TI RESCUE SOC

Tu centinela digital avanzado

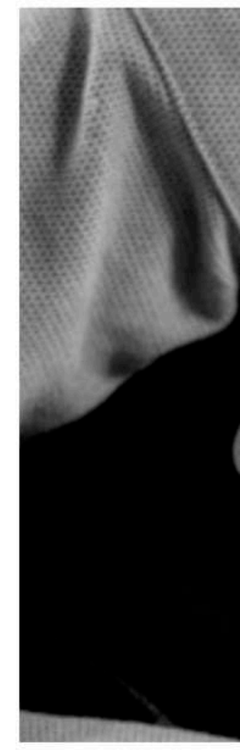
Soluciones avanzadas
en **ciberseguridad**

TI rescue

Especialistas en monitoreo, **detección y respuesta en tiempo real** para garantizar la seguridad y continuidad de tu negocio.

SOCAAS

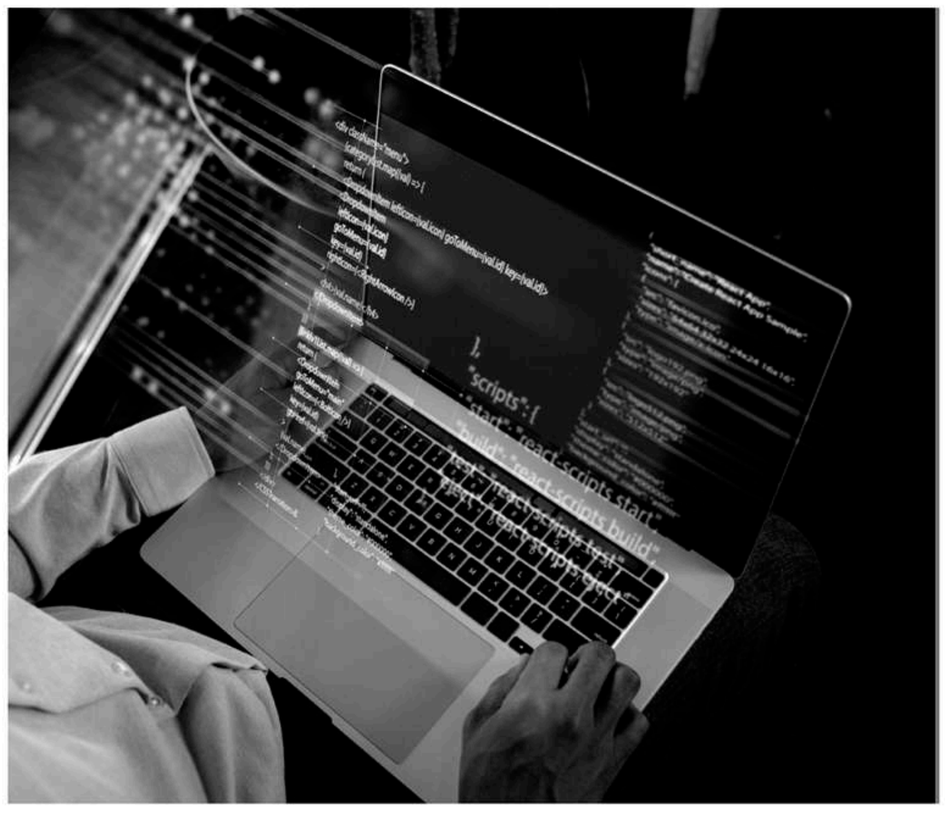
SOBRE **TI RESCUE**



NOSOTROS

Con un equipo altamente calificado, garantizamos soluciones de TI que superan las expectativas.

CONECTA,
COMUNICA
CONVIERTE



OBJETIVOS

Impulsar la transformación digital con estrategias de seguridad personalizadas y soporte tecnológico continuo.

SOMOS UN OUTSOURCING TÉCNOLÓGICO EN COLOMBIA

Soluciones integrales de TI, adaptadas a la innovación y crecimiento de tu empresa

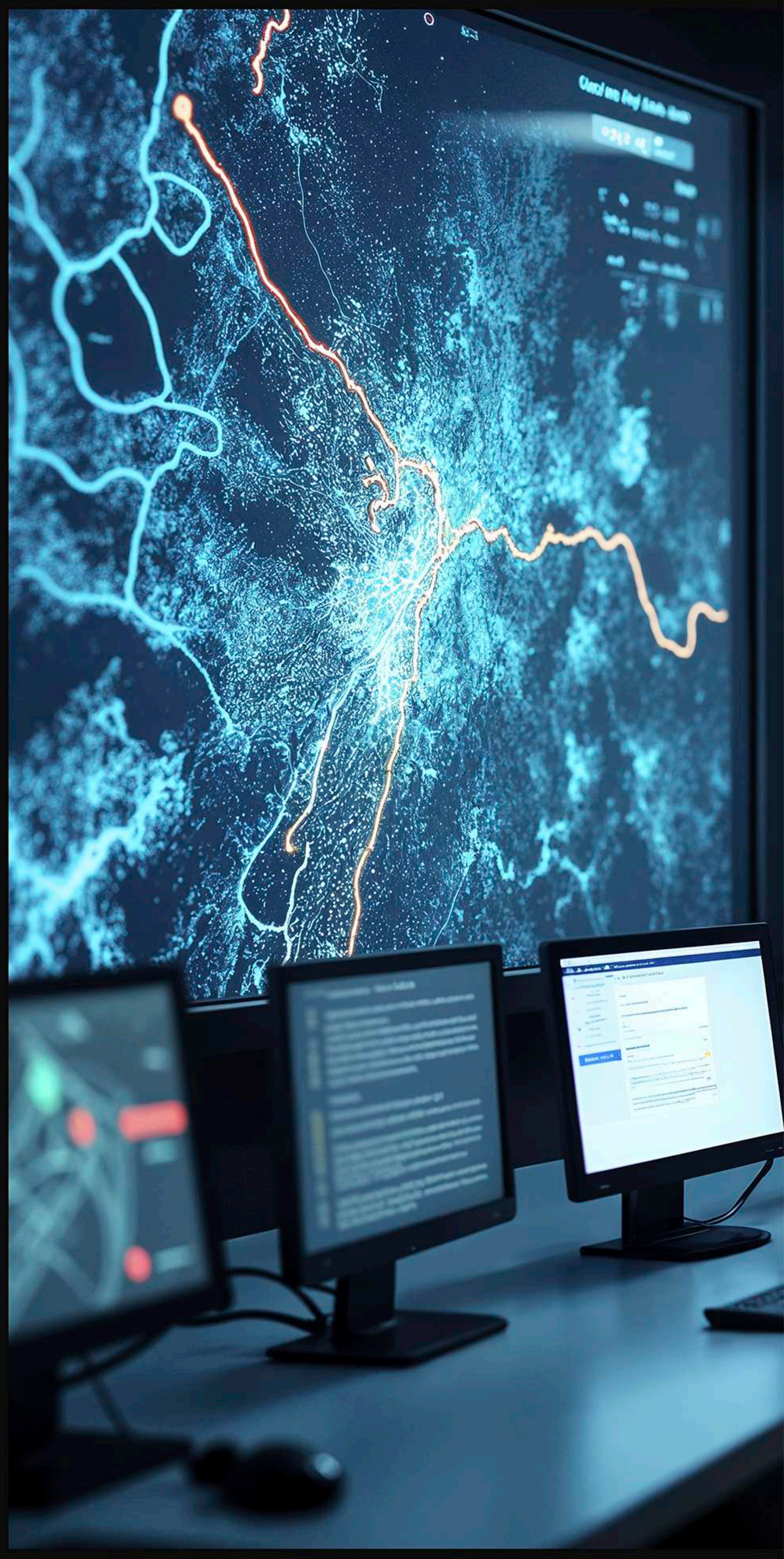
CALIDAD Y SEGURIDAD CERTIFICADAS

Nuestros procesos y servicios están respaldados por normas internacionales de calidad y ciberseguridad.

icontec ISO 9001	icontec ISO / IEC 27001	icontec ISO / IEC 20000-1	icontec ISO 22301	IQNET CERTIFIED MANAGEMENT SYSTEM
SC-CER900888	SI-CER900889	TI-CER988544	CO-CNCER988779	

¿Qué es RESCUE SOCaaS?

