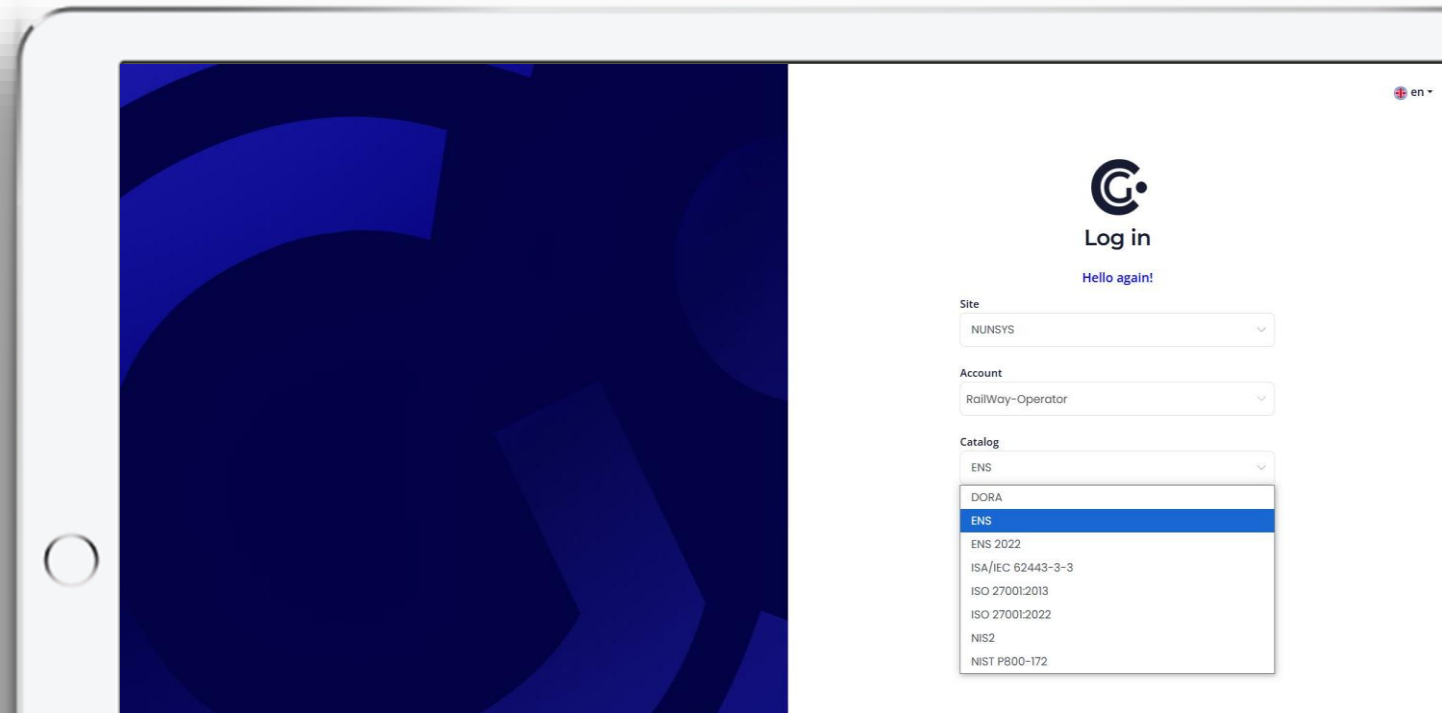


Funcionalidades

Herramienta para el Cumplimiento Normativo

- RGPD (Sistema de Gestión de la Privacidad)
- ENS (Esquema Nacional de Seguridad)
- ISO 27001 Sistema Gestión de Seguridad de la Información)
- Análisis y Gestión de Riesgos conforme MAGERIT
- Plan Director de Seguridad (NIS2, DORA, otras)
- ISO 62443:3-3 (Ciberseguridad Industrial)
- Otros Sistemas de Gestión

Su gestor documental permite adaptarse a cualquier normativa



Funcionalidades

Diagnóstico Diferencial

- Diagnóstico de situación control a control contra los dominios de la norma bajo análisis.
- Comparativas evolutivas respecto de evaluaciones anteriores.
- Comparativas respecto del sector.
- Generación de informes de resultados
- Automatizados.

Assets groups
Home > Assets groups > List
Management of groups used to organize assets.

Code	Name	Activity type
<input type="checkbox"/> SIS	Information system	[SIS] System
<input type="checkbox"/> ORGF	Organization functions	[SP] Services product
<input type="checkbox"/> ENV	Environment	[I] Installations
<input type="checkbox"/> EQ	Equipment	[HW] Hardware

4 records in total

Assets groups
Home > Assets groups > Edit

Information system

Asset group

Code: Name:

Activity Type: Parent Group:

Informe diagnóstico del ENS conforme a la guía CCN-STIC 808

Declaración de aplicabilidad

Inicio > Declaración de aplicabilidad > Lista

A continuación se muestra la Declaración de Aplicabilidad de su organización.

⚠ Hay controles pendientes de definir su aplicabilidad, para completar el SOA, por favor, establezca el estado adecuado.

	Aplicabilidad	Activos Asociados
1 Disposiciones digitales		
1.1 Objeto	Pendiente ⚠	No hay activos asociados
1.2 Ámbito de aplicación	Pendiente ⚠	No hay activos asociados
1.3 Definiciones	Pendiente ⚠	No hay activos asociados
1.4 Principio de proporcionalidad	Aplica ☑	Asociados 24 activos
2 Gestión del riesgo relacionado con las T...		
2.5 Gobernanza y organización		
2.5.1 Marco interno de gobernanza y ...	Pendiente ⚠	No hay activos asociados
2.5.2 Órgano de dirección	Pendiente ⚠	No hay activos asociados
2.5.3 Gestión de terceros	Pendiente ⚠	No hay activos asociados
2.5.4 Formación de la dirección	Pendiente ⚠	No hay activos asociados
2.6 Marco de gestión del riesgo relacionado ...		
2.6.1 Marco interno de gestión del r...	Aplica ☑	Asociados 24 activos
2.6.2 Alcance del marco de gestión d...	Pendiente ⚠	No hay activos asociados
2.6.3 Enfoque de minimizar los riesg...	Pendiente ⚠	No hay activos asociados
2.6.4 Control y gestión del riesgo	Pendiente ⚠	No hay activos asociados

Funcionalidades

Diagnóstico Diferencial

- ▼ Diagnóstico Inicial
- Nuevo Diagnóstico
- Continuar Diagnóstico
- Comparar Diagnóstico
- Recuperar Diagnósticos
- ▼ Usuarios
- Listado de Usuarios

Plan > Diagnóstico y Empresa > Nuevo Diagnóstico

Aspectos Organizativos de la Seguridad de la Información

¿Existe personal asignado para coordinar los aspectos relacionados con la seguridad de la información? ¿Dicha asignación es formal?

