ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"AUTOMATIZACIÓN DE PROCESOS DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA UNA EMPRESA PÚBLICA BASADO EN LA ISO27002"

TRABAJO DE TITULACIÓN

Previo a la obtención del Título de:

MAGISTER EN TELECOMUNICACIONES

MARIA FERNANDA UTRERAS ABAD

GUAYAQUIL – ECUADOR

AÑO: 2017

AGRADECIMIENTOS

Le agradezco a Dios por permitirme seguir cosechando alegrías. Mis más sinceros agradecimientos también a las personas que estuvieron pendientes para que culmine esta etapa de mi vida exitosamente, a mi mamá ya que por ella estudié esta maestría y a mi mejor cómplice y ahora mi esposo por impulsarme a que termine de escribir este trabajo de titulación.

DEDICATORIA

El presente proyecto lo dedico a mi hija Charlotte, para que en un futuro se sienta orgullosa de sus padres.

TRIBUNAL DE EVALUACIÓN

PhD. Sixto García

SUBDECANO

PhD. Josep Pegueroles

DIRECTOR DE TRABAJO DE TITULACIÓN

Msc. Albert Espinal.

MIEMBRO PRINCIPAL DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad y autoría del contenido de este Trabajo de Titulación, me corresponde exclusivamente; y doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta. Difusión y uso público de la producción intelectual"

María Fernanda Utreras Abad

RESUMEN

Hoy en día muchas empresas almacenan todo tipo de información en computadoras, comenzando por información del personal, listado de clientes, sueldos del personal, datos bancarios, marketing, etc; por lo tanto esta información se considera como información "deseable" para dichas empresas. Las pruebas de este argumento están en todas partes: noticias, informes, documentos y más evidentemente en el hecho de que cada día hay una nueva actualización de software, un parche en el sistema operativo e incluso un método de encriptación más.

Este trabajo ayudará a las grandes empresas, sean Públicas o Privadas; sin embargo, está estudiado y diseñado para una empresa pública. Facilitará la concientización para mantener seguros los activos de la entidad y así pueda funcionar correctamente y cumplir con los objetivos planteados.

El objetivo principal es proteger la información sensible y la información de los sistemas de acceso no autorizado y especialmente, de cualquier uso, alteración, modificación o destrucción.

Las herramientas que se utilizaban en CNEL EP eran insuficientes y un cambio era necesario, una reestructuración de flujo de trabajo y una forma adaptada para concentrar y administrar eficientemente toda la Gestión de información y eventos de Seguridad.

Obtener un nivel de seguridad considerable y prevenir ataques informáticos será la meta de este trabajo que mediante la Automatización de procesos de gestión de seguridad de información basado en la ISO27002, agilizará la prevención de posibles incidentes de seguridad, y puede ser aplicado en empresas grandes en donde la generación de información corresponde a infraestructura y sistemas informáticos críticos.

ÍNDICE GENERAL

CAPÍTULO 1

1. DESCRIPCIÓN DEL PROBLEMA

En este capítulo se explicará el problema de CNEL EP y la necesidad de poder adquirir una solución al problema.

1.1. Antecedentes

La Empresa Eléctrica Pública Estratégica Corporación Nacional de Electricidad *CNEL EP* es la empresa más grande de distribución de energía eléctrica del Ecuador, por lo cual cada día se mejoran las tecnologías para automatizar los componentes de conmutación de las línea eléctricas en subestaciones así como la implantación de sistemas informáticos para brindar el servicio a sus clientes; así mismo en la actualidad son complejos los multiniveles de arquitectura de seguridad que se deberán aplicar para proteger dispositivos como servidores, computadores de usuarios, aplicaciones, equipos de comunicaciones que son parte del proceso de transmisión, recepción, almacenamiento y consiguiente procesamiento de los datos.

Los equipos tecnológicos generan voluminosos registros (logs) de su actividad, que son difíciles de interpretar dada la cantidad y complejidad de los mismos además del tiempo que se requiere invertir para correlacionar y detectar un evento específico, el cual puede ser real como un ataque, virus, gusanos que podría influir en la correcta operación de los sistemas o simplemente un falso positivo que induzca a toma de decisiones erróneas.

1.2. Justificación

Cada uno de estos equipos tecnológicos genera información sobre su actividad y funcionamiento de una manera diferente, en un formato diferente, guardados en lugares diferentes y reportados a ubicaciones diferentes. Este incesable flujo de datos (miles de mensajes diarios) de tecnologías incompatibles en la actualidad no están siendo almacenadas o peor aún evaluadas para tener una interpretación real de las vulnerabilidades y el grado de exposición de sistemas como SCADA

OMS-DMS/MWM, sistemas financieros, nómina, comerciales; por ende en CNEL EP no se han implantado salvaguardas preventivas con base en un análisis de registros que permitan identificar y neutralizar las vulnerabilidades ante que estas se materialicen, en los últimos años se han tomado acciones “correctivas” las cuales tiene la característica de ser implantadas una vez que se sufrió el impacto por una amenaza materializada.

Teniendo en consideración lo anteriormente descrito, el 25 de septiembre del 2013 la Secretaría Nacional de la Administración Pública “SNAP”, publicó en el Registro Oficial el Acuerdo No. 166 en el que establece:

“Artículo 1.- Disponer a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información; el presente documento denominado Esquema Gubernamental de Seguridad de la Información (EGSI), está basado en la norma técnica ecuatoriana INEN ISO/IEC 27002 para Gestión de la Seguridad de la Información y está dirigida a las Instituciones de la Administración Pública Central, Dependiente e Institucional” [1].

Adicionalmente, en el Anexo 1 del Acuerdo Nº 166, “Esquema Gubernamental de Seguridad de la Información (EGSI)”, se dispone que las empresas del sector público debe implantar los controles detallados dentro de la norma INEN ISO/IEC 27002 con el objetivo de asegurar la integridad y disponibilidad de la información así como la implantación de controles que permitan tomar decisiones preventivas y no reactivas en el momento que una amenaza llegue a materializarse.

Debido a la gran cantidad de clientes (1’661.000 abonados) que posee CNEL EP, se posiciona como la empresa de distribución de energía eléctrica más grande del ecuador por lo cual se tiene la necesidad de mejorar los controles que permitan evaluar los eventos de seguridad de la infraestructura tecnológica con el objetivo de garantizar la operación ininterrumpida del servicio que se ofrece a nuestros clientes.

Mediante esta mejora, se logrará garantizar de forma razonable la integridad de los datos que se transmiten desde las subestaciones, agencias y demás oficinas de CNEL EP hacia el Centro de Procesamiento de Datos del Salitral, mejorando la atención de los usuario residenciales, comerciales, industriales, asistencia social y entidades públicas u oficiales, mejora que se refleja en la disminución de riesgo por paralización de los servicios eléctricos, atención al cliente, facturación y recaudación debido a ataques a nuestra infraestructura tecnológica lo cual expone a la Corporación a la pérdida de información e incluso daño de los componente electicos en la subestaciones en caso de que un atacante logre acceder a los sistemas SCADA OMS-DMS/MWM.

Con la finalidad de mejorar el nivel de seguridad de CNEL EP, y siguiendo la guía de buenas prácticas internacionales y nacionales, se ha realizado el proyecto de "Mejoramiento de la seguridad, integridad y disponibilidad del equipamiento tecnológico de subestaciones, agencias y Centros de Procesamiento de Datos de CNEL EP" para garantizar la seguridad de la infraestructura tecnológica de CNEL EP alojada en el Centro de Procesamiento de Datos del Salitral.

1.3. Planteamiento del Problema

El Problema principal es la inexistencia de controles que garanticen razonablemente la seguridad de los equipos tecnológicos y que expone a CNEL EP al riesgo de ataques internos (sabotaje) y externos (Hackers) derivando en la paralización de sus servicios, y daño de la imagen institucional.

El hecho de no contar con una herramienta de correlación de eventos y gestión de vulnerabilidades que permita establecer medidas de control preventivas expone de forma directa a CNEL EP. al riesgo de comprometer la continuidad del negocio.

En Junio del 2014 se creó la Gerencia de Seguridad de la Información (GSI). La GSI es un área nueva que desde su creación ha venido trabajando arduamente en temas de seguridad, se comenzó con la elaboración de la política de seguridad, norma técnica, procedimientos, controles y planeación de proyectos para la adquisición de equipamiento para mejorar los niveles de seguridad de los equipos de tecnología que contienen la información crítica de la Corporación.

Como el problema de CNEL EP es la inexistencia de una solución que pueda automatizar la forma de ver los Logs de los equipos y sistemas de la corporación, lo cual se lo hacía manualmente, se planteó este proyecto para agilitar el descubrimiento de eventos de seguridad y actuar de forma preventiva.

1.4. Marco Conceptual

Es importante definir algunos términos que serán de mucha ayuda en el transcurso de este trabajo:

"El Esquema Gubernamental de Seguridad de la Información, más conocido como EGSI, está basado en la norma técnica ecuatoriana INEN ISO/IEC 27002 para Gestión de la Seguridad de la Información y está dirigido a las Instituciones de la Administración Pública Central, Dependiente e InstitucionalEl EGSI establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la Administración Pública.

El EGSI no reemplaza a la norma INEN ISO/IEC 27002 sino que marca como prioridad la implementación de algunas directrices", tal como se cita en el documento del Acuerdo Ministerial 166 de la Secretaria Nacional de Administración Publica.

CNEL EP como Empresa Pública está obligado a implementar el EGSI en la institución.

Esta exigencia Gubernamental es la que dio pie a la creación de la Gerencia de Seguridad de la Información en CNEL EP, en donde el Gerente, es el Oficial de Seguridad de la Información tal y como lo indica el literal a del punto 2.2 de dicho esquema.

Entre las directrices que se implementaron, existían algunas que se necesitaba de una ayuda para poder hacer el trabajo más eficiente, esto por esto que se ve la necesidad de comprar un SIEM.

Security information and event management (SIEM) por sus siglas en inglés, es una solución que proporciona análisis en tiempo real de alertas de seguridad generados por el hardware y las aplicaciones de red de una compañía.

El SIEM consta principalmente de dos áreas, la gestión de eventos de seguridad que se ocupa del monitoreo en tiempo real, correlación de eventos, notificaciones y vistas de la consola y la segunda área, la gestión de la información de seguridad que proporciona un almacenamiento a largo plazo, así como el análisis y la comunicación de los datos de registro.

1.5. Marco de Referencia

El marco de referencia para este proyecto de graduación es la ISO 27002 que consiste en una guía de buenas prácticas que permiten a las organizaciones mejorar la seguridad de su información. Con este fin, define una serie de objetivos de control y gestión que deberían ser perseguidos por las organizaciones.

Éstos se hallan distribuidos en diferentes dominios que abarcan de una forma integral todos los aspectos que han de ser tenidos en cuenta por las organizaciones. En el capítulo dos se explicará a detalle este tema y sus dominios, debido a que es muy importante para la toma de decisiones en una empresa, si esta se basa en la ISO 27002.

1.6. Modelo Propuesto para la solución del problema

Se vio la necesidad de implementar un Sistema de gestión de la información y eventos de seguridad SIEM" del fabricante Splunk. La instalación y configuración del referido sistema se lo deberá realizar en data center del Salitral - Guayaquil, y en las ocho unidades de negocio, las mismas que se detallan en la Tabla 1.

No.	Unidad de negocio	Ciudad
1	Manabí	Manta
2	Esmeraldas	Esmeraldas
3	El Oro	Machala
4	Guayas	Guayaquil
5	Guayas - Los Ríos	Guayaquil
6	Milagro	Milagro
7	Santo Domingo	Santo Domingo
8	Santa Elena	La Libertad

Tabla 1

La plataforma de inteligencia de Seguridad, integrará SIEM, gestión de riesgos y vulnerabilidades, análisis de comportamiento de red y gestión de eventos desde una sola interfaz web, integrando las fuentes de logs y syslogs.

Lo que se desea monitorear está detallado a continuación:

Los log en servidores:

- Mensaje del sistema afín de detectar problemas en el mismo.
- Logs para los mensajes de seguridad.
- Logs de los servicios que estén corriendo a el servidor (apache, samba, httpd, etc)
- Logs de inicio y apagado de un servidor, y considerar logs de del proceso que configura los procesos plug&play.
- Registros de usuarios que están actualmente conectados dentro del sistema/App y quienes estuvieron el sistema y cuando.
- Logs de intentos de ingreso fallido.
- Logs de correo y de cola de impresión

En los Switches, se obtienen logs de:

- Emergencias o eventos inusuales en el sistema
- Alertas que requieran acción inmediata
- Condiciones críticas, errores, advertencias.

A nivel de Directorio Activo considerar:

- Objeto Abierto (Active Directory)
- Windows 566 - Operación de Objetos (W3 Active Directory)
- IDs para eventos del Directorio de Servicios.

CAPÍTULO 2

2. NORMA ISO/IEC 27002:2005

En este capítulo se explicará más a detalle la Norma ISO/IEC 27002:2005

2.1. Justificación

La ISO 27002 es una guía de protocolos a seguir en la implementación del sistema de administración de la seguridad de la información, los cuales se basan en los siguientes puntos:

- Confidencialidad: se refiere a confidencialidad el asegurarnos que solo la persona o personas autorizadas tenga acceso a la información.
- Integridad: se refiere a la garantía de que no se modifique ni altere por personas no autorizadas, la información.
- Disponibilidad: se refiera que la información debe estar disponible o se debe poder acceder a ella cuando las personas autorizadas requieran de ella.

Esta norma, ISO 27002 es quien da el comienzo a la toma de decisiones sobre qué criterios métodos o políticas se deben aplicar con base a seguridad de la información.

2.2. Dominios

Esta norma ISO 27002 contiene 11 dominios de control y controles de seguridad de la información, los cuales contienen un total de 39 sub dominios principales de seguridad.

Cada dominio contiene un número de dominios de seguridad. Estos 11 dominios se detallan en el Anexo 1.

2.3. Dominios que cubre el modelo propuesto para la solución de problema

A continuación se citan tal como se muestra en la guía de splunk para la ISO27002, los dominios que cubre el modelo propuesto para la solución del problema, este se enumera en concordancia al Anexo 1.

1.1.1. “Dirección de seguridad de la información

Con la capacidad de monitorear tanto las amenazas conocidas y desconocidas.

1.1.2. Coordinación de Seguridad de la Información:

Informes automatizados para los miembros o directivos del equipo de seguridad.

1.1.3. Asignación de responsabilidades de la Seguridad de la Información:

Seguimiento de las tareas de seguridad específicos relacionados con los incidentes de seguridad y las métricas y seguimiento de los eventos de seguridad resueltos.

