


PORTAFOLIO Y PLANES

# RESCUE DLP

Antivirus para tus equipos y, como módulo adicional, prevención de fuga de datos.

T.I RESCUE
SEGURIDAD INFORMATICA

# DISTINCIÓN EXCELENCIA

## ISO 9001

Seguridad informática premium, respaldada por el reconocimiento internacional ISO 9001.




SC-CER900888

## ISO 27001

Defendiendo tus datos con rigor internacional: certificación ISO/IEC 27001.




SI-CER900889

## ISO 20000-1

Excelencia en gestión de servicios de TI, fundamentada en estándares mundiales de calidad.




TI-CER988544

## ISO 22301

Continuidad del negocio sin interrupciones, conforme a estándares internacionales.




CO-CNCER988779

# CUATRO CERTIFICACIONES ISO DEFINEN NUESTRA SUPERIORIDAD

Nuestro compromiso con la ciberseguridad trasciende la simple retórica. Es tangible y está validado por cuatro prestigiosas certificaciones **ISO 9001, 27001, 20000-1 y 22301**. No son solo siglas: son el testimonio de nuestra dedicación a ofrecer servicios de primera clase y representan nuestra promesa de calidad, seguridad, **eficiencia y resiliencia**. Al elegirnos no solo escoges un proveedor de ciberseguridad, sino un aliado certificado que entiende y cumple los más altos estándares internacionales.

## COMPROMISO INTEGRAL: **MÁS ALLÁ DE LA SEGURIDAD BÁSICA**

Con nuestras certificaciones garantizamos **calidad, seguridad de la información, excelencia en TI y continuidad del negocio**. Representan nuestro compromiso, profesionalismo e integridad. Elegirnos es optar por una ciberseguridad de élite y con respaldo.



# SOMOS UN ALIADO **ESTRATÉGICO**

Para la seguridad informática e infraestructura tecnológica de las empresas.

# EMPRESA FUNDADA EN **2015 CON BASE EN COLOMBIA**

Con operación en **todo el mundo**

## MISIÓN

Nos especializamos en el soporte y la seguridad informática con los más altos estándares internacionales, incluidas las normas **ISO 9001, 27001, 22301 y 20000-1**. Nuestra misión es garantizar la continuidad operativa de empresas de todos los tamaños con soluciones tecnológicas eficientes y seguras, y servicios personalizados que se ajustan a las necesidades de cada cliente, **evitando interrupciones y promoviendo su éxito**.

## VISIÓN

Ser líderes globales en administración y seguridad informática, con soluciones personalizadas y eficientes que garanticen la continuidad operativa. Estamos comprometidos con **la innovación y el cumplimiento de los estándares de calidad y seguridad más rigurosos**, para ser siempre la primera opción de nuestros clientes.

**Contáctanos**
**info@tirescue.com.co**
**www.tirescue.com**

# TU SEGURIDAD, NUESTRA PRIORIDAD

### Soluciones adaptadas
A la medida de cada cliente, sin importar si la empresa es pequeña o grande.

### Actualización constante
Soluciones inmediatas para prevenir pérdidas de información e ir siempre un paso adelante.

### Comunicación directa
Sin filas ni turnos.

### Ahorro en hardware
Lo que se implementa en software.

### Soporte 24/7
Acompañamiento permanente cuando lo necesitas.

### Personal atento
Un equipo certificado que conoce tu operación.

## NUESTROS VALIOSOS CLIENTES
Asociaciones basadas en la confianza y la excelencia

# TUS EQUIPOS Y TUS DATOS, PROTEGIDOS

PLATAFORMA RESCUEDLP

UN SOLO AGENTE EN CADA EQUIPO

## ANTIVIRUS INCLUIDO, DLP CUANDO LO NECESITES

**RescueDLP** es la plataforma de seguridad para equipos de T.I. RESCUE. Un agente liviano protege cada computador con antivirus y detección de amenazas, y nuestra consola te muestra en un solo lugar qué pasa en toda tu flota.

