Seguridad y Operaciones de OT – Solución de la plataforma OT Mash4GUARD

Servicios de evaluación, implementación y plataforma modular (ACCESS, INSIGHT, RESCUE)

Mashfrog Group

Resumen

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

1. Resumen Ejecutivo

Este documento describe las principales características de la plataforma OT de Mashfrog. La plataforma es una **solución integrada y modular** basada en componentes Edge que asegura:

- Acceso seguro a plantas OT, vinculado a la identidad corporativa, la clave/WebAuthn y un broker de sesiones basado en Edge;
- Visibilidad pasiva y continua del tráfico OT a través de sensores de red y motores DPI, integrados con sistemas SIEM corporativos;
- Protección y versión de PLC, SCADA y configuraciones de dispositivos de red, con orquestación de copias de seguridad, validación automatizada y retroceso verificable.

El modelo estándar de implementación de la solución está estructurado en dos fases.

La **fase inicial de evaluación** produce el inventario de activos OT y sistemas informáticos relacionados, el mapeo de sitios y redes, la clasificación de dispositivos y protocolos, los flujos de comunicación y las dependencias operativas; también define líneas base, criterios de control y requisitos de integración con IdM/SSO, SIEM, CMDB/ITSM y sistemas de respaldo existentes.

Tras la evaluación, se activa la plataforma compuesta por los módulos ACCESS, INSIGHT y RESCUE: ACCESS implementa control de acceso privilegiado y trazabilidad de sesión, aprovechando una autenticación fuerte (SSO, claves de acceso/WebAuthn) y una pasarela Edge que abre las sesiones hacia las plantas solo tras comprobaciones de identidad, contexto y autorización; INSIGHT proporciona visibilidad pasiva del tráfico OT con DPI de protocolo industrial, enriquecimiento contextual (activos, sitios, líneas) y generación de eventos/alertas integrables de forma nativa en sistemas SIEM; RESCUE gestiona la orquestación de copias de seguridad, la revisión de versiones y la validación de configuración con flujos de trabajo de cambios, aprobación y rollback automatizado.

La modularidad permite la adopción selectiva: es posible implementar uno o más módulos, sin la obligación de activarlos todos, por ejemplo, comenzando solo desde el control remoto o solo la visibilidad de la red.

La integración de los tres módulos reduce la fragmentación de herramientas, estandariza interfaces y procesos, y permite la adopción de controles de "seguridad desde el diseño"

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

dentro de los procesos existentes (IdM/SSO, SIEM/SOAR, CMDB/ITSM, ticketing). El resultado es control centralizado, validación automatizada de configuración y gestión operativa medible, con evidencia de auditoría y alineación natural con los requisitos regulatorios y de cumplimiento para la seguridad OT.

2. Contexto y desafíos

Los entornos industriales modernos se enfrentan a desafíos crecientes relacionados con la complejidad de las **redes OT (Tecnología Operativa**). La coexistencia de sistemas heterogéneos, a menudo distribuidos en múltiples sitios, dificulta lograr **una visibilidad unificada de activos** y flujos de comunicación.

En muchos casos, el acceso no se gestiona de forma centralizada y faltan procesos estructurados para **el control de la operación y la trazabilidad** , con riesgo de intervenciones no autorizadas o no documentadas. Además, la ausencia de **versionado de configuración** conduce a cambios manuales no validados y a una capacidad de retroceso limitada en caso de error o fallo.

Estas condiciones conllevan riesgos concretos:

- **Tiempo de inactividad no planificado**, con impactos directos en la producción.
- **Superficie de ataque ampliada**, exponiendo la infraestructura a posibles intrusiones o malware.
- **Dificultad para cumplir** con las normativas de seguridad y los estándares industriales.
- **Aumento de los costes operativos** debido a ineficiencias y gestión fragmentada de herramientas.

Para abordar estos desafíos, es necesario adoptar un enfoque que combine **servicios de evaluación** y una **plataforma integrada** capaz de ofrecer control, automatización y seguridad desde el diseño.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

3. Enfoque por fases

La implementación de la solución está diseñada para seguir un **camino gradual y no disruptivo**, minimizando el impacto de las plantas y asegurando una adopción segura y progresiva.

El calendario se define conjuntamente durante el inicio del proyecto y se documenta en un Plan de Proyecto.

La solución incluye la definición conjunta del alcance mediante un taller de alcance guiado por **el impacto operativo** y **el riesgo cibernético**.

Juntos identificamos las plantas "de referencia" más representativas/críticas y verificamos los requisitos técnicos previos (SSO/PAM, SPAN/TAP/NetFlow, alcance de la dirección).

Para cada planta, se completa una hoja de perfil con clases de dispositivo, protocolos, patrones de acceso, tipos de cambio, restricciones de seguridad y ventanas operativas.

El alcance se congela entonces con puertas de etapa de entrada/salida, definición de RACI y KPIs base para medir el valor y **la reutilización** a través de ACCESS, INSIGHT y RESCUE.