1.1.8. Revisión independiente de la Seguridad de la Información

6.2.1 Identificación de los riesgos derivados del acceso a terceros

7.1.1 Inventario de Activos

7.1.3 Acuerdos sobre el uso aceptable de los activos

7.2.2 Clasificación de la Información

8.1.1 Inclusión de la seguridad en las responsabilidades laborales

8.2.2 Formación y capacitación en Seguridad de la Información

8.3.1 Terminación de responsabilidades

8.3.2 Restitución de los Activos

8.3.3 Cancelación de permisos de acceso

9.1.2 Controles Físicos de Entrada

9.1.4 Protección contra amenazas internas y del entorno

9.2.1 Instalación y protección de equipos.

9.2.6 Seguridad en la reutilización o eliminación de equipos

9.2.7 Traslado de Activos

10.1.2 Control de cambios operacionales

10.1.3 Segregación de tareas

10.1.4 Separación de los recursos para desarrollo y producción

10.2.1 Prestación de servicios
10.2.2 Monitorización y revisión de los servicios contratados
10.3.1 Planificación de capacidades
10.3.2 Aceptación de Sistema
10.4.1 Medidas y controles contra Software malicioso
10.5.1 Recuperación de la información
10.6.1 Controles de red
10.6.2 Seguridad en los servicios de Red
10.7.1 Gestión de soportes extraíbles
10.7.3 Procedimientos de utilización de la información.
10.7.4 Seguridad de la documentación del sistema
10.8.4 Interconexión de sistemas con información de negocio
10.9.1 Seguridad en comercio electrónico
10.9.2 Seguridad en transacciones en línea
10.10.1 Registro de incidencias
10.10.2 Seguimiento del uso de los sistemas
10.10.3 Protección de los registros de incidenticas
10.10.4 Diarios de operación de administrador y operador
10.10.5 Registro de Fallos
10.10.6 Sincronización de reloj
11.1.1 Política de Control de Accesos
11.2.1 Registro de usuario
11.2.2 Gestión de Privilegios
11.2.3 Gestión de contraseñas de usuario
11.3.1 Uso de contraseña
11.3.2 Equipo informático de usuario desatendido
11.4.2 Autenticación de usuario para conexiones externas
11.4.5 Segregación en las redes
11.5.2 Identificación y autenticación de usuario
11.5.4 Uso de los servicios del sistema
11.5.5 Desconexión automática de terminales
11.6.1 Restricción de acceso a la información.

11.6.2 Aislamiento de sistemas sensibles

11.7..2 Tele trabajo

12.3.2 Cifrado

12.4.1 Control de software en explotación

12.4.3 Control de accesos a la librería de programas fuente

12.5.1 Procedimientos de control de cambios

12.5.2 Revisión de técnica de cambios en el sistema operativo

12.5.4 Canales encubiertos y códigos troyanos

12.6.1 Control de las vulnerabilidades técnicas

13.1.1 Comunicación de eventos en seguridad

13.2.2 Evaluación de incidente en seguridad

13.2.3 Recogida de pruebas

14.1.1 Proceso de la gestión de continuidad del negocio

15.1.4 Protección de datos de carácter personal y de la intimad de las personas

15.2.1 Conformidad con la política de seguridad”

CAPÍTULO 3

3. FUNCIONAMIENTO PREVIO DE LA GESTIÓN DE SEGURIDAD EN CNEL

En este capítulo se explica cómo es el proceso de gestión de Seguridad sin ninguna herramienta que mejore o haga más eficiente el trabajo para el área de Seguridad de CNEL EP.

3.1. Descripción del funcionamiento de la Gestión de Seguridad actual

El funcionamiento de la Gestión de Seguridad actual es totalmente manual. La Gerencia de Seguridad de la Información de CNEL EP, elaboró la política de seguridad, norma técnica, procedimientos y controles, los cuales permiten tener una directriz de las actividades a realizar en el área de Seguridad de la Información. Sin embargo debido a que la Gerencia se creó a mediados del año 2014 no se tuvo el presupuesto para comprar herramientas que permitan la automatización de esta gestión. Es por esta razón que se trabajó manualmente.

Si existe algún problema en un sistema de la Corporación, primeramente como área de Seguridad no se puede trabajar preventivamente, únicamente en el momento en que se ya existe el problema o incidencia, se recopila el Log del sistema afectado y se comienza a analizar toda la estructura del registro y a opinión propia del técnico se halla o no con el causante de la afectación. Esto toma mucho tiempo, en ocasiones horas o hasta un par de días analizar la información de los Logs.

3.2. Análisis de ataques reportados vs ataques atendidos

Este análisis se realiza con base a los eventos reportados por los usuarios internos, tal como se detalla en la Tabla 2. Cabe recalcar que como no se tenía una solución que automatizara esta gestión, se esperaba que el usuario final reporte el evento para actuar o atender el incidente, por lo cual este indicador está en verde, debido a que todo lo reportado fue atendido, como se muestra en la Figura 3.1.

Indicador	Porcentaje de eventos de seguridad tecnologicos atendidos
Descripción de Indicador	Este indicador muestra el número de incidentes de seguridad que la GSI atiende con respecto al número de incidentes de seguridad reportados. Un incidente de Seguridad es un acceso, intento de acceso, uso, divulgación, modificación u destrucción no autorizada de información, un impedimento en la operación normal de las redes, sistemas o recursos informáticos.

Tabla 2

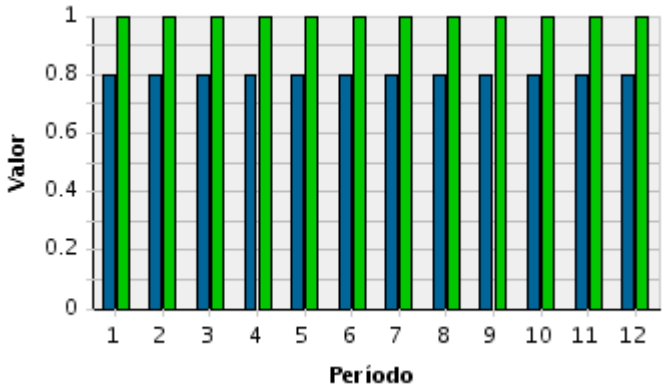

Figura 3.1

3.3. Análisis de Tiempo de respuesta de ataques

Para este análisis solo se tomará en cuenta los ataques tipo Phishing, los cuales son por medio de un correo electrónico, en donde el atacante suplanta la identidad en este caso de la Corporación para pedir usuario y contraseña. Se ha tenido ataques muy bien elaborados y dirigidos a la corporación, en donde el atacante ha podido capturar muchas cuentas de correos corporativos y usuarios. Los tiempos de respuesta ante el bloqueo de la url en los Firewalls de todas las Unidades de Negocio (UN´s) eran muy lentos. Las UN´s tardaban en bloquear la url sospechosa, una muestra del tiempo de respuesta se lo puede ver en la figura 3.2.

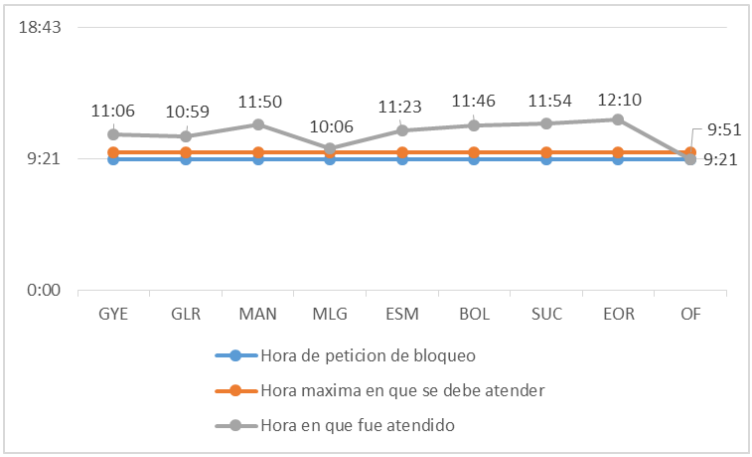

Figura 3.2

3.4. Análisis de Impacto Económico en caso de que se afecte componentes tecnológicos

El proyecto en estudio está dirigido a todas las Unidades de Negocio de la CNEL EP. dependientes de la su plataforma informática y que brindan servicio a los usuarios del servicio eléctrico.

Los usuarios ubicados en el área de concesión de la CNEL EP. requieren que se garantice día a día el suministro del servicio eléctrico; por lo que este proyecto requiere una importante inversión (egreso) y su rentabilidad se medirá evitando la paralización del servicio debido a ataques interno, externos y/o hurto de la información.

La calidad del servicio, continuidad del negocio e imagen corporativa es considerada como un ingreso, al poder determinar que la paralización de un servicio por alguna vulnerabilidad por la cual se reciba un ataque, puede comprometer la distribución del suministro eléctrico generando pérdidas económicas a CNEL EP. y al Estado Ecuatoriano; como ejemplo se considera un ataque a las subestaciones de la Unidad de Negocio Guayas-Los Ríos (UN GLR) las cuales cuentan con equipamiento tecnológico y sistema SCADA mediante el cual se realizan las maniobras de conmutación (switcheo) entre líneas.

Grupo de Consumo UN GLR = 300.447 usuarios

Valor de Energía no suministrada según resolución 2511 del CONELEC = $ 1,33 (dólares).

Proyección de distribución de energía para el año 2015 del CONELEC = 7’981.545,91 MWh.

La UN GLR vende aproximadamente 1’505.700 MWh al año.

kWh de la UN GLRS = (1’505.700 x 1.000) / 8760 = 171.883,56 kWh.

Pérdida por concepto de energía no suministrada en UN GLRS se detalla en la ecuación 3.1:

$$P_s = 171.883{,}56 \times 1{,}33 = \$228.605.14 \tag{3.1}$$

Donde, P_s es pérdida económica por energía no suministrada durante el lapso de una hora

Para este ejercicio se considera una suspensión de la distribución de energía eléctrica por 8 horas como se puede ver en la ecuación 3.2:

$$P_{S4h} = 228.605{,}14 \times 8 = \$1.828.841{,}12 \tag{3.2}$$

El asegurar que las vulnerabilidades que actualmente existen en nuestros sistemas sean detectadas por CNEL EP. y podamos aplicar salvaguardas preventivas, garantizará que no ocurran eventos que paralicen el servicio de distribución de energía con lo cual a la vez se justifica el retorno sobre la inversión.

3.5. Análisis de Impacto Económico en caso de que se afecte los sistemas Comerciales

A fin de determinar el impacto económico que provocaría un ataque o violación a nuestros sistemas informáticos los cuales paralicen su operación se realiza el siguiente cálculo:

1) La recaudación de CNEL EP en agencias durante el segundo semestre del año 2015 se muestra en la Tabla 3.

jun-15	jul-15	ago-15	sep-15	oct-15	nov-15	dic-15
USD RECAUDADOS (TOTAL)	USD RECAUDADOS (TOTAL)	USD RECAUDADOS (TOTAL)	USD RECAUDADOS (TOTAL)	USD RECAUDADOS (TOTAL)	USD RECAUDADOS (TOTAL)	USD RECAUDADOS (TOTAL)
$ 108.966.943,83	$ 108.344.944,45	$ 104.501.303,94	$ 101.148.528,83	$ 101.126.683,71	$ 98.692.606,99	$ 104.543.886,62

Tabla 3

La recaudación promedio mensual durante el segundo semestre del 2015 realizada en las Agencias de las Unidades de Negocio de CNEL EP fue de aproximadamente: $ 103’059.659,09

El cálculo para obtener el promedio recaudado por hora está dado con base al valor promedio obtenido durante un mes del primer semestre, tomando en cuenta el número de días laborables durante una jornada de 8 horas por 5 días a la semana; con lo cual se ha determinado que CNEL EP recaudó aproximadamente $ 643.750,00 por hora promedio durante el primer semestre del 2015 como se muestra en la ecuación 3.3.

$$\text{Recaudación Agencias x Hora} = \frac{\text{Recaudación Promedio Mensual}}{\text{Número de horas laborables por mes}}$$

$$= \frac{103’000.000,00}{160\text{Horas}} = \$\ 643.750,00 \qquad (3.3)$$

Dentro del análisis se ha determinado una escala de pérdida de oportunidad de cobro en agencias versus horas de afectación, que se muestra en la Tabla 4.

Perdida	Hora
$ 321.875,00	0,5
$ 643.750,00	1
$ 1.287.500,00	2
$ 2.575.000,00	4
$ 3.862.500,00	6
$ 5.150.000,00	8
$ 7.725.000,00	12
$ 15.450.000,00	24
$ 30.900.000,00	48

Tabla 4

Por recaudación en línea (a través de entidades financieras), CNEL EP registra un ingreso total aproximado de $ 28’988.862,59 durante el mes de Junio del 2015.

El cálculo para obtener el promedio recaudado por hora está dado con base al valor aproximado recaudado en línea en el mes de Junio del 2015, tomando en cuenta que las instituciones financieras recaudan 24x7, con lo cual se ha determinado que CNEL EP recaudó aproximadamente $40.262,31 por hora, como se muestra en la ecuación 3.4.

$$\text{Recaudación en Línea x Hora} = \frac{\text{Recaudación aprox. mensual}}{\text{\# de Horas laborable x Mes}}$$

$$= \frac{\$\ 28'988.862,59}{720\text{Horas}} = \$\ 40.262,31 \qquad (3.4)$$

Teniendo en cuenta que en el caso de que un ataque llegue a afectar la plataforma tecnológica de CNEL EP., se comprometería de forma directa la continuidad de su operación, exponiéndose al riesgo de paralizar los servicios que se encuentren relacionadas directa o indirectamente con los sistemas implicados en el ataque; se puede determinar que en el caso del sistema comercial, por cada hora de paralización del servicio de recaudación, CNEL EP. tendría una pérdida de oportunidad de cobro aproximadamente $684.012,31, como se muestra en la ecuación 3.5.

$$\text{Recaudación Total x Hora= Rec. x hora Agencia + Rec. x hora en Línea} = \$\ 684.012,31 \tag{3.5}$$

La “Pérdida de Oportunidad de Cobro” afecta directamente al ingreso de flujo de efectivo a las cuentas de CNEL EP., ocasionando desfases en la recaudación y comprometiendo la operación y cumplimiento de las obligaciones adquiridas por la institución; además, se afecta a la imagen corporativa debido a las molestias que originamos a nuestros clientes.

CAPÍTULO 4

4. DISEÑO, ARQUITECTURA Y DESARROLLO DE LA AUTOMATIZACIÓN DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

En este capítulo se detalla la fase del diseño, arquitectura y el desarrollo de la solución, todo esto con base a las necesidades de CNEL EP y adaptándose a la infraestructura tecnológica de la corporación.

4.1. Alcance

El alcance del proyecto es mejorar los niveles de seguridad para el equipamiento tecnológico de agencias, subestaciones y centro de procesamiento de datos a fin de mitigar las crecientes amenazas, persistentes y cambiantes, internas y externas, contra los recursos de información de la Corporación; tales como: bases de datos, servidores, equipos de interconexión entre las redes IT y OT; a través de la implantación de un Sistema de Gestión de Eventos para la Seguridad de la Información (SIEM) que permitirá a CNEL EP disminuir alertas de falso positivo, detectar anomalías de red y amenazas además de poder realizar análisis antes, durante y después de que se haya materializado un ataque mediante el examen de los paquetes capturados en la red.