Un SOCaaS (Centro de Operaciones de Seguridad como Servicio) es como tener un "cuarto de control" para la seguridad digital de tu empresa, pero gestionado de forma remota por expertos. En lugar de invertir en infraestructura propia o un equipo interno, contratas este servicio para que un grupo especializado vigile y proteja tus sistemas 24/7.



¿Qué hace un SOCaaS?

Monitoreo 24/7: Un equipo externo supervisa tus computadoras, redes, correos y aplicaciones en tiempo real para identificar amenazas.

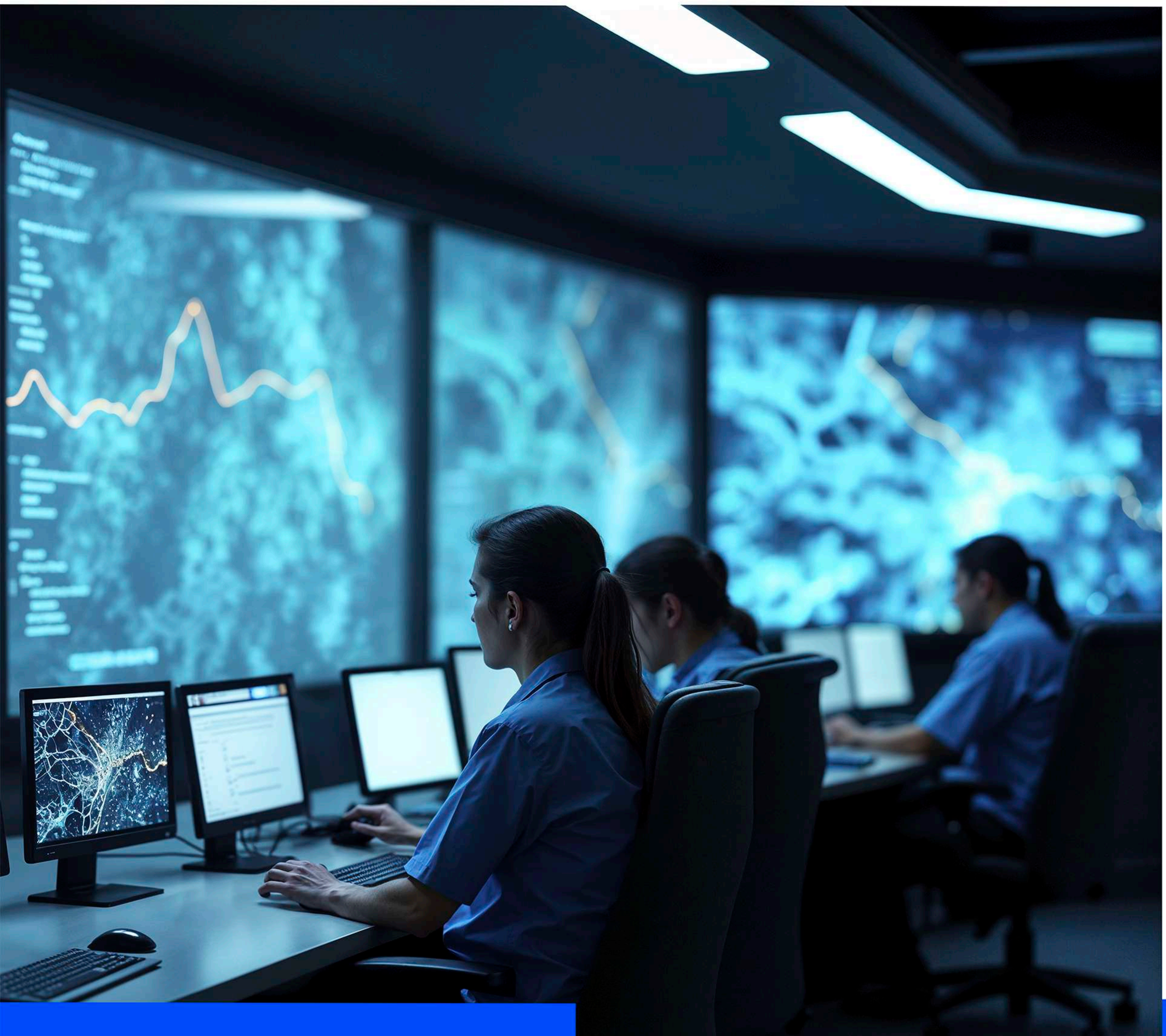
Detectan problemas: Encuentran intentos de hackeo, archivos peligrosos o comportamientos sospechosos en tus sistemas.

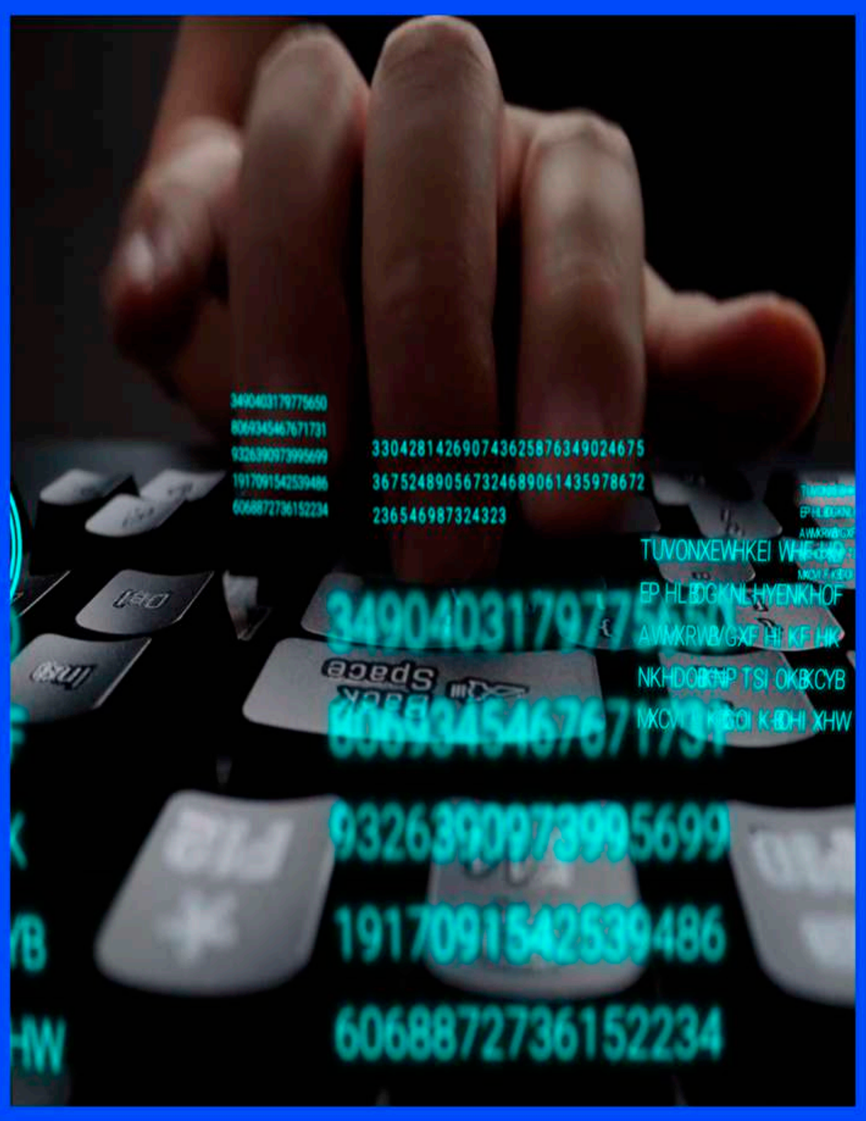
Responden rápido: Mitigan riesgos al bloquear ataques y solucionar problemas antes de que causen daños.

