Sigma360

SEGURIDAD FÍSICA · VISIÓN COMPLETA

MANUAL COMPLETO DEL USUARIO

Guía de referencia detallada · paso a paso

Versión 1.0 · 2026

Contenido

PARTE I · FUNDAMENTOS

1. Introducción a Sigma360

Sigma360 es una plataforma web para la gestión integral de la seguridad física corporativa. Reúne en un solo lugar las principales metodologías de evaluación, análisis de riesgo y gestión que utiliza un profesional de seguridad, y las consolida en un tablero ejecutivo que ofrece una visión completa del estado de seguridad de cada sitio de la organización.

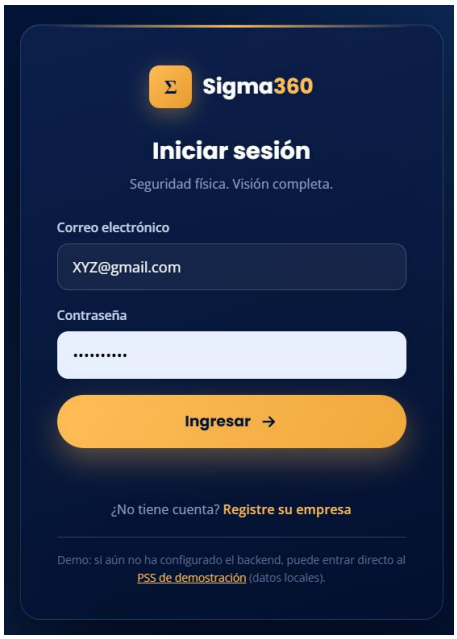
Cómo está organizado este manual

El manual se divide en seis partes: los fundamentos (cómo empezar), y luego un capítulo por cada grupo de módulos. Cada módulo se documenta con su propósito, su acceso según plan, y el paso a paso de uso, con espacios para que usted inserte las capturas de pantalla de su propia plataforma.

> **Sobre las capturas:** a lo largo del manual encontrará recuadros punteados con la leyenda "PEGUE AQUÍ LA CAPTURA". Reemplácelos por los pantallazos correspondientes de su instalación de Sigma360.

Requisitos

- Un navegador web moderno (Chrome, Edge, Firefox o Safari actualizados).
- Conexión a internet.
- Credenciales de acceso (correo y contraseña) creadas durante el registro.



2. Conceptos: planes, roles y multi-tenant

2.1 Planes y qué incluye cada uno

El plan determina cuántos sitios y usuarios puede gestionar, cuántas evaluaciones por sitio al año, y a qué módulos tiene acceso.

Plan	Sitios	Usuarios	Eval./sitio/año	Módulos
Starter	2	5	4	Diagnóstico esencial.
Professional	5	15	12	Análisis de riesgo + Disponibilidad y Cubrimiento.
Enterprise	Ilimitados	Ilimitados	Ilimitadas	Todos, incluidos ROSI, T-FINE, Dashboard y PBIP.

> **Cómo mejorar de plan:** desde el panel de administración, en la sección "Mejore su plan". El cambio es inmediato tras recargar la página.

2.2 Roles de usuario

Rol	Permisos
Administrador	Gestiona usuarios, sitios y configuración. Acceso completo a los módulos del plan.
Ejecutor	Crea y edita evaluaciones y registros.
Aprobador	Revisa y aprueba evaluaciones.
Consulta	Solo lectura.

2.3 Multi-tenant: aislamiento de datos

Cada empresa opera en su propio espacio aislado. Los datos de una empresa nunca son visibles para otra. Este aislamiento se aplica en cada consulta mediante el identificador de empresa contenido en el token de sesión, que no puede ser falsificado.

> **Su información es suya:** todo lo que registra es confidencial, reservado y de su propiedad. Puede exportarlo en cualquier momento (ver capítulo 26).

3. Registro e inicio de sesión (paso a paso)

3.1 Registrar una empresa

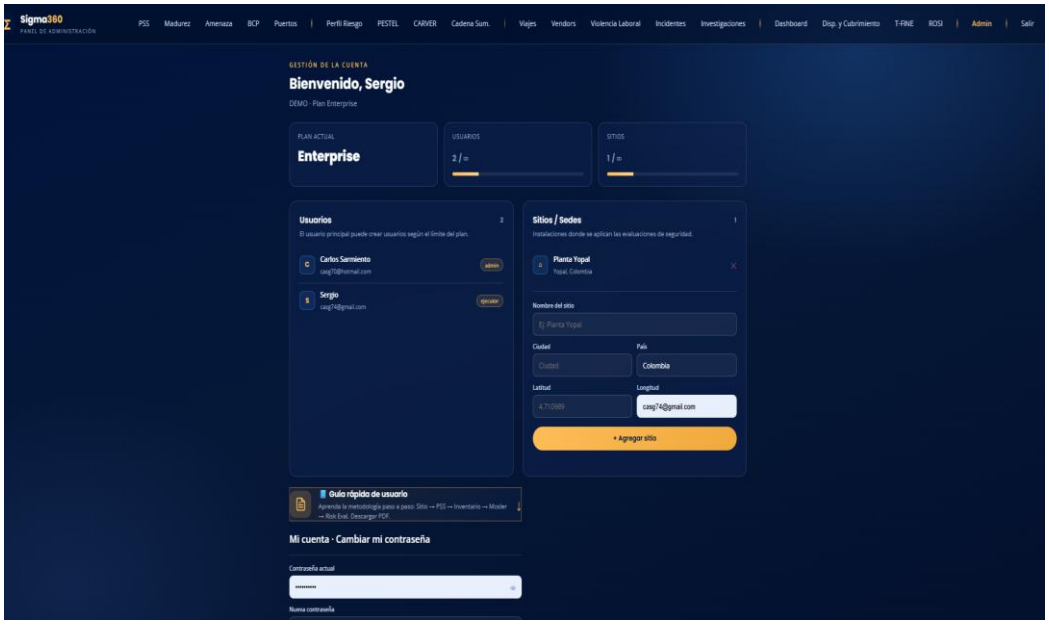
1. **Abrir el registro:** desde la página de inicio, seleccione la opción de registro/crear cuenta.
2. **Datos de la empresa:** ingrese el nombre de la organización y el sector.
3. **Datos del administrador:** su nombre, cargo y correo electrónico.
4. **Contraseña:** defina una contraseña de mínimo 8 caracteres y consérvela en un lugar seguro.
5. **Aceptar términos:** revise y acepte los Términos de Uso y la Política de Tratamiento de Datos.
6. **Confirmar:** al enviar, se crea su empresa y su usuario administrador. Ya puede iniciar sesión.

> **Plan inicial:** toda empresa nueva queda en plan Starter. Para pruebas o contratación de un plan superior, el equipo de Sigma360 lo habilita.

3.2 Iniciar sesión

1. **Ir a inicio de sesión:** ingrese su correo y contraseña.
2. **Acceder:** el sistema valida sus credenciales y lo dirige a su panel según su rol.

Por seguridad, al iniciar sesión se limpian los borradores locales de sesiones anteriores, protegiendo la información en equipos compartidos.



> **Recomendación:** cada persona debe usar su propio usuario. Así los reportes registran correctamente quién elaboró cada evaluación.

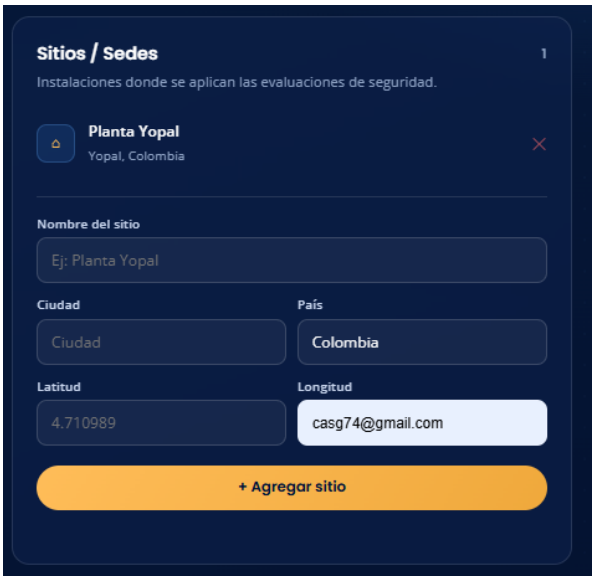
4. Gestión de sitios y usuarios

Estas tareas se realizan desde el panel de administración (opción "Admin" en el menú). El administrador es quien las gestiona.

4.1 Registrar un sitio

Un sitio es una instalación física a evaluar (sede, planta, oficina). La mayoría de módulos permiten asociar la evaluación a un sitio, lo que alimenta el Dashboard y permite comparar entre sedes.

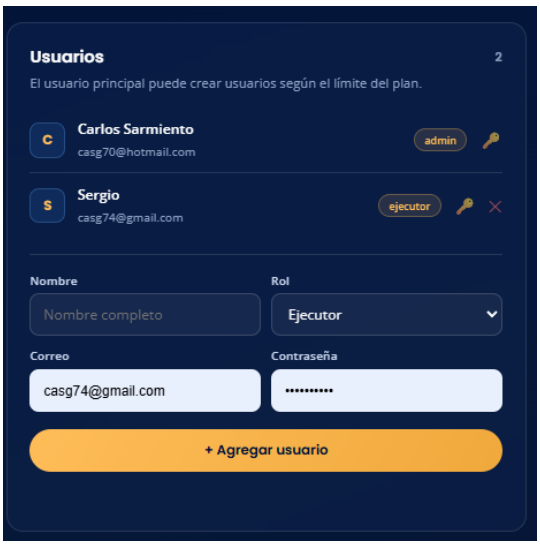
1. **Ir a "Usuarios y sitios":** en el panel de administración.
2. **Agregar sitio:** indique el nombre y, si aplica, ciudad y país.
3. **Guardar:** el sitio queda disponible para todos los módulos.



> **Límite por plan:** Starter permite 2 sitios, Professional 5, Enterprise ilimitados. Si alcanza el límite, mejore su plan.