Puesto que la solución que de aquí en adelante se llamará Splunk es muy completa para la gestión de eventos de seguridad, se han delimitado los ítems que serán implementados dentro de este proyecto que tendrá como resultado que CNEL EP cuente con un “Sistema de gestión de información y eventos de seguridad SIEM”.

A continuación en la Tabla 5, se describe los ítems que están dentro del alcance del proyecto que han permitido que este sea viable en términos de tiempo, costo y calidad.

General	Dentro del alcance	Fuera del alcance
Localidades:	Centro de datos Salitral en Guayaquil de CNEL, donde se implementarán los servidores de la solución. Además se instalará un colector en cada una de las unidades de negocio ubicadas en: • Manta: Avenida 7 s/n y Malecón Edificio CNEL • Esmeraldas: Calle Mejía entre Av. Olmedo y Av. Sucre • Machala: Av. Arizaga y Santa Rosa • Guayaquil: Cdla. La Garzota Sector III Mz 47 • Guayaquil: Malecon 100 y Loja • Milagro: Av. 17 de Septiembre y Ambato • Santo Domingo: Av. Tsáchila 826 y Clemencia de Mora • La Libertad: Barrio General Enríquez Gallo, Av. 12, Intersección de calles 33 y 35	Algún otro sitio remoto o unidad de negocio donde se tengan que instalar en sitio componentes de la solución que no haya sido especificados en la lista previa.

General	Dentro del alcance	Fuera del alcance
Personas:	Los usuarios que integren el equipo de Seguridad de CNEL EP	Usuarios externos al equipo de seguridad de CNEL
Lenguajes:	La solución será instalada en inglés	Cualquier otro idioma.

Tabla 5

4.2. Generalidades de la Solución

La recopilación de requerimientos para la implementación del "Sistema de gestión de información y eventos de seguridad SIEM" se realizó con la participación directa del área de Seguridad de la Información de CNEL EP. Se han identificado como requerimientos de la organización, las siguientes generalidades:

- Tener a través de un navegador web una consola centralizada que permita la visibilidad de estado real de seguridad de los distintos equipos y componentes que tiene CNEL EP.
- Detectar fácilmente falencias de seguridad o vulnerabilidades con base a los logs recopilados y generar alertas
- Permitir fácilmente ver los eventos de seguridad originales de cualquier equipo para hacer investigaciones.
- Realizar análisis de correlación de distintas fuentes de datos.
- Almacenar y permitir búsqueda posterior de los datos históricos de los equipos y aplicaciones monitoreadas.
- Encontrar de manera más ágil el origen de problemas de seguridad.
- Centralizar el repositorio de la información correspondiente a seguridad y su gestión en una sola ubicación.

- Prevenir vulnerabilidades de seguridad a través del constante cumplimiento de las políticas, normas y procedimientos de Seguridad de la Información.
- Obtener reportes periódicos del estado de seguridad de la organización
- Obtener gráficas que permitan rápidamente entender la situación actual en términos de seguridad de la infraestructura de la organización

4.3. Especificaciones Técnicas de la Solución

A continuación en la Tabla 6 se detallan las especificaciones técnicas:

1	**Especificaciones Requeridas**	
1.1	Cantidad	1
1.2	Factor	Appliance
1.3	Capacidad Inicial	5.000 EPS / 100.000 Bidireccional Flows
2	**Administración y Configuración**	
2.1	La plataforma de inteligencia de Seguridad, integra SIEM, gestión de riesgos y vulnerabilidades, análisis de comportamiento de Red y Gestión de eventos de seguridad desde una sola interfaz, la cual es web, fácil de usar, completamente integrada y automatizada.	
2.2	El proveedor provee el Hardware requerido para que la solución funcione de forma óptima.	
2.3	Posee una capacidad de almacenamiento principal (log manager) para eventos de al menos 25 TB.	
2.4	Provee 8 sensores (colectores) con una capacidad de almacenamiento de al menos 1 TB cada uno.	
2.5	La solución es capaz de escalar para permitir un despliegue que aumente progresivamente la cantidad de dispositivos y eventos registrados. Los componentes adquiridos son reutilizables en cualquier estrategia de	

	crecimiento, trasladando las funciones sin necesidad de eliminar datos ya recopilados.
2.6	Se basa en roles y permisos de usuario. Los permisos se configuran para permitir o denegar el acceso a funciones y datos específicos; por ejemplo: acceso a pestañas principales como dashboard, gestión de amenazas, búsqueda de eventos, informes, etc.
2.7	La herramienta tiene la capacidad de realizar auto-descubrimiento de activos que se están protegiendo o supervisando. Permite crear un perfil activo basado en listas de servicios, que se ejecutan en el host, datos de vulnerabilidad y datos de identidad. Este perfil activo se utiliza para supervisar la actividad de los activos y la correlación de eventos para evitar los falsos positivos o el aumento de la gravedad de un delito para los activos críticos del negocio.
2.8	La solución permite el descubrimiento automático de activos categorizándolos según su criticidad basada en los datos anteriormente recolectados (eventos, flujos y datos vulnerables), facilitando de este modo la administración de las reglas para las diferentes categorías.
2.9	Se puede clasificar los activos de la organización por medio de zonas, sistemas operativos, manejos de aplicativos, MAC o nombre de host.
2.10	La solución provee una aplicación, para poder acceder a la información almacenada dentro de las bases de datos, la cual permite la ejecución de sentencias para las consultas de datos de registro y flujos.
2.11	La solución integra sistemas como: RADIUS, TACACS (+), LDAP, Directorio Activo para propósitos de autenticación de los usuarios del sistema.
2.12	Tiene una administración centralizada, aun cuando la solución incluya múltiples componentes

2.13	La Solución ofrece una completa configuración y la gestión de todos los componentes. Esto incluye todas las configuraciones de los dispositivos, la configuración de la política y puesta a punto, gestión de eventos, informes, análisis, y otras funciones relevantes.
2.14	La solución incluye auditoría interna, incluyendo eventos de autenticación, uso y cambios de configuración realizados por los usuarios del sistema. La solución es capaz de detectar si los eventos han sido alterados o eliminados.
2.15	La solución demuestra sin lugar a dudas y a través de los mecanismos adecuados, capacidad de custodia e inalterabilidad de los registros de eventos, es decir, que se guarden de manera segura y confiable y puedan ser datos adecuados como evidencia en los casos de análisis forense.
3	**Funcionamiento**
3.1	La herramienta permite el monitoreo y análisis de cualquier solución de terceros que emita logs o syslog.
3.2	La solución puede monitorearse a sí misma e identificar posibles problemas con alguno de sus componentes. Para los incidentes más críticos, la solución puede enviar alertas por correo electrónico (SMTP) y mostrarlos en la consola de administración Web.
3.3	La solución permite la elaboración de informes, análisis forense y análisis de construcción de módulos de inteligencia de seguridad.

3.4	La solución permite: • Detección automática de las aplicaciones • Detección automática de las fuentes de registro • Auto – agrupación de los activos • El autoajuste • Auto – detección de amenazas • Filtrado de eventos • Seguridad de analítica avanzada • Priorización basado en activos • Seguridad de analítica avanzada • Priorización basado en activos • Actualización automática de amenazas, soporte de dispositivos y actualizaciones de software.
3.5	La solución actualiza automáticamente la configuración que se hace.
3.6	La solución es admisible con una interfaz gráfica online para gestionar y , analizar la información.
3.7	El acceso a la consola web es configurable para que utilice HTTPS con SSLv3 o TLSv1. Soporta certificados creados por una autoridad certificadora externa.
3.8	La solución es compatible con los requisitos de alta disponibilidad en una forma incrustada y sin la necesidad de software adicional de terceros.
3.9	La solución permite la recolección independiente de eventos mediante sensores en 8 Unidades de Negocio, mediante un sistema de almacenamiento mínimo de 1 TB.
3.10	La solución asegura continuidad del servicio, es decir que la arquitectura es distribuida esto nos asegura que siga funcionando cuando cualquier otra parte del sistema falla.

3.11	La solución permite un proceso de backup en cualquier solución de almacenamiento disponible.
3.12	La solución proporciona la capacidad de ofrecer múltiples paneles en el Dashboard que se pueden personalizar para satisfacer las necesidades específicas de los diferentes usuarios del sistema.
3.13	Widgets personalizables que la solución proporciona y muestra información de seguridad relevante para los usuarios del sistema.
3.14	Se crea una base de datos de todos los activos descubiertos en la red.

Tabla 6

4.4. Arquitectura

La solución debe ser software instalado en hardware ó Hardware Appliance. Posee mecanismos que le permiten soportar Sistemas Windows, Linux, AIX, z/OS, dispositivos de red e integrarse con otras soluciones de inteligencia de red y seguridad (Firewalls, IPS, Sistemas de Análisis de Vulnerabilidades, Sistemas Antivirus, y de prevención de fugas de información, Monitoreo de Bases de Datos, etc). Los usuarios pueden desarrollar sus propios espacios de trabajo con vistas personalizadas de los datos de seguridad (Dashboards). Además los usuarios pueden desarrollar reglas para casos de uso específicos para la gestión de amenazas, seguimiento de las políticas y el cumplimiento (reglas de correlación). La solución debe ser escalable para satisfacer la demanda adicional.

A continuación en la figura 4.1 el diagrama de implementación:

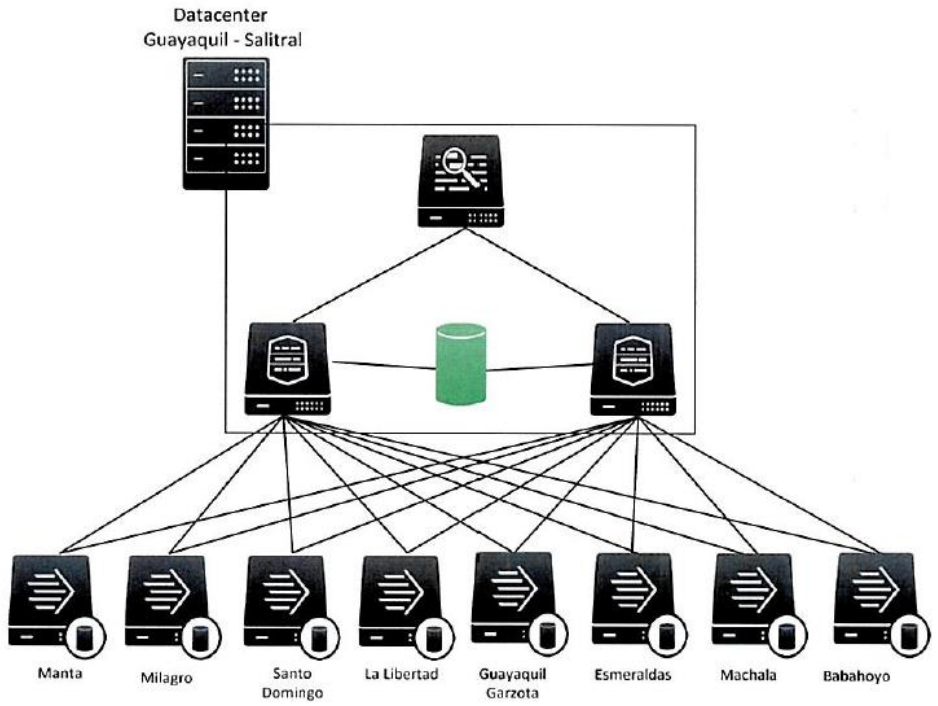

Figura 4.1

Componentes de la solución:

- Search Head / Deployment Server: La unidad principal de la solución. En este componente se realizan las configuraciones principales que serán desplegadas hacia los demás componentes y servirá de administrador general. Además es esta instancia la que manejará las consultas de búsquedas de los usuarios.
- Indexer: Una instancia de Splunk Enterprise que indexa los datos, transformando los datos originales en eventos y colocando los resultados en índices y generando “buckets”. También realiza búsquedas en respuesta a peticiones del “Search Head”.
- Storage: Componente de la solución donde serán almacenados los datos resultado de la indexación.
- Forwarder: Es una instancia de Splunk Enterprise que reenvía información a otra instancia de Splunk Enterprise o a una solución de terceros. Comúnmente conocida como el agente de Splunk [2]

4.5. Requerimientos

A continuación Se detalla los requerimientos mínimos que la solución debe tener.

4.5.1. Administración de Logs

Tiene una recolección de logs y la arquitectura de almacenamiento es compatible a corto plazo (en línea) y almacenamiento a largo plazo de eventos (offline).

- Es compatible con archivos de log en el almacenamiento de terceros.
- Proporciona capacidades para el almacenamiento mediante la compresión de los datos recogidos de una manera eficiente.
- Es compatible con la mayoría de los métodos de recopilación de registro de la industria (Syslog , OPSEC, WMI , RDEP, SDEE, JDBC , SNMP , calls MS-SQL, LEA Checkpoint , etc).
- Es configurable para mantener en línea los datos capturados, aplicando períodos de retención diferentes para distintos tipos de fuentes de datos. Como mínimo, debe ser capaz de manejar un período de retención de 1 año de los datos de las fuentes que el cliente considere críticas.
- Proporciona colección de registros de eventos con o sin agentes siempre que sea posible, en caso de pérdida de comunicación o fallos en la entrega de los datos, el componente/agente deberá almacenar los eventos bajo una cache de tamaño configurable, hasta que se restablezca la comunicación, realizando la transmisión de los eventos pendientes.
- Es capaz de archivar eventos tanto crudos como procesados o normalizados a un almacenamiento fuera de línea, (Cinta Magnética, DVDs, DLT, etc.) luego de mantenerlos disponibles en el sistema para aumentar su tiempo de retención. Estos eventos archivados serán re activables o reintegrables bajo demanda para poder realizar búsquedas, análisis y reportes desde la misma consola de administración regular.

4.5.2. Normalización y Clasificación de Eventos

Normaliza campos de eventos comunes (usuario, direcciones IP, nombres de hosts y dispositivos de origen de registro, etc) de los dispositivos dispares o de diferentes proveedores.

- Proporciona una taxonomía común de los acontecimientos.
- Proporciona la capacidad de almacenar logs, los normalizados y el formato original del registro de eventos con fines forenses.
- Ante cualquier incidente que se genere, tiene la capacidad de poder visualizar fácilmente los datos originales.
- Soporta de manera nativa el manejo de grandes cantidades de información (terabytes).

4.5.3. Filtrado y Análisis de Eventos

La solución proporciona análisis en tiempo real de los eventos (Interfaz de usuario, filtrado y correlación).

- Cuenta con un motor de correlación basado en reglas como componente básico, sin embargo y de ser requerido se puede agregar una funcionalidad para realizar correlación basada en riesgo.
- Permite crear reglas de correlación utilizando como plantilla las que ya trae el sistema por defecto.
- Realiza el cálculo estadístico de los eventos procesados para identificar posibles anomalías relacionadas con los volúmenes de datos procesados.
- Proporciona análisis de tendencias a largo plazo de los acontecimientos.
- Proporciona alertas sobre de los evento sospechosos y los cambios en la red y eventos de seguridad, así como evalúa diferentes criterios para la generación de alarmas.
- Utiliza mecanismos para identificar el origen de cualquier ataque con una granularidad que permita poder identificar hasta la ciudad o punto de origen de la comunicación.