Previenen amenazas: Mantienen tus sistemas protegidos y actualizados para evitar futuros ataques.

¿Por qué es importante SOCaaS?

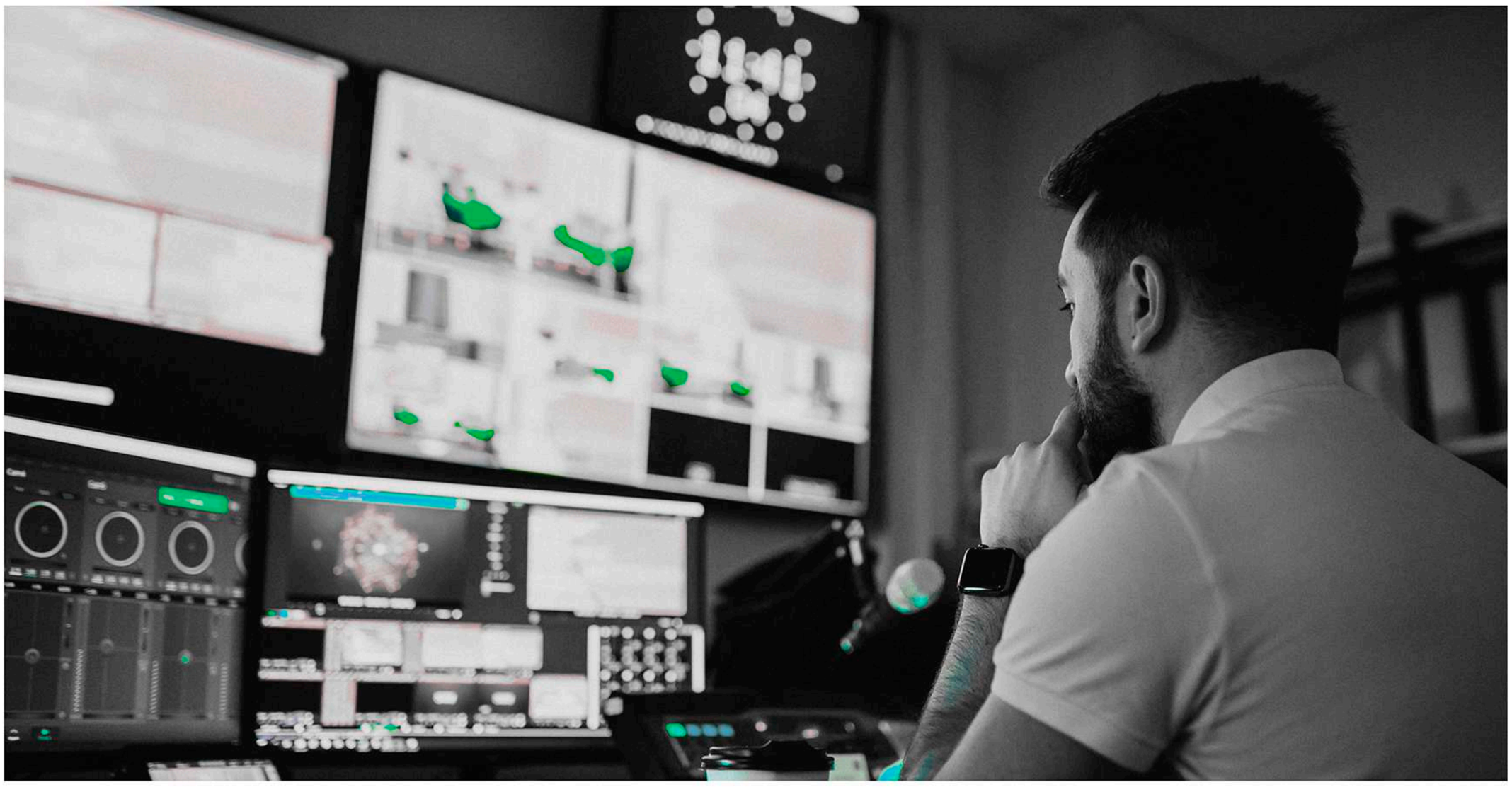
Con los ataques digitales aumentando cada día, un SOCaaS actúa como un escudo para proteger tu información y **asegurar que tu empresa siga operando sin interrupciones.** Además, como es un servicio gestionado, no necesitas grandes inversiones: los expertos lo hacen todo por ti.

