**ACTIVIDAD 7: ACTIVIDAD FINAL - 30% NOTA FINAL - EQUIPOS**

**Elaborado por:**

JUAN CAMILO TAMAYO GIRALDO

LUIS FERNANDO MALDONADO ARANGO

Grupo 1

**Entregado a:**

PAOLA ELVIRA ORTEGA JURADO

Docente Virtual

**Fecha de presentación:**

Marzo 05 de 2017

**FUNDACION UNIVERSITARIA CATOLICA DEL NORTE.**

Facultad de Ingeniería, Programa Académico Ingeniería Informática

Curso Sistemas de Información

Medellín, Colombia

**CONTENIDO**

-Proyecto de monitoreo para continuidad de servicio-----------------------------------------------pag.3

-Planeación del proyecto--------------------------------------------------------------------------------pag.4

-Referenciación y selección del SI---------------------------------------------------------------------Pag.6

-Análisis del sistema-------------------------------------------------------------------------------------Pag.7

-A qué tipo de arquitectura hace referencia---------------------------------------------------------Pag.10

- Aplicar las diferentes perspectivas-----------------------------------------------------------------Pag.11

-Referencias---------------------------------------------------------------------------------------------Pag.14

**PROYECTO DE MONITOREO PARA CONTINUIDAD DE SERVICIO**

**ANTECEDENTES**

La compañía **DISTRIBUCIONES MEDELLIN S.A.S** es la mayor distribuidora de productos de uso industrial a nivel nacional, para su operación cuenta con diferentes tipos sistemas de información que ayudan a soportar los diferentes procesos internos de la compañía.

**DISTRIBUCIONES MEDELLIN S.A.** ha establecido las siguientes metas para el sistema informático de monitoreo:

* Generar información oportuna a nivel de los componentes de hardware que se involucran en las operaciones de la compañía.
* Generar alertas con base en umbrales preestablecidos de los componentes de hardware que se involucran en las operaciones de la compañía.
* Generar un Panel de control (Dashboard) que permita visualizar de forma fácil y rápida el estado de salud de los principales sistemas de información de la compañía.
* Generar análisis predictivos del uso de los sistemas de información y componentes de hardware.
* Generar información que le permita al negocio tomar acciones.

1. **PLANEACIÓN DEL PROYECTO**

**OBJETIVO**

**DISTRIBUCIONES MEDELLIN S.A.** busca una oferta integral servicio, para la gestión del monitoreo informático, que permita un aseguramiento de la continuidad operacional de los sistemas de información y telecomunicaciones, sostenido en el tiempo con un óptimo uso de los activos y un mejoramiento continuo del desempeño, asegurando las metas proyectadas en su plan estratégico de calidad.

**JUSTIFICACIÓN**

**DISTRIBUCIONES MEDELLIN S.A.** Necesitan cumplir con un SLA del 99.99% de disponibilidad y confiabilidad en sus operaciones ya que por medio de estas se interactúan con clientes, proveedores, distribuidores, áreas contables y administrativas, las necesidades se deben cubrir con monitoreo y alertas tempranas de sus aplicativos y sistemas de información como son:

**Redes de datos:** Intranet, Extranet e Internet.

**Servidores:** Bases de datos, Servicios Web, ERP, CRM, Correo.

**Aplicaciones:** Nomina, Ventas, logística, Inventarios.

Todos estos sistemas de información deben tener siempre disponibilidad ya que todos son de gran importancia para la operación de la compañía **DISTRIBUCIONES MEDELLIN S.A.**, por esto se requiere de la implementación de una infraestructura de monitoreo y análisis de datos que permita tener indicadores claves para la operación, como también que tenga la capacidad de generar alerta temprana por medio de un correo electrónico al personal de soporte (Mesa de ayuda), permitiendo diagnosticar y encontrar la causa raíz de la falla de una manera más fácil y rápida. Finalmente la plataforma debe también ofrecer capacidades analíticas que la compañía pueda usar para tener indicadores de negocio en tiempo real y tomar decisiones oportunas.