- Muy Alto
 Alto
 Medio
 Bajo
 Muy bajo

Hallazgos/Observaciones

¿Está la Dirección de la organización implicada en las iniciativas y proyectos de seguridad de la información? ¿Se realizan comités de seguimiento de seguridad periódicamente?

- Muy Alto
 Alto
 Medio
 Bajo
 Muy bajo

Hallazgos/Observaciones

¿Se firman acuerdos de confidencialidad con los empleados de la entidad? ¿Se revisa periódicamente que han sido firmados por todos los empleados?

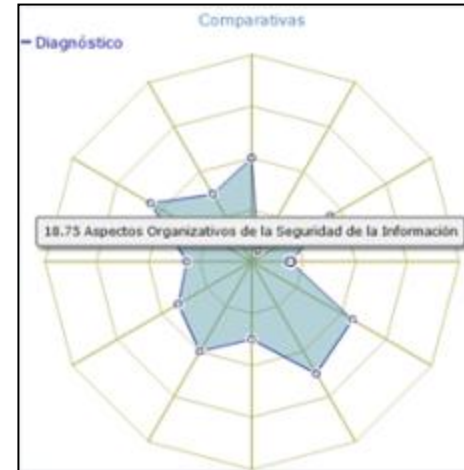
- Muy Alto
 Alto
 Medio
 Bajo
 Muy bajo

Hallazgos/Observaciones

¿Se realizan revisiones o auditorías externas a intervalos planificados o cuando se producen cambios significativos que afectan a la seguridad de la información?

- Muy Alto
 Alto
 Medio
 Bajo
 Muy bajo

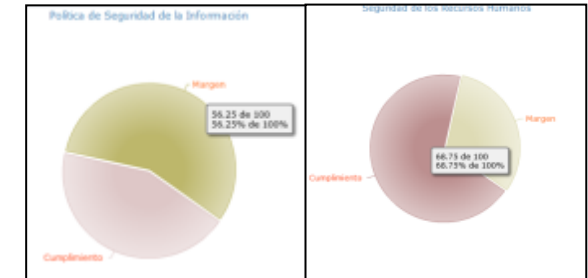
Hallazgos/Observaciones



EL RESULTADO DE SU DIAGNÓSTICO INICIAL HA SIDO...

dominio	↑↓	resultado	↑↓
Política de Seguridad de la Información		62.5	
Aspectos Organizativos de la Seguridad de la Información		37.5	
Gestión de Activos		50.0	
Seguridad de los Recursos Humanos		68.75	
Seguridad Física y Ambiental		68.75	
Gestión de Comunicaciones y Operaciones		50.0	
Control de Acceso		0.0	
Adquisición, Desarrollo y Mantenimiento de los Sistemas		62.5	
Gestión de Incidentes de Seguridad		43.75	
Gestión de la Continuidad del Negocio		75.0	
Cumplimiento		62.5	

Total: 53.0



Nombre: ISO 27001

Política de Seguridad de la Información Cumplimiento: 100%

La empresa presenta un cumplimiento medio respecto a los requisitos de Política de Seguridad de la Información según la norma ISO 27001. Bajo el nivel de que se elabora de una política de seguridad, que está documentada. Asimismo, se realiza una auditoría de conformidad con la política de seguridad y auditorías de seguridad, aunque existen aspectos mejorables en la seguridad de la norma.

Algunas acciones para el mejoramiento de la norma son:

- Documentar la política de seguridad de la información.
- Revisar la política de seguridad de la información.

Política de Seguridad de la Información

Cumplimiento: 100%

Aspectos Organizativos de la Seguridad de la Información Cumplimiento: 37.5%

La empresa presenta un cumplimiento medio respecto a los requisitos de Aspectos Organizativos de la Seguridad de la Información según la norma ISO 27001. Actualmente esto se hace a que el Director de la Empresa se encarga de revisar el plan de seguridad de la información pero no se realiza de manera formal. Tal vez se forme que se realice de forma formal un comité de seguimiento de la seguridad de la información y que se realice auditorías de conformidad con la norma ISO 27001. En cuanto a la realización de Auditorías externas de seguridad de la información, se tiene que se realiza cuando se ven la necesidad y cuando se debe.

Algunas acciones para el mejoramiento de la norma son:

- Crear un comité de gestión de seguridad de la información.
- Asignar responsabilidades relativas a la seguridad de la información.
- Realizar auditorías de conformidad con la norma ISO 27001.
- Realizar Auditorías externas respecto a la seguridad de la información.
- Controlar el acceso de terceros de seguridad de la información.