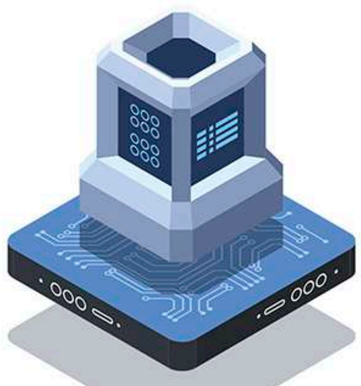


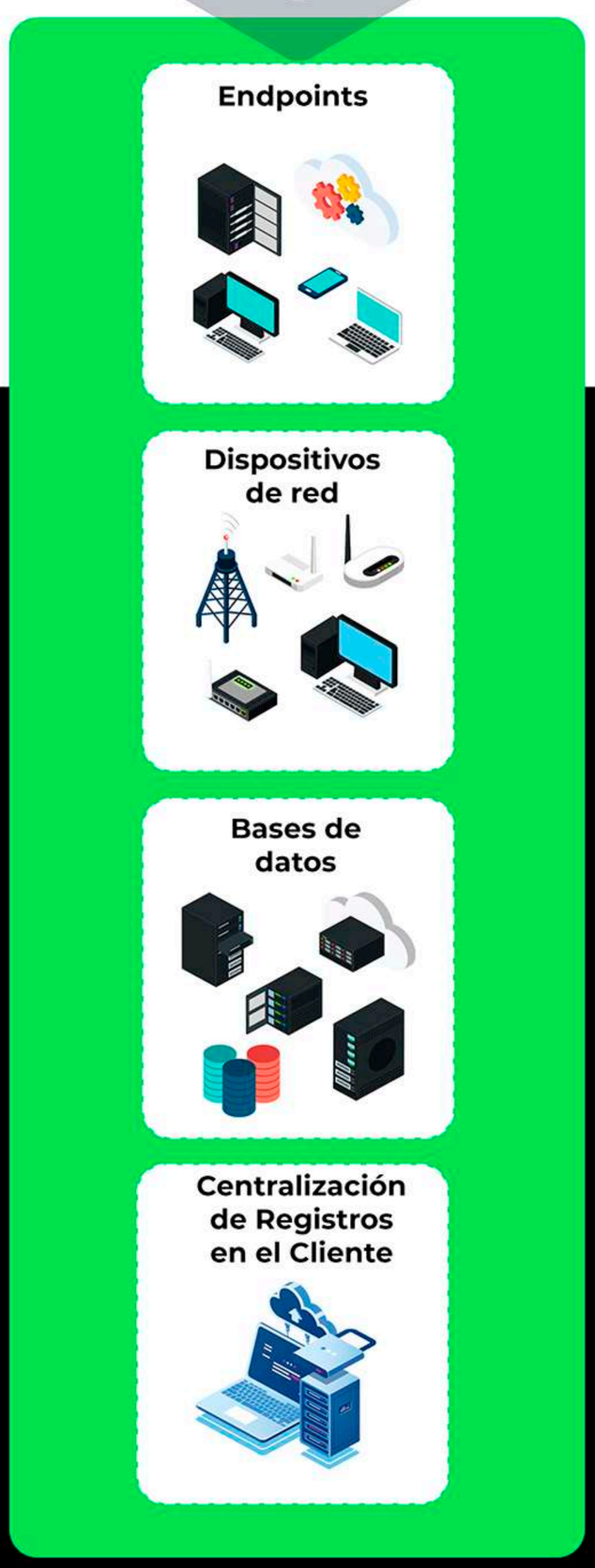


Inteligencia en Seguridad

Con SOCaaS, no solo tienes monitoreo y respuesta, también accedes a inteligencia en ciberseguridad. Esto significa que **utilizamos datos globales sobre amenazas emergentes** para proteger tus sistemas antes de que ocurra un ataque. Gracias a esta inteligencia proactiva, tu empresa siempre estará un paso adelante, reduciendo riesgos y fortaleciendo su infraestructura.







Componentes clave del servicio gestionado

SOCaaS protege dispositivos, redes, aplicaciones y bases de datos, **detectando riesgos y centralizando registros** con Syslog Forwarder. Un equipo experto analiza y responde a las amenazas de forma rápida y eficaz.

Endpoint Protection: Supervisión de dispositivos del cliente.

Dispositivos de red: Monitoreo de firewalls, routers y switches.

Aplicaciones críticas: Detección de vulnerabilidades en aplicaciones empresariales.

Bases de datos: Protección contra accesos no autorizados y anomalías.

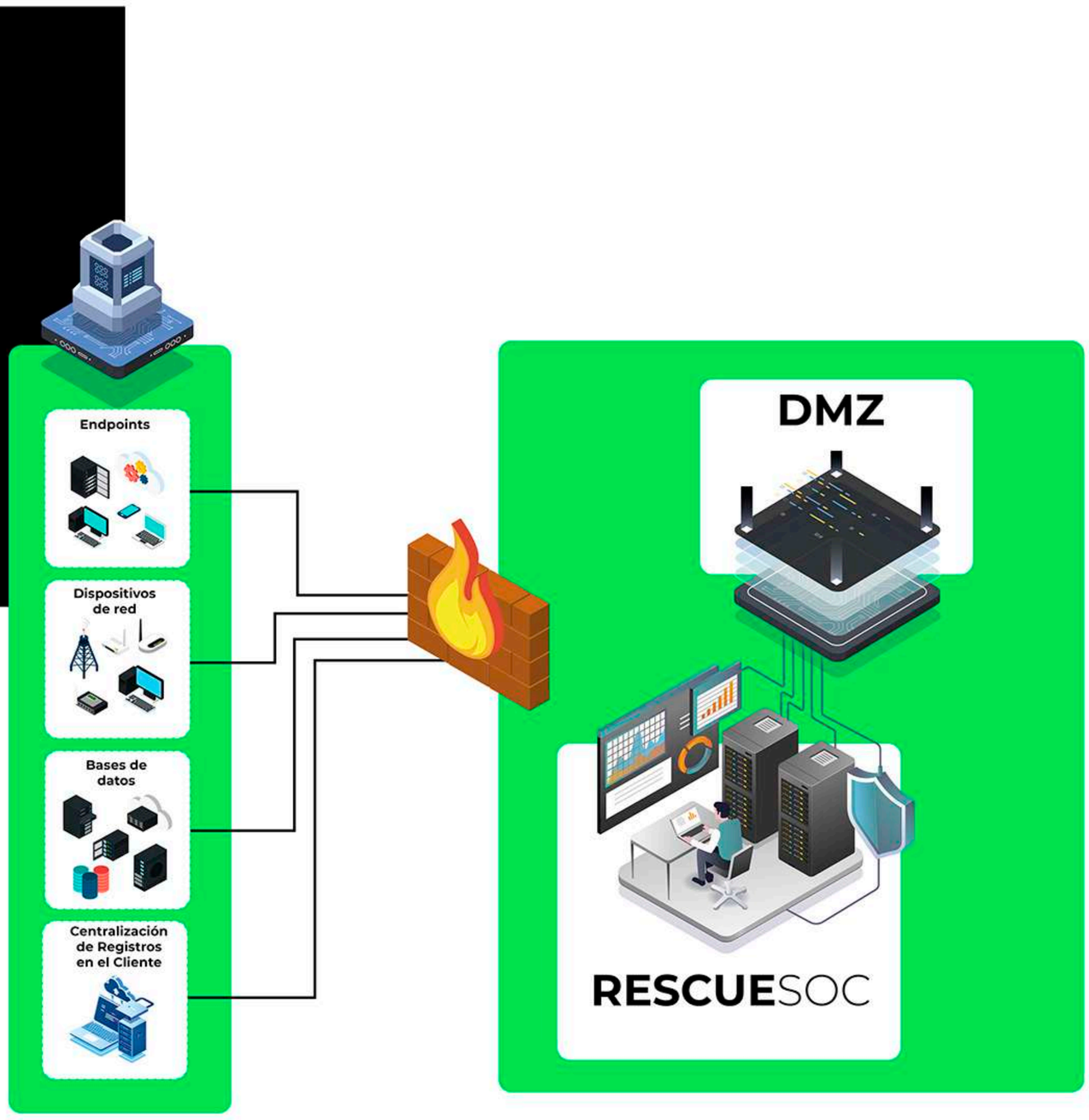
Syslog Forwarder: Centralización y envío de logs al SOC.