**ALCANCE DEL PROYECTO**

* Monitoreo de capacidad de los componentes de hardware
* Monitoreo de navegación de los usuarios
* Monitoreo de disponibilidad de los canales de comunicación
* Monitoreo de autenticación de los usuarios
* Monitoreo de los servicios comerciales web (Portal de ventas)
* Monitoreo de transacciones del sistema contable (OpenERP)
* Monitoreo de transacciones del sistema financiero (OpenERP)
* Monitoreo de transacciones del sistema de logística (OpenERP)

**2.  REFERENCIACIÓN Y SELECCIÓN DEL SI**

El Sistema de información que se plantea para este proyecto es de tipo transaccional, Apoyo a decisiones y Estratégico. Este SI se encarga de automatizar los diferentes procesos del área de soporte técnico (Mesa de ayuda), evaluando y monitoreando los diferentes indicadores claves para el buen funcionamiento de la infraestructura tecnológica y de información.

Es el sistema de información seleccionado para este proyecto ya que nos facilita la recopilación, el análisis y el uso del valor oculto de los big data generados por la infraestructura tecnológica, sistemas de seguridad y las aplicaciones core de la compañía, lo que le proporciona la información necesaria para lograr un rendimiento operacional y resultados empresariales excelentes.

Con este SI se pretende capturar los eventos generados por los **Sistema de Procesamiento de Operaciones (SPO) - Transaction Processing Systems (TPS) de la compañía DISTRIBUCIONES MEDELLIN S.A.**, con base en estos eventos se construyen los paneles de control y gestión de los procesos necesarios para el funcionamiento de la empresa y garantizaremos disponibilidad evitando y prediciendo posibles fallas con personal operativo capacitado para las rápidas soluciones.



1. **ANÁLISIS DEL SISTEMA**

**Splunk Enterprise** recolecta datos estructurados o no estructurados de diferentes fuentes como son Logs de aplicaciones, Métricas de capacidad, tramas SNMP ó TCP, Syslog, REST, Base de datos, inyección directa por desarrollo, Scripts, Colas de mensajería.

Las características de Splunk Enterprise permiten capturar eventos de:

**Redes de datos: LAN, Intranet, Extranet e Internet.**

Para este segmento, estas redes de datos se componen de Routers, Switches y Servidores, estos equipos por estándar, todos generan eventos que pueden ser centralizados en la plataforma de Splunk por medio del protocolo syslogs en tiempo real. De estos componentes podemos analizar indicadores como, pérdidas de conexión, nivel de procesamiento, temperatura, ancho de banda en la conexión, el tráfico utilizado, muestra perdida de conexiones por reinicios o caídas de energía.

Splunk Enterprise recopila estos datos en tiempo real enviando al personal de soporte alarma por correo electrónico informando cuando cualquier componente de comunicación tenga posible falla como:

* Procesamiento en Switches, Routers, Firewalls y host al 80% o más.
* Temperaturas de los equipos a 27.5° o más
* Pérdidas de conexión inmediatas.
* Pérdidas de paquetes en datos de 10% o más.
* Ocupación del canal de datos al 80% o más.
* Nivel de carga en las baterías de las UPS cuando bajen a 20% o menos.

**Servidores.**

Haciendo uso de una pequeña capa de software podemos capturar las métricas de uso a nivel de componentes de hardware y de software. Aplicando este agente en todos los servidores que están en el centro de cómputo tales como Base de datos, Middelware, Capa web, CRM, Correo Electrónico, Directorio Activo, algunos de los indicadores que se pueden generar.

* Supervisar e investigar los abusos relacionados con el uso de Internet.
* Patrones de uso e información de seguridad.
* Detección de errores en aplicaciones crítica.
* Fallos de autenticación y violación de seguridad.
* Métricas de capacidad de los servidores.

**Aplicaciones.**

La mayoría de las aplicaciones propias y en paquetes escriben archivos de registro locales, a menudo mediante el registro de marcos de trabajo como log4j o log4net, de servicios creados en servidores de aplicaciones como WebLogic, WebSphere y JBoss o .Net, PHP, etc. Estos archivos son esenciales para la depuración diaria de aplicaciones de producción por parte de desarrolladores y de la asistencia técnica de las aplicaciones. Suelen ser también la mejor forma de informar sobre la actividad comercial y del usuario y detectar situaciones de fraude, ya que reflejan todos los detalles de las transacciones.