Aspectos Organizativos de la Seguridad de la Información

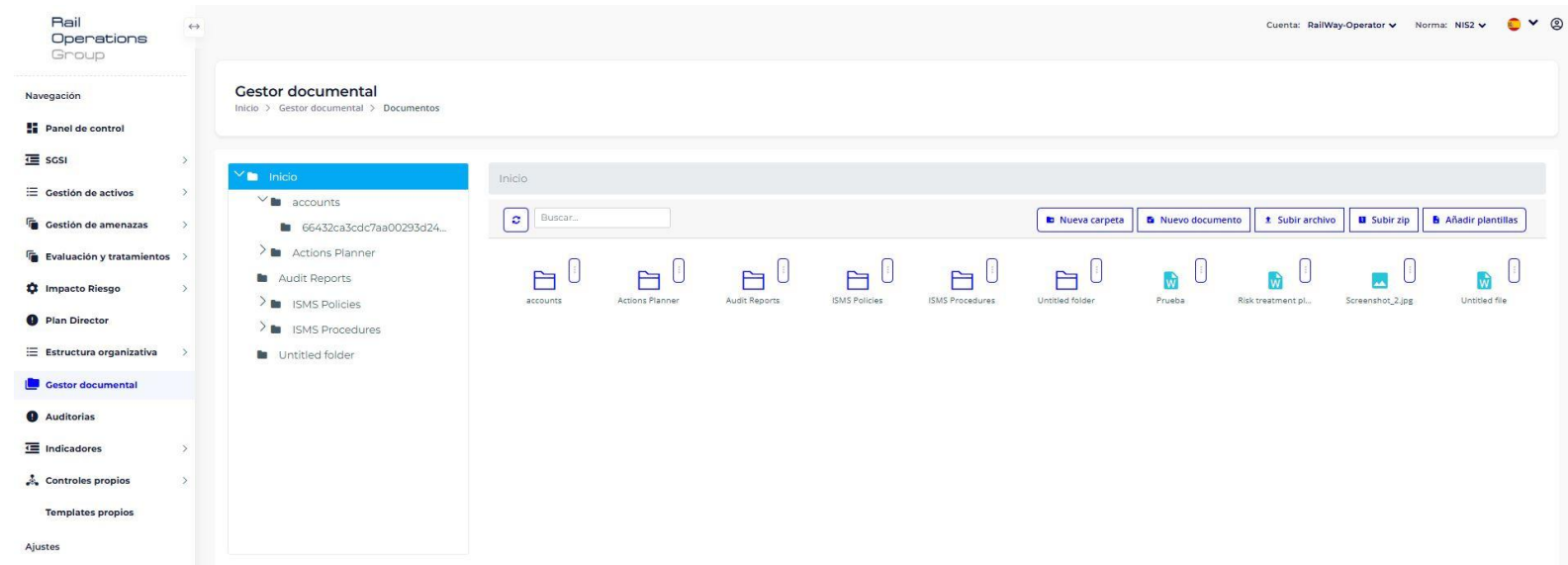
Cumplimiento: 37.5%

Funcionalidades

Documentación de los Sistemas de Gestión

- Incorpora pre-cargado un sistema de Gestión Completo para la norma bajo Análisis (SGP, SGSI, ENS, SGC, etc.) validado por numerosas implantaciones y certificaciones exitosas.
- La documentación se edita y se particulariza a la situación de la entidad
- Edición y almacenamiento de todos los registros, informes, actas, no conformidades, etc. exigidos por la norma para implantar y certificar un sistema de gestión.

Fácil implantación de un Sistema de Gestión con documentación precargada

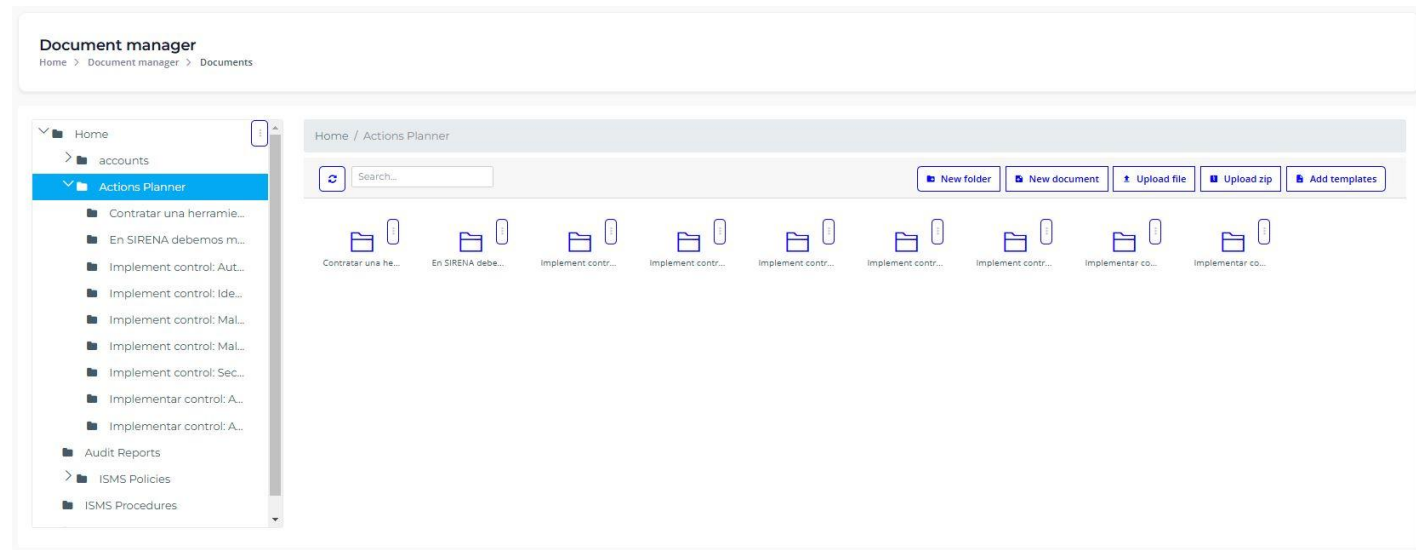


Funcionalidades

Gestor Documental

- Se pueden incorporar procedimientos y documentos externos (ofimáticos, por ejemplo) e incorporarlos al sistema de gestión.
- Permite realizar una gestión ordenada y coherente de la documentación asociada al Sistema de Gestión.
- Distintos roles y permisos para los flujos de aprobación de documentos.
- Control de versiones.

Se integra fácilmente con herramientas más complejas de gestión de documentación (CMS)



Funcionalidades

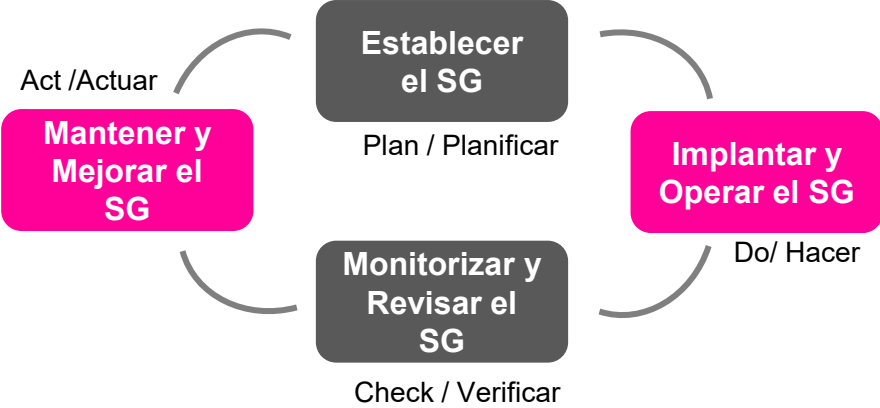
Asistente en Implantación de normas

- Adoptar acciones preventivas y correctivas
- Implantar las mejoras propuestas
- Comunicar las mejoras
- Verificar que las mejoras cumplen su objetivo

Fácil implantación de los registros de un Sistema de Gestión

MÓDULOS SEGÚN NORMA

- Definir el alcance del SG
- Definir la política del SG
- Análisis y gestión del riesgo
- Declaración de Aplicabilidad



MÓDULOS SEGÚN NORMA

- Implantar controles seleccionados
- Implantar el Sistema de Gestión
- Indicadores y métricas
- Formación y concienciación

- Establecimiento de registros
- Revisar regularmente el SG
- Auditar internamente el SG

Funcionalidades

Asistente en Implantación de Normas

- De esta manera, al consultor y al cliente 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
- El interfaz está personalizado según el o los Sistema de Gestión integrados que la empresa dispone.