SOC AAS

Arquitectura Centralizada para Monitoreo y Análisis

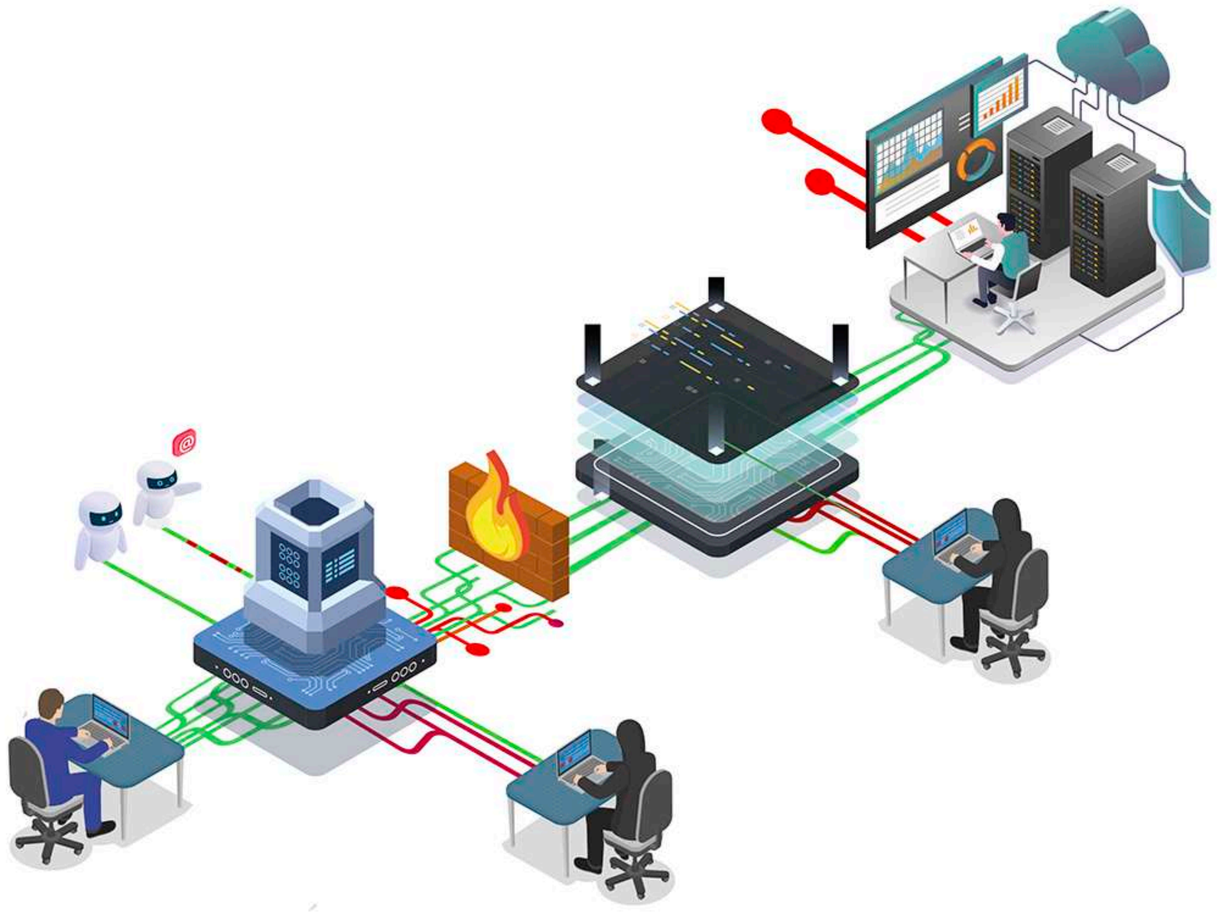
Esta sección muestra cómo la DMZ filtra y distribuye el tráfico hacia el backend, donde herramientas como **Wazuh, Greylog y Grafana** procesan y analizan los datos de seguridad. Esta arquitectura permite un monitoreo y análisis centralizado para garantizar protección en tiempo real.

Recolección y Gestión de Datos para Seguridad Total



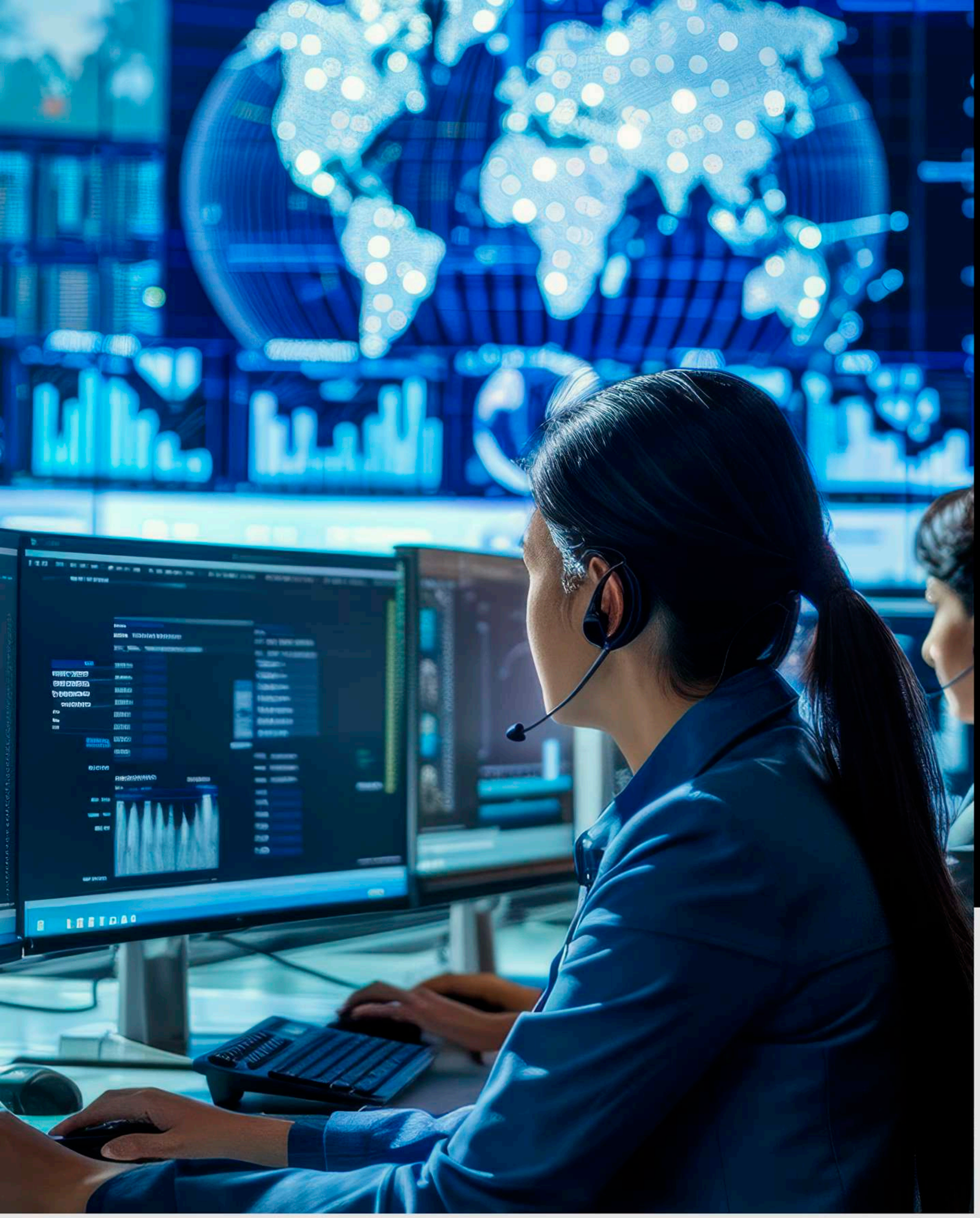
La arquitectura de RESCUE SOCaaS **permite recopilar datos críticos desde end-points, dispositivos de red y bases de datos del cliente.** Esta información es centralizada y pasa por un firewall, donde se filtra y asegura antes de llegar a la DMZ. Desde allí, el tráfico legítimo se distribuye al SOC, donde herramientas avanzadas y analistas especializados procesan los datos para garantizar una supervisión integral y protección en tiempo real.

Control y Supervisión Total del Tráfico



En RESCUE SOCaaS, se supervisa el tráfico generado por u**suarios, bots (buenos y maliciosos) y hackers**. Desde los dispositivos del cliente, el tráfico pasa por un firewall y la DMZ, donde se filtra y distribuye de forma segura. Esto garantiza que c**ualquier actividad sospechosa, ya sea interna o externa, sea detectada** y gestionada en tiempo real por el

www.tirescue.com



SERVICIOS

Servicios de RESCUE SOC

Monitoreo continuo: Supervisión 24/7 de la infraestructura.

Análisis de eventos: Correlación avanzada de logs para detectar amenazas.

Gestión de incidentes: Respuesta rápida a incidentes para minimizar daños.

Visualización de datos: Dashboards interactivos para reportes y métricas.

Cumplimiento normativo: Seguimiento a estándares como ISO 27001, 22301 y 20000-1.

www.tirescue.com

¿Cómo el SOC detecta amenazas y riesgos potencia-les en los sistemas del cliente?

Un SOC **detecta y responde** a cualquier actividad que represente una amenaza para la seguridad de la in-fraestructura del cliente.