- Apoya y mantiene un historial de la actividad de la autenticación de usuario en un repositorio, por activo.

4.5.4. Informes

La solución incluye informes por defecto: Autenticación, Identidad, Actividad de usuarios, Cumplimiento, Gestión de la configuración de cambios, informes ejecutivos, informes específicos de dispositivo (aplicación, sistema operativo, bases de datos, etc.), gestión de red, Seguridad, etc.

- Proporciona información de los elementos disponibles para la gestión a través de la interfaz gráfica de usuario.
- Proporciona motor de informes que se puede configurar para la elaboración de informes personalizados.
- Es compatible con la capacidad de programar informes.
- La solución incluye informes por defecto de cumplimientos de regulaciones como PCI, SOX, HIPAA, FISMA, NIST, NERC, GLBA, ISO 27000 y marcos de control (CoBIT, ISO).
- Proporciona un Dashboard para la visualización rápida de la seguridad y la información de la red.
- Es compatible con la distribución automática de informes, y los formatos soportados son: HTML, PDF, XML, CSV / XLS, RTF.
- Es compatible con la capacidad de proporcionar informes de tendencias históricas [3].

4.5.5. Alertas

La solución proporciona alertas con base a las amenazas de seguridad observados en los dispositivos monitoreados.

- Proporciona alertas de los incidentes sospechosos y los cambios de en la red (flujo) de datos.
- Proporciona alertas en base a la política establecida. (por ejemplo, no se permite el tráfico de IM).

- Es compatible con alertas ponderados para tener en cuenta las prioridades.
- Proporciona la habilidad de mostrar alertas con protocolos y mecanismos a otras soluciones de gestión.
- Proporcionar asistencia y capacidades basadas en la interfaz de usuario para minimizar los falsos positivos y entregar resultados precisos.
- Es compatible con la capacidad de tomar medidas después de recibir una alerta. Por ejemplo, la solución apoya la capacidad de iniciar una secuencia de comandos, ejecutar un script o enviar un mensaje de correo electrónico. (Crear un registro del delito en el sistema de gestión de incidentes, encender una captura SNMP, Enviar un mensaje Syslog, Respuesta IF- MAP).
- Cuando las condiciones especificadas de una alerta se cumplen y se envía un correo electrónico, la solución es capaz de adjuntar los eventos/resultados/condiciones que generaron la alerta en formato PDF y/o CSV en el cuerpo del correo.
- La solución emplea una serie de amenazas y fuentes de seguridad para proporcionar el contexto de seguridad y el contexto geográfico. Este está integrado en todos los puntos de vista y capacidades dentro del producto. Deberá incluir fuentes por defecto y no limitar el ingreso de nuevas; como por ejemplo: Geográfica, Principales puertos focalizados, Botnets : amenazas emergentes, Bogon IPs, Nets hostiles, Smurfs.
- Vigila y alerta cuando hay una interrupción en la recopilación de registros de un dispositivo específico. En otras palabras, si los registros no son vistos desde un servidor en 5 minutos, a continuación, generar una alerta [4].

4.5.6. Monitoreo de Actividad de Red

La solución muestra perfiles de tráfico en términos de bytes, carga de paquetes y número de hosts que se comunican.

Estas pantallas deben estar disponibles para las aplicaciones, puertos, protocolos. Las amenazas y cada punto de control en la red, y puntos de vista que deben apoyar ubicación de red de manera que puedan presentar la información desde una única ubicación, toda la red o cualquier otro conjunto definido de dispositivos.

- Es compatible con la definición de aplicación más allá del protocolo y el puerto. El sistema es compatible con la identificación de las aplicaciones que utilizan puertos que no sean el conocido y aplicaciones túneles mismos en otros puertos (por ejemplo , HTTP como transporte para Messenger MS- debe ser detectada como mensajería instantánea - no HTTP).
- Detecta eventos de día cero.
- Aprende dinámicamente las normas de comportamiento y exponer los cambios que se produzcan.
- Detecta ataques de denegación de servicio y ataques de denegación de servicio distribuido (DDoS) (DoS).
- Detecta y presenta puntos de vista de tráfico, relativos a las amenazas observadas en la red.
- Identifica el tráfico de red de las aplicaciones potencialmente peligrosas (por ejemplo, uso compartido de archivos peer-to -peer, etc.).
- Perfila y presenta la información en varios marcos de tiempo. Perfiles están disponibles para la semana, día y hora.
- Es capaz de perfilar la comunicación procedente de, o con destino a la Internet por regiones geográficas en tiempo real.
- Crea perfiles claramente independientes y diferenciados de tráfico local vs de origen o destino en el Internet.
- Permite a los usuarios crear perfiles y vistas personalizadas usando cualquier propiedad de un flujo, registro, fuente de datos o tráfico.

- Es compatible con el perfil de tráfico basado en direcciones IP, grupos de direcciones IP, los pares IP de origen / destino , etc.
- Es compatible con la recopilación y el análisis de los datos de captura de paquetes.
- Proporciona la capacidad de extraer campos específicos, definidos por el usuario, a partir de los datos de captura de paquetes y el uso de los campos en las reglas de correlación.
- Identifica el tráfico de red dentro de un entorno de red virtual.

4.5.7. Gestión de Amenazas avanzadas

La solución ofrece la posibilidad de enlazar contextualmente actividad de la red con los eventos de seguridad de los dispositivos monitorizados.

- Ofrece la posibilidad de enlazar contextualmente los eventos de seguridad reportados en tiempo real, de los activos que están en la mira.
- Proporciona la capacidad de ponderar de forma automática la gravedad de los sucesos de seguridad notificados de acuerdo a la vulnerabilidad de los activos seleccionados.
- Ofrece la posibilidad de asignar calificaciones de credibilidad a los dispositivos de seguridad controlados.
- Proporciona una visión de eventos en tiempo real de la información de seguimiento en formato RAW / original y procesada / normalizada.
- Es capaz de cambiar automáticamente los coeficientes de credibilidad de los dispositivos de seguridad en respuesta a los ataques de toda la red.

4.5.8. Integración con Infraestructura critica

La solución deberá integrarse a través de todas las zonas y ambientes de producción que conforman la Infraestructura Crítica de la Corporación: Tecnologías de Información (TI), Sistemas SCADA, Sistemas de Control Industrial (ICS).

- Posee capacidades de defensa en cuanto a soportar el descubrimiento, prevención, detección, auditoría de amenazas que

puedan amenazar a los endpoints, redes y data que conforman los sistemas de control SCADA.

- Posee Soporte Nativo para el monitoreo de aplicaciones y protocolos SCADA, así como la gestión y correlación de logs y eventos de dispositivos y sistemas SCADA que lo permitan.
- Permite la integración mediante API´s a otras soluciones.
- Posee capacidades de análisis y reportería forense para la investigación de causas y realización de auditorías sobre Sistemas de Control Industrial ICS.

4.6. Desarrollo

En este apartado se observa los detalles de la instalación de la solución

4.6.1. Instalación y Configuración

Configuraciones Base

Configuraciones de Linux

Cambio de nombre de hostname

Para realizar el cambio del nombre del equipo se debe realizar el cambio en el siguiente archivo: /etc/hostname.

Para realizar el cambio se utilizó el comando vi. Quedaría de la siguiente manera: vi /etc/hostname

Dentro del archivo editar el nombre del servidor.

Cambio de Tarjeta de Red

Ejecutar el comando: nmtui como se observa en la Figura 4.2

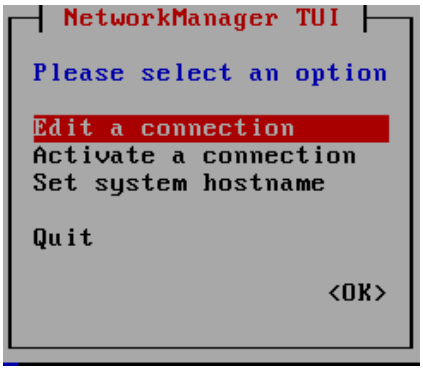

Figura 4.2

Instalación y configuración de NTP.

Para mantener la sincronización del tiempo entre los distintos servicios de Splunk se debe utilizar la herramienta NTP. Ejecutar las siguientes líneas para la instalación de NTP como se puede observar en la Figura 4.3.

- yum install epel-release
- yum -y install ntp
- systemctl start ntpd
- systemctl enable ntpd
- systemctl status ntpd

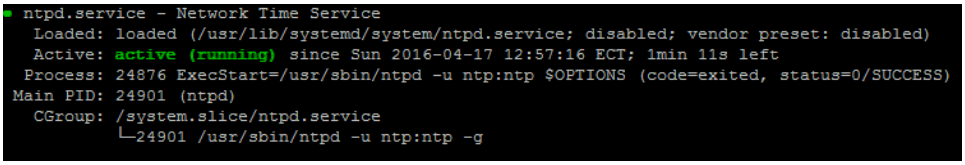

Figura 4.3

Adicional se requiere la configuración del servicio CHRONYD para el funcionamiento del NTP

Ejecutar los siguientes comandos:

- yum -y install chronyd
- systemctl start chronyd
- systemctl enable chronyd
- systemctl enable chronyd
- cd /etc/
- Agregar la siguiente línea en el archivo: vi /etc/chrony.conf -server 172.30.1.79 iburst

Ejecutar los siguientes comandos:

- chronyc sources
- systemctl restart chronyd
- systemctl restart ntpd

Instalación Splunk Search Head

Para instalar Splunk Enterprise se debe ser usuario root y ejecutar:

- Descargar el archivo splunk-6.3.3-f44afce176d0-Linux-x86_64.tgz en el servidor
- Ejecutar: tar xvzf splunk-6.3.3-f44afce176d0-Linux-x86_64.tgz –C /opt
- Una vez descomprimido el archivo ir a la ruta: /opt/splunk/bin
- Ejecutar el comando para el inicio automático ./splunk enable boot-start root
- Para iniciar Splunk ejecutar: ./splunk start
- Aceptar la licencia

Configuración Splunk Search Head

Instalación de Licencia

El archivo .license que se recibió por correo debe ser instalado en el servidor principal de Splunk y se siguein los pases que se detallan mas adelante y como se muestra en la Figura 4.4 y 4.5.

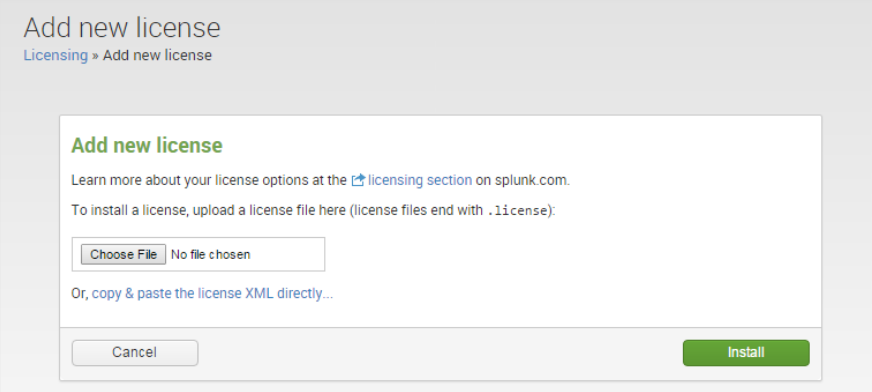

Figura 4.4

- Ir a Settings > Licensing
- Seleccionar add licence
- Seleccionar con el botón browser y escoger el archivo de licencia

- Seleccionar Install
- Se deberá reiniciar el servicio de Splunk
- Luego reingresar a la configuración de licencia
- Seleccionar change to slave
- Seleccionar Designate this Splunk instance, SALVSERV-SIEM1, as the master license server
- Save

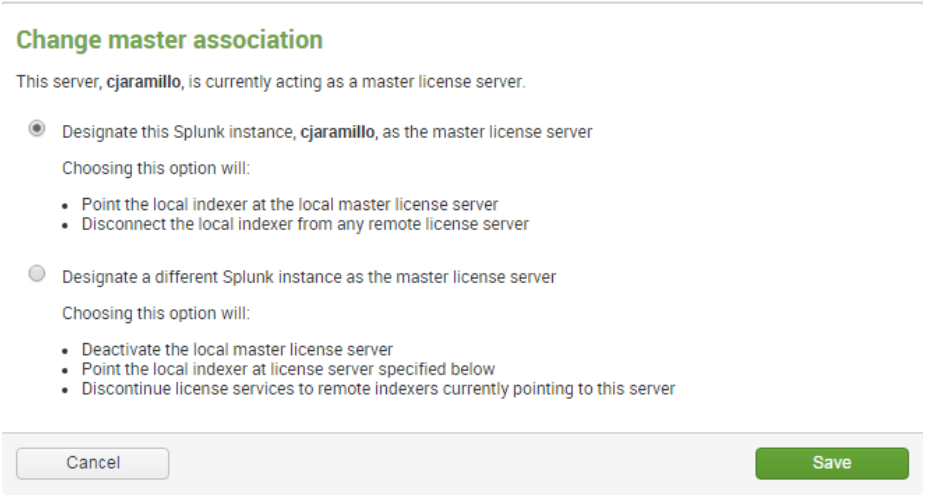

Figura 4.5

Configuración de los Search Peers

(Para realizar este procedimiento primero deben estar instalados los indexers), ventana de interfaz gráfica se detalla en Figura 4.6.

- Ir a Settings > Distributed Search
- Seleccionar Add New Search Peers
- Escribir las IPs de los indexers uno a la vez:
  - 1xx.xx.xx.xx
  - 1xx.xx.xx.xx

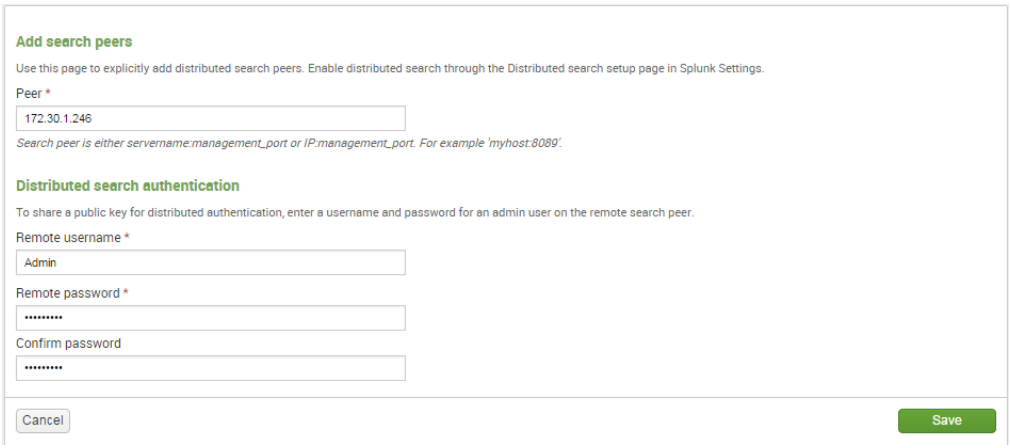

Figura 4.6

- La configuración debe quedar como se muestra en la Figura 4.7.