Navegación

- SGSI >
- Gestión de activos >
- Gestión de amenazas >
- Evaluación y tratamientos >
- Impacto Riesgo >
- Plan Director
- Estructura organizativa >
- Gestor documental
- Auditorías
- Indicadores >
- Controles propios >
- Plantillas propios
- Ajustes
- Gestión de cuentas
- Gestión de usuarios
- Perfil documental
- Catálogos >

Gestión de activos

- Activos
- Dependencias
- Evaluación
- Grupos de activos

Evaluación y tratamientos

- Tratamiento de riesgos
- Declaración de aplicabilidad
- Planificador de Acciones
- Proyectos

Estructura organizativa

- Departamentos
- Empleados
- Puestos de trabajo

Indicadores

- Definición de indicadores
- Monitor de indicadores

Gestión de amenazas

- Amenazas
- Valoración de amenazas

Impacto Riesgo

- Impacto acumulado
- Riesgo Acumulado
- Impacto Repercutido
- Riesgo Repercutido
- Tabla Resumen

Controles propios

- Controles propios
- Amenazas
- Procedimientos
- Grupo de controles propios

Funcionalidades

Recursos Humanos y Responsabilidades

- GConsulting está dotado de un potente gestor de Recursos Humanos, exigido por cualquier norma.
- Este módulo permite:
 - Volcar un organigrama, definir departamentos, puestos y roles
 - Asignar funciones y responsabilidades al personal, segregación de funciones
 - Dotar de acceso y personalización del entorno de gestión para cada perfil.

Cumple los puntos exigibles por norma de Recursos Humanos, Formación, Segregación de Funciones y Responsabilidades

The screenshot displays a tablet interface for managing employees. The page title is "Employees" with a breadcrumb "Home > Employees > Edit". The employee's name "Rafael" is shown at the top. Below this, there are two tabs: "Data" (selected) and "Documents". Under the "Data" tab, there is an "Information" section with the following fields:

- Name: Rafael
- Lastname: Vidal Gonzalez
- DNI: [Empty]
- Phone: 610297346
- Email: rafael.vidal@singlarinnovacion.com
- GDPR Information: Yes No
- Job: Select an option... (dropdown menu)
- Department: Networks
- Figure: Select an option... (dropdown menu)
- Start working day: [Empty]
- Leaving day: [Empty]

At the bottom of the form, there are two expandable sections: "Personal Information" and "Internal Date Operation".

Funcionalidades

Módulo de auditorías

- GConsulting permite planificar las auditorías de los Sistemas de Gestión y desarrollarlas conforme a una o varias normas simultáneamente, permitiendo realizar de manera sencilla tanto auditorías internas como externas.
- Finalmente, el informe de auditorías alimenta al resto del sistema de modo que pueda gestionarse mediante un ciclo de mejora continua como exige cualquier Sistemas de Gestión.

Cumple los puntos exigibles por norma de Planificación y Seguimiento de Auditorías

The screenshot displays the 'Business Audits' form in the GConsulting system. The form is titled 'Business Audits' and includes a breadcrumb trail: 'Home > Business Audits > New'. It features three tabs: 'Data' (selected), 'Planification', and 'Evidences'. The 'Data' tab is divided into two sections: 'Information' and 'Ambit'. The 'Information' section contains the following fields: 'Framework to be audited', 'Object/scope', 'Chief auditor', 'Team', 'Start date', and 'End date'. The 'Status' field is a dropdown menu currently set to 'In progress'. The 'Ambit' section includes 'All the company' (Yes/No radio buttons), 'Areas/Department' (a dropdown menu with a plus icon), and 'Treatment activities' (a dropdown menu with a plus icon). At the bottom of the form, there are 'Cancel' and 'Save' buttons.

Funcionalidades

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. Determinar impacto/riesgo acumulado.
 7. Determinar impacto/riesgo repercutido.
 8. Elaboración del Plan de Adecuación al ENS

Integrable con PILAR,
comparte metodología
y catálogos

EAR /
PILAR

Valoración de amenazas
Inicio > Valoración de amenazas > Lista

A continuación debe valorar para cada activo la frecuencia con la que se verá afectado por la amenaza elegida, así como la degradación en cada dimensión del activo producida por dicha amenaza.

Buscar... Cambiar Frecuencia Se modificará en registros seleccionados. Despreciable Actualizar Vista Simplificada Importar Exportar

Activo	Frecuencia	Disponibilidad (D)	Integridad (I)	Confidencialidad (C)	Autenticidad (A)	Trazabilidad (T)
[SIS-RAILWAY] Passenger Transportation		50	50	0	0	0
[A.7] Intended Use	Despreciable	Medio	Medio	Ninguno	Ninguno	Ninguno
[A.11] Unauthorized access	Despreciable	Ninguno	Ninguno	Ninguno	Ninguno	Ninguno
[S-ALUM] Railway lighting service		100	50	0	0	0
[A.11] Unauthorized access	Frecuente	Alto	Medio	Ninguno	Ninguno	Ninguno
[E.1] User errors	Normal	Critico	Ninguno	Ninguno	Ninguno	Ninguno
[S-RAILWAY] Railway management service		10	0	0	0	0
[A.10] Sequence Alteration	Despreciable	Ninguno	Ninguno	Ninguno	Ninguno	Ninguno
[A.24] Denial of Service	Poco frecuente	Bajo	Ninguno	Ninguno	Ninguno	Ninguno
[BKP-BDD] Backup Base de datos		100	0	0	0	0
[E.19] Divulgación de información	Poco frecuente	Critico	Ninguno	Ninguno	Ninguno	Ninguno
[HW- Industrial network analysis and SIEM1] management device		0	0	0	0	0

Funcionalidades

Análisis y Gestión de Riesgos

Plan de acciones

- Plan de acciones asociado a la puesta en marcha de la norma
- Plan de acciones para seguimiento de incidencias (RGPD, Compliance, etc.)
- Plan de acciones asociado a las No Conformidades de revisiones

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



Integrable con
herramientas de
gestión de proyectos

Rail Operaciones Group

Compte: RailWay-Operator Norma: NIS2

Tratamiento de riesgos

Inicio > Tratamiento de riesgos > Lista

Legendas de estados
 Comenzó aplicación Transferencia a terceros No inicio Asesoría Comenzó de revisión asesoría

Nivel de riesgo aceptable: 2.3

Proyectos: [Buscar...] [Selecciona un Proyecto...]