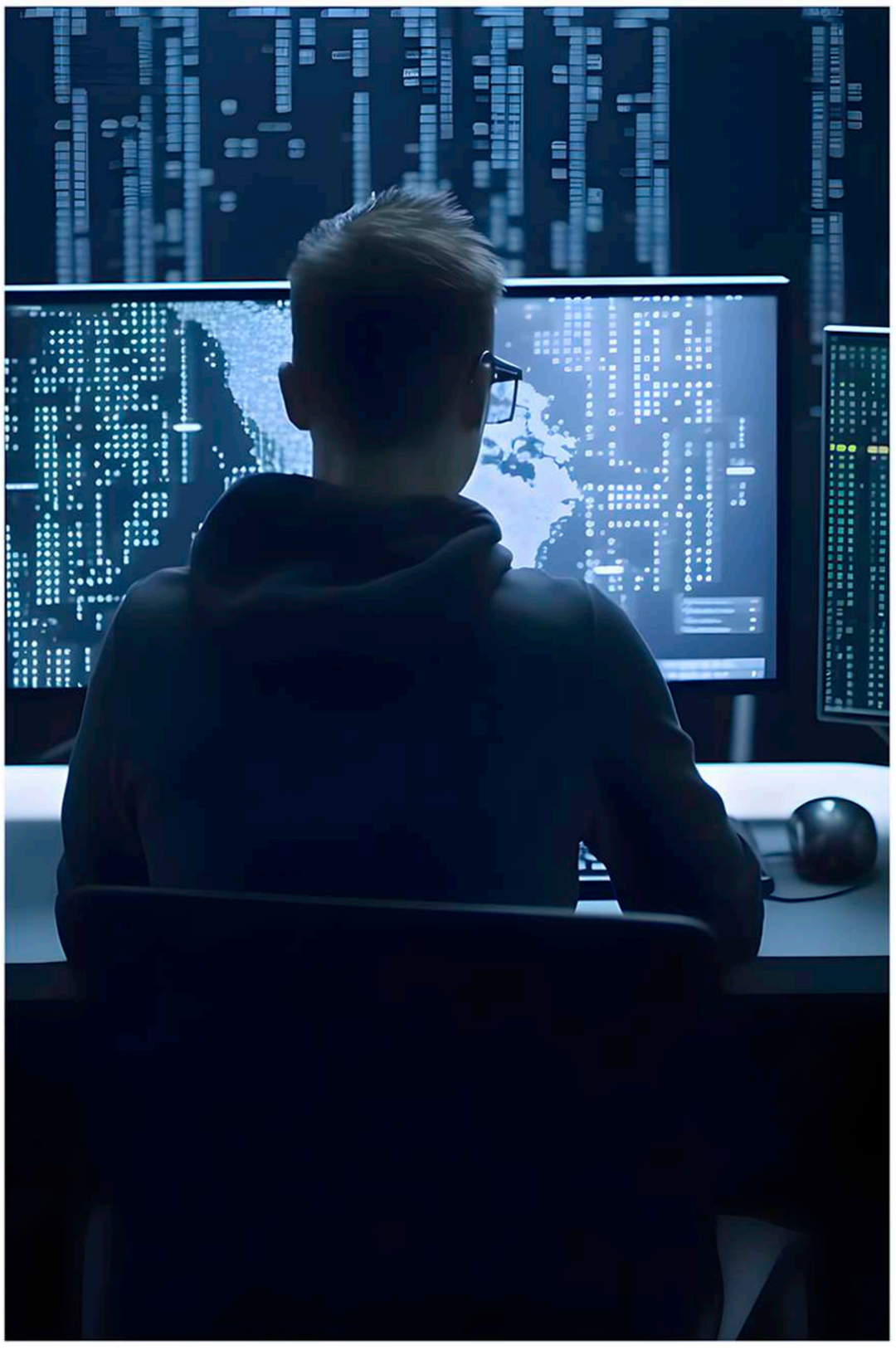
Esto incluye:

1. Actividades Maliciosas (Malware y Virus)

Qué busca: Archivos sospechosos, procesos desconocidos o com-portamientos típicos de **ransomware y spyware.**

Cómo lo detecta: Herramientas como agentes de monitoreo en endpoints (por ejemplo, Wazuh) **analizan cambios en el sistema, ejecuciones de procesos y patrones que coinciden con malware** conocido.

Ejemplo: Un archivo que se copia rápidamente entre carpetas podría ser un **ransomware en acción.**

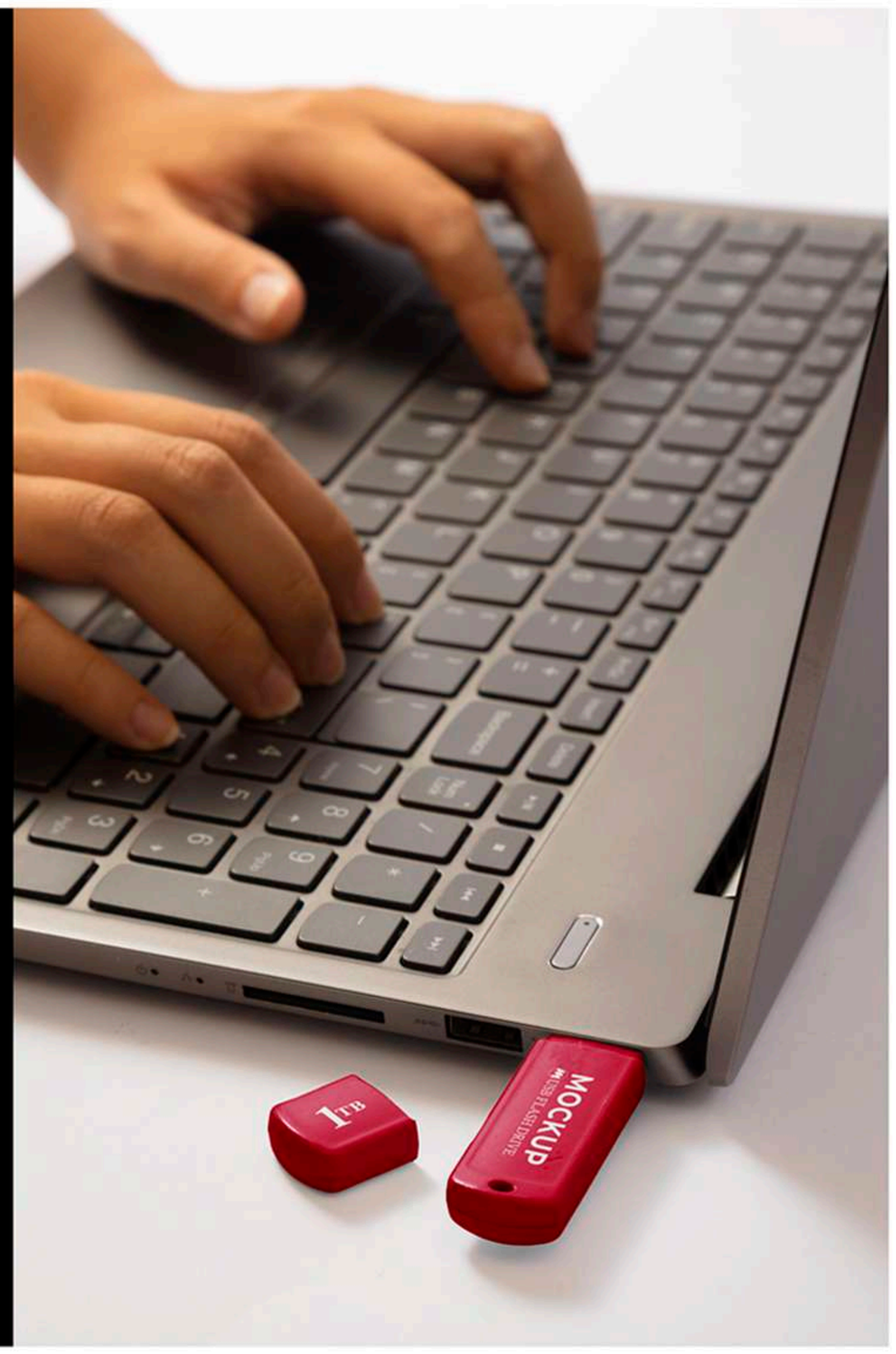


2. Accesos No Autorizados

Qué busca: Intentos de acceso no autorizados a sistemas, bases de datos o redes.