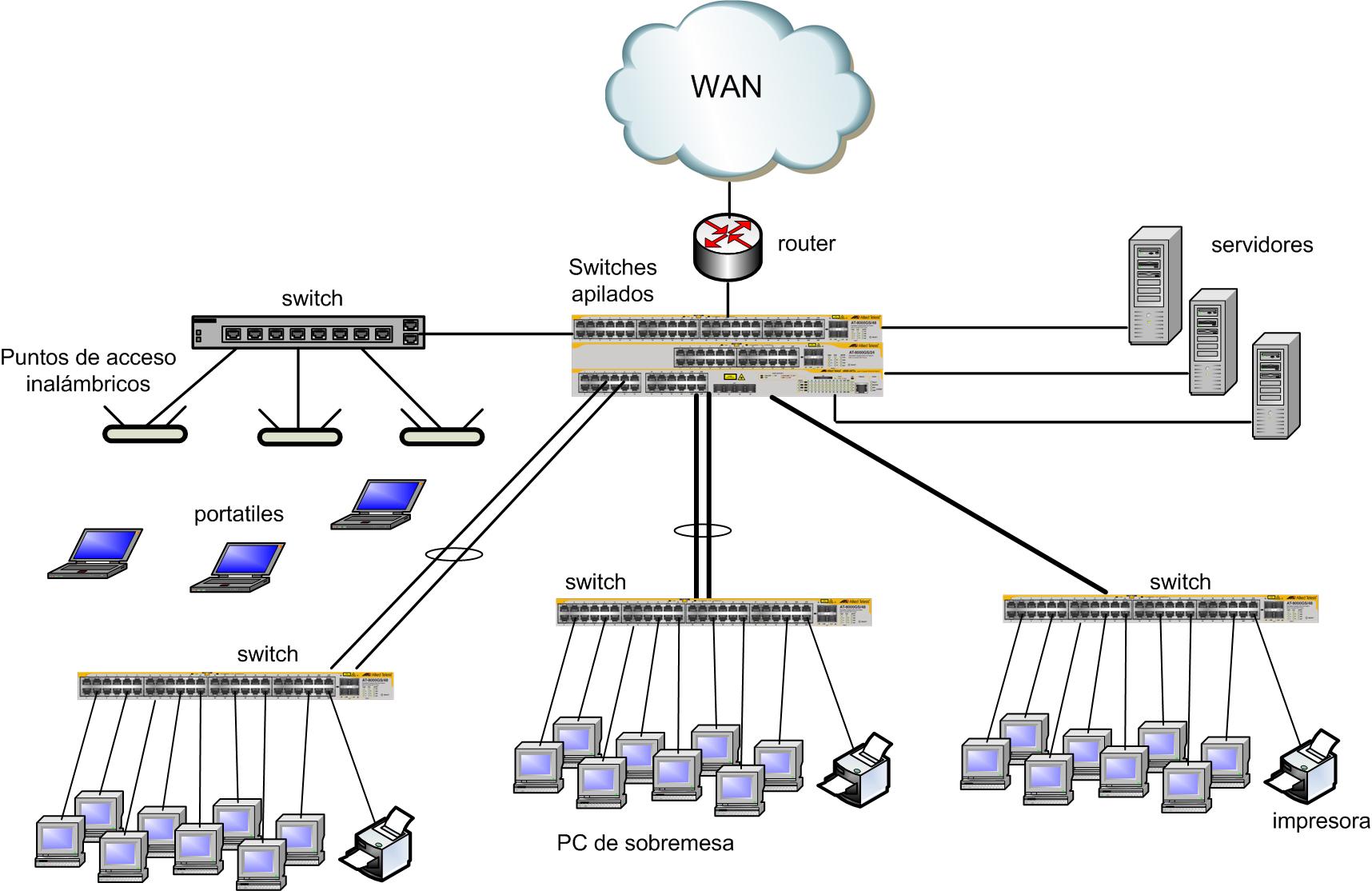
* Solicitudes procesadas por un servidor Web.
* Detección de fallos a nivel de desarrollo de las aplicaciones.
* Uso de las aplicaciones.
* Tiempo de transacciones.
* Detección de fraudes.
* Análisis Web para marketing

Con este tipo de información logramos mantener la empresa en funcionamiento sin interrupciones de las operaciones logrando un costo beneficio alto.