- **Antivirus y detección** de comportamiento en cada equipo.
- **Navegación segura**: bloquea sitios de riesgo por categoría y por grupo.
- **Módulo DLP** para que la información sensible no salga de tu empresa. **Se cobra aparte.**
- **Soporte local** en español con el mismo equipo que opera la plataforma.

### Antivirus con firmas

Análisis al acceso, análisis bajo demanda y cuarentena cifrada.

### Detección de amenazas

Reglas de comportamiento mapeadas a MITRE ATT&CK y respuesta en el equipo.

### Navegación web

Bloqueo por categorías, búsqueda segura y control USB por grupo.

### Equipos y parches

Inventario de la flota y actualizaciones pendientes priorizadas por riesgo.

### Módulo DLP

Detecta datos sensibles y decide por dónde pueden salir. **Se cobra aparte.**

### Consola y reportes

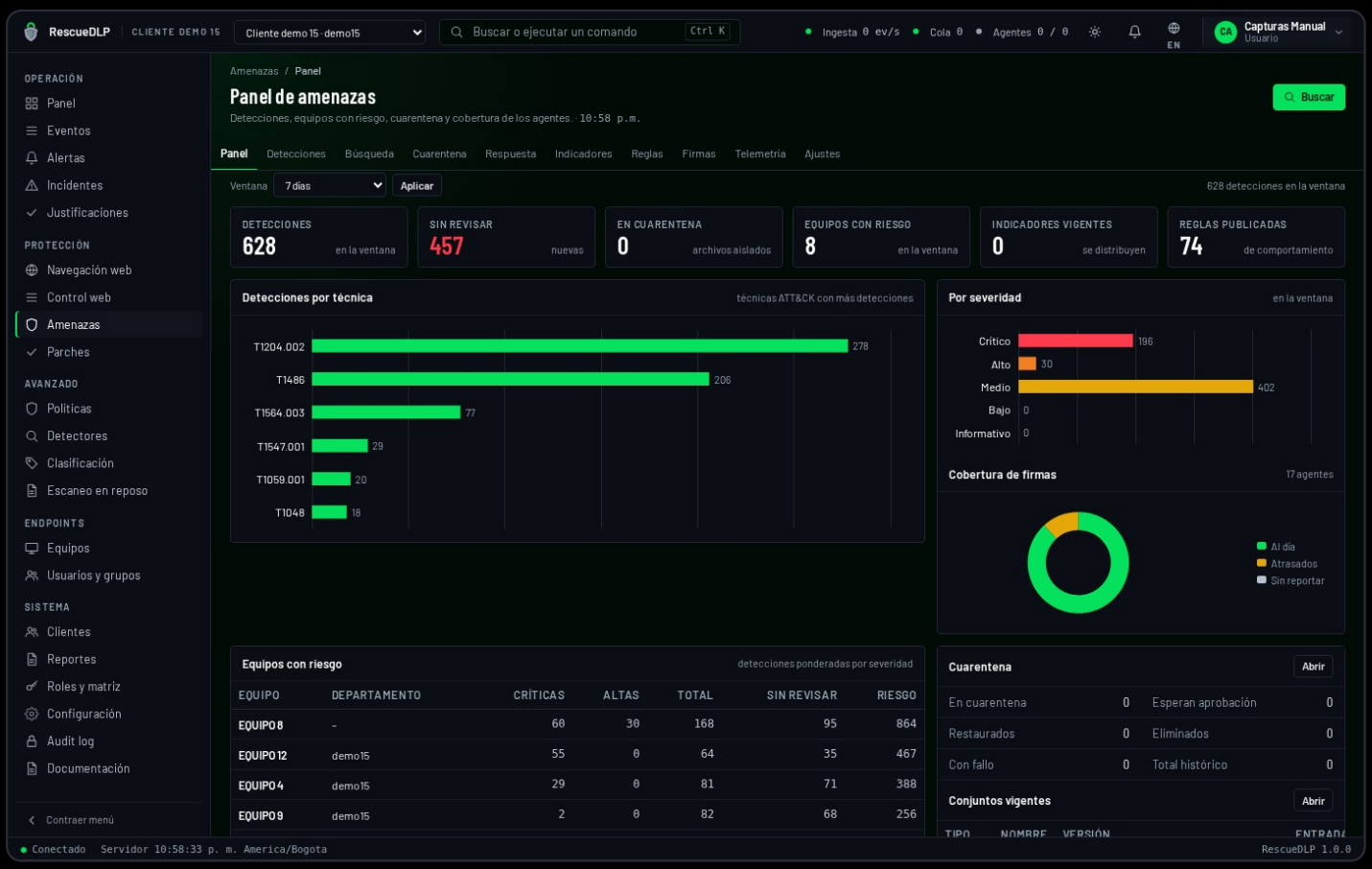
Alertas, incidentes, auditoría y reportes programados.

