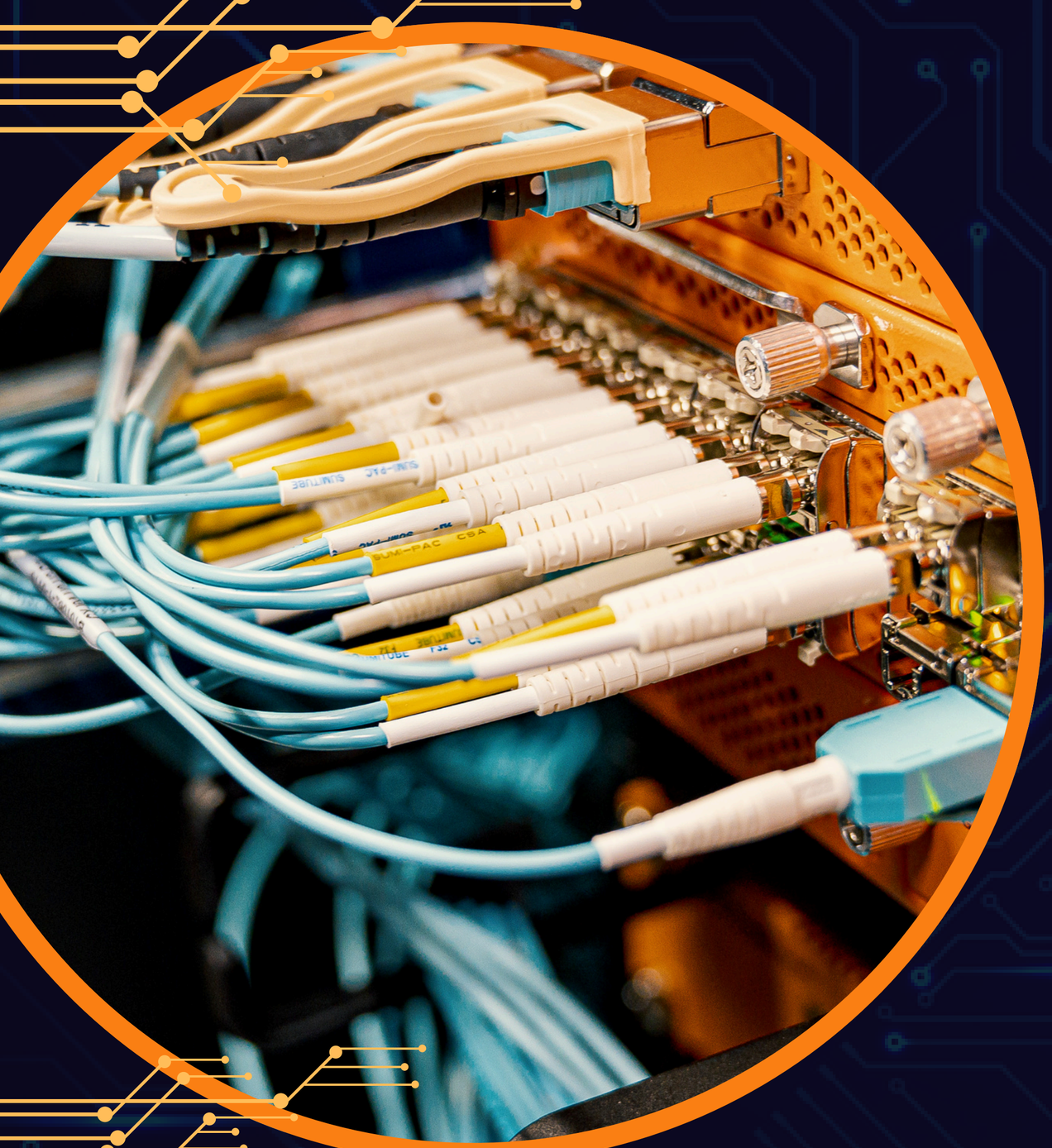

TIC

TALENTO TECH

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 2 -UNIDAD 2

Universidad Tecnológica de Pereira

faceIT

Lección 2: Control de aplicaciones y registros

Los registros o logs son información que generan todo tipo de sistemas digitales. Tantos programas, aplicaciones, controladores, y todo software que ejecute un procesador puede dejar registros de su actividad. Con estos registros es posible detectar fallas, rastrear eventos, determinar si un proceso ha salido bien o no, mirar qué sucesos han ocurrido a lo largo del tiempo y validar los cambios que los programas han hecho.

