Controlled networks | Technology Focused Cloud Driven.

EVIDENCIA E INVESTIGACIÓN

DOCE MESES DE REGISTROS DE FIREWALL · ILUSTRATIVO

AÚN EN EL EQUIPO



**Inicia la intrusión**
Los registros que la explican se sobrescriben

**Se descubre la intrusión**
Los investigadores piden los registros

| | | | |
|---|---|---|---|
| ~~Mes 1 · 02:14:07~~ | ~~vpn-gateway~~ | ~~Inicio de sesión desde nueva ubicación~~ | ~~SOBRESCRITO~~ |
| ~~Mes 1 · 02:31:52~~ | ~~file-server-02~~ | ~~Cuenta privilegiada creada~~ | ~~SOBRESCRITO~~ |
| Mes 12 · 09:03:18 | file-server-02 | Modificación masiva de archivos | DISPONIBLE |

RETENCIÓN FORENSE DE REGISTROS

# La intrusión fue hace meses. ¿Todavía tiene los registros?

Muchas intrusiones se descubren semanas o meses después de iniciar. La retención forense conserva la evidencia: recolectada fuera de los sistemas de origen, protegida contra alteración y lista para consultarse cuando un investigador, auditor o aseguradora pregunte qué pasó.

## POR QUÉ LA EVIDENCIA CASI SIEMPRE YA NO EXISTE

01

### Los equipos sobrescriben su propia historia

Firewalls, servidores y switches guardan un registro local limitado y lo rotan. La semana que necesita quizá ya no existe.

02

### Los atacantes borran sus huellas

Los registros guardados en un sistema comprometido pueden ser editados o borrados por quien lo controla.

03

### Registros dispersos no hacen una cronología

Consolas, formatos y relojes distintos convierten una investigación en una docena de búsquedas manuales.

**Sepa qué podría demostrar mañana.**

800-700-7500
www.controllednetworks.com

# Lo que le da la retención forense de registros

Un registro protegido de lo ocurrido en todo su entorno, conservado el tiempo que exijan su política, sus contratos y sus reguladores.

### Recolección centralizada

Eventos de firewall, servidores, red, identidad y aplicaciones reunidos en un solo lugar, fuera de los sistemas que los generaron.

### Retención a largo plazo

Un nivel de búsqueda para la actividad reciente y un nivel de archivo para el largo plazo, dimensionados a su volumen de datos.

### Controles contra alteración

Control de acceso, verificación de integridad y almacenamiento protegido, para detectar cualquier cambio en un registro.

### Investigación de incidentes

Analistas autorizados consultan cronologías y correlacionan fuentes para reconstruir quién hizo qué y cuándo.

### Retención legal

Un proceso definido para congelar registros específicos cuando la retención normal debe suspenderse.

### Exportación de evidencia

Entrega controlada de los registros relevantes con historial de acceso documentado y cadena de custodia.

## QUIÉN LE VA A PEDIR LOS REGISTROS

### Equipos de respuesta

Para definir qué fue tocado, cuándo empezó y si ya terminó.

### Auditores y reguladores

Para ver que sus controles operaron durante todo el periodo.

### Aseguradoras

Para sustentar una reclamación con un registro del evento.

### Asesores legales

Para preservar registros bajo retención legal y responder requerimientos.

## CÓMO TRABAJAMOS

01

### Inventariar

Mapeamos sus fuentes de registros y encontramos los huecos de cobertura.

02

### Modelar

Volumen de datos, periodos de retención y niveles de búsqueda y archivo.

03

### Construir

Recolección, almacenamiento protegido, controles de acceso e integridad.

04

### Operar

Vigilamos la recolección y apoyamos investigaciones y exportaciones.

## Solicite una evaluación de registros y retención forense.

Revisamos qué registra hoy, cuánto tiempo sobrevive y quién podría alterarlo, y le mostramos los huecos.

**800-700-7500**

**www.controllednetworks.com**

325 S. River St., 2nd Floor, Hackensack, NJ 07601

Los periodos de retención varían según industria, regulación y contrato. La admisibilidad de los registros como evidencia depende también del método de recolección, la custodia y las normas aplicables. © 2026 Controlled Networks Solution LLC (CNS). Todos los derechos reservados.