1. **A QUÉ TIPO DE ARQUITECTURA HACE REFERENCIA**

**Arquitecturas basadas en componentes.**

**Splunk Enterprise es un SI de arquitectura basada en componentes ya que su insumo principal son los datos de máquina, esto quiere decir que si algún SI de la compañía falla como puede ser componentes de Red, Aplicaciones, etc, esta no influye en la operación, su única afectación es que no lograra registrar eventos mientras este componente no esté disponible. Sin embargo, por sus procesos de análisis y monitoreo se podrá identificar y notificar a tiempo el incidente.**



1. **APLICAR LAS DIFERENTES**

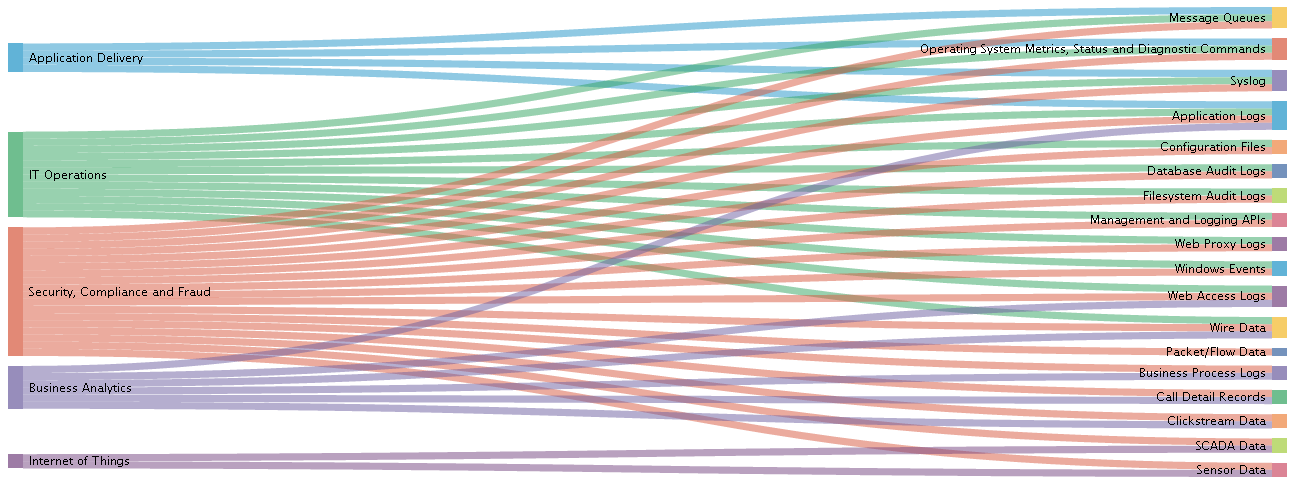
**Perspectiva de Integración**

Splunk Enterprise captura los eventos en tiempo real haciendo uso de una pequeña capa de software a nivel de sistema operativo y por otros medios como Syslog o SNMP para componentes de hardware. El transporte de estos eventos se hace por medio de red protocolo TCP.