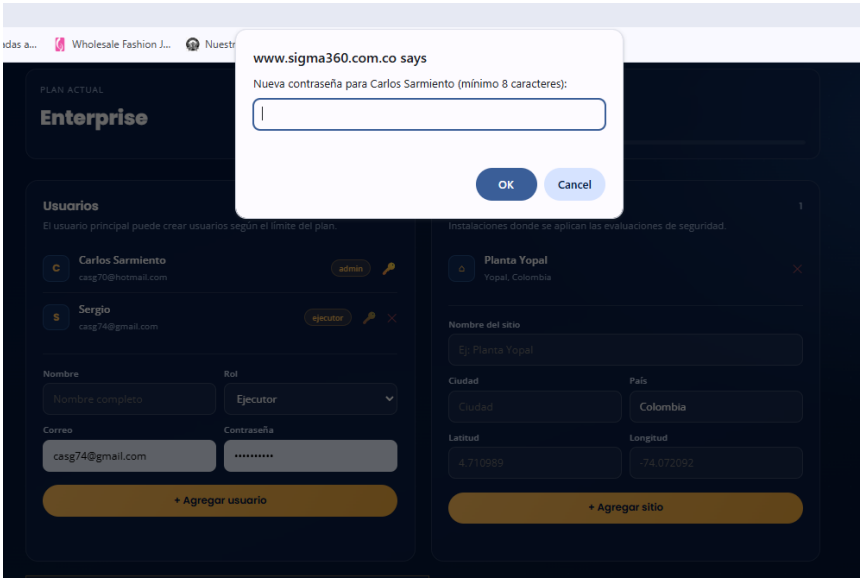
4.2 Crear y administrar usuarios

1. **Ir a "Usuarios y sitios":** en el panel.
2. **Agregar usuario:** ingrese nombre, correo, rol y una contraseña inicial.
3. **Activar/desactivar:** puede suspender el acceso de un usuario sin eliminarlo.



4.3 Cambiar mi contraseña

Cada usuario puede cambiar su propia contraseña desde el panel, en la sección "Mi cuenta · Cambiar mi contraseña".

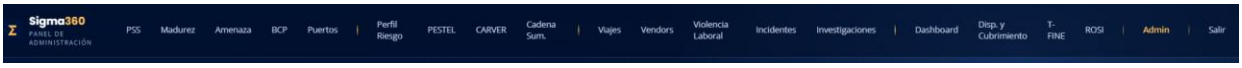


5. Navegación e interfaz común

Todos los módulos comparten una estructura visual coherente, lo que facilita moverse entre ellos.

5.1 La barra superior

- El logo (izquierda) siempre regresa al inicio.
- El menú de navegación agrupa los módulos por categoría, con separadores dorados.
- El nombre del módulo actual se resalta en dorado.
- La opción "Salir" cierra la sesión.



5.2 Elementos comunes en los módulos

- **Selector de sitio —** permite asociar la evaluación a una instalación registrada.
- **Campo evaluador —** se completa automáticamente con el usuario en sesión y aparece en el PDF.
- **Botón Guardar —** almacena la evaluación en la plataforma.
- **Botón Descargar PDF —** genera el reporte con la identidad de Sigma360.
- **Historial / listado —** muestra las evaluaciones previas para abrirlas o continuarlas.

> **Menú móvil:** en pantallas pequeñas, el menú se colapsa en un botón ☰ que despliega las opciones.

6. PSS · Physical Security Survey

El PSS es el módulo base de Sigma360. Realiza una evaluación integral de la seguridad física de una instalación a través de un cuestionario estructurado por áreas, y encadena tres etapas de análisis: el survey, el análisis Mosler y la evaluación de riesgos, para terminar en un dashboard de resultados.

6.1 Flujo general del PSS

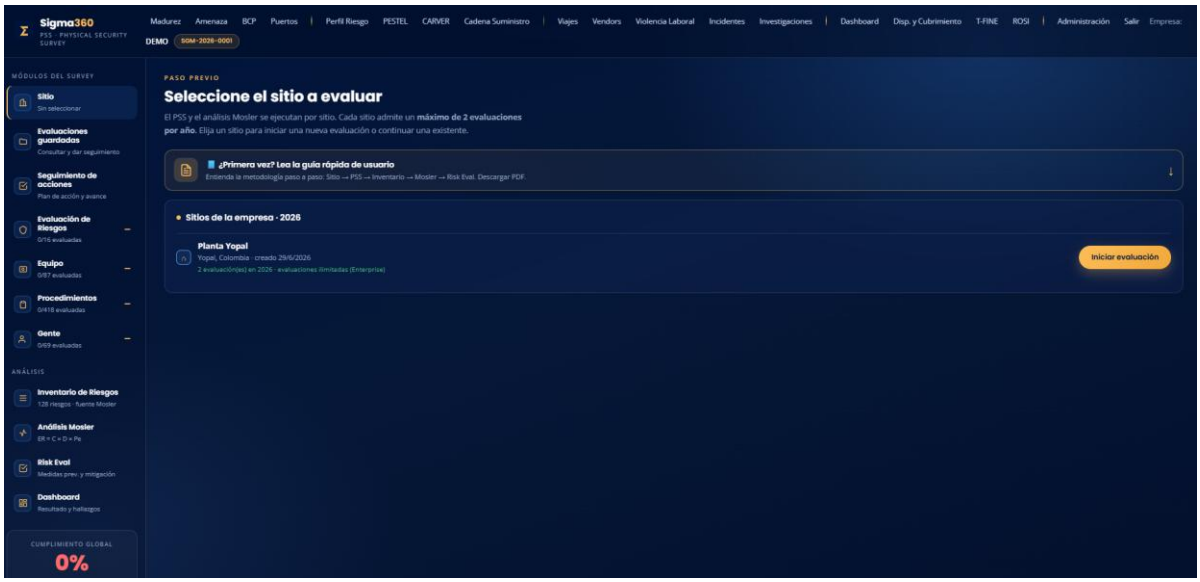
El módulo se recorre en este orden:

1. **Survey:** responder el cuestionario por módulos temáticos.
2. **Mosler:** analizar los riesgos seleccionados con el método Mosler.
3. **Risk Eval:** completar la evaluación de riesgos y sus medidas.
4. **Dashboard PSS:** ver el puntaje y los resultados consolidados.

6.2 Datos iniciales de la evaluación

Antes de responder, complete los datos de cabecera:

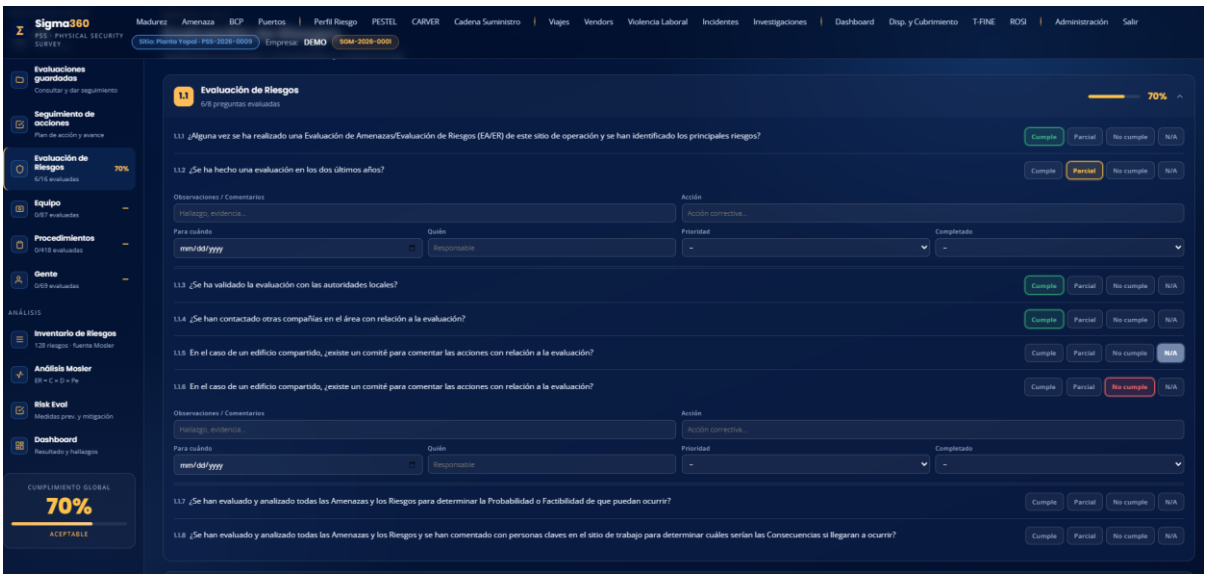
- **Sitio a evaluar —** la instalación objeto de la evaluación.
- **Fecha de la evaluación —** fecha en que se realiza.
- **Responsable de la evaluación —** se toma del usuario en sesión; aparece en el PDF.



6.3 Responder el survey

El survey está dividido en módulos temáticos. En cada uno, responda las preguntas y, si lo desea, agregue observaciones. Puede avanzar y retroceder entre módulos con los botones de navegación (por ejemplo, "Siguiente" y el botón para regresar al módulo anterior).

- **Respuestas —** marque la opción que corresponda a cada pregunta.
- **Observaciones / Comentarios —** texto libre para matizar o sustentar una respuesta.



> **Modo demostración:** el botón "Modo demostración" completa el survey con datos de ejemplo, útil para conocer el flujo sin llenar todo manualmente.