[Nuevos ciclo de análisis] [Exportar] [Historial de ciclos] [Acciones masivas]

Activo	Amenaza	Riesgo reportado	Riesgo residual esperado	Estado	
[HW-COINC] PLC Hub	[N.1] Natural Disasters	9.8	2.8	↑	Tratar el Riesgo
[HW-SCADA1] SCADA HMI for railway management	[E.2] Administrator errors	9.6	1.5	↑	Tratar el Riesgo
[SW-MONITOR] Monitoring platform	[A.11] Unauthorized access	8.7	2.3	↑	Tratar el Riesgo
[SW-MONITOR] Monitoring platform	[N.1] Natural Disasters	8.7	2.3	↑	Tratar el Riesgo
[L-TRAIN1] Train 1	[A.7] Intended Use	4.1	2.2	↑	Tratar el Riesgo
[L-TRAIN1] Train 1	[A.11] Unauthorized access	6.3	2.2	↑	Tratar el Riesgo
[L-SEM2] Traffic light Station exit	[A.7] Intended Use	2.0	2.0	↑	Tratar el Riesgo
[HW-PCOP] Operator PC	[E.2] Administrator errors	3.7	2.0	↑	Tratar el Riesgo
[HW-PCOP] Operator PC	[E.4] Configuration errors	7.4	2.0	↑	Tratar el Riesgo
[HW-SCADA1] SCADA HMI for railway management	[N.1] Natural Disasters	7.4	2.0	↑	Tratar el Riesgo
[HW-PCOP] Operator PC	[E.8] Spreading Harmful Software	7.0	1.9	↑	Tratar el Riesgo
[SW-MONITOR] Monitoring platform	[A.7] Intended Use	1.7	1.7	↑	Tratar el Riesgo

Navegación: Panel de control, SCS, Gestión de acciones, Gestión de amenazas, Evaluación y tratamientos, Impacto Riesgo, Plan Director, Estructura organizativa, Gestor documental, Auditorías, Indicadores, Controles propios, Plantillas propias, Ajustes, Gestión de cuentas, Gestión de usuarios, Perfil documental, Catálogos, Catalog Controls, Configuración

Funcionalidades

Cuadro de Mando e Indicadores

- Este módulo permite la gestión de Métricas e Indicadores según marca el Sistema de Gestión.
- Permite incorporar la información de manera manual o automatizada de cualquier del resto de módulos o herramientas externas (KPIs).
- Dispone de sistema de alertas tanto al encargado de una métrica como al consultor si existe.
- Este módulo permite la parametrización de indicadores de Calidad y Seguridad y/o de rendimiento a partir de las incidencias y eventos
- Se comparan los indicadores con los valores objetivo para facilitar los comités de Seguimiento del Sistema de Gestión.
- Genera un cuadro de mando completo con entorno gráfico, que permite a la empresa controlar su nivel de cumplimiento respecto de los indicadores bajo análisis.

Dependencies
Home > Dependencies > List
Dependencies between assets. You must select an asset to get its dependencies

Search...

Asset	Type	Responsible
[SIS] Information system	[SIS] System	
[SIS-RAILWAY] Passenger Transportation	[SIS] System	Alberto Salinas
[ORG.F] Organization functions	[SP] Services product	
[S-ALLUM] Railway lighting service	[SP] Services product	Antonio Zabaldá
[S-RAILWAY] Railway management service	[SP] Services product	Chief, Train Management with trains
[S-TERM] Train management service	[SP] Services product	Manager, Operations Management with trains
[BKP-BBDD] Backup Base de datos	[INF] Information	Fernando Petasne
[Prueba] Activo prueba		Fernando Petasne

The selected asset depends on:

Asset	Grade
[L-STL1] Streetlight loading area	25 %
[L-STL2] Streetlight loading area 2	25 %
[L-STL3] Streetlight Station	25 %
[L-STL4] Streetlight train area	25 %

Add dependent asset

Depends on the selected asset:

Asset	Grade
[SIS-RAILWAY] Passenger Transportation	30 %
[S-RAILWAY] Railway management service	30 %



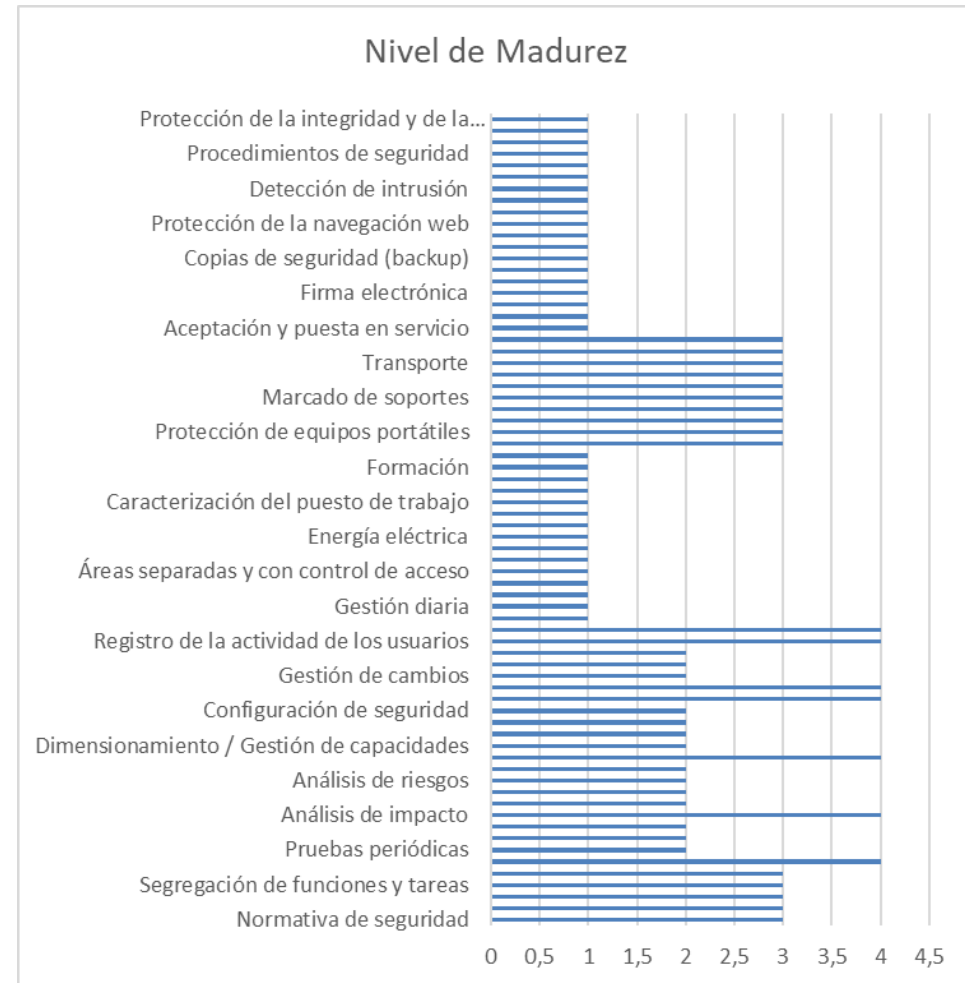
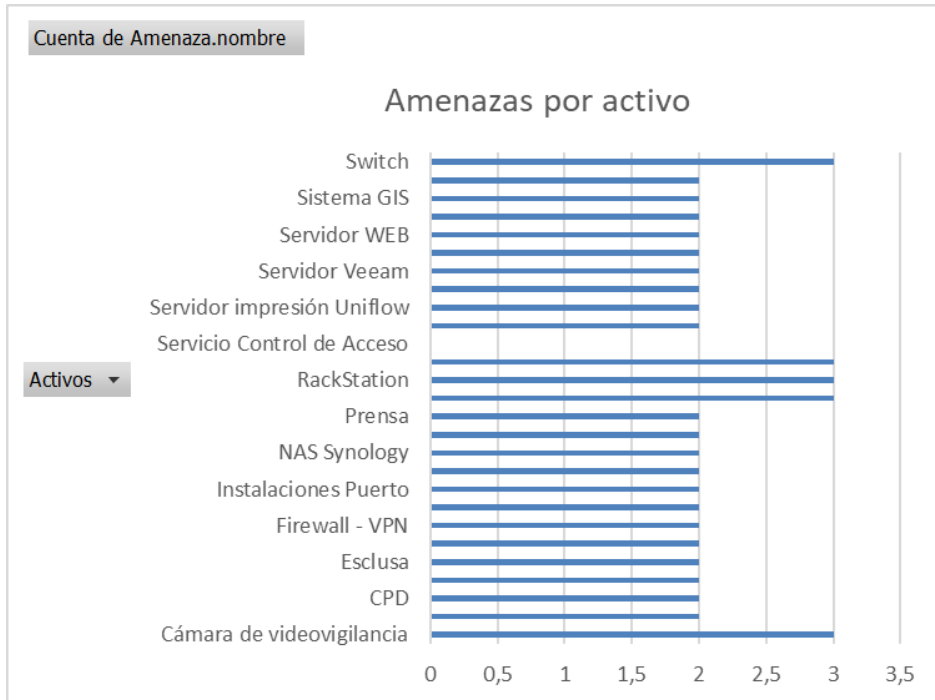
Informes