El plan está estructurado en tres fases principales:

➤ **Fase 1 – Evaluación**

- **Encuesta de sitios, redes y dispositivos OT/IT/IoT:** Un equipo de expertos realiza un análisis exhaustivo para identificar y mapear sitios, redes y todos los dispositivos OT/IT/IoT, incluidos los protocolos industriales en uso.
- **Población de la base de datos de activos con información estructurada y correlacionada**: Los datos recopilados se introducirán en una base de datos central para crear un inventario estructurado y dinámico de activos, completo con información sobre riesgos y vulnerabilidades.
- **Definición de una línea base operativa como punto de referencia para fases posteriores:** se establece una "línea base" operativa, que proporciona un punto de referencia para el rendimiento normal del sistema y para la monitorización futura.

➤ **Fase 2 – Implementación en el borde**

- **Instalación y configuración de dispositivos Edge en sitios piloto:** Instalación y configuración de dispositivos Edge en sitios piloto (en el caso de módulos INSIGHT o ACCESS), que actuarán como gateways para la recopilación de datos industriales.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

- **Integración de protocolos estándar y propietarios**: Se implementa la integración con protocolos estándar (como Modbus, OPC-UA) y propietarios para iniciar la recogida del tráfico de red y garantizar la visibilidad operativa completa.
- **Activación de la recogida de tráfico de red** para permitir visibilidad y monitorización.

➤ **Fase 3 – Operaciones**

- **Activación progresiva de los módulos ACCESS, INSIGHT y RESCUE**: Los módulos se activan y configuran progresivamente para el sitio piloto, haciendo que la solución esté totalmente operativa.
- **Habilitación del seguimiento centralizado y control del acceso privilegiado**: Habilitar la gestión centralizada del acceso privilegiado. Cada sesión de control y modificación se rastrea y monitoriza en tiempo real.
- **Monitorización continua del tráfico OT con generación e informes de alertas:** La plataforma comienza a monitorizar el tráfico OT, identificando anomalías y generando alertas e informes detallados para una respuesta oportuna.
- Implementación de **versionado de configuración**, con procesos de validación y capacidad de retroceso en caso de anomalías: Se implementa el versionado automático de configuraciones de dispositivos. Esto incluye habilitar procesos de validación (aprobación de cambios) y la posibilidad de **revertir** inmediatamente a una versión anterior y segura en caso de problemas, asegurando la continuidad operativa.

4. Andén Mash4GUARD

4.1 Resumen

La plataforma representa un único **panel** centralizado para la gestión integrada de **entornos OT, TI e IoT** . A través de una sola interfaz, consolida y gestiona el inventario de activos, los perfiles de usuarios y acceso, los registros de sesiones y actividades, y las configuraciones de los dispositivos.

Este enfoque elimina la fragmentación de las herramientas y garantiza **una visibilidad completa de todo el ecosistema tecnológico**, mejorando la eficiencia operativa, la postura de seguridad y la gobernanza general. La plataforma actúa como una "fuente única de verdad" para todos los datos de seguridad y operativos.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

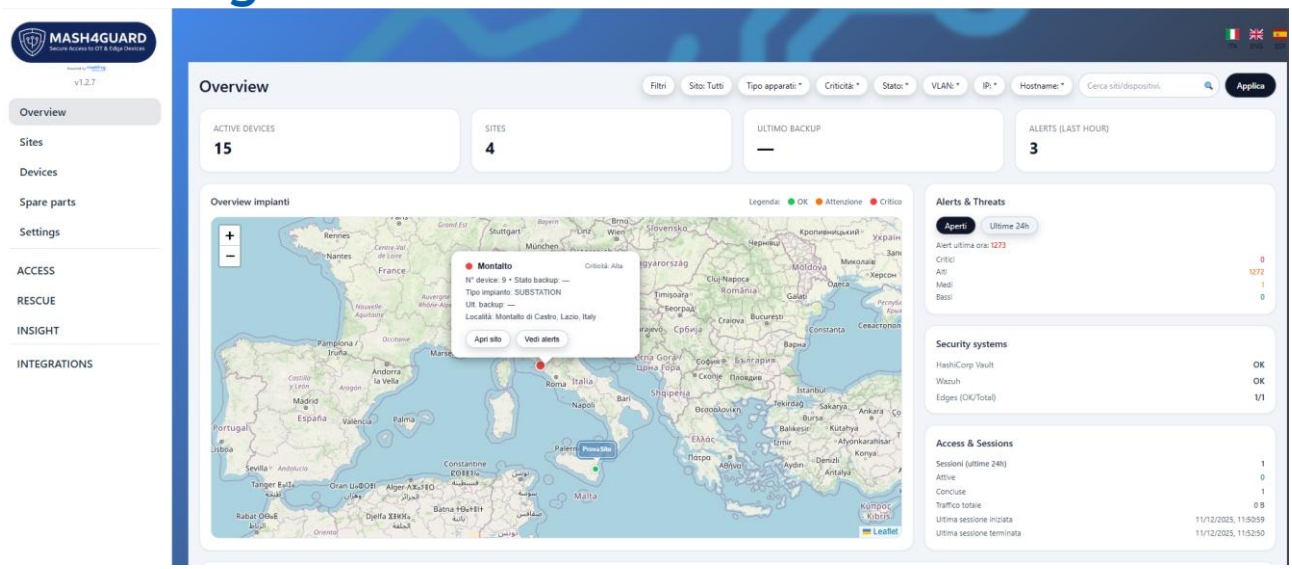

Imagen 1- Panel centralizado

4.2 Módulo ACCESS

El módulo **ACCESS** gestiona el acceso privilegiado seguro a plantas y sistemas OT, actuando como un punto de entrada único para operadores internos, mantenedores y proveedores externos. Se integra de forma nativa con servicios de identidad como Active Directory, LDAP y Entra ID, aprovechando SSO corporativo, autenticación multifactor y contraseña/WebAuthn.