6.4 Análisis Mosler

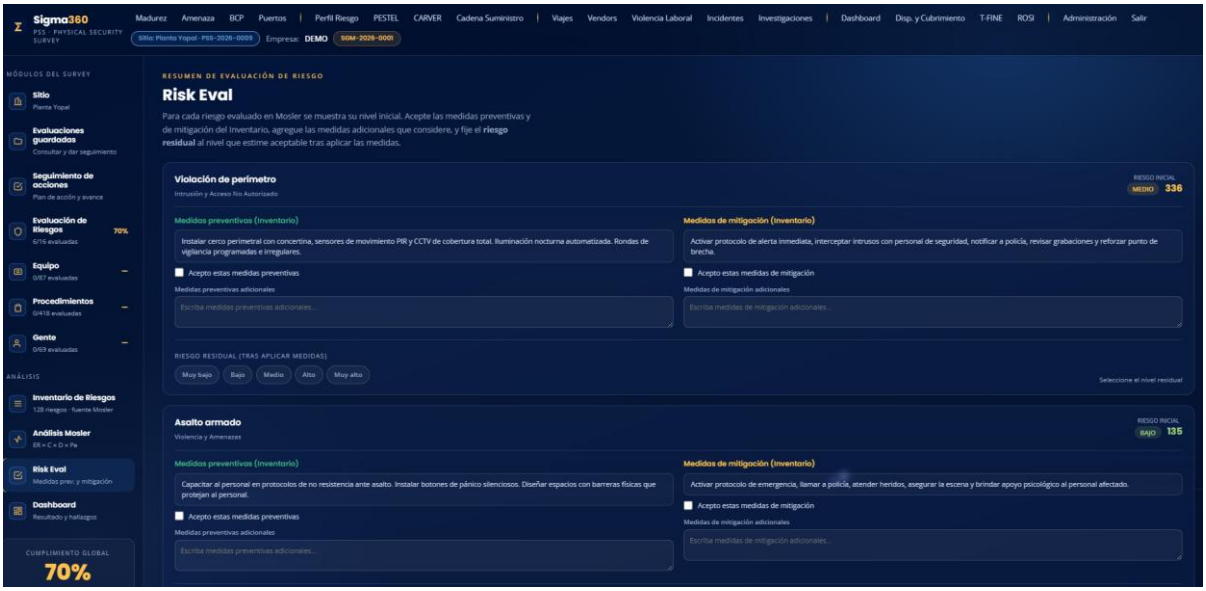
Tras guardar el survey, avanza al análisis Mosler sobre los riesgos seleccionados. El método Mosler valora cada riesgo según sus criterios para obtener una clase de riesgo.

- **Nombre del riesgo —** identificación del riesgo analizado.
- **Categoría —** clasificación del riesgo.
- **Criterios Mosler —** valore cada criterio según la escala presentada.

6.5 Evaluación de riesgos (Risk Eval)

En esta etapa se documentan los riesgos con sus medidas preventivas y de mitigación.

- **Nombre del riesgo —** el riesgo evaluado.
- **Actores / Factores —** quiénes o qué originan el riesgo.
- **Medidas preventivas —** controles para evitar que el riesgo se materialice.
- **Medidas de mitigación —** acciones para reducir el impacto si ocurre.
- **Medidas preventivas/de mitigación adicionales —** controles complementarios propuestos.



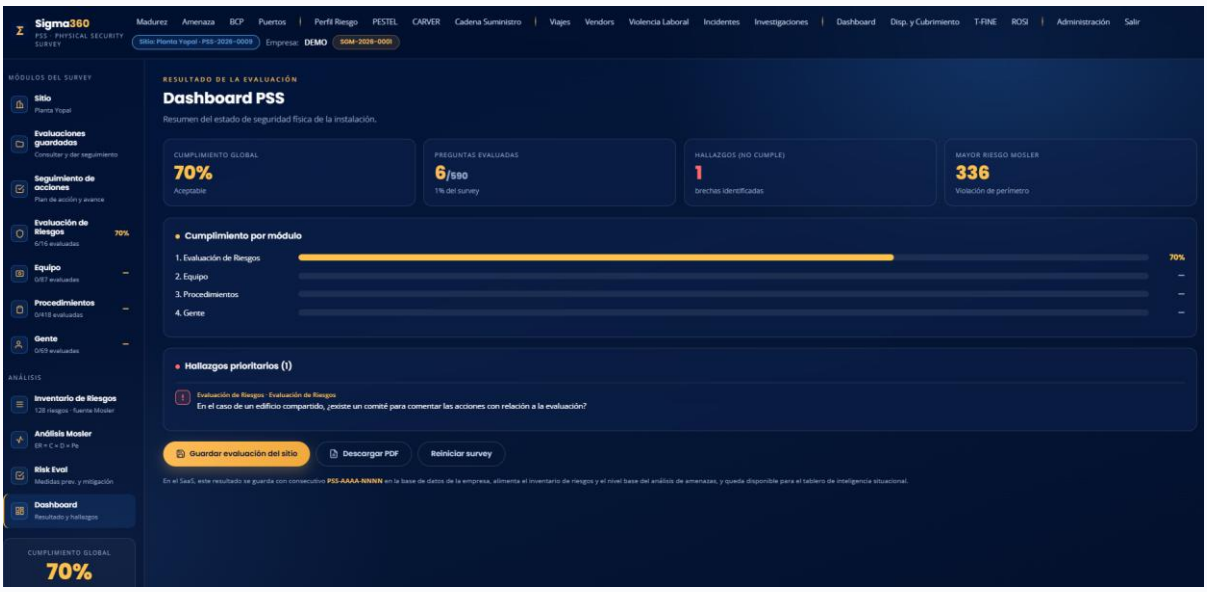
6.6 Plan de acción

Puede registrar acciones de mejora con responsable y fecha:

- **Acción —** qué se debe hacer.
- **Quién —** responsable de ejecutarla.
- **Para cuándo —** fecha compromiso.
- **Prioridad —** nivel de importancia.
- **Completado —** marca de avance.

6.7 Dashboard PSS y resultados

Al finalizar, el módulo muestra el puntaje de la evaluación y sus resultados. Desde aquí puede descargar el reporte PDF y, si tiene plan Enterprise, ver el resultado reflejado en el Dashboard Ejecutivo.



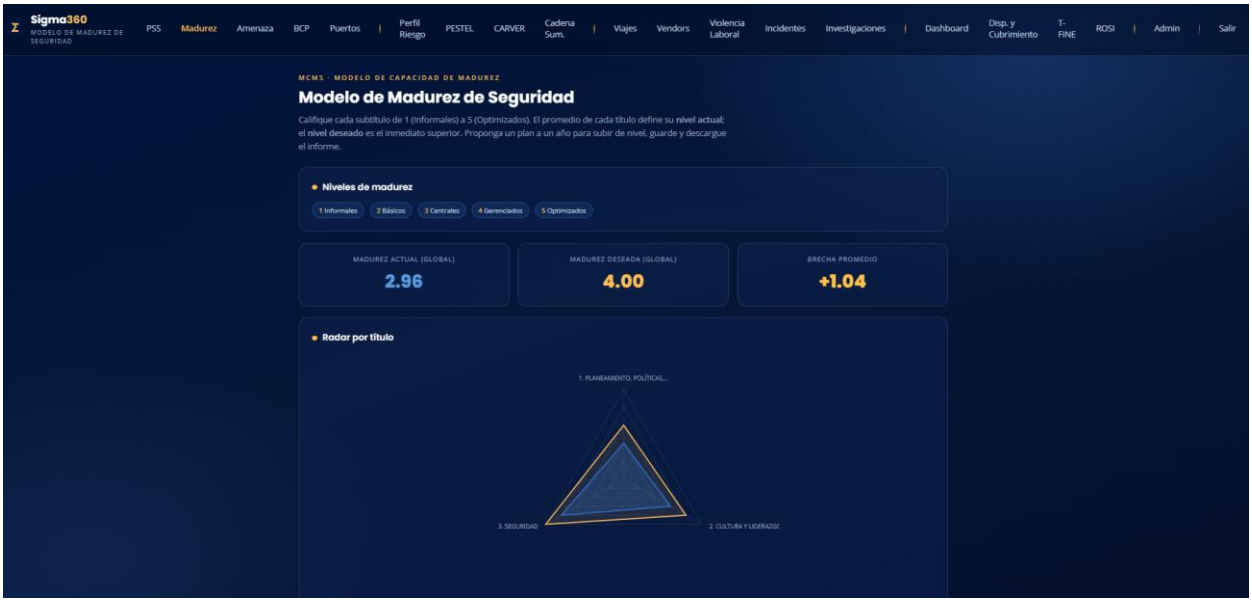
Reiniciar: el botón "Reiniciar survey" limpia la evaluación en curso para comenzar de nuevo. Úselo con cuidado si no ha guardado.

7. Madurez del Programa

Evalúa el grado de desarrollo del programa de seguridad de la organización, más allá de una instalación puntual, midiendo políticas, procesos y capacidades.

7.1 Cómo se usa

1. **Datos iniciales:** indique el sitio (si aplica), la fecha y el responsable.
2. **Responder los ítems:** valore cada ítem de madurez según la escala propuesta.
3. **Guardar:** almacene la evaluación.
4. **Descargar PDF:** genere el reporte.
    - **Ítems de madurez —** cada aspecto del programa se valora en una escala de nivel de desarrollo.



> **Interpretación:** un mayor puntaje indica un programa más consolidado. Los resultados alimentan el Dashboard (Enterprise).

8. Evaluación de Amenazas

Identifica y valora las amenazas a las que está expuesta la organización o el sitio, según su probabilidad e impacto.

8.1 Cómo se usa

1. **Datos iniciales:** sitio, fecha y responsable.
2. **Registrar amenazas:** identifique cada amenaza relevante.
3. **Valorar:** asigne probabilidad e impacto a cada una.
4. **Guardar y descargar PDF:** con los botones "Guardar evaluación" y "Descargar PDF".

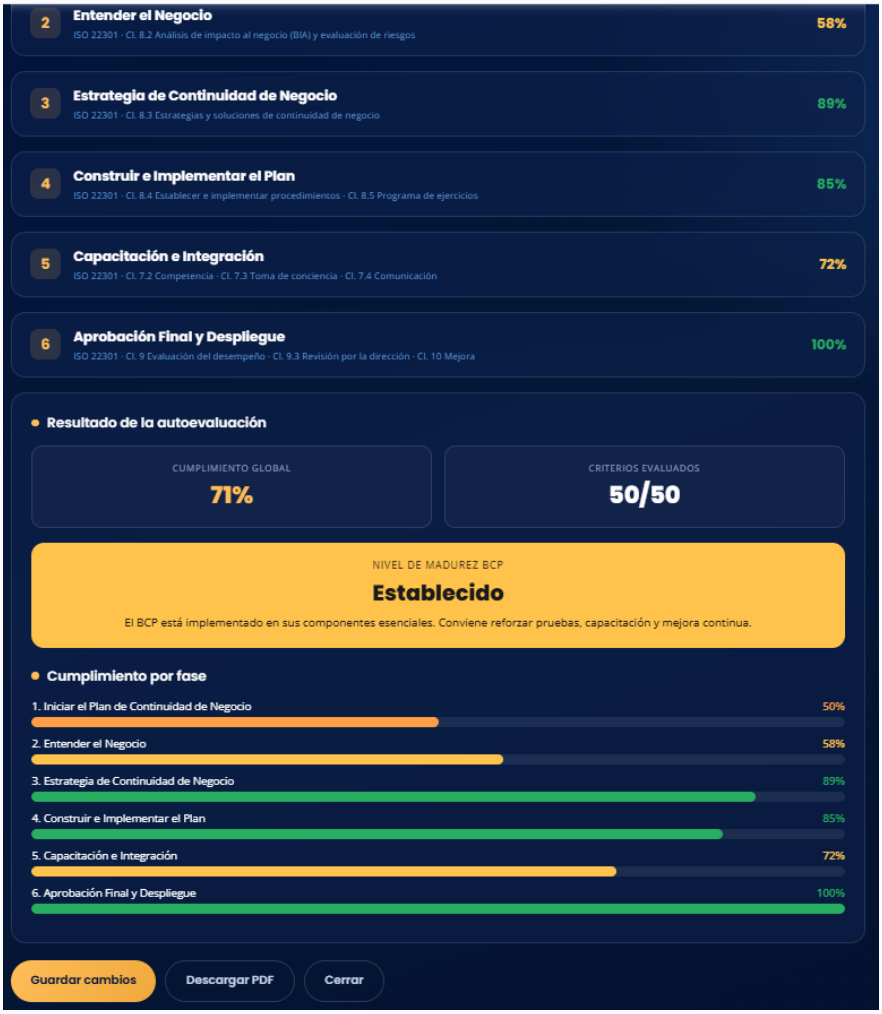
> **Reiniciar:** el botón "Reiniciar" limpia la evaluación en curso.