**INCLUIDO EN EL PLAN**

## ANTIVIRUS Y DETECCIÓN

# CADA EQUIPO SE DEFIENDE SOLO

El agente revisa los archivos cuando se abren, aísla lo malicioso en una cuarentena cifrada y vigila el comportamiento de los procesos. Si algo se ve como un ataque, lo detiene en el equipo y te lo muestra en la consola con su contexto completo.



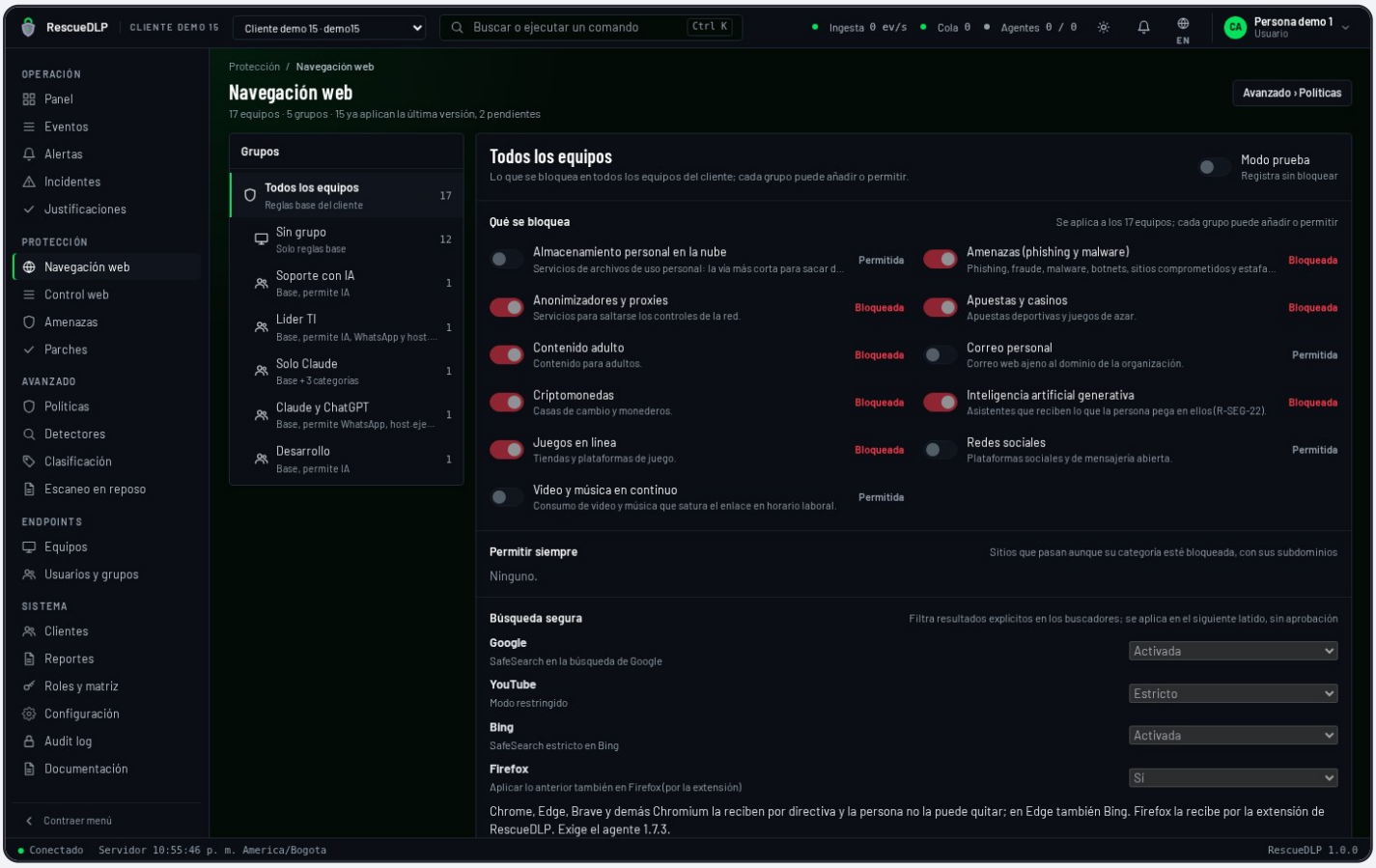

- **Análisis al acceso** y bajo demanda, con firmas que se actualizan varias veces al día.
- **Cuarentena cifrada**: restaurar o eliminar exige la aprobación de una segunda persona.
- **Comportamiento**: reglas Sigma con su técnica de MITRE ATT&CK.
- **Respuesta**: terminar el proceso, aislar el archivo, bloquear su huella o recoger el triaje.
- **Árbol de procesos** y línea de tiempo de cada detección.
- **Inteligencia de amenazas** desde MISP, TAXII o listas propias.

**INCLUIDO EN EL PLAN**

## NAVEGACIÓN Y DISPOSITIVOS

# LO RIESGOSO SE BLOQUEA POR GRUPO

Organiza los equipos en grupos (Contabilidad, Gerencia, Desarrollo…) y decide con un interruptor qué categorías de sitios se bloquean en cada uno. Un técnico lo hace en minutos, sin escribir reglas.




## Categorías

Phishing y malware, apuestas, anonimizadores, contenido adulto y más, con lista de sitios siempre permitidos.

## Búsqueda segura

Filtro estricto en Google, YouTube y Bing, aplicado desde la directiva del navegador.