El acceso a las plantas se realiza a través de un broker de sesiones basado en Edge (no por conexión directa ni credencial compartida). El usuario se autentica en la plataforma, solicita acceso a un activo OT específico y solo tras una autorización positiva se abre una sesión controlada (RDP, SSH, VNC, web) desde Edge a través del dispositivo. Las credenciales técnicas son gestionadas y protegidas por la plataforma (evitando su exposición a operadores y terceros y reduciendo el riesgo de mal uso).

Se admiten el control granular de RBAC, los ámbitos temporales, las ventanas de mantenimiento, la separación de funciones (SoD) y los flujos de trabajo de aprobación (por ejemplo, abrir el acceso solo si está asociado a un ticket o un cambio autorizado)

El control es granular y basado en roles (RBAC), con la capacidad de definir plazos, ventanas de mantenimiento, separación de funciones (SoD) y, cuando sea necesario, flujos de trabajo de aprobación (por ejemplo, abrir accesos solo si está asociado a un ticket o un cambio autorizado). Cada sesión puede ser rastreada y, cuando sea necesario, grabada, generando

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

registros detallados para auditoría y cumplimiento (quién hizo qué, cuándo y en qué dispositivos).

El principal valor es la capacidad de mantener siempre una visión clara y centralizada del acceso a los sistemas OT, reduciendo drásticamente el riesgo de acceso no autorizado o no rastreable. Un sólido sistema de registro y auditoría también proporciona la evidencia necesaria para el cumplimiento y la presentación de informes a auditores internos y externos.

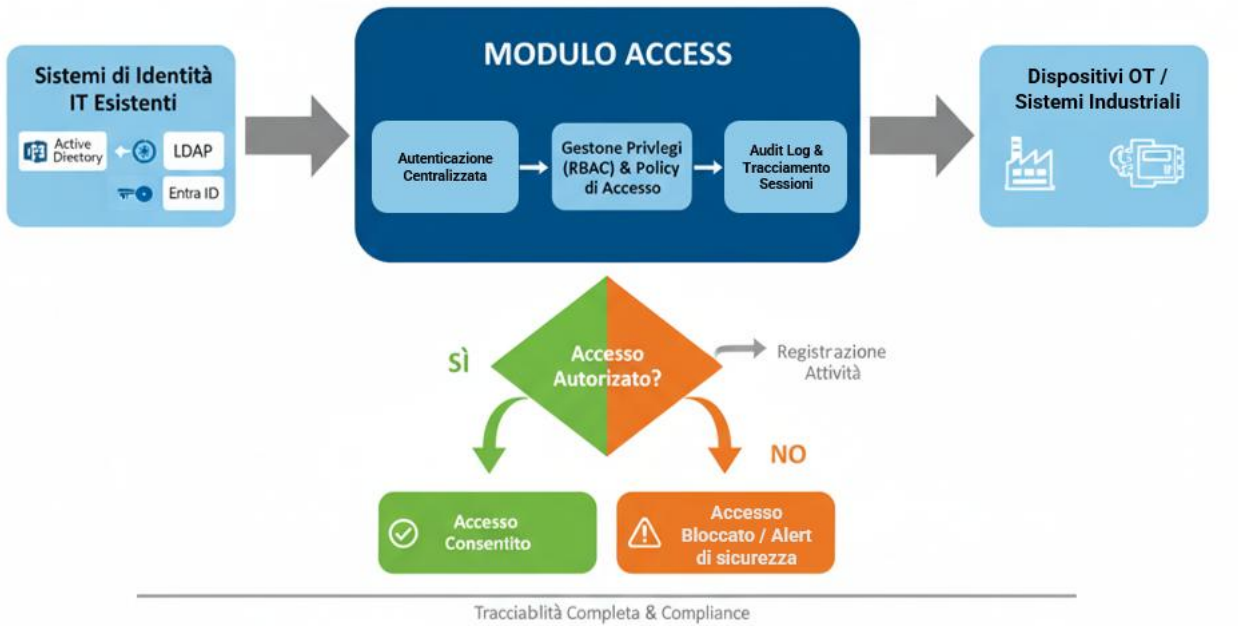

Imagen 2 – Proceso de acceso

4.3 Módulo INSIGHT

El módulo **INSIGHT** recopila y analiza el tráfico de red OT en tiempo real, proporcionando una visibilidad profunda de los flujos de comunicación entre PLCs, SCADA, HMIs, dispositivos de red y sistemas de supervisión. La solución se basa en sensores pasivos instalados en dispositivos Edge utilizando motores DPI avanzados (por ejemplo, Suricata, Zeek y analizadores de protocolos industriales) para decodificar los principales protocolos OT (Modbus, OPC-UA, Ethernet/IP, etc.) y enriquecer eventos con contexto operativo.

