BRENDA CICLALI ORTIZ FONSECA
803-A

BITACORAS

Una bitácora en redes (también conocida como log) es un registro cronológico de eventos, actividades y cambios realizados en un sistema informático o red. Estas bitácoras son fundamentales para el monitoreo, la auditoría, la resolución de problemas y el análisis de seguridad.

Función

Registran eventos y actividades de los sistemas, aplicaciones y redes, lo que facilita el monitoreo y la resolución de problemas. También son importantes para la seguridad de la información.

Contenido

Una entrada típica en una bitácora incluye:

- Fecha y hora del evento.
- Origen (IP, dispositivo o usuario).
- Tipo de evento (error, advertencia, información).
- Descripción detallada (qué ocurrió).
- Severidad (nivel de criticidad: info, warning, error, critical)

Tipos

- **Bitácoras del Sistema (System Logs)**: Registran eventos del sistema operativo, como arranques, apagados y errores de hardware.
- **Bitácoras de Seguridad (Security Logs)**: Almacenan intentos de acceso, autenticaciones fallidas y actividades sospechosas.
- **Bitácoras de Aplicación (Application Logs)**: Registran eventos generados por programas específicos (servidores web, bases de datos, etc.).
- **Bitácoras de Red (Network Logs)**: Capturan tráfico y eventos de dispositivos de red (routers, switches).
- **Bitácoras de Auditoría (Audit Logs)**: Documentan cambios en configuraciones, permisos y accesos privilegiados.

Herramientas

Splunk

Splunk es una plataforma SIEM (Security Information and Event Management) y análisis de logs que indexa datos en tiempo real para búsquedas, visualizaciones y alertas.

ELK Stack

Conjunto de herramientas open-source para gestionar logs:

- Logstash: Recoge y procesa datos.
- Elasticsearch: Motor de búsqueda y almacenamiento.
- Kibana: Visualización mediante dashboards.

Graylog

Herramienta open-source de gestión de logs centralizada, enfocada en usabilidad y seguridad.
ntegración con MongoDB (almacenamiento) y Elasticsearch (índices).

Grafana Labs

Proporciona una solución simple, altamente disponible y compatible con Prometheus para unificar las métricas de múltiples sistemas, habilitando el análisis histórico y en tiempo real de las mismas a escala.