## USB y permisos

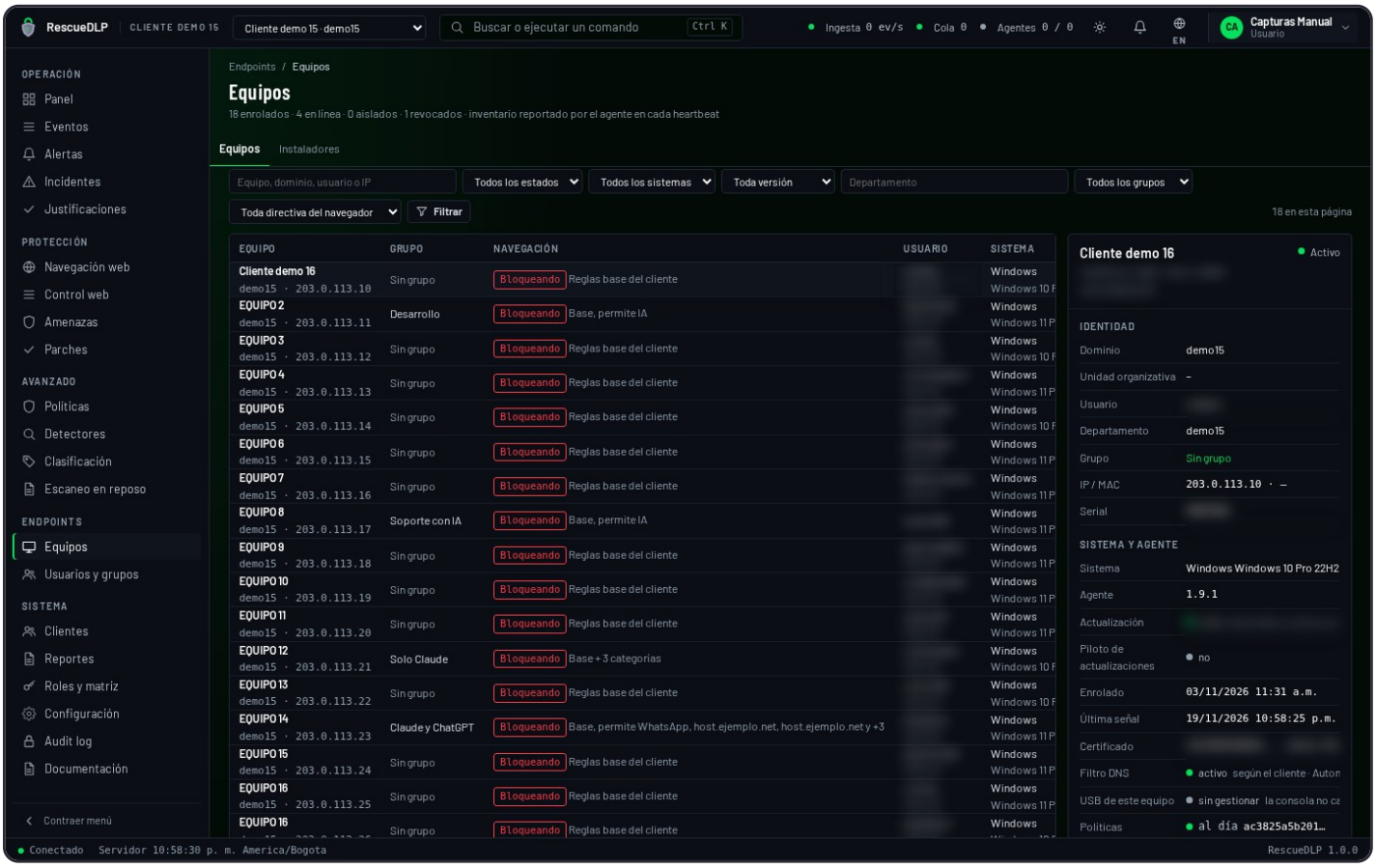
Modo USB por grupo, modo prueba antes de bloquear y permisos temporales que vencen solos.

**INCLUIDO EN EL PLAN**

TODA TU FLOTA

# CADA EQUIPO, A LA VISTA

Inventario en vivo de cada computador: sistema, versión del agente, usuario, grupo y estado de la protección. Los parches pendientes se ordenan primero por las vulnerabilidades que ya se están explotando (catálogo KEV).




**3**
SISTEMAS: WINDOWS, LINUX Y MACOS

**mTLS**
CANAL CIFRADO Y AUTENTICADO

**KEV**
PARCHES CRÍTICOS PRIMERO

**2**
PERSONAS APRUEBAN LAS ACCIONES CRÍTICAS

- **Instalación sencilla**: instalador MSI firmado para Windows y paquetes deb, rpm o tar.gz para Linux y macOS.
- **Sin red, no se pierde nada**: el agente guarda los eventos cifrados y los envía cuando vuelve la conexión.

MÓDULO ADICIONAL · SE COBRA APARTE

PREVENCIÓN DE FUGA DE DATOS

# CADA ARCHIVO SENSIBLE SE REVISA ANTES DE SALIR

Cuando alguien intenta sacar información por una memoria USB, el correo, una página web o la impresora, el agente la analiza en el propio equipo y aplica tu política: alertar, bloquear, cifrar o pedir una justificación. A la consola llega el resultado («este archivo tenía tres cédulas»), nunca el contenido.

| **Archivo** | **Detector** | **Política** | **Acción** | **Alerta** | **Revisión** |
|---|---|---|---|---|---|
| sale del equipo | cédulas, tarjetas, NIT | firmada y aprobada | bloquea o cifra | en la consola | justificación o incidente |