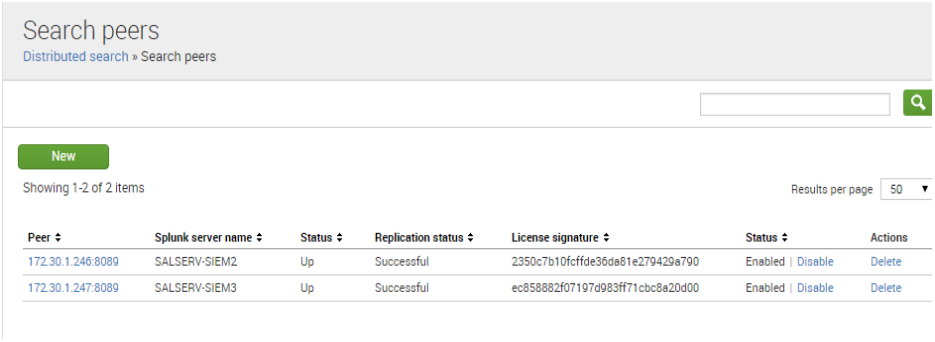

Figura 4.7

Configuración de Nombre de la Instancia de Splunk y Puertos Web

Esto se muestra en la Figura 4.8

- Ir a Settings > General Settings
- Poner el Nombre de la instancia (SALSERV-SIEM1)
- Enable SSL: YES
- Web Port : xxxx

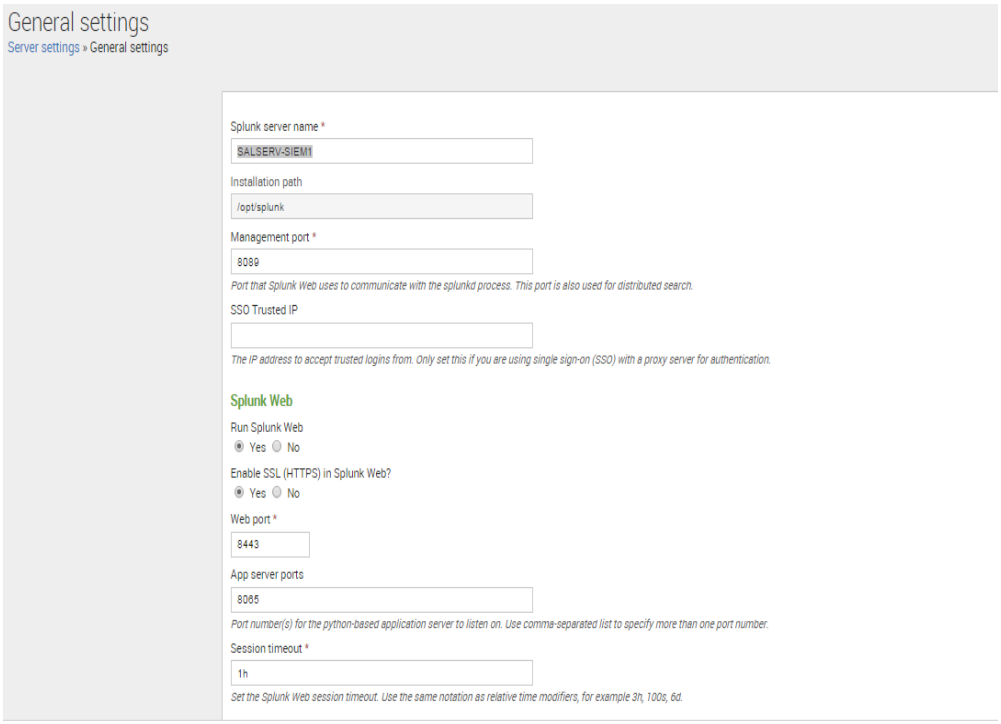

Figura 4.8

Instalación Splunk Indexers

Para instalar Splunk Enterprise se debe ser usuario root y ejecutar:

- Descargar el archivo splunk-6.3.3-f44afce176d0-Linux-x86_64.tgz en el servidor
- Ejecutar: tar xvzf splunk-6.3.3-f44afce176d0-Linux-x86_64.tgz –C /opt
- Una vez descomprimido el archivo ir a la ruta: /opt/splunk/bin
- Ejecutar el comando para el inicio automático ./splunk enable boot-start root
- Para iniciar Splunk ejecutar: ./splunk start
- Aceptar la licencia

Configuración Splunk Indexers

Ejecutar el siguiente comando para que las instancias de Splunk sean configurables desde el Search Head, en la ruta /opt/splunk/bin

- ./splunk set deploy-poll 1xx.xx.xx.xx:xxxx

Ejecutar el siguiente comando para que los Indexadores de Splunk puedan recibir los datos de los agentes, en la ruta /opt/splunk/bin

- ./splunk enable listen xxxx

Configuración de licencia en Indexers

La licencia es administrada por el Search Head, se debe realizar los siguientes pasos para configurar los indexers como dependientes:

- Ingresar via web al indexador (1xx.xx.xx.xx:xxxx / 1xx.xx.xx.xx:xxxx)
- Ir a Settings > licensig
- Seleccionar change to slave
- Seleccionar la segunda opción
- Escribir la URL del servidor central de la licencia

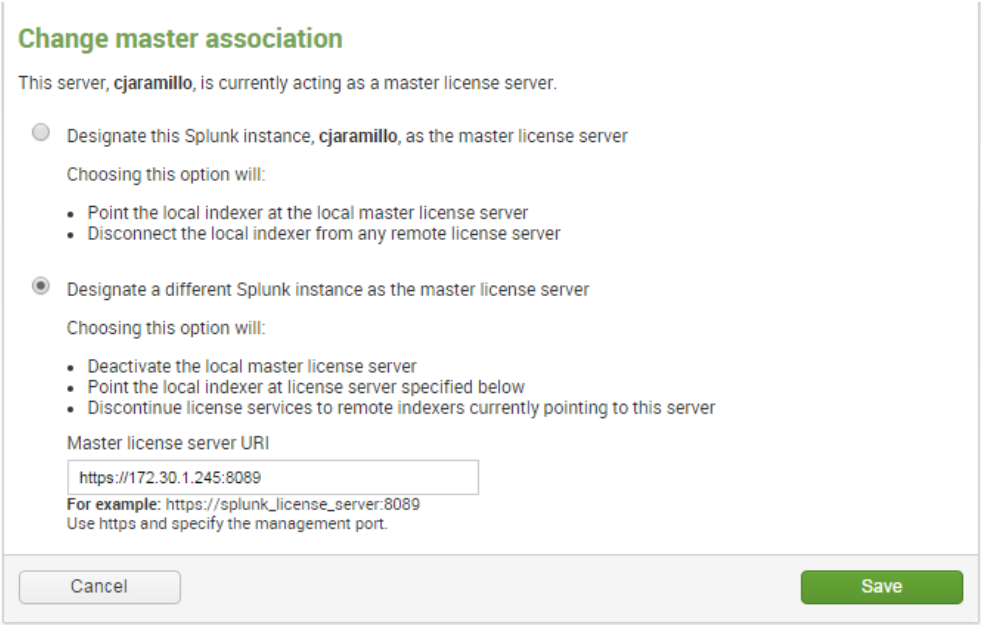

Figura 4.9

En el Anexo 2 se observa el detalle de la configuración global que se realizó a toda la solución.

CAPÍTULO 5

5. PRUEBAS Y ANÁLISIS DE RESULTADOS

En este último capítulo se observa las pruebas y análisis que se realizaron una vez implementada la solución.

5.1. Pruebas realizadas

Una vez efectuada la instalación de la infraestructura necesaria para el funcionamiento de la solución, se procede con la certificación de los casos de uso, los mismos que serán probados con un guion de pruebas, que nos permitirá seguir la ejecución del procedimiento de los casos y llegar a una aceptación consensuada del presente documento.

Se identificó los requerimientos de CNEL EP y se probaron los siguientes casos de uso:

- UC-01 Acceso a la consola principal de Splunk
- UC-02 Búsqueda y filtrado de información
- UC-03 Gestión de Dashboards
- UC-04 Creación y configuración de alertas
- UC-05 Categorización de activos
- UC-06 Utilizar y verificar el sistema de monitoreo propio Splunk On Splunk (SOS)
- UC-07 Utilización de indicadores y análisis de datos
- UC-08 Gestión de la base de conocimientos de amenazas
- UC-09 Correlacionar eventos
- UC-10 Análisis de incidentes
- UC-11 Captura de información
- UC-12 Generación de reportes

A continuación se detallan los planes de prueba para los casos de uso.

- Caso de uso 01 - Acceso a la consola principal de Splunk como se obseva en la Tabla 7 y Tabla 8.

Objetivo	Acceso a la consola principal de Splunk
Actor(es)	Usuario de Seguridad
Descripción	Que un usuario que se encuentre en el Grupo Splunk en Active Directory pueda ingresar a la herramienta. El usuario podrá utilizar la consola principal mediante un navegador web después de hacer el ingreso al sistema y accederá a reportes y Dashboards según su nivel de autorización.
Frecuencia	Cada vez que un usuario quiera hacer uso de la herramienta
Pre-procesamiento	El usuario debe existir en el grupo de seguridad
Post-procesamiento	El usuario podrá hacer uso de la herramienta
Caso(s) de uso incluido(s)	No
Caso(s) de uso extendido(s)	No

Tabla 7

Escenario: Acceso a la consola principal de Splunk, utilizando un usuario del dominio de CNEL	
Pasos	**Resultado esperado**
1. Digitar en el buscador de Windows el URL: https://172.30.1.245:8443	Se despliega la siguiente la pantalla de bienvenida de Splunk:
2. Digitar el usuario y la contraseña del dominio	Se ingresa a la pantalla de Splunk con los accesos

	definidos de acuerdo al rol del usuario.
Observaciones:	
• En caso de error en el paso 1: Verificar con el administrador del dominio que los usuarios que realizan la prueba estén el grupo de seguridad especificado para el uso de Splunk. • En caso de error en el paso 2: Si el usuario no tiene acceso a Enterprise Security o no tiene acceso a búsquedas, verificar los roles asignados.	

Tabla 8

- Caso de uso 02 - Búsqueda y filtrado de información como se observa en la Tabla 9 y Tabla 10.

Objetivo	Búsqueda y filtrado de información
Actor(es)	Usuario de Seguridad
Descripción	Acceder a la ventana principal de búsqueda y visualizar la información recopilada de los distintos sistemas y verificar, según el contenido, que detecte IPs e información relevante de forma que facilite la búsqueda por campos.
Frecuencia	Cada vez que los usuarios quieran hacer filtrados de información, búsquedas por rangos de fechas, búsquedas en tiempo real y verificar el ingreso de información de una nueva fuente de datos
Pre-procesamiento	
Post-procesamiento	No

Caso(s) de uso incluido(s)	No
Caso(s) de uso extendido(s)	No

Tabla 9

Escenario: Realizar búsqueda y filtrado de Información utilizando Splunk	
Pasos	**Resultado esperado**
1. Ir al app (modulo) de Search & Reporting (búsquedas y reportes).	Debe aparecer la pantalla principal del módulo de búsquedas. Dentro de la misma una caja de texto para realizar consultas.
2. Seleccionar rango de tiempo de una hora	Por defecto se ha configurado la herramienta que el tiempo de búsqueda sea por 15 minutos. Se puede seleccionar al extremo derecho una de las distintas opciones de tiempo. Para esta prueba seleccione una hora (last 60 minutes)
3. Dentro de la caja de búsqueda escribir la palabra error	La ejecución de esta búsqueda demorara un poco por el gran volumen de información que se tiene en la herramienta. Como resultado de la búsqueda se tendrán todos los eventos que contengan la

	palabra Error de los últimos 60 minutos. De lado izquiersdo se observaran los servidores (host), fuentes (sources), formato (sourcetype) y todos los campos que han extraído. Además debajo de la línea de comando de búsqueda aparecerá el timeline de los eventos.
4. Filtrar la información por tipo error. Escoger solo los elementos que sean de tipo error seleccionando de la lista de campos type = Error.	Automáticamente el comando type = Error se agregara a la búsqueda y se ejecutara nuevamente la búsqueda. Esta vez los resultados serán del tipo error.
5. Filtre la búsqueda por el servidor que contenga la mayor cantidad de eventos tipo error. (En los host seleccione el primero de la lista)	Automáticamente se agregará el servidor a la búsqueda. Nótese que mientras más específica es la búsqueda, más rápido se obtienen resultados.
Observaciones:	
• Nótese que el tiempo de respuesta de esta prueba podrán verse afectado si la red esta cogestionada. • En el paso 4 podría no haber un campo tipo error (type = error) si en los últimos 60 minutos ninguna fuente de datos generó un error. En caso de que este escenario suceda se puede cambiar el rango de tiempo, intentar esta prueba más luego, o usar oro tipo de evento	

Tabla 10

- Caso de uso 03 - Gestión de Dashboards, como se observa en la Tabla 11 y Tabla 12.

Objetivo	Gestión de Dashboards
Actor(es)	Usuario de Seguridad
Descripción	Los usuarios según su nivel de autorización podrán crear nuevos dashboards o graficas basadas en la información que la herramienta ha recopilado. Además se podrán configurar y visualizar los dashboards que vienen por defecto con el módulo SIEM
Frecuencia	Cuando se requiera visualización gráfica de la información de seguridad
Pre-procesamiento	Debe existir información recopilada para generar las gráficas. El usuario debe tener permisos para acceder.
Post-procesamiento	No
Caso(s) de uso incluido(s)	No
Caso(s) de uso extendido(s)	No

Tabla 11

Escenario: Creación y modificación de Dashboard	
Pasos	**Resultado esperado**
1. Hacer una búsqueda desde el modulo app Search & Report que contenga la búsqueda Type=Error con un rango de tiempo de 15 minutos	Se verán todos los eventos tipo error. Y del lado izquierdo de los eventos se verán los campos
2. En la lista de campos seleccionar host y en la opciones que aparecen seleccionar top values	Automáticamente se generará una gráfica explicativa de cuantos eventos tipo error

	existen por cada servidor en la pestaña de visualización. En la pestaña de estadísticas generará un reporte con información similar pero en formato de texto
3. En la pestaña de visualización seleccionar el grafico tipo pie, en el menú dropdown.	La información se presentará en tipo pastel
4. Para guardar la gráfica panel en la parte derecha escoger save as dashboard Luego: Seleccionar existing, Seleccionar Casos de prueba. En Panel Title escribir el nombre del usuario_dashboard Seleccionar Save Dar click en view dashboard	Se podrá ver la gráfica guardada en un dashboard donde se podrá gestionar
5. Editar el dashborad y la gráfica: En el botón edit, seleccionar edit panel, luego seleccionar add input, Seleccionar time, Dar clic en el lápiz encima del gráfico que se añadió, En las opciones de time que el default sea 15 minutos, Dar clic en apply, En el gráfico de pastel hacer clic en la lupa, Seleccionar edit search string	Se espera poder crear un input para que las gráficas del dashborad puedan hacer consultas dependiendo del rango del tiempo.