INSIGHT construye un mapa dinámico de activos, identificando qué dispositivos se comunican con quién, sobre qué protocolos y con qué patrones de tráfico. Según este mapa, genera eventos/alertas en caso de anomalías (nuevos dispositivos no registrados, cambios repentinos en los flujos, comandos no estándar, intentos de acceso anómalos) que pueden filtrarse y correlacionarse para reducir el ruido y centrarse en escenarios realmente significativos.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

Se integra con los principales **sistemas SIEM ya configurados en la empresa (por ejemplo, Wazuh, Splunk, QRadar, Microsoft Sentinel) para correlacionar eventos OT y TI dentro de una única vista**. De este modo, el equipo de seguridad obtiene un conocimiento integral del panorama de amenazas y puede adoptar casos de uso y manuales específicos para el entorno industrial (por ejemplo, detección de escaneos en puertos OT, comandos potencialmente destructivos, propagación lateral de TI a OT).

INSIGHT representa el componente de visibilidad NDR (Network Detection and Respons)/de la plataforma OT: permite pasar de una visibilidad parcial y fragmentada a una monitorización continua y estructurada, alineada con los requisitos de detección, análisis y respuesta establecidos en los estándares de seguridad OT.

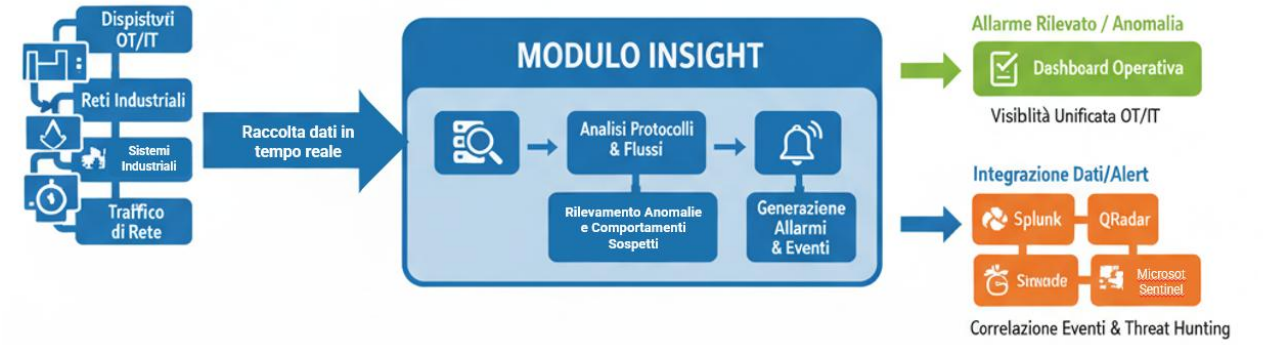

Imagen 3 – Proceso de inspección

4.4 Módulo de RESCUE

El módulo **RESCUE** introduce un nivel avanzado de gestión y protección de configuración, incorporando los principios de Gestión del Cambio, el versionado y la validación continua típicos de los procesos CI/CD en el mundo de TI al entorno OT. Su objetivo es garantizar la continuidad del negocio y la consistencia de las configuraciones entre PLC, RTUs, HMIs, equipos de red y sistemas de supervisión, evitando errores humanos y cambios no conformes que puedan comprometer la producción. El módulo nació de un requisito cibernético (integridad, trazabilidad, separación de funciones) que genera un impacto directo y medible en las operaciones (calidad de los cambios, tiempos de recuperación, reducción de errores).

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

RESCUE actúa como un orquestador central de configuraciones de respaldo y OT: las configuraciones se extraen de forma estructurada del equipo, se almacenan en un repositorio versionado, relacionadas con las plantas y los cambios asociados. Esto te permite saber en todo momento qué versión de configuración está en producción, quién la aprobó y qué comprobaciones se realizaron antes del lanzamiento.

Las características clave incluyen:

- **Editor de Reglas y Políticas**: Definir políticas de configuración estandarizadas y políticas de cumplimiento para todas las clases de dispositivos. Las reglas actúan como un proceso de gestión digital del cambio, estructurando los cambios antes de su aplicación y asegurando que cada operación esté alineada con los estándares de seguridad y operativos de la empresa.
- **Gestión de variables y rangos permitidos**: cada parámetro configurable (direcciones IP, subredes, puertos, tiempos de espera, configuraciones de seguridad, etc.) puede definirse con valores permitidos o rangos numéricos/lógicos. Esto garantiza que todos los ajustes sean consistentes y compatibles, eliminando el riesgo de configuraciones arriesgadas o no estándar.
- **Validación automática y despliegue controlado**: antes de la aplicación, cada cambio se comprueba automáticamente según las reglas definidas. En caso de incumplimiento, el sistema bloquea el cambio, genera una alerta y mantiene activa la configuración anterior, evitando impactos negativos en las operaciones. La misma lógica permite despliegues progresivos (por línea, sitio, conjunto de equipos) con controles previos y posteriores al cambio.

RESCUE transforma la gestión de configuración de una actividad manual a un proceso controlado: cada cambio es versionado, "lint" por un módulo dedicado de Validación Sintáctica, aprobado por un tercero y liberado con pruebas firmadas. En caso de anomalía o incidente, se dispone de un retroceso seguro a la línea base y, si es necesario, de una recuperación rápida de copias de seguridad conocidas y validadas.