9. Continuidad del Negocio (BCP)

Apoya la evaluación de la capacidad de la organización para mantener sus operaciones ante una interrupción, alineado con las buenas prácticas de continuidad de negocio.

9.1 Cómo se usa

1. **Datos iniciales:** sitio, fecha y responsable.
2. **Completar la evaluación:** responda los aspectos de continuidad planteados.
3. **Guardar y descargar PDF:** para conservar el resultado.



> **Resultado:** la evaluación refleja el nivel de preparación ante interrupciones y alimenta el Dashboard (Enterprise).

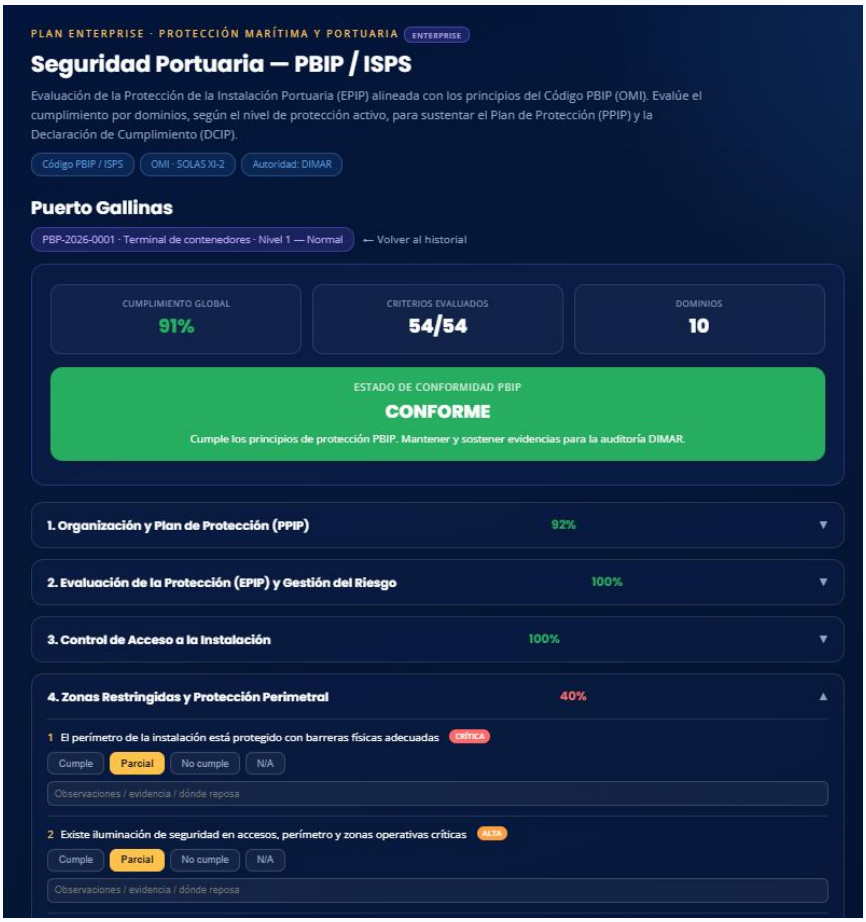
10. Seguridad de Puertos (PBIP)

Disponible en el plan Enterprise.

Evaluación orientada a instalaciones portuarias según el marco de protección de buques e instalaciones portuarias.

10.1 Cómo se usa

1. **Seleccionar el sitio:** indique el sitio portuario registrado. El módulo permite asociar la evaluación a un sitio para el Dashboard.
2. **Completar la evaluación:** responda los aspectos de protección portuaria.
3. **Guardar y descargar PDF:** para conservar y compartir el resultado.

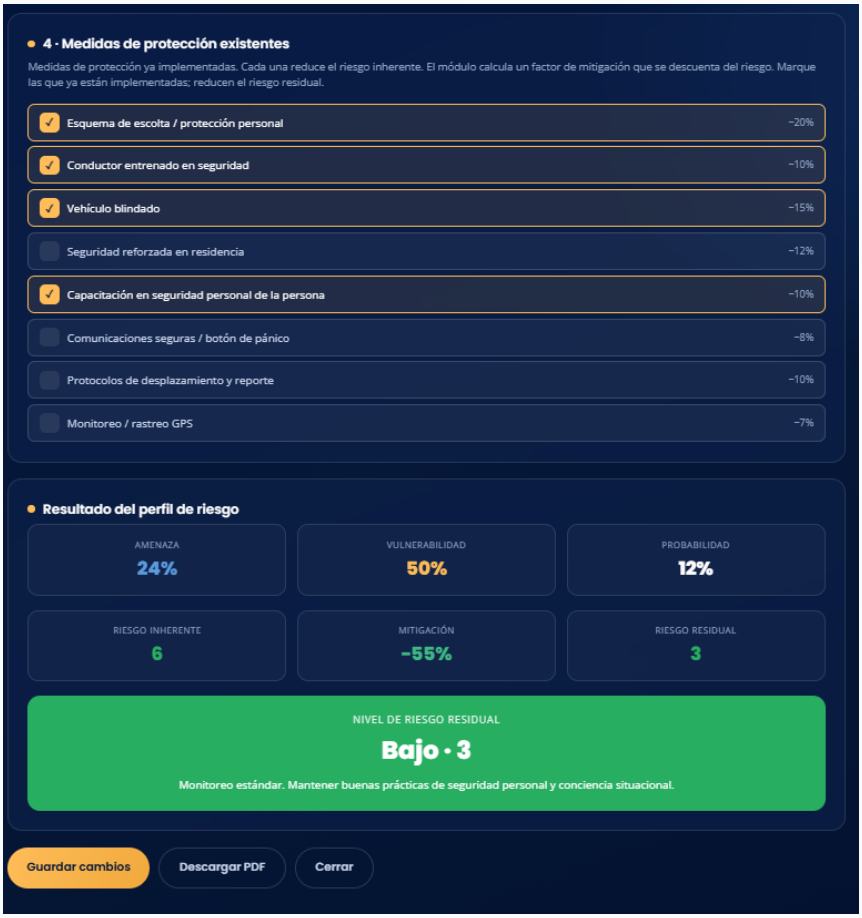


> **Filtro por sitio:** PBIP se integra al Dashboard Ejecutivo filtrando por sitio, junto con los demás módulos.

11. Perfil de Riesgo

Construye un perfil consolidado del riesgo del sitio o la organización, integrando distintos factores en una valoración global.

1. **Datos iniciales:** sitio, fecha y responsable.
2. **Completar factores:** valore los factores que componen el perfil.
3. **Guardar y descargar PDF:** para conservar el resultado.



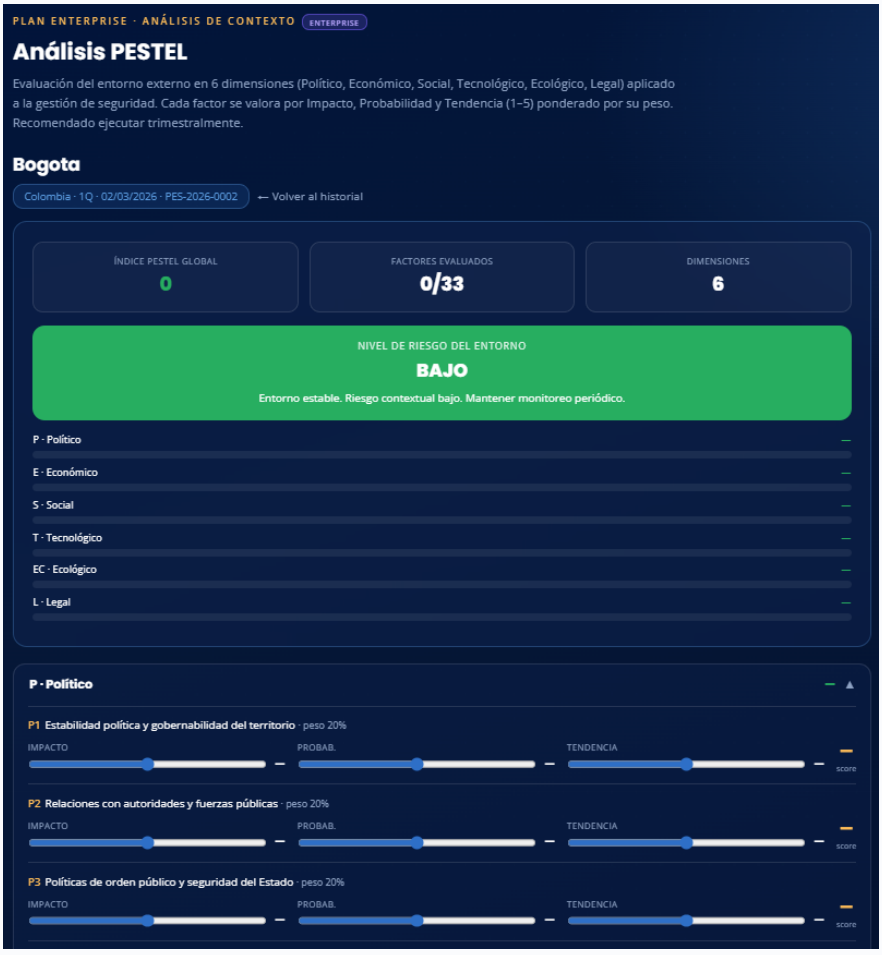
12. PESTEL

Análisis del entorno bajo seis dimensiones: Política, Económica, Social, Tecnológica, Ecológica y Legal, aplicado al contexto de seguridad.