Cuadros de Mando

03

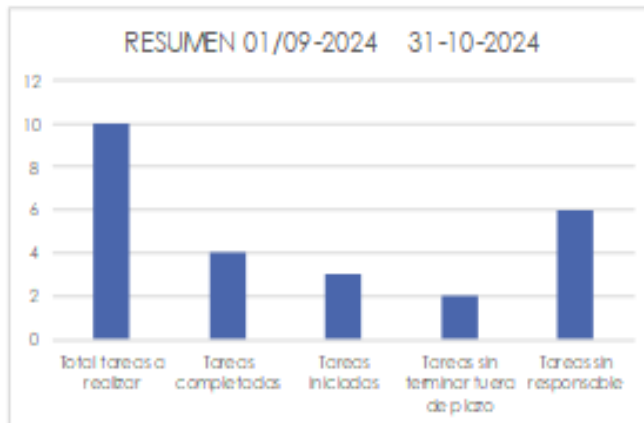
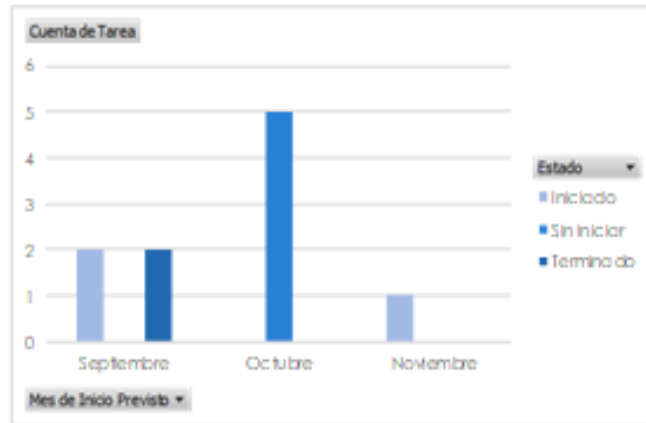


Informe de activos, amenazas y riesgos



Informe de estado de las tareas (única entidad)