**Perspectiva de Aplicación**

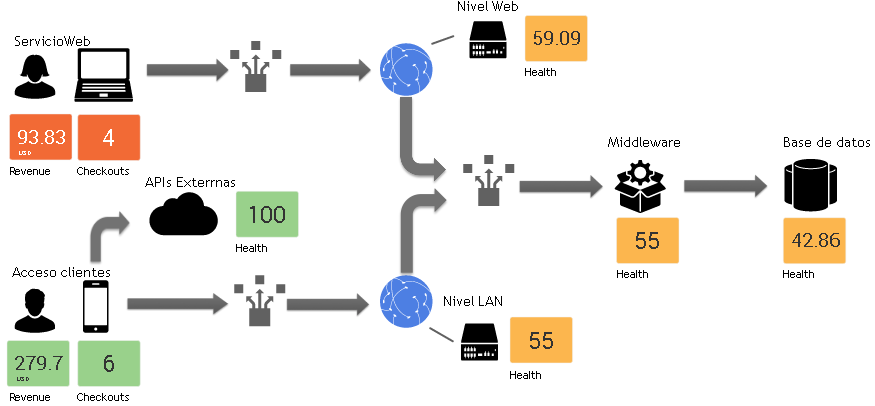
Splunk Enterprise tiene la capacidad de:

* Recopilar e indexar datos de maquina estructurados o no estructurados.
* Búsqueda e investigación sobre los eventos capturados.
* Correlaciones y análisis.
* Visualización y presentación de informes.
* Supervisión y creación de alertas.
* Seguro y administrable.



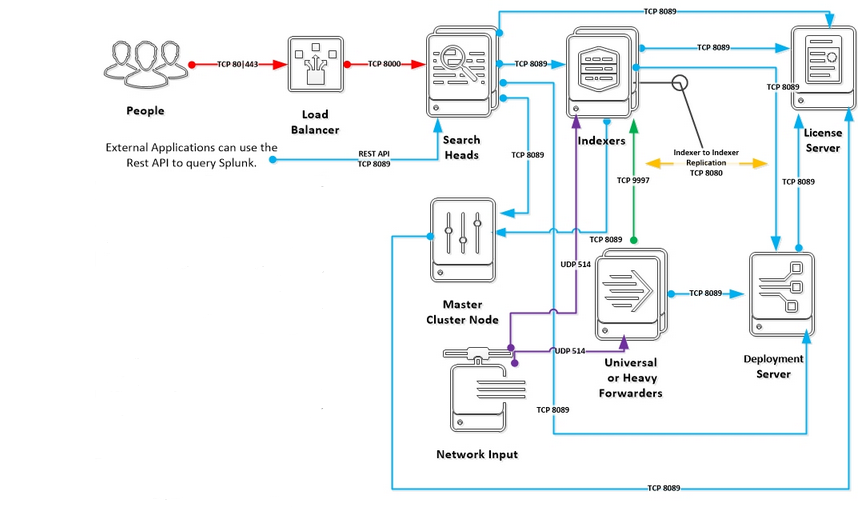
**Perspectiva de Información**

Splunk Enterprise, nos entrega datos precisos sobre los procesos y eventos ocurridos ya que este realiza un filtrado de la información, mostrándonos por medio de alarmas la información requerida por unos umbrales establecidos dependiendo de las necesidades evaluadas en la empresa, con esto logramos obtener solo la información necesaria para su correcto funcionamiento.



**Perspectiva de Técnica**

Splunk Enterprise, requiere un gran conocimiento para su desarrollo técnico ya que si la empresa es demasiado grande en su infraestructura, se necesitaran buen hardware para lograr el objetivo, pero con la gran ventaja que este puede ser administrado por un nivel más bajo de conocimiento ya que luego de ser instalado su manejo necesario para la operación es de ambiente amigable, con este software se reducirá la necesidad de conocimiento técnico muy alto ya que este nos dirá directamente cual es el problema a resolver.



**REFERENCIAS**

-Universidad Católica del norte:

Unidad 2: <https://aulavirtualbb.ucn.edu.co/bbcswebdav/institution/Facultades/Facultad%20de%20Ingenieria/Pregrado%20Ingenieria%20Informatica/sistemas%20de%20informacion/U2-index.html>

Unidad 3:

<https://aulavirtualbb.ucn.edu.co/bbcswebdav/institution/Facultades/Facultad%20de%20Ingenieria/Pregrado%20Ingenieria%20Informatica/sistemas%20de%20informacion/U3-index.html>