12.1 Las seis dimensiones

- **Política —** factores de gobierno, estabilidad y políticas públicas.
- **Económica —** condiciones económicas que afectan el riesgo.
- **Social —** factores sociales y culturales del entorno.
- **Tecnológica —** cambios tecnológicos relevantes.
- **Ecológica —** factores ambientales.
- **Legal —** marco normativo aplicable.

1. **Completar cada dimensión:** registre los factores identificados en cada una.
2. **Guardar y descargar PDF:** para conservar el análisis.



13. CARVER

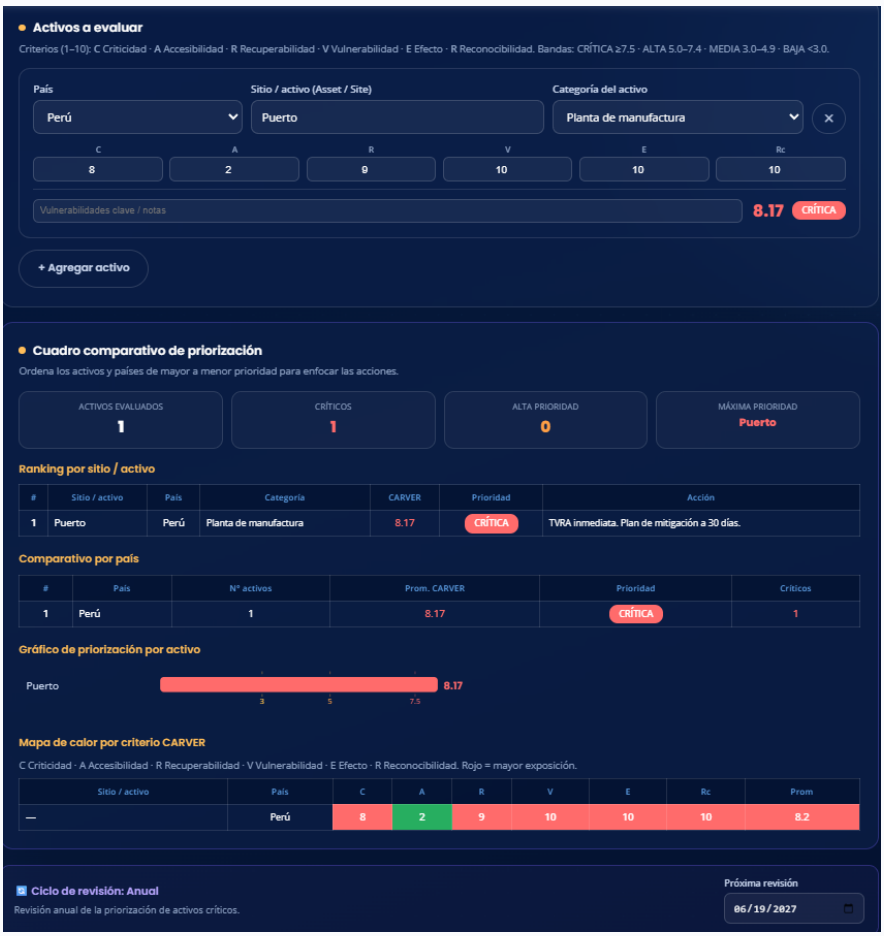
Metodología para evaluar la criticidad de activos y priorizar cuáles proteger. Cada activo se valora según seis criterios.

13.1 Los seis criterios CARVER

- **Criticidad —** importancia del activo para la operación.
- **Accesibilidad —** facilidad con que un adversario puede alcanzarlo.
- **Recuperabilidad —** tiempo y recursos para reponerlo si se pierde.
- **Vulnerabilidad —** facilidad para causarle daño.
- **Efecto —** impacto de su afectación en la organización.
- **Reconocibilidad —** facilidad con que el activo puede ser identificado.

13.2 Cómo se usa

1. **Agregar activos:** registre cada activo a evaluar.
2. **Valorar los seis criterios:** asigne una puntuación a cada criterio por activo.
3. **Revisar el ranking:** el módulo prioriza los activos según su puntaje total.
4. **Guardar y descargar PDF:** para conservar el análisis.

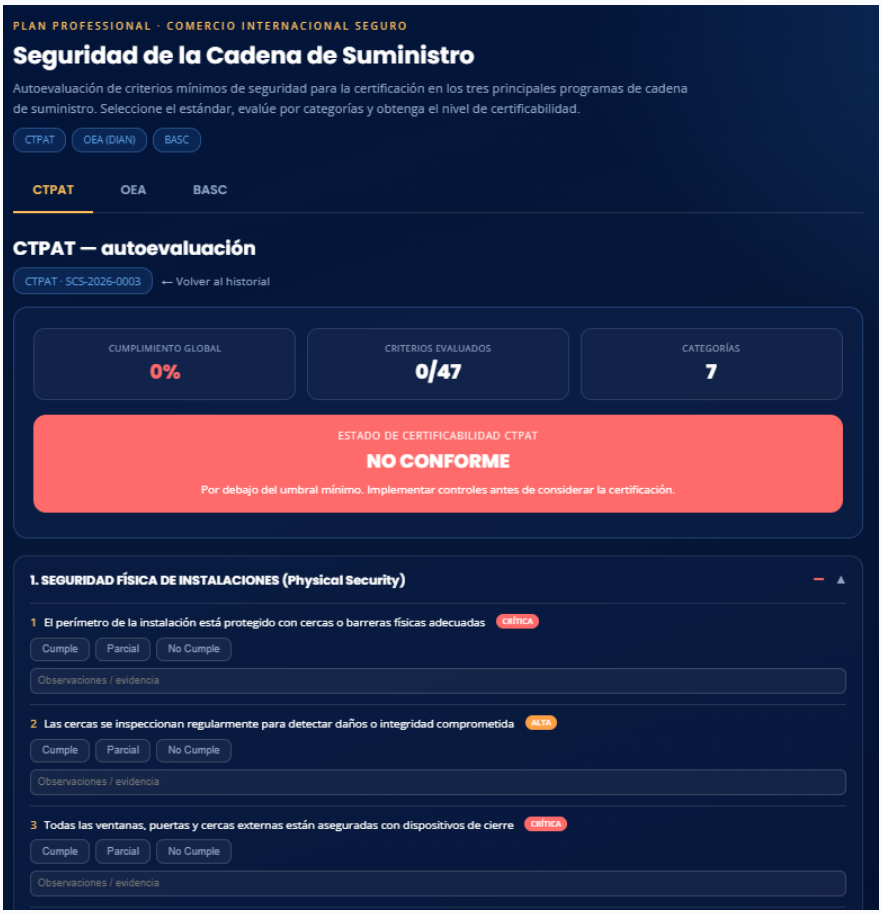


14. Cadena de Suministro

Disponible en el plan Enterprise.

Evalúa los riesgos de seguridad asociados a la cadena de suministro de la organización.

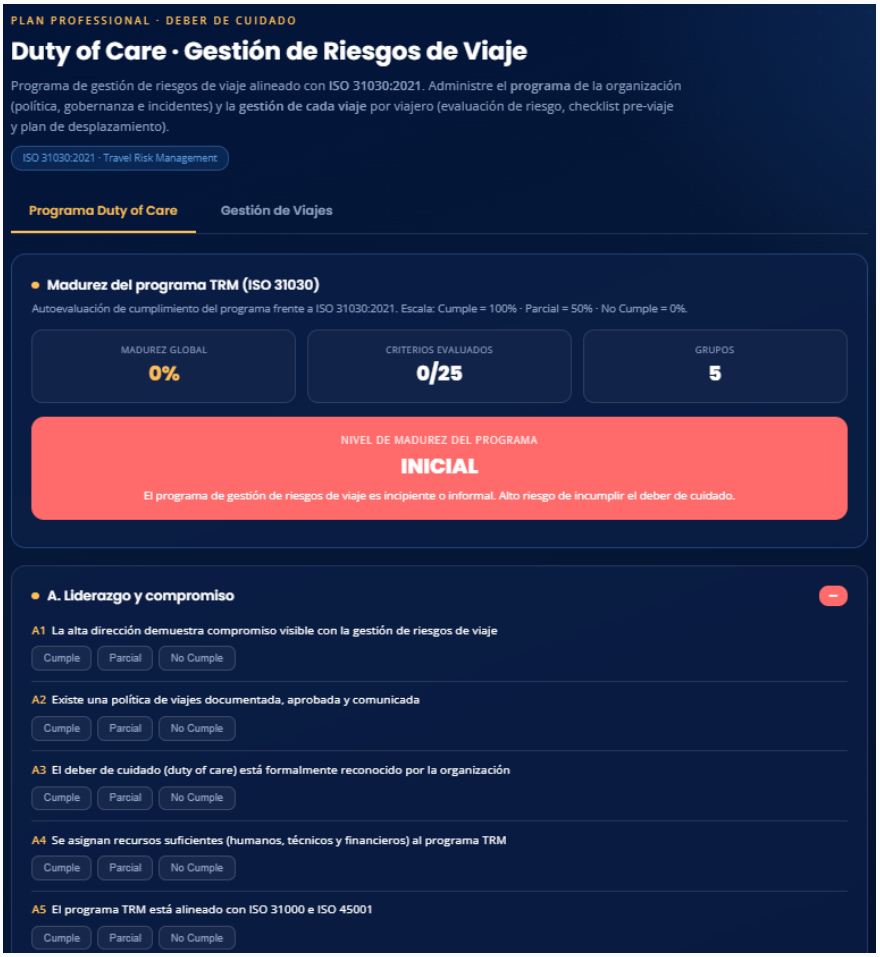
1. **Datos iniciales:** sitio, fecha y responsable.
2. **Completar la evaluación:** valore los aspectos de la cadena de suministro.
3. **Guardar y descargar PDF:** para conservar el resultado.