Plan Director de Seguridad o equivalente

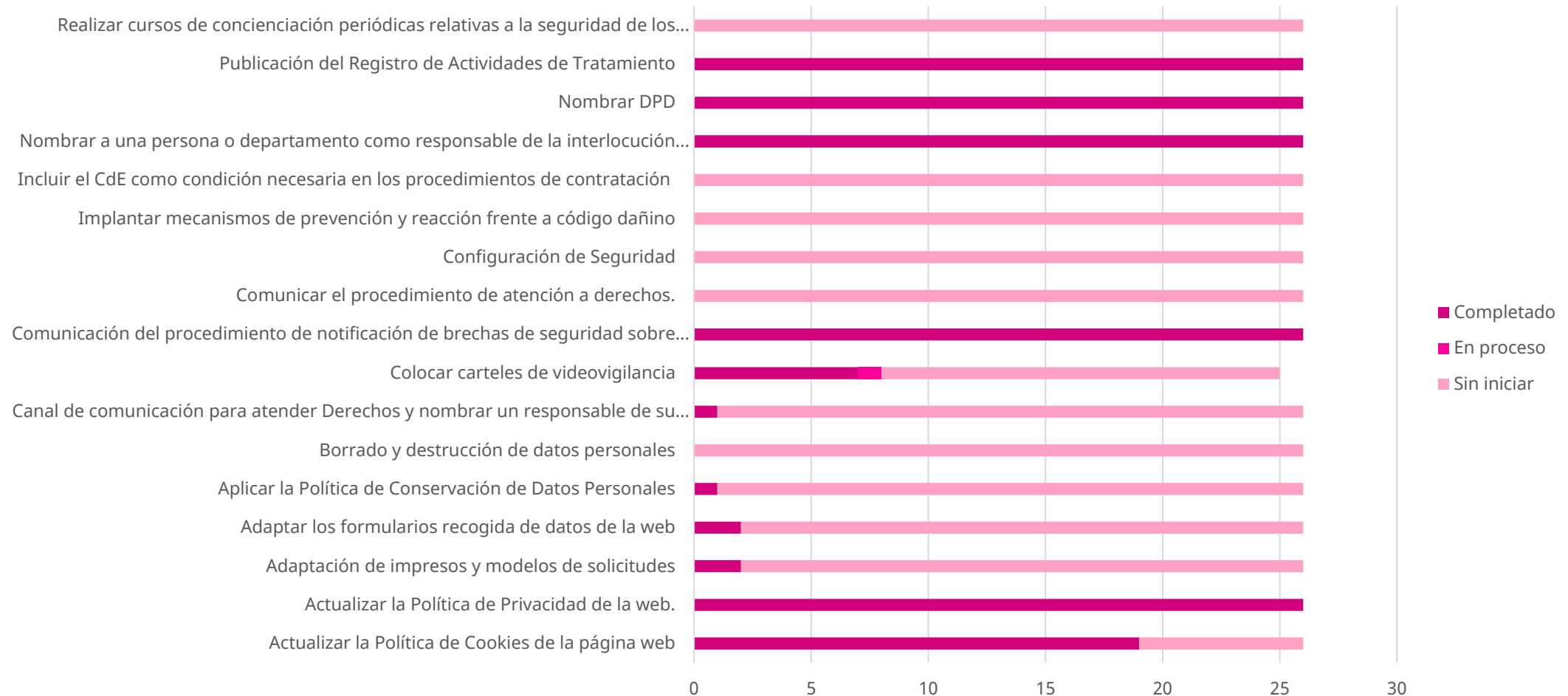


RESUMEN

Rango de fechas	01/09-2024	31-10-2024
Total tareas a realizar	10	
Tareas completadas	4	
Tareas iniciadas	3	
Tareas sin terminar fuera de plazo	2	
Tareas sin responsable	6	

Informe de estado por tareas (multiorganización)

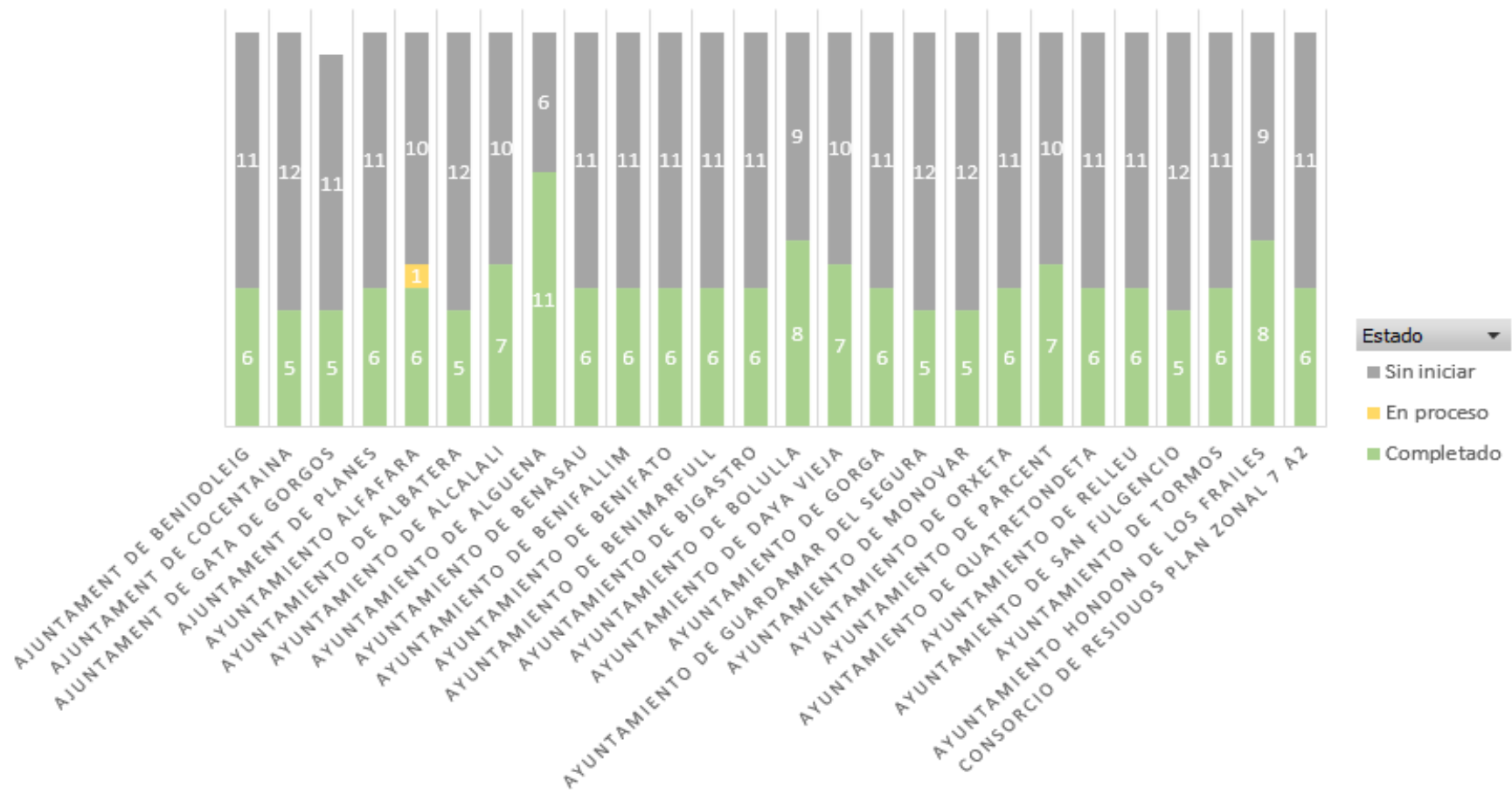
25 entidades bajo el paraguas del proyecto



Informe de estado por tareas cuyo inicio está retrasado (multiorganización)

Para dinamizar

Cuenta de Tarea





Razones de uso

G-Consulting

04

10 razones para utilizarlo

G-Consulting Compliance

- 1 Establece un marco de referencia para la implantación y operación de Sistemas de Gestión de una manera fácil y ordenada.
- 2 Monitoriza y centraliza toda la información de modo ordenado y óptimo, facilitando la localización de informes, registros e indicadores.
- 3 Permite gestionar de una manera ágil y sencilla Sistemas de Gestión complejos, integrando los diferentes Sistemas de Gestión en la empresa: SGP, SGC, SGSI, SGIDI.
- 4 Dispone de un interfaz web visual e intuitiva, que recoge todos los requisitos de las normas para operar Sistemas de Gestión.
- 5 Es un desarrollo en constante evolución, que se adapta y mejora en sus sucesivas versiones para ofrecer un servicio más completo al consultor y a la empresa final. Está incorporado en un proyecto Financiado por CDTI, IVACE, y con garantías de continuidad a largo plazo.

10 razones para utilizarlo

G-Consulting Compliance

- 6 GConsulting permite mantener en constante evolución y actualización un Sistema de Gestión.
- 7 GConsulting permite que cada perfil que intervenga en un Sistema de Gestión disponga de un interfaz único y personalizado.
- 8 GConsulting permite a un consultor o grupo de consultores gestionar totalmente su cartera de clientes en las que lleva a cabo su trabajo de una manera sencilla y coordinada, mediante un interfaz de gestión.