De este modo, RESCUE no solo actúa como un sistema de respaldo, sino como un verdadero Gestor de Elementos OT: el Operador trabaja más rápido y, con menos errores, la TIC obtiene control y prueba de conformidad. Mismo proceso, dos beneficios: continuidad y control.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

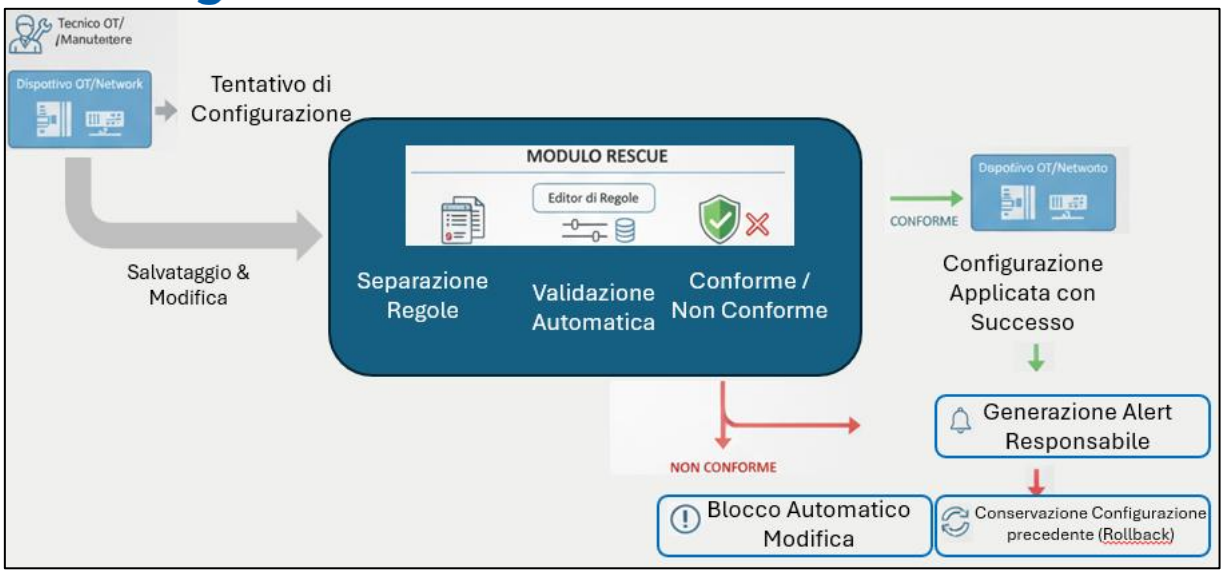

Imagen 4 – Proceso de gestión de configuración/versiones

RESCUE es el **Gestor de Elementos OT** que lleva la disciplina CI/CD a configuraciones de planta: el Operador trabaja más rápido y con menos errores, el TIC obtiene controles y pruebas de conformidad. Mismo proceso, dos beneficios: continuidad y control.

5. Integración con sistemas externos

Nuestra plataforma está diseñada con una arquitectura abierta y modular, que no pretende reemplazar los sistemas existentes, sino mejorarlos y ampliar su funcionalidad. Gracias al uso de **APIs** y conectores estándar, la solución se integra de forma nativa y bidireccional con las herramientas ya presentes en el ecosistema de TI y OT. Este enfoque maximiza el valor de las inversiones pasadas y permite flujos de trabajo más seguros, consistentes y eficientes.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