15. Viajes

Gestiona la seguridad de los viajes corporativos: itinerarios, nivel de riesgo del destino y recomendaciones (duty of care).

1. **Registrar el viaje:** datos del desplazamiento y destino.
2. **Valorar el riesgo del destino:** según la información disponible.
3. **Documentar recomendaciones:** medidas de protección para el viajero.
4. **Descargar PDF:** el reporte indica "Elaborado por" con el evaluador.



16. Vendors (Evaluación de Proveedores)

Evalúa y compara proponentes/proveedores de servicios de seguridad, y hace seguimiento a su desempeño.

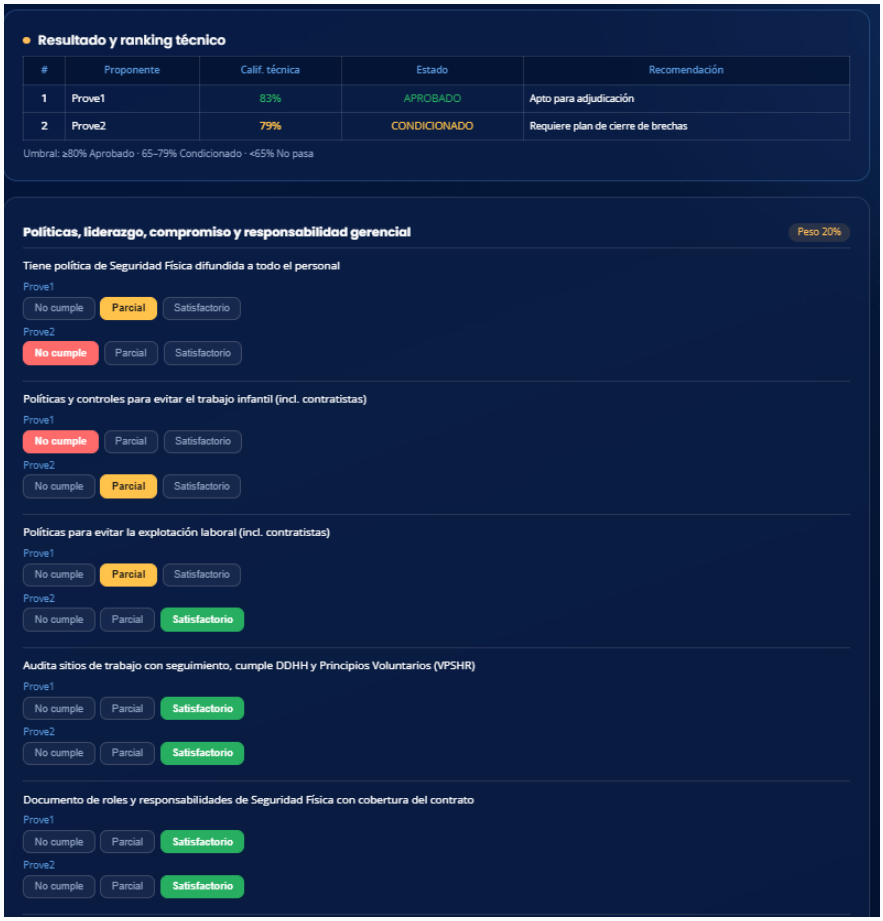
16.1 Evaluación de proponentes

1. **Registrar proponentes:** agregue los proveedores a comparar.
2. **Evaluar:** valore cada uno según los criterios del módulo.
3. **Comparar:** revise el resultado comparativo.

16.2 Seguimiento de desempeño

Registre el desempeño del proveedor a lo largo del tiempo para su control.

1. **Descargar PDF:** genera los reportes correspondientes con el evaluador.



17. Violencia Laboral (ERV)

Evaluación del riesgo de violencia en el entorno laboral, con análisis de controles físicos y de acceso.

17.1 Particularidad de la escala de controles

En la sección de controles físicos y de acceso, la escala está diseñada de forma que, a mejor control existente, menor es el riesgo resultante. Es decir, contar con controles sólidos reduce la valoración de riesgo.

17.2 Cómo se usa

1. **Datos iniciales:** sitio registrado, área y responsable.
2. **Responder las secciones:** incluida la de controles físicos y de acceso.
3. **Escribir la conclusión:** el evaluador documenta su conclusión.
4. **Guardar y descargar PDF:** el PDF incluye el sitio evaluado, el área y el evaluador.

> **Filtro por sitio:** ERV se integra al Dashboard mostrando el resultado por sitio, con escala de riesgo (riesgo bajo = verde).

18. Registro de Incidentes

Bitácora estructurada de incidentes de seguridad. Es la base para el análisis de tendencias y para las investigaciones.

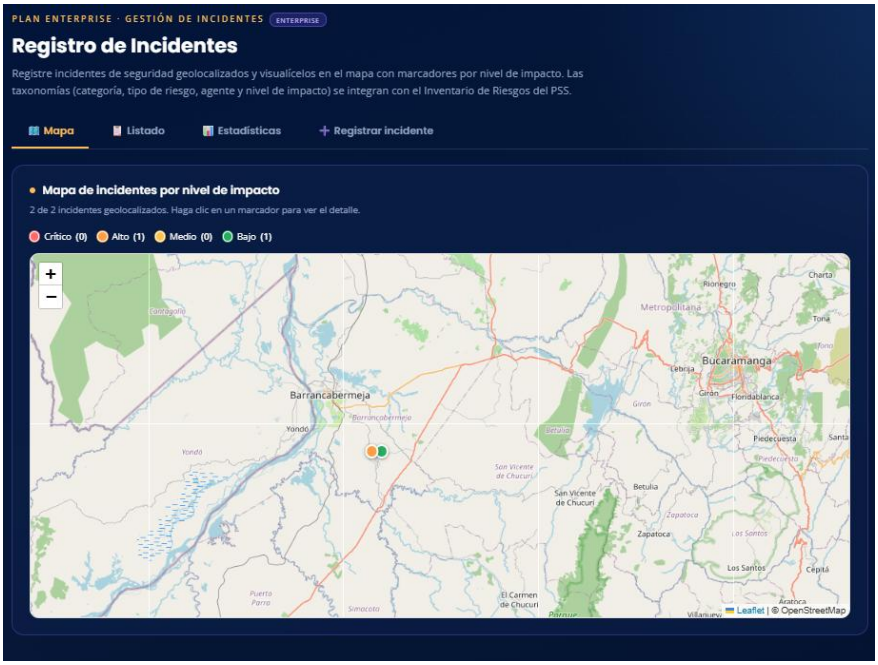
18.1 Registrar un incidente

Use el botón "Registrar incidente" y complete los campos:

- **Fecha del incidente y Hora —** cuándo ocurrió.
- **Tipo de ubicación —** sitio registrado o sitio externo.
- **Sitio / instalación —** la instalación donde ocurrió (o el sitio externo).
- **Área específica —** ubicación puntual dentro del sitio.
- **Ciudad y País —** ubicación geográfica.
- **Categoría de riesgo —** clasificación general.
- **Tipo de riesgo materializado —** qué tipo de evento ocurrió.
- **Factor de riesgo y Agente de riesgo —** qué y quién lo originó.
- **Nivel de impacto —** severidad del incidente.
- **Latitud / Longitud —** coordenadas para su ubicación en el mapa.

18.2 Vistas del módulo

- **Lista —** todos los incidentes registrados.
- **Mapa —** ubicación geográfica de los incidentes.
- **Estadísticas —** análisis y tendencias.

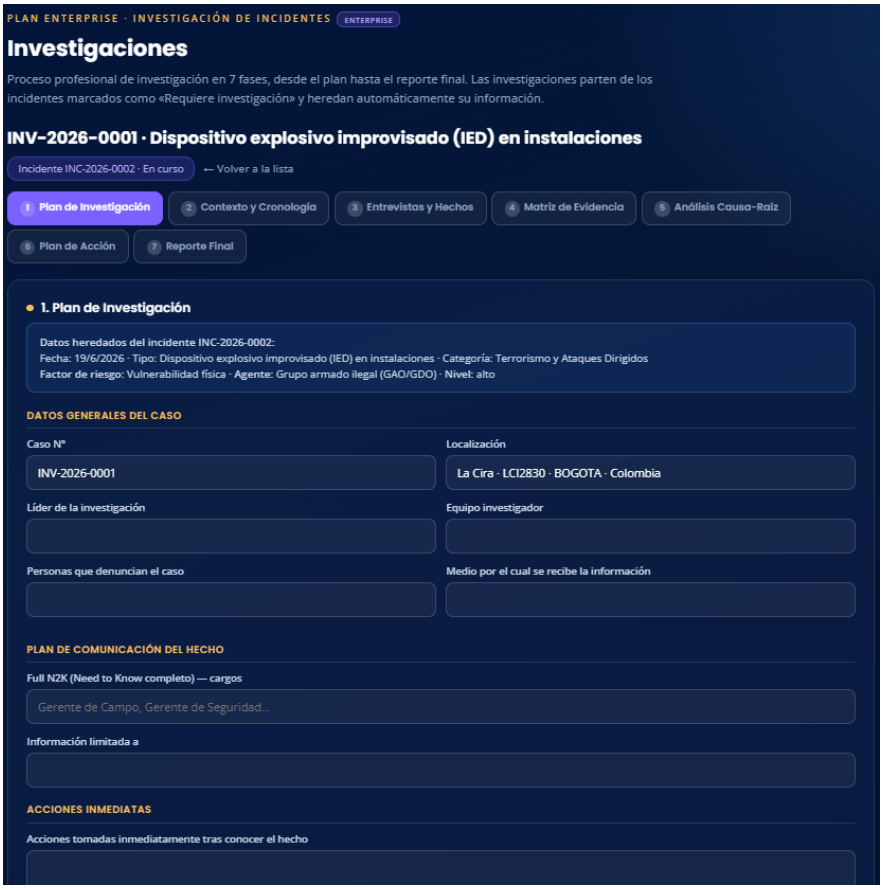


19. Investigaciones

Gestión de investigaciones asociadas a incidentes, con seguimiento del estado (abiertas/cerradas) y su porcentaje de cierre.