10 razones para utilizarlo

G-Consulting Compliance

- 9 Sus módulos han sido evaluados por el Centro Demostrador de Tecnologías de Seguridad del INCIBE con opinión y resultados muy favorables respecto del mercado.
- 10 Está incluida como Solución en el Catálogo de Empresa y Soluciones de Seguridad TIC del INCIBE.

Tabla 2: Resultados de las pruebas funcionales

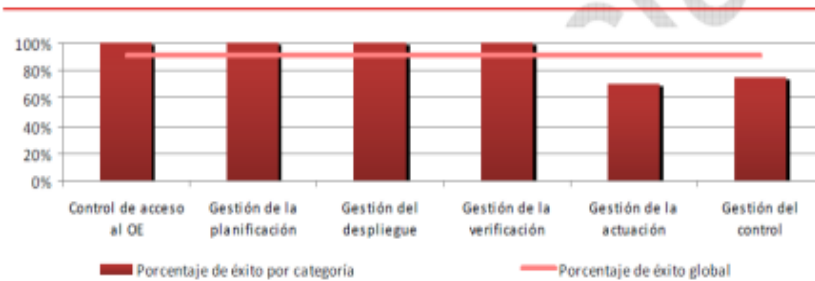
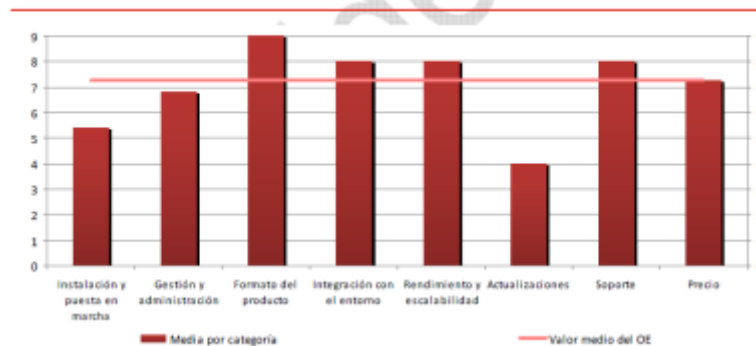


Tabla 3: Resultado de las pruebas de usuario





Otros productos

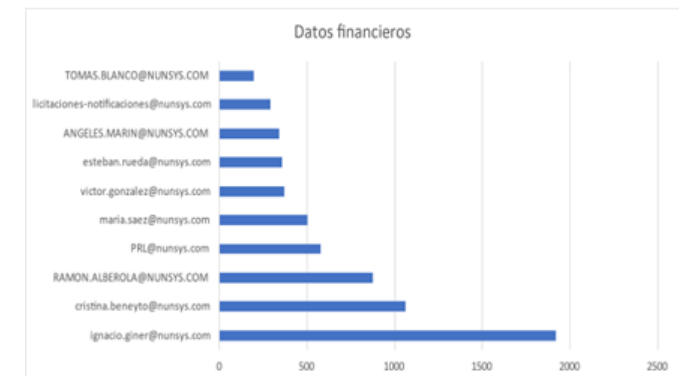
Ámbito ciberseguridad

05

Protección de la Información

Apuesta firme por el producto propio

- Diseñamos y ponemos a disposición del mercado un conjunto de soluciones propias que aportan valor en diferentes ámbitos de la gestión, poniendo el foco en la innovación como principio de actuación en todas las áreas de crecimiento de la Compañía.
- SAFECLOUD es un portal agregador de información para el Responsable de Seguridad o de Privacidad (CIO, DPO) de la organización que permite gobernar y mejorar la protección de la información de la organización
- Almacenamiento e intercambio seguro de la información configurado sobre Microsoft Azure Information Protection

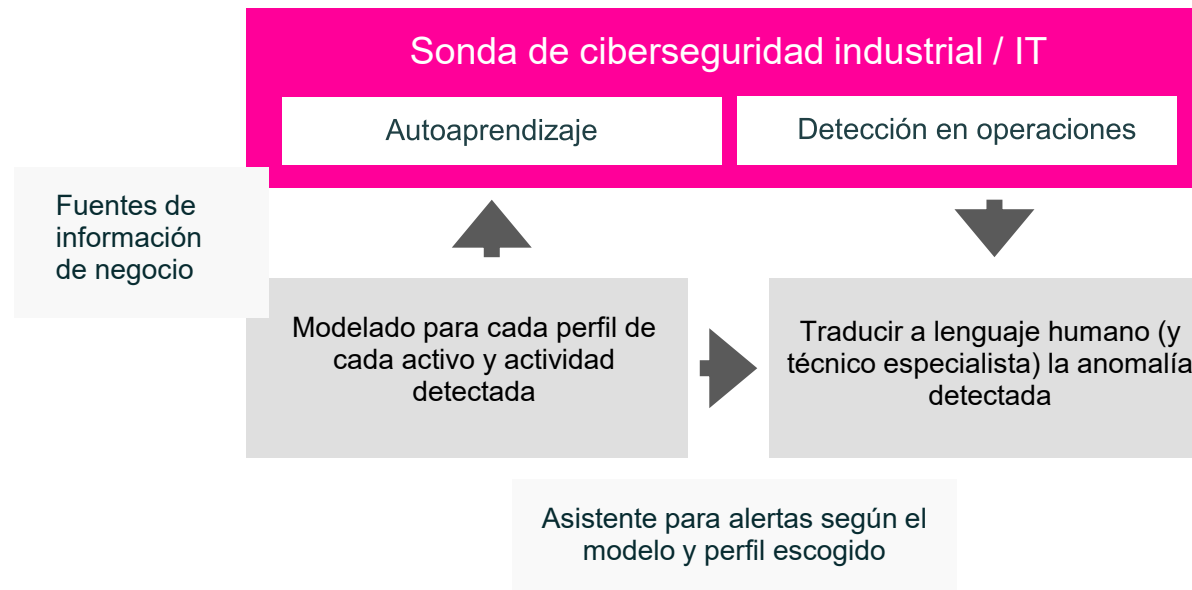




Solución de Seguridad Semántica

Apuesta firme por el producto propio

- SIRENA es una herramienta para dotar tu organización de capacidades extra para la toma de decisiones ante anomalías e incidencias
- Añadimos información de negocio a las incidencias para optimizar la respuesta a incidentes



1. Seguridad semántica aplicada a entornos de operaciones
2. Información en la red OT para toma rápida de decisiones
3. Dotar nuevas funcionalidades a sondas industriales
4. Interlocutar con cada perfil en su lenguaje natural



G·CONSULTING
COMPLIANCE