Cómo lo detecta: Logs de autenticación y herramientas de monitoreo como EDR/XDR pueden identificar intentos fallidos repetidos (ataques de fuerza bruta) o accesos desde ubicaciones geográficas inusuales.

Ejemplo: Un usuario interno intentando acceder a una base de datos restringida sin permisos.



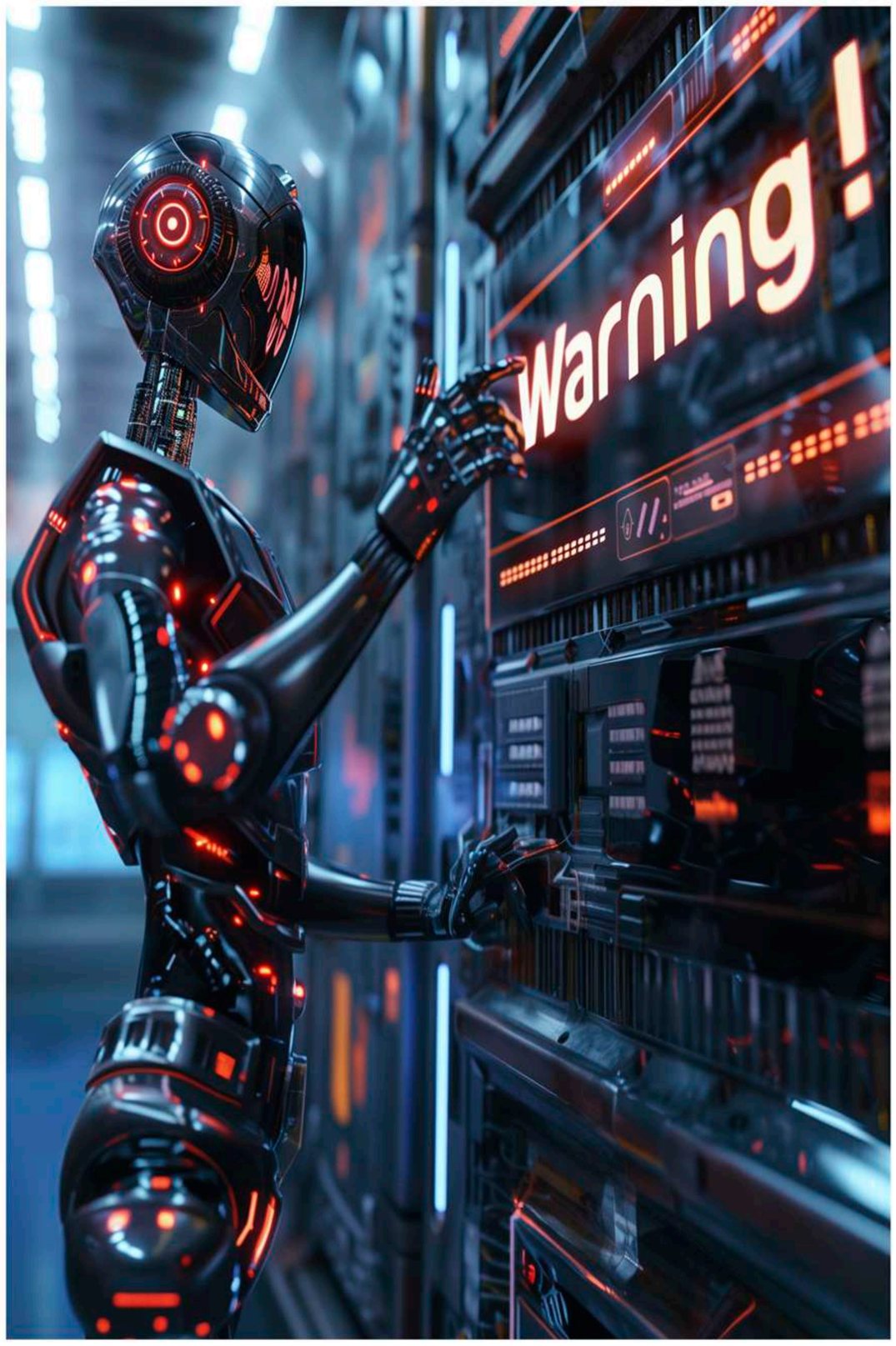
3. Comportamientos Anómalos

Qué busca: Actividades que no coinciden con el comportamiento típico de los usuarios o sistemas.

Cómo lo detecta: Los sistemas SIEM y herramientas de análisis comportamental (UBA) identifican anomalías

como: Usuarios que descargan grandes volúmenes de datos. Servicios que inician procesos no habituales.

Ejemplo: Un empleado descargando toda la base de datos fuera del horario laboral.



5. Bots y Actividad Automatizada

Qué busca: Presencia de bots buenos (motores de búsqueda) o malos (**bots maliciosos** para extracción de datos o ataques).

Cómo lo detecta: Herramientas en la **DMZ identifican patrones** de solicitudes automatizadas inusuales.

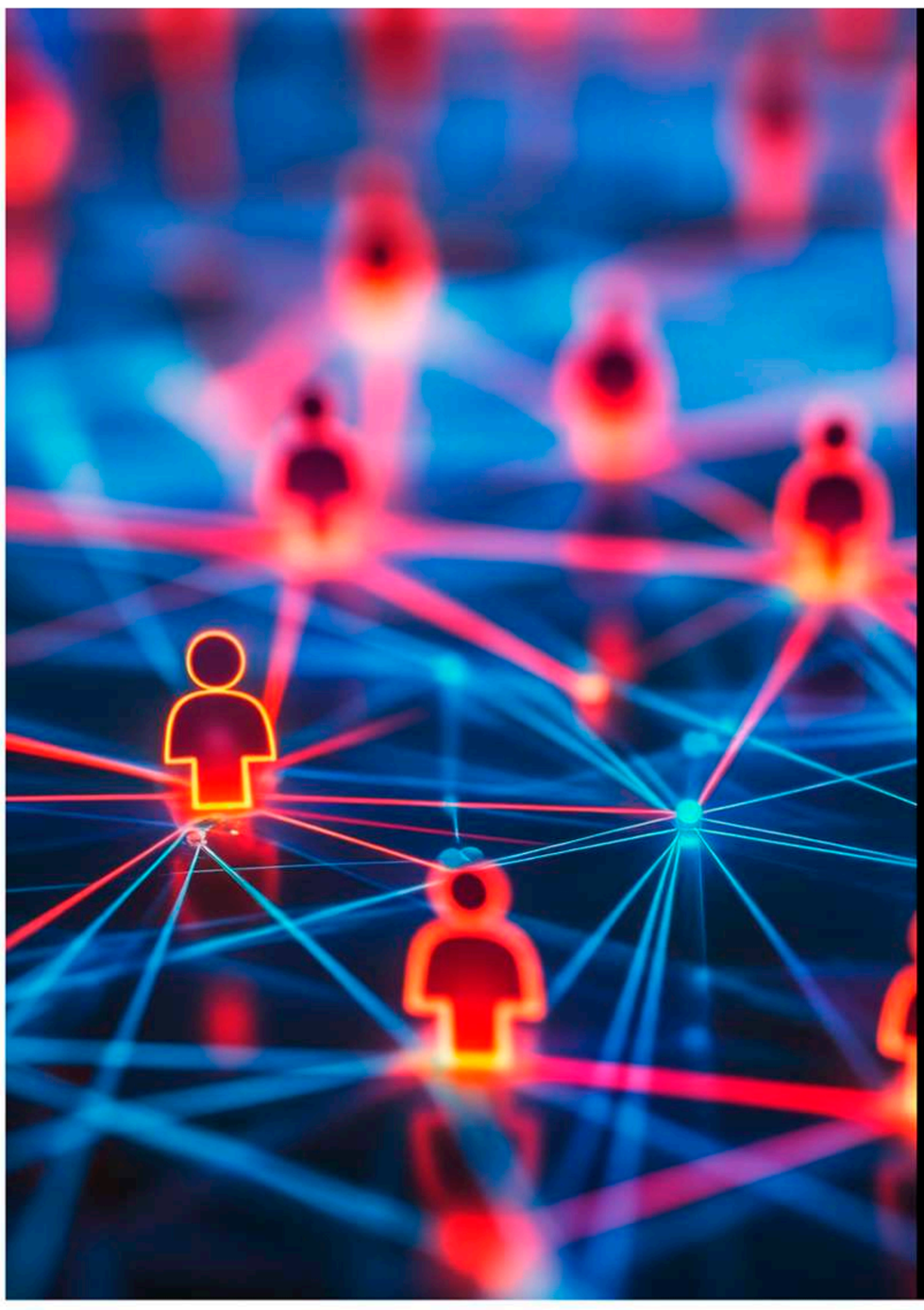
Ejemplo: Un bot que intenta extraer información de una API sin autorización.