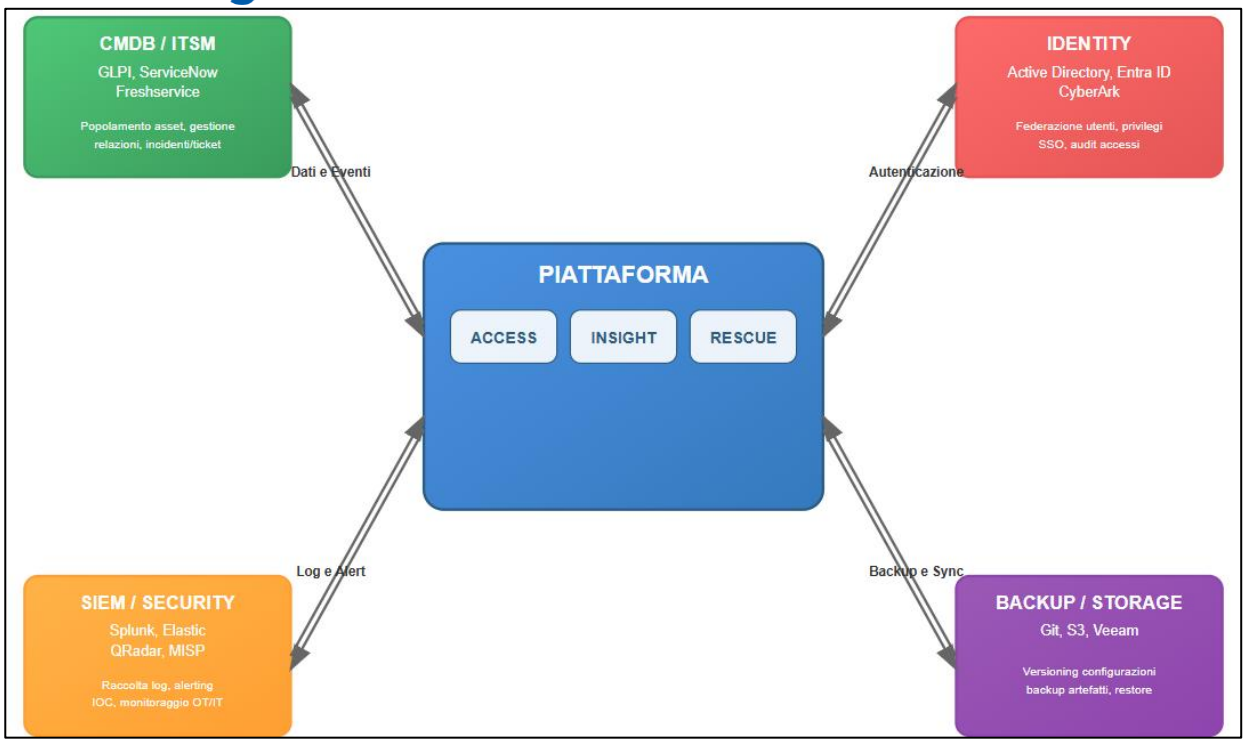

Imagen 5 - Integración con sistemas externos

La fortaleza de nuestra arquitectura radica en su capacidad para actuar como un puente entre diferentes mundos tecnológicos. Esto permite el uso de herramientas existentes, enriqueciendo los flujos de trabajo con datos específicos del entorno OT. Todo esto se realiza mediante **APIs estándar**, **webhooks** y **conectores nativos**, asegurando que los flujos operativos existentes no se interrumpan.

La integración con sistemas externos, como CMDB/ITSM, consolida el inventario de activos y automatiza los procesos de gestión. De manera similar, conectarse a sistemas de gestión de identidades y SIEM mejora la postura general de seguridad, proporcionando visibilidad unificada y control centralizado. Por último, la integración con sistemas de Copia de Seguridad y Almacenamiento garantiza la resiliencia y la continuidad del negocio, aspectos cruciales en cualquier entorno industrial.

6. Entrega (Deliverable)

Al finalizar la implementación, se entregarán los entregables técnicos y operativos esperados (documentación, configuraciones, libros de ejecución y pruebas de prueba), necesarios para una gestión autónoma y segura del entorno OT.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

Entrega	*Descripción*
Evaluación de activos e informe de inventario	Documento detallado que destaca el estado actual de los activos OT/IT/IoT, su clasificación, vulnerabilidades encontradas y recomendaciones de mejora.
Panel Operativo Funcional	Una interfaz activa y poblada con datos en tiempo real del sitio piloto, lista para monitorización, análisis y gestión centralizada.
Plataforma y módulos operativos	La plataforma completa, con **módulos ACCESS**, **INSIGHT** y **RESCUE** , implementada y probada en el sitio piloto, está lista para su uso diario.
Informe de validación de configuración	Un informe que certifica la efectividad del proceso de versiones y validación (tipo CI/CD), demostrando la seguridad y consistencia de las configuraciones aplicadas.
Formación operativa y manual de usuario	Sesiones de formación dedicadas para el personal de TI y OT, acompañadas de un manual detallado para garantizar plena autonomía en el uso de la plataforma.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