En la parte time range scope seleccionar shared time picker.	
6. En el botón edit, seleccionar edit source, En la parte xml donde se abre <title>, poner Nombre y Apellido del usuario	Se podrá hacer modificación directa al XML de los dashboards. Se podrá ver el nombre y apellido como nombre de la grafica
Observaciones:	
• Nótese que el tiempo de respuesta de esta prueba podrán verse afectado si la red esta cogestionada. • En el paso 1 podría no haber un campo tipo error (type = error) si en los últimos 15 minutos ninguna fuente de datos generó un error. En caso de que este escenario suceda se puede cambiar el rango de tiempo, intentar esta prueba más luego, o usar oro tipo de evento.	

Tabla 12

- Caso de uso 04 - Creación y configuración de alertas, como se observa en la Tabla 13 y Tabla 14.

Objetivo	Creación y configuración de alertas
Actor(es)	Usuario de Seguridad
Descripción	Los usuarios según su nivel de autorización podrán crear y configurar alarmas basadas en las políticas establecidas, amenazas y vulnerabilidades. En caso de requerirse la alerta deberá enviar un correo electrónico

	con información correspondiente a la alerta, ejecutar un script o alertar por consola. Deberán aplicarse controles para evitar el “overflow” de alarmas por un mismo evento
Frecuencia	Cuando se requiera la creación o actualización de una alarma
Pre-procesamiento	No
Post-procesamiento	No
Caso(s) de uso incluido(s)	No

Tabla 13

Escenario: Creación y configuración de alert basado en un error	
Pasos	**Resultado esperado**
1. Hacer una búsqueda desde el modulo app Search & Report que contenga la búsqueda index=kaspersky Type=Error con un rango de tiempo de 15 minutos	La búsqueda retornará con los resultados de errores en el index indicado. Nótese que esta búsqueda retorna varios resultados.
2. Seleccionar Save As / Alert Escoger como titulo: TEST ALERTA Permisos: Privada Permission: Real Time Trigger alert when: Per-result Throttle: Activado Suppress results containing field value: Type Suppress triggering for: 1 Hour Trigger Actions: Add to trigger events	Se creara la Alerta que estará constantemente monitoreando. A pesar de que existan muchas coincidencias solo generara una alerta por cada hora.

3. Ir al administrado de Alertas: En la barra verde superior seleccionar Alert. Seleccionar la alerta creada	Se deberá ver cuántas veces se ha ejecutado la alerta por el evento creado
Observaciones:	
El resultado de la prueba puede verse afectado según los eventos que lleguen al momento de realizar la misma.	

Tabla 14

- Caso de uso 05 - Categorización de Información, como se observa en la Tabla 15 y Tabla 16.

Objetivo	Categorización de Información
Actor(es)	Usuario de Seguridad
Descripción	Se podrá categorizar los datos para indicar el nivel de criticidad del equipo al que pertenecen. Así mismo la información se podrá ordenar y categorizar por otros parámetros
Frecuencia	Cada vez que se ingrese un nuevo tipo de información o nueva fuente de datos
Pre-procesamiento	No
Post-procesamiento	No
Caso(s) de uso incluido(s)	No

Tabla 15

Escenario: Categorización de Activos	
Pasos	**Resultado esperado**
1. Ir al módulo de Enterprise Security seleccionando la pestaña superior izquierda junto al logo de Splunk Seleccionar Configure Seleccione Data Enrichment Seleccionar Assets	Se verá la lista de los activos que se han registrado en la herramienta. En esta pantala se parametriza por varios campos la información incluyendo la criticidad, ubicación, etc. No modificar.
Escenario: Categorización o Agrupación de información según distintas fuentes	
Pasos	**Resultado esperado**
2. Settings Eventtype Seleccionar New Destination App: Search Name: test_eventtype Search string: host=GLRSRV-KAV OR host=SUCNLOS002-E OR host=LRSSRV-AV01 Dejar vacio Tags Priority: 1 Default Ir hacia la ventana de busqueda y escrbir: eventtype= test_eventtype	Esta forma de categorización permite que con comando de búsqueda más sencillos se ubique rápidamente las fuentes de información o activos necesarios. Nótese que en el resultado de la búsqueda solo aparecen los activos incluidos dentros del eventtype.
Observaciones:	

Tabla 16

- Caso de uso 06 - Utilizar y verificar el sistema de monitoreo propio Splunk On Splunk (DMC), como se observa en la Tabla 17 y Tabla 18.

Objetivo	Utilizar y verificar el sistema de monitoreo propio (DMC)
Actor(es)	Usuario de Seguridad
Descripción	El usuario accederá a la consola de DMC para verificar el correcto funcionamiento de la solución. En caso de alguna anomalía o desconexión de algunos de los componentes, se alertará sobre la situación
Frecuencia	Cada vez que se necesite verificar la situación de funcionamiento de la solución
Pre-procesamiento	No
Post-procesamiento	No
Caso(s) de uso incluido(s)	No

Tabla 17

Escenario: Utilizar y verificar el sistema de monitoreo propio (DMC)	
Pasos	**Resultado esperado**
1. En settings seleccionar Distributed Management Console. Secciónar Overview	Se podrá ver el estado general de los servidores principales de la solución Splunk. En la parte inferior se encuentra la lista de alertas activadas en caso de que se encuentre alguna anomalia
2. En Alerts en la parte inferior seleccionar enable o disable.	Se observara la lista de todas las alarmas activadas.
3. En la primera alarma seleccione edit	Se procederá a ver una nueva pestaa con la página de

	configuración de esta alarma. No haga ningún cambio
4. Presione Cancel y regrese a la pestaña original Presione Cancel Nuevamente En la barra superior verde seleccione Forwarders Luego Forwarders Deployment	Se observará el estado general de los agentes que envían información a los servidores centrales
Observaciones:	
En la pantalla de forwarders se vera todos los forwarders incluidos los de los endpoints. Es normal que algunos de reporten como “missing”	

Tabla 18

- Caso de uso 07 - Utilización de indicadores y análisis de datos, como se observa en la Tabla 19 y Tabla 20.

Objetivo	Utilización de indicadores y análisis de datos
Actor(es)	Usuario de Seguridad
Descripción	En combinación con dashboards de seguridad y la herramienta de búsqueda, realizar investigaciones y análisis de datos, basando en la información original de los dispositivos que se están monitoreando
Frecuencia	Cada vez que se requiera una investigación más profunda de los datos visualizados en los dashboards
Pre-procesamiento	No
Post-procesamiento	No
Caso(s) de uso incluido(s)	No

Tabla 19

Escenario: Utilización de indicadores y análisis de datos de Enterprise Security.	
Pasos	**Resultado esperado**
1. Ingresar al módulo de Enterpise Security. Utilizando el menú dropdown en la parte superior izquierda junto al logo de Splunk. En caso de encontrarse en la pantalla de inicio, utilizar el menú de apps que se encuentra al lado izquierdo	Se ingresa a la pantalla de bienvenida de Enterpise Security
2. Seleccionar Security Posture en la barra de opciones de Entrepsie security en la parte superior con fondo negro.	Se presentará en la parte superior de la pantalla todos los indicadores de riesgo configurados. Estos números se denominan eventos notables. En los cuadros intermedios se presentara un resumen de los eventos tanto por criticidad de la amenaza y otro por tipo de fuente. En la parte inferior se tiene los tipos de ataques más frecuentes y los activos que tienen mayor cantidad de eventos.
3. En el cuadro Top Notable Events, seleccionar Brute Force Access Behavior Detected	Se muestra la pantalla Incident Review. En esta pantalla se detalla cada uno

	de los eventos de “Brute Force Access Behavior Detected”
4. En la lista que se encuentra en el cuadro inferior, seleccionar un evento y expandirlo utilizando la flecha del lado izquierdo	Se expande la lista dando todos los detalles del evento.
5. Del lado derecho en los detalles del evento seleccionar la opción Contributing events	Se abrirá una ventana nueva donde se realizará una búsqueda utilizando los comandos de búsqueda propios de Splunk. Y tendrán como resultados los logs originales que originaron la información.
6. Regresar a la primera pantalla y en el detalle del evento buscar Source y el nombre del Activo. Del lado derecho del nombre hacer clic en la flecha de Action. En el menú que se despliega utilizar Asset investigator	En esta pantalla se visualizará toda la información de las actividades detectadas del activo
7. Seleccionar alguno de los cuadros de colores (cuadro de tiempo) de la gráfica central.	Del lado izquierdo se despliega un resumen de detalles del cuadro de tiempo seleccionado
Observaciones:	
Tener en cuenta que dependiendo del volumen de información y el estado de la red algunas opciones pueden tomar tiempo en mostrar resultados. En el paso numero 3 puede que no haya la opción Brute Force Access Behavior Detected, se puede seleccionar cualquier otro evento notable y seguir el miso procedimiento	

Tabla 20

- Caso de uso 08 - Gestión de la base de conocimientos de amenazas, como se observa en la Tabla 21 y Tabla 22.

Objetivo	Gestión de la base de conocimientos de amenazas
Actor(es)	Usuario de Seguridad
Descripción	Que los usuarios actualicen la base de conocimiento de amenazas de la herramienta para que esté al día. La información de las bases de conocimiento puede ser configurada tanto para que tome información de terceros o ingresada de forma manual
Frecuencia	Cada vez que se requiera actualizar la base de conocimientos de amenazas
Pre-procesamiento	No
Post-procesamiento	No
Caso(s) de uso incluido(s)	No

Tabla 21

Escenario: Gestión de la base de conocimientos de amenazas. Agregar una fuente de información	
Pasos	**Resultado esperado**
1. En el módulo de Enterprise Security. Ir a Configure, seleccionar Data Enrichment y luego Threat Intelligence Downloads	Se accederá a la consola principal de administración de las fuentes de información de amenazas de Splunk Enterprise Security

2. Hacer clic en New, Completar los siguientes datos: Name: hijacked_ip_addresses_test Type: hijacks Description: Lista de IPs hijacked URL: http://list.iblocklist.com/?list=tbnuqfclfkemqivekikv Delimiting regular expression: : (dos puntos) Fields: description:$1,ip:$2 Ignoring regular expression: (^#\|^\s*$) Los demás valores dejarlos en blanco o con valor de defecto Regresar a Enterprise Security. Ir a Audit en la barra principal, luego Threat List Audit Confirme que hijacked_ip_addresses_test ha sido descargado	La nueva lista de información de amenazas ha sido agregada y está siendo utilizada.
Observaciones:	
Puede que la lista configurada en el paso 2 tome unos minutos en descargar.	

Tabla 22

- Caso de uso 09 - Correlacionar eventos, como se observa en la Tabla 23 y Tabla 24.

Objetivo	Correlacionar eventos
Actor(es)	Usuario de Seguridad
Descripción	Que el usuario pueda a partir de la información recopilada, correlacionar distintos eventos basados en parámetros comunes entre las distintas fuentes de datos dentro de distintos rango se tiempo.

Frecuencia	Cada vez que se necesite correlacionar dos o más eventos
Pre-procesamiento	No
Post-procesamiento	No
Caso(s) de uso incluido(s)	No

Tabla 23

Escenario: Investigar búsqueda correlacionada de Enterprise Security	
Pasos	**Resultado esperado**
1. En el moduloSplunk Enterprise Security, seleccionar configure en la barra principal, luego seleccione content management. En el menú de esta opción filtrar por type:correlation search Seleccione una de las búsquedas que aparece en la lista. No realice ningún cambio.	Se verá la lista de búsquedas correlacionadas que incluye Splunk Enterprise por defecto y puede tomarse de ejemplo para crear nuevas búsquedas. Las búsquedas que incluye Splunk Enterprise por defecto son complejas, pero el usuario administrador de seguridad puede crear las que considere necesarias sin importar el nivel complejidad.
2. Copiar la búsqueda y ejecutarla en la opción de búsqueda que incluye Splunk Enterprise Security	Se podrá demostrar que la estrucutura de las búsquedas es correcta. Sin embargo si no hay eventos que coincidan la busqueda puede retornar cero.
Escenario: Crear búsqueda correlacionada utilizando un modelo de datos de Enterprise Security	

Pasos	Resultado esperado
1. En el moduloSplunk Enterprise Security, seleccionar configure en la barra principal, luego seleccione content management. Seleccione New Content Seleccione Correlation Search Complete los siguientes valores: Search name: SSH login detected Application Context: DA-ESS-AccessProtection Search Description: SSH login detected	Se ingresara a la ventana de creación de búsquedas correlacionadas, y se editaran los datos de cabecera de la búsqueda
2. Clic en Edit search in guided mode, clic en next Paso 1 Souce: data Model Select Data: Authentication Object: Successful_Authentication. Clic next. Preset time range : Last 15 minutes. Paso 2 Dejar filtro en blanco Clic next Paso 3 No agregar nada Clic next Paso 4 Attribute: Authentication.app, Operation :Equal	Esta es la creación de una busqueda basada en el modelo de datos Athentication. Se busca las autenticaciones exitosas utilizando sshd. La búsqueda puede que no retorne resultados

Value : “sshd” (case sensitive e incluye las comillas). Paso 5 clic en Run search	
3. Regresar a la ventana Original y hacer clic en Save Cron Schedule: */5 * * * * (cada cinco minutos) Habilitar create notable event Title: conexión exitosa SSH en host $host$ Description: Existe una conexión SSH en host $host$ Severity: High Default Status and Owner: defaults Drill-down name: Ver eventos SSH en $host$ Drill-down search: host=$host$1*sshd*	En estas opciones se crea las condiciones para que por cada conexión SSH detectada en la búsqueda creada previamente, cree eventos notables.
4. Clic en Cancel	
Observaciones:	
No se guarda la búsqueda correlacionada creada, para poder realizar el ejercicio varias veces. Una vez creada la búsqueda no se puede eliminar, solo se deshabilita.	

Tabla 24

- Caso de uso 10 - Análisis de incidentes, como se observa en la Tabla 25 y Tabla 26.