19.1 Cómo se usa

1. **Originar desde un incidente:** la investigación hereda la información del incidente de origen, incluido su sitio.
2. **Documentar la investigación:** avance, hallazgos y estado.
3. **Cerrar:** marque la investigación como cerrada al concluir.
4. **Descargar PDF:** con el evaluador y los detalles.



> **En el Dashboard:** Investigaciones muestra el porcentaje de casos cerrados por sitio (por ejemplo, "7/10 cerradas").

PARTE V · JUSTIFICACIÓN DE INVERSIÓN

20. ROSI · Retorno de la Inversión en Seguridad

Disponible en el plan Enterprise.

ROSI traduce la inversión en seguridad a lenguaje financiero: cuánto ahorra la organización al prevenir incidentes. Se calcula en dos pasos.

> **Fórmula:** ROSI = (ALE × Mitigación − Costo) / Costo, donde ALE = SLE × ARO.

20.1 Datos del análisis

- **Título del análisis —** nombre descriptivo (ej. "Sistema de control de acceso perimetral").
- **Sitio —** opcional, para asociarlo a una instalación.
- **Fecha y Evaluador —** fecha del análisis y responsable.

20.2 Paso 1 — SLE (pérdida por un evento)

Sume los componentes del costo de un solo incidente. Puede agregar tantos componentes como necesite con "+ Agregar componente".

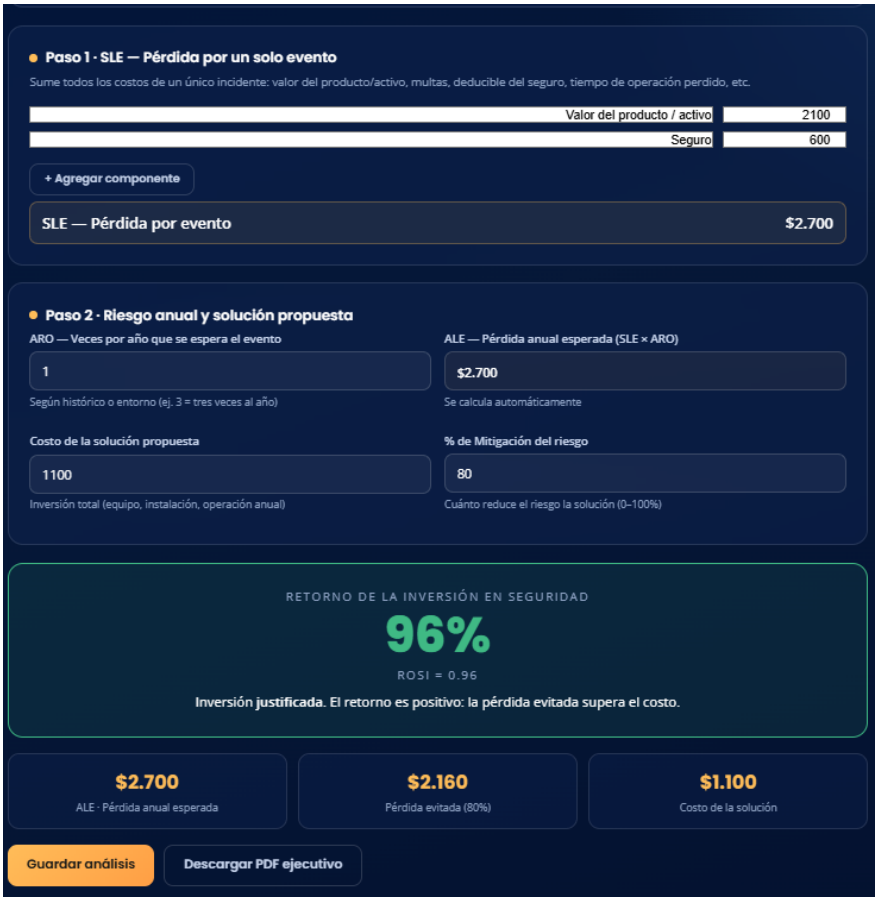
- **Componentes del SLE —** valor del activo, multas, deducible, tiempo de operación perdido, etc.

20.3 Paso 2 — Riesgo anual y solución

- **ARO —** número de veces por año que se espera el evento.
- **ALE —** se calcula automáticamente (SLE × ARO).
- **Costo de la solución —** inversión total de la medida propuesta.
- **% de Mitigación —** cuánto reduce el riesgo la solución (0–100%).

20.4 Resultado y acciones

El módulo muestra el ROSI en porcentaje, con métricas de apoyo (ALE, pérdida evitada, costo). Puede guardar el análisis, consultarlo en "Análisis guardados", y generar un PDF ejecutivo con "Descargar PDF ejecutivo".



> **Interpretación:** un ROSI positivo indica que la inversión evita más pérdidas de lo que cuesta. Por ejemplo, ROSI = 2 significa 200% de retorno.

21. T-FINE · Método Fine

Disponible en el plan Enterprise.

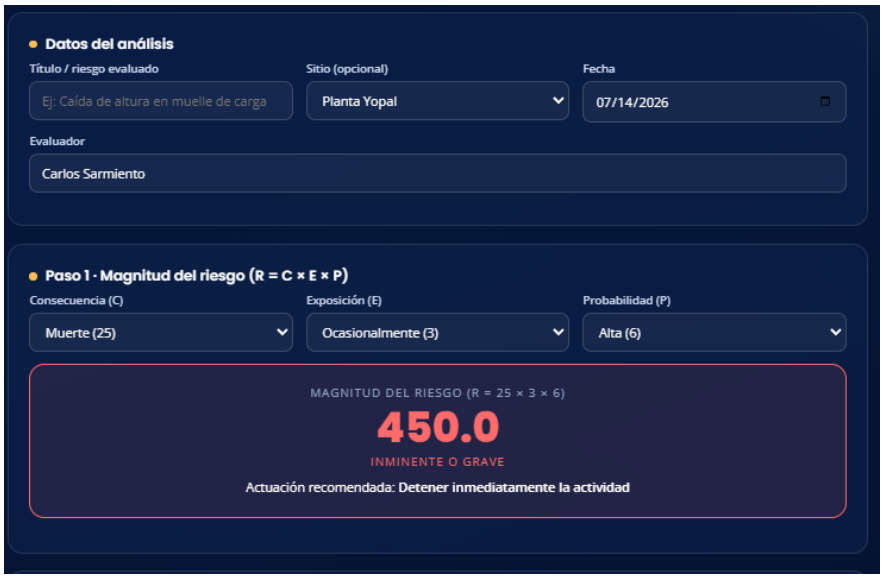
Calcula la magnitud de un riesgo y determina si la inversión para corregirlo está justificada. La primera pestaña, "Configurar costos (FC)", debe completarse antes de calcular.

> **Fórmulas:** Magnitud R = Consecuencia × Exposición × Probabilidad. Justificación J = R / (Factor de Costo × Grado de Corrección).

21.1 Configurar costos (FC) — primero

Cada empresa define sus propios rangos de costo para el Factor de Costo, ya que la estructura de costos varía entre organizaciones.

1. **Abrir "Configurar costos (FC)":** es la primera pestaña del módulo.
2. **Definir la moneda:** USD, COP u otra.
3. **Establecer los rangos:** para cada nivel de FC, indique el rango de montos (desde / hasta).
4. **Guardar configuración:** con el botón correspondiente.



21.2 Calculadora

Paso 1 — Magnitud del riesgo (R = C × E × P)

- **Consecuencia (C) —** severidad esperada.
- **Exposición (E) —** frecuencia de exposición al riesgo.
- **Probabilidad (P) —** probabilidad de que ocurra.

El módulo muestra R y el nivel de actuación recomendado.

Paso 2 — Justificación (J)

- **Costo de la medida —** se traduce automáticamente a Factor de Costo según su configuración.
- **Grado de Corrección (GC) —** cuánto reduce el riesgo la medida.

El módulo calcula J e indica si la inversión está justificada (J > 20), es probable (10–20) o no se justifica (< 10).

> **Guardar y PDF:** guarde el análisis para el historial y descargue el PDF para la sustentación.

22. Disponibilidad y Cubrimiento

Disponible desde el plan Professional.

Monitorea el estado operativo de los sistemas de seguridad física de cada sitio. Trabaja con cuatro sistemas: Cámaras (CCTV), Control de acceso, Vigilantes y Sensores de alarma.

22.1 Estructura

El módulo presenta una pestaña por cada sitio de la empresa. Dentro de cada sitio, los cuatro sistemas se muestran como tarjetas.

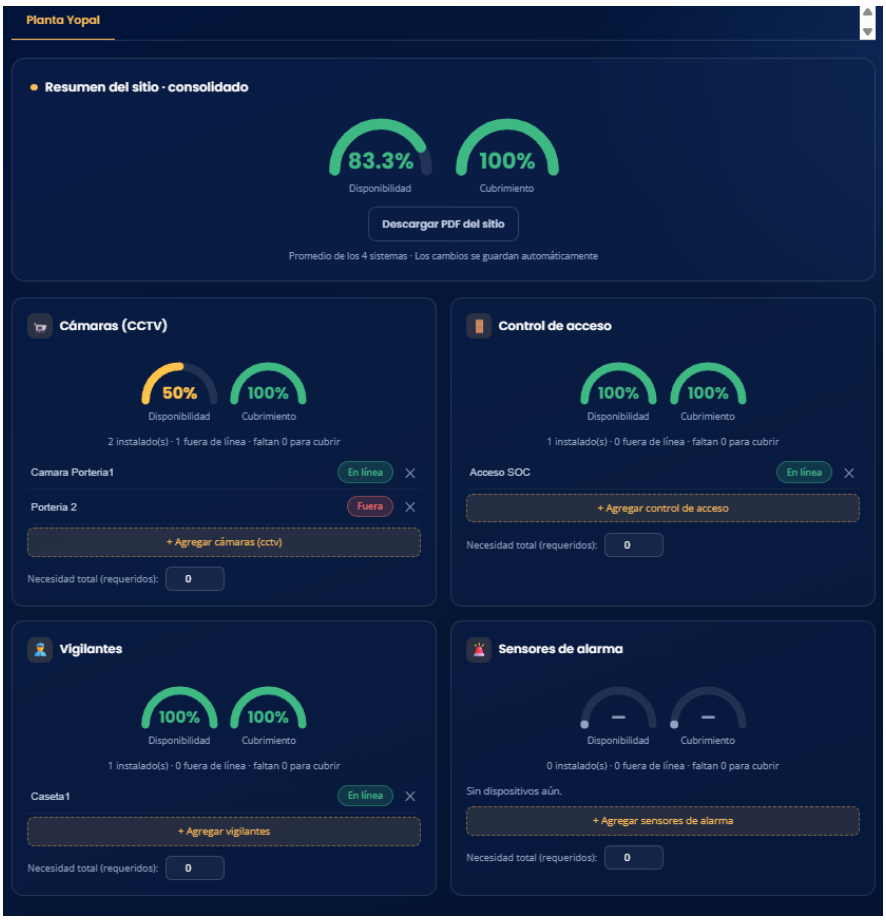
22.2 Registrar dispositivos

1. **Seleccionar el sitio:** use las pestañas superiores.
2. **Agregar dispositivo:** en la tarjeta del sistema, use "+ Agregar" y asigne un nombre descriptivo (ej. "Cámara portería principal", "Vigilante parqueadero", "Control acceso SOC", "Sensor intrusión Presidencia").
3. **Marcar estado:** indique si cada dispositivo está "En línea" o "Fuera" con el botón de estado.
4. **Definir necesidad:** en cada sistema, indique la necesidad total (cuántos dispositivos se requieren).