7. Arquitectura lógica y diagrama de alto nivel

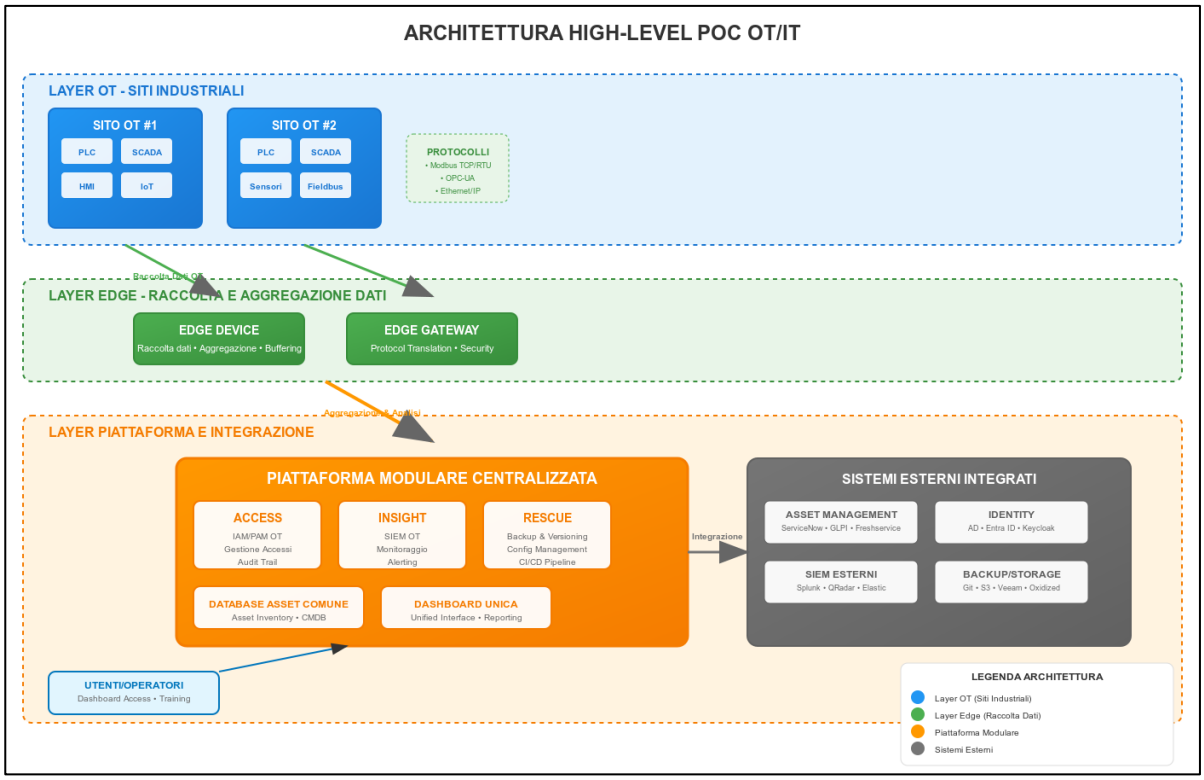

Imagen 6 – Diagrama de alto nivel

El diagrama muestra cómo la solución a través de nuestra plataforma OT/IT opera directamente en el sitio industrial. En **los sitios** OT (capa **azul**), máquinas, PLCs, SCADAs y sensores IoT generan datos constantemente durante las operaciones diarias.

Estos datos son recopilados por **Dispositivos Edge** (capa **verde**), dispositivos posicionados localmente que agregan tráfico de maquinaria, traducen protocolos industriales (como Modbus y OPC-UA) y aseguran que la información sea segura y lista para su procesamiento.

Desde la capa Edge, los datos se envían a la **Plataforma Modular central** (capa **naranja**), donde los módulos ACCESS, INSIGHT y RESCUE permiten la gestión de accesos, la monitorización de infraestructura OT, la copia de seguridad y la configuración de versiones, respectivamente.

La plataforma cuenta con una **base de datos común de activos** y un **único panel** de control, que ofrece a los operadores una visión completa y actualizada del estado de sus plantas. Finalmente, la plataforma se integra con **sistemas externos** como herramientas de gestión de activos, identidad, SIEM o soluciones de respaldo, permitiendo la sincronización e

interoperabilidad con TI empresarial. En la práctica, el flujo operativo es claro: los datos nacen en el sitio OT, son recogidos y preparados por el Edge, analizados y gestionados por la plataforma, y finalmente integrados con sistemas externos, permitiendo que operadores y gestores dispongan siempre de información fiable, en tiempo real, sin interrumpir la producción.

8. Hoja de ruta

La plataforma implementada define la línea base técnica para gestionar la seguridad y operación del entorno OT. Los resultados de la fase piloto permiten la extensión a un modelo multisitio, con aplicación uniforme de políticas, estandarización de procesos y visibilidad centralizada en todas las plantas.

Las evoluciones planificadas incluyen la extensión multi-sitio con escalabilidad de colectores y templatización de políticas; la automatización de cambios (despliegue de canarios, despliegue progresivo); la ampliación de la biblioteca de reglas DPI con soporte para protocolos adicionales (por determinar); la evolución de la API a la versión 2 con mecanismos de suscripción, consultas avanzadas y exportaciones en formatos adicionales; y mejoró la HA/DR con reducción de RPO/RTO y optimización de almacenamiento.

Nuestra hoja de ruta futura incluye:

- **Expansión multisitio**: Replicar el modelo exitoso en otros sitios de producción.
- **Evolución a la solución de** fabricación: Transición del sistema a una infraestructura de fabricación completa, con un plan continuo de mantenimiento y actualización.
- **Soporte** continuo: Ofrecer soporte técnico y servicios de consultoría para maximizar el retorno de la inversión a largo plazo.

Imagen 7 - Próximos pasos y beneficios

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

9. Alineación regulatoria (NIS 2 / IEC 62443)

La plataforma OT propuesta está diseñada para apoyar concretamente la adopción de las principales normativas y directrices en el ámbito industrial:

- la Directiva NIS 2 y su transposición nacional, con especial referencia a las obligaciones de gestión de riesgos, control de acceso, monitorización continua y gestión de incidentes;
- la serie IEC 62443 de normas, que definen los requisitos para sistemas de automatización y control industrial, con un enfoque en la gestión de accesos, la seguridad de las comunicaciones, la gestión de configuración y las capacidades de recuperación.

La contribución de la plataforma se organiza en torno a los tres módulos ACCESS, INSIGHT y RESCUE, que actúan como "ladrillos" tecnológicos para soportar los controles exigidos por la normativa.

9.1 Aproximación general

Desde un punto de vista regulatorio, la plataforma no se limita a introducir nuevas tecnologías, sino que estructura los procesos OT en una clave de "ciber por diseño":

- gobernanza: trazabilidad de accesos, cambios de configuración y actividades de mantenimiento en plantas y redes OT;
- medidas técnicas: autenticación fuerte, segregación de rutas de acceso, monitorización pasiva, gestión centralizada de copias de seguridad y configuraciones;
- Evidencia y auditorías: producción automática de registros, informes y referencias que constituyen la base documental para auditorías internas, inspecciones y comprobaciones de cumplimiento.