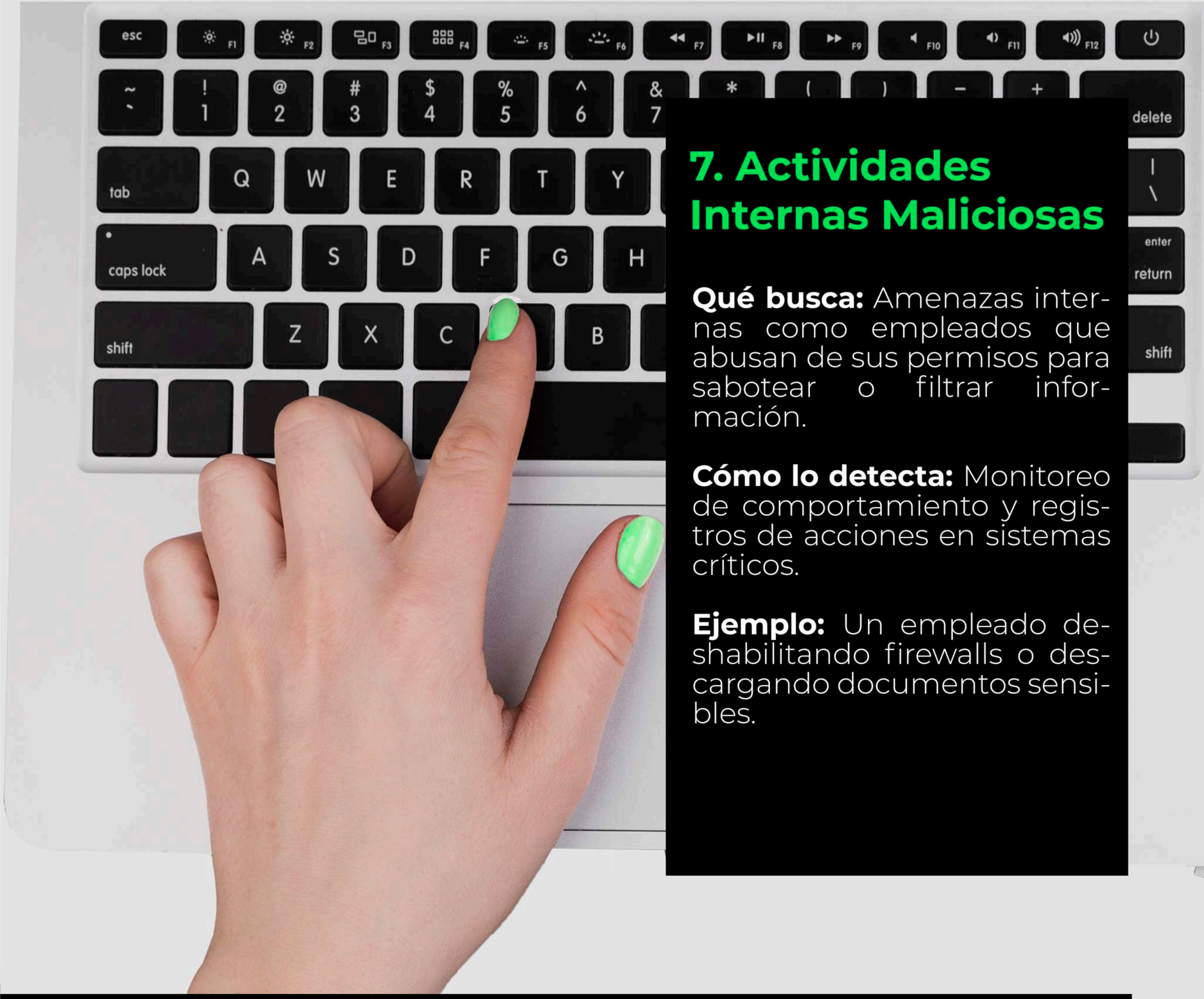
6. Tráfico de Red Sospechoso

Qué busca: Conexiones inusuales hacia servidores externos, picos de tráfico inesperados o intentos de comunicación con servidores maliciosos.

Cómo lo detecta: Herramientas como **Suricata (IDS/IPS)** y análisis de logs de red identifican patrones de tráfico que coinciden con ataques conocidos (DDoS, exfiltración de datos, etc.).

Ejemplo: Un dispositivo interno enviando datos a una dirección IP conocida como maliciosa.





7. Actividades Internas Maliciosas

Qué busca: Amenazas internas como empleados que abusan de sus permisos para sabotear o filtrar información.

Cómo lo detecta: Monitoreo de comportamiento y registros de acciones en sistemas críticos.

Ejemplo: Un empleado deshabilitando firewalls o descargando documentos sensibles.

Cómo lo hace el SOC:

Monitoreo 24/7: Supervisando constantemente logs, tráfico de red y actividades en dispositivos.

Correlación de Eventos: Detectando patrones al unir datos de múltiples fuentes para identificar amenazas complejas.

Análisis en Tiempo Real: Herramientas como SIEM procesan y priorizan alertas para que los analistas puedan actuar rápidamente.

Respuesta Proactiva: Aislamiento de dispositivos comprometidos, bloqueo de accesos no autorizados o eliminación de procesos maliciosos.

Beneficios del SOCaaS

01 **Ahorro de costos:** Sin necesidad de invertir en infraestructura propia.

02 **Seguridad gestionada:** Reduce la carga del equipo interno.

03 **Tecnología avanzada:** Acceso a herramientas de última generación sin costos adicionales.

04 **Respuesta proactiva:** Mitigación de incidentes antes de que impacten tu negocio.

05 **Escalabilidad y flexibilidad:** Adaptado a empresas de cualquier tamaño.

T.I RESCUE

SEGURIDAD INFORMATICA

WWW.TIRESCUE.COM

Expertos en Ciberseguridad