22.3 Cálculos automáticos

- **Disponibilidad =** 100 − (fuera de línea × 100) / instalados.
- **Cubrimiento =** (instalados × 100) / (instalados + faltantes).

Los resultados se muestran en gráficas tipo reloj (medidor): uno por cada sistema y un consolidado del sitio (promedio de los cuatro sistemas). Los colores siguen un semáforo: verde (≥80%), amarillo (≥50%), rojo (<50%).



22.4 Reporte PDF

El botón "Descargar PDF del sitio" genera un reporte con los consolidados, la tabla por sistema, el detalle de dispositivos con su estado, y la metodología.

> **En el Dashboard:** este módulo aparece en el Dashboard Ejecutivo mostrando el sistema más crítico (el peor resultado) de cada sitio.

23. Dashboard Ejecutivo

Disponible en el plan Enterprise.

El Dashboard consolida los resultados de los módulos en una sola vista, con filtro por sitio. Es la herramienta para presentar el estado de seguridad a la alta gerencia.

23.1 Qué muestra

- El estado de cada módulo que tenga datos, con semáforos (verde / amarillo / rojo).
- Para los módulos de riesgo, la escala se invierte: un riesgo bajo se muestra en verde.
- El filtro por sitio permite ver una instalación específica o el consolidado general.

23.2 Módulos que alimentan el Dashboard

Entre otros: PSS, Madurez, Amenazas, BCP, PBIP, ERV, Investigaciones (con % de casos cerrados) y Disponibilidad y Cubrimiento (sistema más crítico).

> **Consejo:** asocie siempre sus evaluaciones a un sitio. Así el Dashboard mostrará el panorama por instalación y permitirá comparar entre sedes.

24. Reportes PDF y evaluador

La mayoría de módulos permiten descargar un reporte en PDF con la identidad de Sigma360, listo para imprimir o compartir.

24.1 Contenido común de los reportes

- Encabezado con la marca Sigma360.
- Sitio evaluado, fecha y código consecutivo.
- El nombre del evaluador (usuario que elaboró la evaluación).
- Los resultados y el detalle propios de cada módulo.

> **Evaluador:** el nombre del evaluador corresponde al usuario en sesión al crear la evaluación. Por eso cada persona debe usar su propio usuario.

24.2 Cómo generar el PDF

1. **Abrir la evaluación:** o terminar de completarla.
2. **Descargar PDF:** use el botón correspondiente del módulo.
3. **Imprimir o guardar:** se abre el cuadro de impresión del navegador; elija "Guardar como PDF" o imprima.

Sigma360 · Informe Ejecutivo de Seguridad

Empresa · Toda la compañía · Generado el 14 de jul de 2026 · 10 módulos incluidos

AVANCE GLOBAL	MÓDULOS	EN ÓPTIMO	CRÍTICOS
54%	10	4	3

Avance por módulo

Madurez del Programa

• Atención
Última: 15 de jun de 2026

Continuidad (BCP)

• Atención
Última: 29 de jun de 2026

Perfil de Riesgo

• Óptimo · Bajo
Última: 17 de jun de 2026

Cadena de Suministro

• Crítico
Última: 01 de jul de 2026

Análisis PESTEL

• Óptimo · BAJO
Última: 29 de jun de 2026

CARVER — Criticidad

• Crítico · CRÍTICA
Última: 19 de jun de 2026

Evaluación de Vendors

• Óptimo
Última: 14 de jul de 2026

Seguridad Portuaria (PBIP)

• Óptimo
Última: 22 de jun de 2026

Riesgo de Violencia Laboral

• Atención · ELEVADO
Última: 01 de jul de 2026

Investigaciones

25. Administración y superadmin

25.1 Panel de administración (empresa)

El administrador de la empresa gestiona desde el panel: usuarios y sitios, su cuenta (cambio de contraseña), y la mejora de plan.

25.2 Superadministración (Sigma360)

El superadministrador gestiona todas las empresas de la plataforma. Puede:

- Cambiar el plan de una empresa (Starter / Professional / Enterprise).
- Activar o suspender empresas.
- Exportar los datos de una empresa (ver capítulo 26).

> **Acceso restringido:** el rol de superadministrador está reservado a la operación de Sigma360 y no está disponible para los clientes.

26. Exportación y portabilidad de datos

La información registrada es propiedad de cada cliente. La plataforma permite exportar todos los datos de una empresa de forma íntegra y segura, por ejemplo cuando un cliente decide retirarse.

26.1 Cómo exportar (superadmin)

1. **Ir al panel de superadmin:** ubique la empresa en el listado.
2. **Pulsar "Exportar":** confirme la acción.
3. **Descargar archivos:** se generan dos: un Excel y un JSON.

26.2 Qué contiene

- **Excel —** una hoja por módulo, legible directamente; incluye portada y usuarios.
- **JSON —** todos los datos estructurados, para integración con otros sistemas (incluido Power BI).
- Todos los datos de negocio: sitios, evaluaciones, incidentes, investigaciones, análisis y sus detalles.

26.3 Seguridad de la información (tríada CIA)

- **Integridad —** exporta todos los datos con metadatos de generación.
- **Confidencialidad —** nunca incluye contraseñas; solo el superadmin puede generarla.
- **Disponibilidad —** en formatos estándar (Excel/JSON) usables de inmediato.

Cada exportación queda registrada en auditoría (quién, cuándo, qué empresa).

26.4 Cómo usa el cliente los archivos

- El Excel se abre directamente para consultar o conservar la información.
- El JSON puede cargarse en Power BI, Excel Power Query u otro sistema para análisis o migración.

> **Entrega segura:** para la entrega, se recomienda comprimir los archivos con contraseña y compartir la clave por un canal distinto, además de dejar constancia de la entrega.

27. Privacidad y cumplimiento legal

Sigma360 procura alinear el tratamiento de datos con las normativas de los principales países de Latinoamérica donde opera: Colombia, México, Argentina, Chile, Perú y Ecuador.

- Aviso de cookies con consentimiento previo real: la analítica solo se activa si el visitante acepta.
- Política de Tratamiento de Datos y Términos de Uso adaptados a la región.
- Respeto a los derechos de los titulares: acceso, rectificación, actualización, supresión y oposición.

> **Importante:** los documentos legales constituyen una base que debe ser revisada por un asesor legal antes del uso comercial definitivo, y completada con los datos del responsable del tratamiento.

28. Buenas prácticas

- Registre primero sus sitios: casi todos los módulos se benefician de asociar la evaluación a un sitio.
- Asigne un usuario a cada miembro del equipo, para trazabilidad en los reportes.
- Configure los rangos de costo (FC) en T-FINE antes de usar la calculadora.
- Realice evaluaciones periódicas para observar tendencias en el Dashboard.
- Descargue y archive los reportes PDF como respaldo documental.
- Use ROSI y T-FINE para preparar las sustentaciones de inversión.
- Mantenga actualizado el módulo de Disponibilidad y Cubrimiento.
- Cierre sesión al terminar en equipos compartidos.

29. Solución de problemas frecuentes

Situación	Qué hacer
Un módulo aparece con candado	Su plan no lo incluye. Los de justificación de inversión (ROSI, T-FINE) y el Dashboard requieren Enterprise; Disponibilidad y Cubrimiento requiere Professional o superior.
No veo un cambio reciente	Recargue la página forzando la actualización (Ctrl+Shift+R) para omitir la caché del navegador.
No aparecen mis sitios en un módulo	Verifique que los sitios estén registrados en el panel de administración.
El reporte no muestra mi nombre	Asegúrese de haber iniciado sesión con su propio usuario antes de crear la evaluación.
Alcancé el límite de sitios o usuarios	Mejore su plan desde el panel de administración.

30. Glosario

- **ALE (Annual Loss Expectancy) —** pérdida anual esperada = SLE × ARO.
- **ARO (Annual Rate of Occurrence) —** número de veces por año que se espera un evento.
- **CARVER —** metodología de criticidad de activos (Criticidad, Accesibilidad, Recuperabilidad, Vulnerabilidad, Efecto, Reconocibilidad).
- **Cubrimiento —** porcentaje de la necesidad de dispositivos que está satisfecha.
- **Disponibilidad —** porcentaje de dispositivos que están operativos (en línea).
- **Duty of care —** deber de cuidado de la organización hacia sus colaboradores.
- **Evaluador —** usuario que elabora una evaluación; aparece en el reporte PDF.
- **Factor de Costo (FC) —** en T-FINE, nivel asociado al costo de una medida; sus rangos los define cada empresa.
- **Método Fine —** metodología para calcular la magnitud de un riesgo y justificar su corrección.
- **Mosler —** método de análisis y clasificación de riesgos usado en el PSS.
- **Multi-tenant —** arquitectura donde varios clientes comparten el sistema con datos aislados.
- **PESTEL —** análisis del entorno (Político, Económico, Social, Tecnológico, Ecológico, Legal).
- **PSS (Physical Security Survey) —** evaluación integral de seguridad física.
- **ROSI —** retorno de la inversión en seguridad.
- **SLE (Single Loss Expectancy) —** pérdida esperada por un solo evento.