Esto resulta en una alineación natural con los requisitos de los principios de NIS 2 e IEC 62443 en relación con la gestión de riesgos, la defensa en profundidad y la separación entre plano de control y plano de datos.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

9.2 Contribución del módulo ACCESS

ACCESS aborda los requisitos de identidad, acceso privilegiado y trazabilidad:

- Autenticación y gestión de identidades de usuario
  - integración con la empresa IdM/SSO (AD, Entra ID, LDAP);
  - uso de claves de acceso/WebAuthn y MFA para acceder a los sistemas;
  - Reducción de credenciales locales en activos OT en favor de un broker de acceso centralizado.
- Gestionar y registrar el acceso remoto privilegiado a los activos
  - un broker de sesiones basado en Edge Gateway, que abre sesiones solo tras la verificación de identidad y autorización;
  - vinculación entre sesión, identidad, activos involucrados y motivación (ticket, cambio, intervención de mantenimiento).
- Separación de Roles y Deberes (SoD)
  - definición de roles distintos para operadores, técnicos de mantenimiento, administradores OT/TI y proveedores de servicios;
  - Capacidad para introducir aprobaciones multinivel para los accesos más críticos.
- Registro, asesoramiento y gestión de vulnerabilidades
  - generación de registros de acceso completos, exportables a sistemas SIEM y de auditoría;
  - integración con herramientas de ticketing/ITSM para vincular el acceso y los cambios a planes de remediación y gestión de vulnerabilidades.

De este modo, **ACCESS** contribuye directamente a la gestión de identidad y acceso, el registro y los controles de responsabilidad requeridos por NIS 2, ACN e IEC 62443.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

9.3 Contribución del módulo INSIGHT

INSIGHT cumple con los requisitos de monitorización, detección de amenazas y registro centralizado:

- Monitorización continua de los activos OT y los flujos de comunicación
  - sensores de red pasivos basados en motores de equipo de protección personal, instalados en los Edges;
  - Descubrimiento y mapeo dinámico de dispositivos industriales, líneas, celdas y protocolos.
- Registro y análisis de registros y eventos de OT
  - normalización de eventos de red OT y envío a SIEM;
  - correlación con eventos de TI para una visión integrada de las amenazas;
  - construcción de líneas de base conductuales con las que comparar nuevas actividades.
- Mecanismos de detección y alerta de amenazas
  - reglas y casos de uso específicos de la OT (comandos anómalos, escaneo, nuevos dispositivos, desviaciones de los flujos esperados);
  - alertas a SOC/CSIRT o a personas de contacto de OT para acciones de respuesta coordinadas.

INSIGHT permite la transición de la monitorización manual y parcial a un sistema estructurado de registro y detección, en línea con los requisitos de NIS 2 y ACN para monitorización continua, detección de incidentes e informes tempranos, y con los requisitos IEC 62443 para protección de comunicaciones y detección de condiciones anormales.

9.4 Contribución del módulo RESCUE

RESCUE cubre los requisitos relacionados con la gestión de configuración, la salud y las capacidades de recuperación:

- Copia de seguridad centralizada de configuraciones OT
  - extracción y almacenamiento de configuraciones de PLC, RTU, HMI, switches, cortafuegos, etc.;
  - Repositorio versionado, con trazabilidad de quién hizo la última modificación y cuándo.
- Optimización de la gestión del cambio

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

  - flujos de trabajo estructurados para propuestas, validación, aprobación y despliegue de cambios;
  - Comprobaciones automáticas de cumplimiento respecto a las normas y políticas de la empresa antes de aplicar los cambios.
- Preservación de la integridad de las configuraciones
  - validación sintáctica y lógica (linting) de configuraciones;
  - separación de deberes entre quienes proponen, aprueban y aplican los cambios;
  - evidencia histórica que nos permite demostrar que la configuración "en producción" es conocida y está bajo control.
- Soluciones de recuperación
  - Capacidad para volver rápidamente a una configuración base conocida en caso de fallo o incidente;
  - soporte para planes de continuidad del negocio y recuperación ante desastres para el entorno OT.

Estas capacidades abordan directamente los requisitos de NIS 2 y ACN para copias de seguridad, continuidad del negocio y gestión de configuración, así como los objetivos de IEC 62443 para la gestión del ciclo de vida de activos, niveles de seguridad y protección frente a cambios no autorizados.

9.5 Resumen de la cobertura

En resumen:

- **ACCESS** proporciona el "pilar de identidad y acceso", haciendo que los accesos remotos OT sean fuertemente autenticados, autorizados, rastreados y rastreables a personas y procesos empresariales.
- **INSIGHT** crea el "pilar de visibilidad y monitorización", garantizando capacidades de registro, detección y análisis de flujo OT integradas con el SOC de la empresa.
- **RESCUE** introduce el "pilar de configuraciones y resiliencia", transformando los cambios de respaldo y OT en procesos controlados, versionados y verificables.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

La adopción conjunta de los tres módulos permite a la organización demostrar un nivel de madurez coherente con los requisitos del NIS 2, con las medidas técnicas y organizativas indicadas por la ACN y con los principios de seguridad descritos en la serie IEC 62443, construyendo un marco robusto, sostenible y auditable de seguridad industrial.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com