**14**
CANALES VIGILADOS

**0**
CONTENIDO QUE VIAJA A LA CONSOLA

**2**
PERSONAS PARA PUBLICAR UNA POLÍTICA

**AES-256**
CIFRADO AL COPIAR A USB

## Canales que vigila

- USB y discos extraíbles
- Portapapeles
- Impresión
- Captura de pantalla
- Navegación web
- Correo saliente
- Subida web (navegador)
- Sincronización en la nube
- Carpetas de red
- Archivos abiertos por herramientas de IA (Cursor, VS Code, Codex...)
- Bluetooth
- Escritorio remoto
- Ejecución de aplicaciones
- Asistentes de IA locales

### Estricto por defecto

Un equipo sin políticas vigentes protege en modo estricto: ante la duda, bloquea y registra. Puedes empezar en **solo observar** para medir sin interrumpir a nadie.

**MÓDULO ADICIONAL · SE COBRA APARTE**

QUÉ DETECTA Y QUÉ HACE

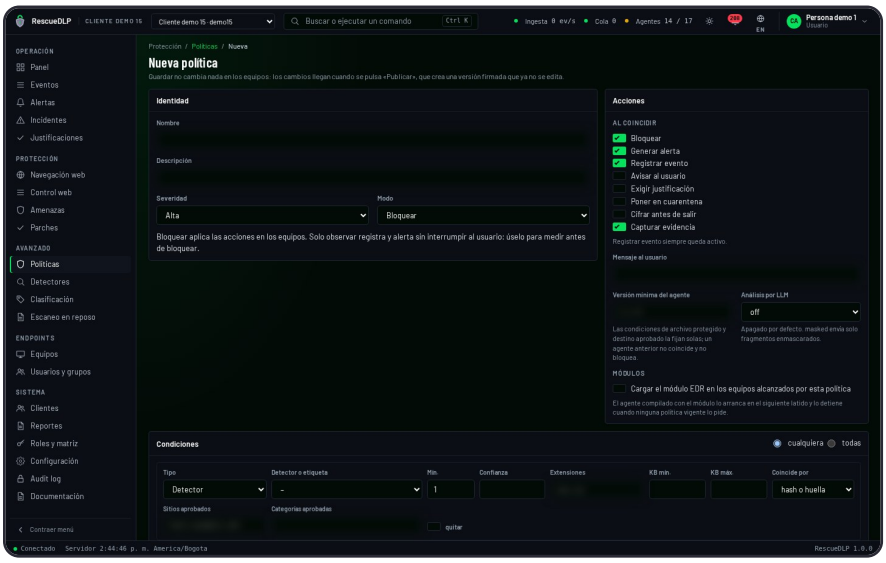
# TUS DATOS, CON NOMBRE PROPIO

## Cómo reconoce la información

- **Detectores listos**: cédula, NIT, tarjetas, cuentas bancarias, correos y teléfonos.
- **Reglas propias**: expresiones y diccionarios de palabras clave.
- **Huellas de documentos**: contratos o planos, aunque copien solo una parte.
- **Datos exactos (EDM)**: tu lista de clientes o empleados, guardada solo como huellas.
- **Clasificación** por etiquetas y archivos protegidos en RescueCloud.

## Qué puede hacer

- **Bloquear** y avisarle a la persona por qué.
- **Exigir justificación**: un revisor la aprueba o la rechaza.
- **Cifrar antes de salir**: el archivo en la USB solo abre en equipos de la empresa.
- **Cuarentena y evidencia** cifrada para la investigación.
- **Alertar** y abrir un incidente con todo el contexto.




## Plantillas de cumplimiento

Arranca con políticas alineadas con la **Ley 1581** de protección de datos, **PCI-DSS**, **GDPR** e **ISO 27001**.

## Escaneo en reposo

Encuentra lo sensible que ya está guardado en carpetas compartidas, servidores SFTP y buckets, antes de que intente salir.

### Privacidad de las personas

El análisis ocurre en el equipo. No hay registro de teclas ni capturas periódicas, y nada se envía a terceros. Cerrar un incidente o borrar evidencia exige la aprobación de dos personas.