Los registros son muy importantes tanto para el desarrollo de software como para el mantenimiento del mismo. Con registros es posible determinar si un programa ha tenido un error y el motivo por el que el programa ha fallado. También es posible determinar las causas del error y arreglarlo.

Los sistemas operativos también tienen registros que permiten revisar cambios en la configuración, intentos de conexión, errores, eventos de cuando un usuario accede o un dispositivo se conecta al sistema y eventos de cuando un programa se instala o se elimina.

Si bien puede parecer innecesario el monitoreo de los registros cuando todo parece funcionar bien, es importante incluir revisiones periódicas de estos registros como parte de una estrategia de seguridad de la información.

Con la información de los registros se pueden identificar y analizar posibles fallas y brechas de seguridad, intentos de acceso, accesos no autorizados o cambios en el sistema por parte de los usuarios y establecer si los cambios son autorizados o no.

Con el crecimiento de la cantidad de usuarios y las necesidades de seguridad, la revisión manual de los registros es casi imposible. Por este motivo existen alternativas de software que permiten medir sucesos en muchos dispositivos y establecer cuáles de estos sucesos son incidentes de seguridad.

Para un monitoreo adecuado los logs se suelen centralizar para poder tener una vista detallada y rápida del funcionamiento de muchos componentes de un sistema grande o de una organización. Al tener los logs centralizados es posible analizarlos

y ver cuando han ocurrido incidentes de forma rápida. Una vez un incidente es detectado se reduce el tiempo de respuesta.

Junto con el monitoreo se debe incluir la automatización de la revisión de los logs. Esto brinda observabilidad, lo que permite detectar posibles fallas de seguridad a tiempo y corregirlas.

Algunos de los eventos que se deben considerar siempre al administrar un sistema son:

- Cambios de contraseñas
- Inicios de sesión no autorizados
- Intentos fallidos de inicio de sesión
- Nuevos eventos de inicio de sesión
- Detección de malware
- Ataques de malware
- Escaneo de puertos abiertos y cerrados
- Ataques de denegación de servicio
- Errores en dispositivos de red

- Cambios en nombres de archivos protegidos o en su contenido
- Datos exportados y almacenados en dispositivos extraíbles
- Eventos de instalación de programas o servicios
- Creación de cuentas de usuario
- Eventos de inicio de sesión por fuera de horarios laborales

De igual manera, en las aplicaciones se deben establecer y revisar los eventos. Por lo general se determinan algunos niveles de registro en las aplicaciones como son:
Info: eventos de información, casi siempre están disponibles e informan el estado de la aplicación

Error: Se registran cuando ocurre cualquier tipo de error y permiten encontrar las causas

Warning: son registros opcionales cuando no ocurre algún comportamiento esperado, sin embargo, este suceso no impide el funcionamiento de un programa

Debug: Son registros que solo deben estar presentes durante el desarrollo de un programa. Estos registros los utilizan los desarrolladores para analizar el comportamiento general de un programa, detectar errores y mejorar el software. En software que está en un estado productivo deben estar deshabilitados.

Como buena práctica los registros deben contener información relevante que permita el análisis de lo que sucede en el software. Adicionalmente, si el software que se desarrolla se instala en múltiples dispositivos, es necesario centralizar los registros, enviándolos a algún servidor que permita su análisis y tener observabilidad de los eventos.