PLANES POR EQUIPO

# PAGAS LA PROTECCIÓN, Y EL DLP SI LO NECESITAS

El plan de protección cubre el antivirus y todo lo que mantiene sano cada equipo. El módulo DLP se agrega cuando tu empresa necesita controlar la salida de información, y **se cobra aparte**.

| Qué incluye | Protección<br>Antivirus · plan base | Módulo DLP<br>Adicional · se cobra aparte |
|---|---|---|
| Antivirus, análisis al acceso y cuarentena | Sí | — |
| Detección de comportamiento y respuesta | Sí | — |
| Navegación web, búsqueda segura y USB por grupo | Sí | — |
| Inventario de equipos y parches priorizados | Sí | — |
| Consola, alertas, reportes y auditoría | Sí | Sí |
| Políticas DLP en 14 canales | — | Sí |
| Detectores, huellas de documentos y EDM | — | Sí |
| Cifrado a USB, justificaciones e incidentes | — | Sí |
| Escaneo en reposo y plantillas de cumplimiento | — | Sí |
| **Valor** | **Por equipo**<br>según el tamaño de la flota | **Se cobra aparte**<br>se suma al plan de protección |

### Cotización a la medida

Te entregamos la propuesta según el número de equipos y los módulos que actives. El módulo DLP puedes agregarlo desde el inicio o más adelante.

## Hecho por nosotros, para nosotros

RescueDLP es desarrollo propio de T.I. RESCUE. La operamos todos los días y el código pasa por nuestro pipeline de seguridad.

## Un solo proveedor

Consola, agente, soporte y respuesta con el mismo equipo, certificado en ISO 9001, 27001, 20000-1 y 22301.

FICHA TÉCNICA

# SEGURIDAD Y ESPECIFICACIONES

| | |
|---|---|
| **Agente** | Windows (MSI firmado), Linux (deb, rpm o tar.gz) y macOS. Servicio con ícono en la bandeja para avisos y justificaciones. |
| **Comunicación** | Canal exclusivo de agentes con mTLS; eventos cifrados en el equipo mientras no hay red. |
| **Antivirus** | Firmas que se actualizan varias veces al día, análisis al acceso y bajo demanda, cuarentena cifrada con doble control. |
| **Detección y respuesta** | Reglas de comportamiento Sigma con técnica MITRE ATT&CK, indicadores MISP/TAXII, terminar procesos, bloquear huellas y recoger triaje. |
| **Políticas** | Versiones firmadas e inmutables; una persona redacta y otra aprueba. Modo «solo observar» para medir antes de bloquear. |
| **DLP (adicional)** | 14 canales, detectores, huellas, EDM, clasificación, cifrado a USB, justificaciones y escaneo en reposo. Análisis en el equipo: el contenido no sale. |
| **Acceso a la consola** | Segundo factor obligatorio, SSO con OIDC o SAML, LDAP/Active Directory, roles y matriz de permisos por departamento. |
| **Integraciones** | SIEM, webhooks, Slack y Teams, correo, RescueCloud y Rescue Remoto. |
| **Trazabilidad** | Registro de auditoría verificado de forma periódica; reportes en PDF, XLSX y CSV, con envíos programados. |
| **Privacidad** | Sin registro de teclas ni capturas periódicas; nada se envía a terceros. La retención de la telemetría se acuerda contigo. |
| **Cumplimiento** | Apoya los controles de ISO/IEC 27001 y la Ley 1581 de protección de datos personales. |
| **Soporte** | Mesa de ayuda de T.I. RESCUE en español: implantación, ajuste de políticas y acompañamiento. |

# TUS EQUIPOS Y TUS DATOS, PROTEGIDOS



## CONTÁCTANOS

Pídenos una cotización con el número de equipos de tu empresa y te entregamos la propuesta exacta, con el plan de protección y, si lo necesitas, el módulo DLP.


• Cra. 65 #8B-91 Ofic. 485, Guayabal, Medellín, Antioquia • WhatsApp: +57 315 893 7873
• Teléfono fijo: +57 4 6073303 • info@tirescue.com.co • www.tirescue.com