Objetivo	Análisis de incidentes
Actor(es)	Usuario de Seguridad
Descripción	Que el usuario pueda crear un ticket a partir de un incidente, amenaza o vulnerabilidad y hacer seguimiento a través del flujo de trabajo de Splunk
Frecuencia	Cuando se genere un incidente de seguridad que necesite ser investigado a profundidad
Pre-procesamiento	No
Post-procesamiento	No
Caso(s) de uso incluido(s)	No

Tabla 25

Escenario: Análisis de incidentes. Creación de Investigaciones	
Pasos	**Resultado esperado**
1. Dentro de Splunk Enterprise Security ir a Security Posture Seleccionar el evento notable que tenga el mayor conteo En la ventana de incident review, seleccionar un evento. Luego hacer clic en Add Selected to Investigation Hacer clic en Create Investigation Title: Investigacion test Clic Save	Se escogerá un evento notable y se lo agregara a un nuevo flujo de investigación

Sleccione la investigación que se ha creado y clic en Save Cierre el cuadro de dialago	
2. En la barra superior de Enterprise Security seleccione My Investigations Seleccione la investigación Investigacion test	Aparecerá el flujo de la información de la investigación. En este momento solo aparecerá un evento
3. En la parte derecha se observaran un circulo con un símbolo más (+), selecciónelo y agregue a otro usuario.	Se agregaran otros usuarios para que sean parte de la investigación
4. En la parte de Create New Entry agregue Note. Escriba un pequeño texto: Esta es una nota de prueba clic add to investigation	Se agrega una nota del avance de la investigación. Si se desea también se agrega archivos adjuntos de hasta 4 mb. La nueva aparecerá en el timeline.
5. En la parte de Create New Entry agregue Action History. Filter por incident_review y agreguelo	Se agrega una acción de investigación al flujo de la investigación.
Observaciones:	

Tabla 26

- Caso de uso 11 - Captura de información, como se observa en la Tabla 27 y Tabla 28.

Objetivo	Captura de información
Actor(es)	Usuario de Seguridad
Descripción	Que los usuarios pueden incorporar nuevas fuentes de datos a Splunk para su visualización y posterior uso
Frecuencia	Cuando se requiera monitorear una nueva aplicación o dispositivo
Pre-procesamiento	No
Post-procesamiento	No
Caso(s) de uso incluido(s)	No

Tabla 27

Escenario: Capturar información de un archivo de log via interfaz grafica	
Pasos	**Resultado esperado**
1. Ir a settings. Luego add data Seleccionar Upload Hacer clic en Select file y tomar el archivo de logs Clic Next Hacer clic donde dice Segment in path Escriba “1” en la caja de texto (sin comillas) En index seleccione TEST Clic Next	Se subirá los datos de un log por una única vez utilizando la interfaz gráfica

Clic submit	
2. Poner en búsqueda index=TEST para verificar	Se deben visualizar los logs recién agregados
Escenario: Capturar información de un archivo via comandos	
Pasos	**Resultado esperado**
1. Abrir linea de comandos Ir a la carpeta bin de splunk C:\Program Files\Archivos de Programa\Splunk\bin Ejecutar el commando: ./splunk add oneshot c:\PATH -index scratch -host 1	Se subirá los datos de un log por una única vez utilizando la línea de comandos
2. Poner en búsqueda index=TEST host=1 para verificar	Se deben visualizar los logs recién agregados
Observaciones:	
Esta prueba deber realizarse en un equipo de pruebas y NO en producción.	

Tabla 28

- Caso de uso 12 - Generación de reportes, como se observa en la Tabla 29 y Tabla 30.

Objetivo	Generación de reportes
Actor(es)	Usuario de Seguridad
Descripción	Que los usuarios de seguridad puedan crear reportes o informes a partir de la información que se encuentra almacenada en el repositorio central de Splunk. Además los usuarios pueden programar los reportes de manera que se generen periódicamente.
Frecuencia	Cada vez que se requiera crear un reporte

Pre-procesamiento	No
Post-procesamiento	No
Caso(s) de uso incluido(s)	No

Tabla 29

Escenario: Generar reporte a partir de una búsqueda nueva	
Pasos	**Resultado esperado**
1. Ejecute la siguiente busqueda en la pantalla de busqueda de Splunk en los últimos 60 minutos * | stats count AS Eventos by sourcetype | sort –Eventos	Esta búsqueda devolverá todos los eventos por tipo de fuente de datos en los últimos 60 minutos.
2. Se selecciona Save As en la parte superior derecha, luego seleccionar Report. Poner de nombre: Test Report1 Time Range Picker: NO	El reporte se guarda para ser consultado o utilizado
3. Clic en Schedule Report En la nueva ventana habilitar Schedule report. Dejar los valores por defecto En enable actions seleccione Send Mail To: test@cnel.gob Dejar los demás valores por defecto.	Se configura para que llegue por correo la notificación de que un nuevo reporte está listo.

Escenario: Generar reporte a partir de una búsqueda de Enterprise Security	
1. Clic en settings , luego en Searches, reports, and alerts Haga clic en run en la busqueda Audit - ES View Activity Over Time	Buscar y utilizar una búsqueda preexistente
2. Se selecciona Save As en la parte superior derecha, luego seleccionar Report. Poner de nombre: Test Report2 Time Range Picker: NO	El reporte se guarda para ser consultado o utilizado
3. Clic en Schedule Report En la nueva ventana habilitar Schedule report. Dejar los valores por defecto En enable actions seleccione Send Mail To: test@cnel.gob Dejar los demás valores por defecto	Se configura para que llegue por correo la notificación de que un nuevo reporte está listo.
Escenario: Generar reporte a partir de un Dashboard de Enterprise Security	
1. En el módulo de Enterprise Security, seleccionar Security Posture. En el botón Edit en la parte superior derecha de la gráfica hacer clic en edit. Seleccionar Schedule PDF delivery. Las opciones dejar las de defecto y poner un mail valido. Al final seleccionar Send Test Mail	Enviar un correo de prueba de configuración de reporte programado con la información que se encuentra en Security Posture

Observaciones:	
Los correos de prueba pueden demorar un poco dependiendo del proveedor del servicio de correos	

Tabla 30

5.2. Reportes de las Pruebas realizadas

Todas las pruebas se realizaron con éxito, con lo cual existe un “Acta de Aprobación y Recepción – PRUEBAS DE ACEPTACIÓN DE LA SOLUCION” generado para este proyecto, sin embargo es un documento confidencial y de propiedad de CNEL EP, por lo cual no se adjunta en este documento.

5.3. Análisis del antes y después de la solución

Antes se esperaba que el usuario final reporte el evento para actuar o atender el incidente, por ende como se explicó en el capítulo 3 con este proyecto se pretendía automatizar esto, lo cual se pudo realizar.

CNEL EP, cuenta con esta herramienta desde donde se puede ver los eventos de todos los aplicativos informáticos, red corporativa y servidores críticos de la corporación.

Se puede detectar eventos sospechosos y actuar previamente antes que el ataque se realice o abrir casos de investigación y correlacionar eventos para analizar si se trata del mismo ataque.

Con esta herramienta se logró llegar a actuar más rápido y así bajar el número de ataques e infecciones a la red de la Corporación.

CONCLUSIONES Y RECOMENDACIONES

Splunk tiene una mejor inteligencia de amenazas, por lo cual se ha colocado entre los líderes del cuadrante de Gartner, además tiene cientos de aplicaciones, para interpretar casi cualquier formato de información de log, que va desde la seguridad hasta la inteligencia analítica.

Es una excelente herramienta de monitoreo de infraestructura, posee herramientas de búsqueda y gráficos tan completos e inteligentes que probablemente no existe ningún conjunto de datos al que no puedas acceder a través de su interfaz de usuario.

En este proyecto no se pudo integrar Splunk con SCADA, por motivos fuera del alcance de los técnicos debido a que la herramienta estuvo lista para dicha integración, pero no se obtuvieron los permisos por parte del MEER para poder realizarlo por lo cual se recomienda en una segunda fase gestionar y llegar a una autorización para la integración de SCADA con Splunk, además se recomienda ampliar el plazo para las integraciones de las herramientas que se deseen con Splunk, debido a que la inserción de datos a splunk es muy compleja y requiere de análisis previo, investigación, conocimiento y tiempo extra.

BIBLIOGRAFÍA

[1] Administración publica. (2013, Septiembre 25). Acuerdo Gubernamental de Seguridad de la Información. [Online]. Disponible en:

http://www.administracionpublica.gob.ec/wp-content/uploads/downloads/2016/02/Esquema-Gubernamental-de-Seguridades-de-la-Informacion.pdf.

[2] Splunk. (2015, Septiembre 21). Componentes de Splunk. [Online]. Disponible en: https://docs.splunk.com/Special:SplunkSearch/docs?q=search+head.

[3] Splunk. (2015, Septiembre 21). Splunk Reports. [Online]. Disponible en: http://docs.splunk.com/Documentation/Splunk/6.6.1/Search/Aboutrealtimesearches.

[4] Splunk. (2015, Septiembre 21). Splunk Alerts. [Online]. Disponible en: http://docs.splunk.com/Documentation/Splunk/6.6.1/Alert/Aboutalerts.

[5] Splunk. (2015, Septiembre 21). How to install splunk. [Online]. Disponible en: http://docs.splunk.com/Documentation/Splunk/6.6.1/SearchTutorial/InstallSplunk.

[6] Splunk. (2015, Septiembre 21). Forwarder install on Linux. [Online]. Disponible en: http://docs.splunk.com/Documentation/Splunk/6.6.1/Installation/InstallonLinux.

[7] Splunk. (2015, Septiembre 21). Getting data in. [Online]. Disponible en: http://docs.splunk.com/Documentation/Splunk/6.6.1/Data/Usingforwardingagents.

[8] ISO27002. (2013, Octubre). ISO27002:2013. [Online]. Disponible en:

http://www.iso27000.es/.

ANEXOS

Anexo 1

A continuación se enumeran los dominios de la ISO 27002 [8].

1. “Organizando la seguridad de información
   1.1. Estructura para la seguridad de la información
      1.1.1. Comité de gestión de seguridad de la información
      1.1.2. Coordinación de seguridad de la información
      1.1.3. Asignación de responsabilidades para la seguridad de la información
      1.1.4. Proceso de autorización de recursos para el tratamiento de la información
      1.1.5. Acuerdos de confidencialidad
      1.1.6. Contacto con las autoridades
      1.1.7. Contacto con organizaciones de especial interés
      1.1.8. Revisión independiente de la seguridad de la información
   1.2. Terceros
      1.2.1. Identificación de los riesgos derivados del acceso de terceros
      1.2.2. Tratamiento de la seguridad en la relación con los clientes
      1.2.3. Tratamiento de la seguridad en contratos con terceros

2. Gestión de activos
   2.1. Responsabilidad sobre los activos.
      2.1.1. Inventario de activos.
      2.1.2. Responsable de los activos.
      2.1.3. Acuerdos sobre el uso aceptable de los activos.
   2.2. Clasificación de la información
      2.2.1. Directrices de clasificación.
      2.2.2. Marcado y tratamiento de la información.
3. Seguridad ligada a recursos humanos
   3.1. Seguridad en la definición del trabajo y los recursos.

5.1.4. Separación de los recursos para desarrollo y producción.

5.2. Supervisión de los servicios contratados a terceros.

5.2.1. Prestación de servicios.

5.2.2. Monitorización y revisión de los servicios contratados.

5.2.3. Gestión de los cambios en los servicios contratados.

5.3. Planificación y aceptación del sistema.

5.3.1. Planificación de capacidades.

5.3.2. Aceptación del sistema.

5.4. Protección contra software malicioso y código móvil.

5.4.1. Medidas y controles contra software malicioso.

5.4.2. Medidas y controles contra código móvil.

5.5. Gestión interna de soportes y recuperación.

5.5.1. Recuperación de la información.

5.6. Gestión de redes.

5.6.1. Controles de red.

5.6.2. Seguridad en los servicios de red.

5.7. Utilización y seguridad de los soportes de información.

5.7.1. Gestión de soportes extraíbles.

5.7.2. Eliminación de soportes.

5.7.3. Procedimientos de utilización de la información.

5.7.4. Seguridad de la documentación de sistemas.

5.8. Intercambio de información y software.

5.8.1. Políticas y procedimientos de intercambio de información y software.

5.8.2. Acuerdos de intercambio.

5.8.3. Soportes físicos en tránsito.

5.8.4. Mensajería electrónica

5.8.5. Sistemas de información empresariales.

5.9. Servicios de comercio electrónico.

5.9.1. Seguridad en comercio electrónico.

5.9.2. Seguridad en transacciones en línea.

5.9.3. Seguridad en información pública.

5.10. Monitorización

5.10.1. Registro de incidencias.

5.10.2. Seguimiento del uso de los sistemas.

5.10.3. Protección de los registros de incidencias.

5.10.4. Diarios de operación del administrador y operador.

5.10.5. Registro de fallos.

5.10.6. Sincronización de reloj.

6. Control de acceso

6.1. Requisitos de negocio para el control de accesos.

6.1.1. Política de control de accesos.

6.2. Gestión de acceso de usuario.

6.2.1. Registro de usuario.

6.2.2. Gestión de privilegios.

6.2.3. Gestión de contraseñas de usuario.

6.2.4. Revisión de los derechos de acceso de los usuarios.

6.3. Responsabilidades del usuario.

6.3.1. Uso de contraseña.

6.3.2. Equipo informático de usuario desatendido.

6.3.3. Políticas para escritorios y monitores sin información.

6.4. Control de acceso en red.

6.4.1. Política de uso de los servicios de red.

6.4.2. Autenticación de usuario para conexiones externas.

6.4.3. Autenticación de nodos de la red.

6.4.4. Protección a puertos de diagnóstico remoto.

6.4.5. Segregación en las redes.

6.4.6. Control de conexión a las redes.

6.4.7. Control de encaminamiento en la red.

6.5. Control de acceso al sistema operativo.

6.5.1. Procedimientos de conexión de terminales.

6.5.2. Identificación y autenticación de usuario.

6.5.3. Sistema de gestión de contraseñas.

6.5.4. Uso de los servicios del sistema.

6.5.5. Desconexión automática de terminales.

6.5.6. Limitación del tiempo de conexión.

6.6. Control de acceso a las aplicaciones.

6.6.1. Restricción de acceso a la información.

6.6.2. Aislamiento de sistemas sensibles.

6.7. Informática móvil y tele trabajo.

6.7.1. Informática móvil.

6.7.2. Tele trabajo.

7. Adquisición, desarrollo y mantenimiento de sistemas de información

7.1. Requisitos de seguridad de los sistemas.

7.1.1. Análisis y especificación de los requisitos de seguridad.

7.2. Seguridad de las aplicaciones del sistema.

7.2.1. Validación de los datos de entrada.

7.2.2. Control del proceso interno.

7.2.3. Autenticación de mensajes.

7.2.4. Validación de los datos de salida.

7.3. Controles criptográficos.

7.3.1. Política de uso de los controles criptográficos.

7.3.2. Cifrado.

7.4. Seguridad de los ficheros del sistema.

7.4.1. Control del software en explotación.

7.4.2. Protección de los datos de prueba del sistema.

7.4.3. Control de acceso a la librería de programas fuente.

7.5. Seguridad en los procesos de desarrollo y soporte.

7.5.1. Procedimientos de control de cambios.

7.5.2. Revisión técnica de los cambios en el sistema operativo.

7.5.3. Restricciones en los cambios a los paquetes de software.

7.5.4. Canales encubiertos y código Troyano.

7.5.5. Desarrollo externalizado del software.

7.6. Gestión de las vulnerabilidades técnicas.

7.6.1. Control de las vulnerabilidades técnicas.

8. Gestión de incidentes de los sistemas de información

8.1. Comunicación de eventos y debilidades en la seguridad de la información.

8.1.1. Comunicación de eventos en seguridad.

8.1.2. Comunicación de debilidades en seguridad.

8.2. Gestión de incidentes y mejoras en la seguridad de la información.

8.2.1. Identificación de responsabilidades y procedimientos.

8.2.2. Evaluación de incidentes en seguridad.

8.2.3. Recogida de pruebas.

9. Gestión de la continuidad del negocio

9.1.1. Aspectos de la gestión de continuidad del negocio.

9.1.2. Proceso de la gestión de continuidad del negocio.

9.1.3. Continuidad del negocio y análisis de impactos.

9.1.4. Redacción e implantación de planes de continuidad.

9.1.5. Marco de planificación para la continuidad del negocio.

9.1.6. Prueba, mantenimiento y reevaluación de planes de continuidad.

10. Cumplimento

10.1. Conformidad con los requisitos legales.

10.1.1. Identificación de la legislación aplicable.

10.1.2. Derechos de propiedad intelectual (IPR).

10.1.3. Salvaguarda de los registros de la Organización.

10.1.4. Protección de datos de carácter personal y de la intimidad de las personas.

10.1.5. Evitar mal uso de los dispositivos de tratamiento de la información.

10.1.6. Reglamentación de los controles de cifrados.

10.2. Revisiones de la política de seguridad y de la conformidad técnica.

10.2.1. Conformidad con la política de seguridad.

10.2.2. Comprobación de la conformidad técnica.

10.3. Consideraciones sobre la auditoria de sistemas.

10.3.1. Controles de auditoria de sistemas.

10.3.2. Protección de las herramientas de auditoria de sistemas”.

Anexo 2

Configuración para reconocimiento de SAM

Se agrega la siguiente línea al final del archivo /etc/fstab:

/dev/mapper/mpatha /opt/splunk/var/lib/splunk xfs defaults 0 0

Con esta configuración se especifica que los archivos del repositorio de Splunk vayan al Storage

Instalación y configuración de SYSLOG

Ejecutar los siguientes comandos, para instalación de syslog-ng:

- yum –y install syslog-ng
- yum install epel-release
- yum install syslog-ng

Editar la siguiente línea en el archivo: vi /etc/selinux/config

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#  enforcing – SELinux security policy is enforced.
#     permissive – SELinux prints warnings instead of enforcing.
#     disabled – No SELinux policy is loaded.
SELINUX=disabled
```

Agregar en el archivo: vi /etc/rc.d/rc.local

```
#!/bin/bash
# THIS FILE IS ADDED FOR COMPATIBILITY PURPOSES
#
```

```
# It is highly advisable to create own 78uawei services or udev rules
# to run scripts during boot instead of using this file.
#
# In contrast to previous versions due to parallel execution during boot
# this script will NOT be run after all other services.
#
# Please note that you must run 'chmod +x /etc/rc.d/rc.local' to ensure
# that this script will be executed during boot.

Touch /var/lock/subsys/local

if test –f /sys/kernel/mm/transparent_hugepage/enabled; then
    echo never > /sys/kernel/mm/transparent_hugepage/enabled
fi
if test –f /sys/kernel/mm/transparent_hugepage/defrag; then
    echo never > /sys/kernel/mm/transparent_hugepage/defrag
fi
```

Ejecutar el siguiente comando:

chmod +x /etc/rc.d/rc.local

Agregar las siguientes 78uawei al final del archivo: vi /etc/security/limits.conf

```
*               soft    nofile          102400
*               hard    nofile          102400
# End of file
```

Reiniciar, ejecutar el comando:

init 6

Cambiar el siguiente archivo con los siguientes datos: /etc/sysconfig-ng/sysconfig-ng.conf

```
@version:3.5
@include “scl.conf”

options {
    flush_lines(0);
    time_reopen(10);
    log_fifo_size(1000);
    chain_hostnames(off);
    use_dns(yes);
    use_fqdn(yes);
    keep_hostname(yes);

    owner(“root”);
    group(“root”);
    perm(0644);

    dir_owner(“root”);
    dir_group(“root”);
```

```
    dir_perm(0755);
    create_dirs(yes);

    log_msg_size(18192);
};

source s_net {
    udp(ip(0.0.0.0) port(xxx));
    udp(ip(0.0.0.0) port(xxxx));
    udp(ip(0.0.0.0) port(xxxx));
};

filter f_huawei_firewalls {
    host("^xx\.xx\.xx\.xx")   or
    host("^xx\.xx\.xx\.xx")   or
    host("^xx\.xx\.xx\.xx")   or
    host("^xx\.xx\.xx\.xx")   or
    host("^xx\.xx\.xx\.xx")  or
    host("^xx\.xx\.xx\.xx")  or
    host("^xx\.xx\.xx\.xx")  or
};

filter f_huawei_switches {
    host("^CORE-") or
    host("^xx\.xx\.xx\.xx") or
```

```
        host("^xx\.xx\.xx\.xx")

};

destination d_files_huawei_firewalls {
   file("/opt/splunk/var/lib/splunk/xxxx/$HOST/81uawei_firewall_$YEAR-$MONTH-$DAY.log" create_dirs(yes));
};

destination d_files_huawei_switches {
   file("/opt/splunk/var/lib/splunk/xxxx/$HOST/81uawei_switch_$YEAR-$MONTH-$DAY.log" create_dirs(yes));
};

destination d_files_splunk {
   file("/opt/splunk/var/lib/splunk/xxxx/$HOST/$YEAR-$MONTH-$DAY.log" create_dirs(yes));
};

log { source(s_net); filter(f_huawei_firewalls); destination(d_files_huawei_firewalls); flags(final); };
log { source(s_net); filter(f_huawei_switches); destination(d_files_huawei_switches); flags(final); };
log { source(s_net); destination(d_files_splunk); flags(fallback); };
```

Agregar la siguiente línea para configuración del siguiente archivo para eliminación automática de archivos que tengan más de 7 dias : vi /etc/crontab

33 03 * * * root find /var/log/splunk/ -daystart –mtime +7 –type f –exec rm {} \;

Instalación Splunk Forwarder Colectores

Para instalar Splunk Enterprise se debe ser usuario root y ejecutar:

- Descargar el archivo splunkforwarder-6.3.3-f44afce176d0-Linux-x86_64.tgz en el servidor
- Ejecutar: tar xvzf splunkforwarder-6.3.3-f44afce176d0-Linux-x86_64.tgz –C /opt
- Una vez descomprimido el archivo ir a la ruta: /opt/splunkforwarder/bin
- Ejecutar el comando para el inicio automático ./splunk enable boot-start root
- Para iniciar Splunk ejecutar: ./splunk start
- Aceptar la licencia

Las credenciales por defecto al instalar Splunk son:

- user: xxxx
- password: xxxx

Ejecutar el siguiente comando para que las instancias de Splunk sean configurables desde el Search Head, en la ruta /opt/splunkforwarder/bin

- ./splunk set deploy-poll xx.xx.xx.xx:xxxx

Ejecutar el siguiente comando para que las instancias de Splunk envíen información a los Indexers, en la ruta /opt/splunkforwarder/bin

- ./splunk add forward-server xx.xx.xx.xx:xxxx –method autobalance
- ./splunk add forward-server xx.xx.xx.xx:xxxx –method autobalance

Ejecutar el siguiente comando para que las instancias de Splunk reciban información por el puerto 9997, en la ruta /opt/splunkforwarder/bin

- ./splunk enable listen xxxx

[5]

Instalación y configuración de SYSLOG

Ejecutar los siguientes comandos, para instalación de syslog-ng:

- yum –y install syslog-ng
- yum install epel-release
- yum install syslog-ng

Editar la siguiente línea en el archivo: vi /etc/selinux/config

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#  enforcing – SELinux security policy is enforced.
#     permissive – SELinux prints warnings instead of enforcing.
#     disabled – No SELinux policy is loaded.
SELINUX=disabled
```

Agregar en el archivo: vi /etc/rc.d/rc.local

```
#!/bin/bash
# THIS FILE IS ADDED FOR COMPATIBILITY PURPOSES
#
# It is highly advisable to create own 83uawei services or udev rules
# to run scripts during boot instead of using this file.
#
```

```
# In contrast to previous versions due to parallel execution during boot
# this script will NOT be run after all other services.
#
# Please note that you must run 'chmod +x /etc/rc.d/rc.local' to ensure
# that this script will be executed during boot.

Touch /var/lock/subsys/local

if test –f /sys/kernel/mm/transparent_hugepage/enabled; then
    echo never > /sys/kernel/mm/transparent_hugepage/enabled
fi
if test –f /sys/kernel/mm/transparent_hugepage/defrag; then
    echo never > /sys/kernel/mm/transparent_hugepage/defrag
fi
```

Ejecutar el siguiente comando:

chmod +x /etc/rc.d/rc.local

Agregar las siguientes 84uawei al final del archivo: vi /etc/security/limits.conf

```
*           soft    nofile          xxxxxx
*           hard    nofile          xxxxxx
# End of file
```

Reiniciar, ejecutar el comando:

init 6

Cambiar el siguiente archivo con los siguientes datos: /etc/sysconfig-ng/sysconfig-ng.conf

```
@version:3.5
@include “scl.conf”

options {
    flush_lines(0);
    time_reopen(10);
    log_fifo_size(1000);
    chain_hostnames(off);
    use_dns(yes);
    use_fqdn(yes);
    keep_hostname(yes);

    owner(“root”);
    group(“root”);
    perm(0644);

    dir_owner(“root”);
    dir_group(“root”);
    dir_perm(0755);
    create_dirs(yes);
```

```
    log_msg_size(18192);
};

source s_net {
    udp(ip(0.0.0.0) port(xxx));
    udp(ip(0.0.0.0) port(xxxx));
    udp(ip(0.0.0.0) port(xxxx));
};

filter f_huawei_firewalls {
    host("^xx\.xx\.xx\.xx")   or
    host("^xx\.xx\.xx\.xx")   or
    host("^xx\.xx\.xx\.xx")   or
    host("^xx\.xx\.xx\.xx")   or
    host("^xx\.xx\.xx\.xx")   or
    host("^xx\.xx\.xx\.xx")   or
    host("^xx\.xx\.xx\.xx")   or
    host("^xx\.xx\.xx\.xx")   or
};

filter f_huawei_switches {
    host("^CORE-") or
    host("^xx\.xx\.xx\.xx")   or
        host("^xx\.xx\.xx\.xx")
};
```

```
destination d_files_huawei_firewalls {
   file("/opt/splunk/var/lib/splunk/xxxx/$HOST/87uawei_firewall_$YEAR-$MONTH-$DAY.log" create_dirs(yes));
};

destination d_files_huawei_switches {
   file("/opt/splunk/var/lib/splunk/xxxx/$HOST/87uawei_switch_$YEAR-$MONTH-$DAY.log" create_dirs(yes));
};

destination d_files_splunk {
   file("/opt/splunk/var/lib/splunk/xxxx/$HOST/$YEAR-$MONTH-$DAY.log" create_dirs(yes));
};

log { source(s_net); filter(f_huawei_firewalls); destination(d_files_huawei_firewalls); flags(final); };
log { source(s_net); filter(f_huawei_switches); destination(d_files_huawei_switches); flags(final); };
log { source(s_net); destination(d_files_splunk); flags(fallback); };
```

Agregar la siguiente línea para configuración del siguiente archivo para eliminación automática de archivos que tengan más de 7 dias : vi /etc/crontab

33 03 * * * root find /var/log/splunk/ -daystart –mtime +7 –type f –exec rm {} \;

Instalación de Forwarders Linux

Para instalar Splunk Enterprise se debe ser usuario root y ejecutar **[6]:**

- Descargar el archivo splunkforwarder-6.3.3-f44afce176d0-Linux-x86_64.tgz en el servidor
- Ejecutar: tar xvzf splunkforwarder-6.3.3-f44afce176d0-Linux-x86_64.tgz –C /opt
- Una vez descomprimido el archivo ir a la ruta: /opt/splunkforwarder/bin
- Ejecutar el comando para el inicio automático ./splunk enable boot-start root
- Para iniciar Splunk ejecutar: ./splunk start
- Aceptar la licencia

Las credenciales por defecto al instalar Splunk son:

- user: xxx
- password: xxxxxx

Ejecutar el siguiente comando para que las instancias de Splunk sean configurables desde el Search Head, en la ruta /opt/splunkforwarder/bin

- ./splunk set deploy-poll xx.xx.xx.xx:xxxx

Ejecutar el siguiente comando para que las instancias de Splunk envíen información a los Indexers o al colector según corresponda, en la ruta /opt/splunkforwarder/bin:

Si el agente es instalado en un Servidor de Salitral:

- ./splunk add forward-server xx.xx.xx.xx:xxxx –method autobalance
- ./splunk add forward-server xx.xx.xx.xx:xxxx –method autobalance

Si el agente es instalado en un Servidor de Garzota:

- ./splunk add forward-server xx.xx.xx.xx:xxxx –method autobalance

Si el agente es instalado en un Servidor de Machala:

- ./splunk add forward-server xx.xx.xx.xx:xxxx –method autobalance

Si el agente es instalado en un Servidor de Santo Domingo:

- ./splunk add forward-server xx.xx.xx.xx:xxxx –method autobalance

Si el agente es instalado en un Servidor de Libertad:

- ./splunk add forward-server xx.xx.xx.xx:xxxx –method autobalance

Si el agente es instalado en un Servidor de Milagro:

- ./splunk add forward-server xx.xx.xx.xx:xxxx –method autobalance

Si el agente es instalado en un Servidor de Manta:

- ./splunk add forward-server xx.xx.xx.xx:xxxx –method autobalance

Si el agente es instalado en un Servidor de Guayas – Los Rios:

- ./splunk add forward-server xx.xx.xx.xx:xxxx –method autobalance

Si el agente es instalado en un Servidor de Esmeraldas:

- ./splunk add forward-server xx.xx.xx.xx:xxxx –method autobalance

Instalación Forwarder Silenciosa en Windows

Para realizar instalaciones masivas en Windows se puede utilizar al gun programa de software delivery y ejecturar el siguiente comando:

msiexec.exe /i splunkforwarder-6.3.3-f44afce176d0-x64-release.msi AGREETOLICENSE=Yes SPLUNK_APP=”SplunkForwarder” DEPLOYMENT_SERVER=”172.30.1.245:8089” WINEVENTLOG_SEC_ENABLE=1 /quiet

Configuración de Servicio de Mail

Para la configuración de la cuenta de correo que Splunk Enterprise utilizará para enviar los correos se debe en el Search Head, como se muestra en la figura A2.1:

1. Ir a Settings > Server Settings
2. Seleccionar Email Settings
3. Ingresar la ip o el nombre del servidor de correos
4. Seleccionar la seguridad del correo
5. Nombre de Usuario de la cuenta
6. Contraseña
7. Especificar en el formato del correo el nombre del servidor que es usados para la creación de los URL, y al cual los usuarios se conectaran para ver los reportes y las alarmas
8. El nombre de la cuenta que aparecerá como “from” cuando se reciban correos
9. Pie del correo
10. Adicionalmente se pueden realizar configuraciones para PDF, esta categoría esta por defecto

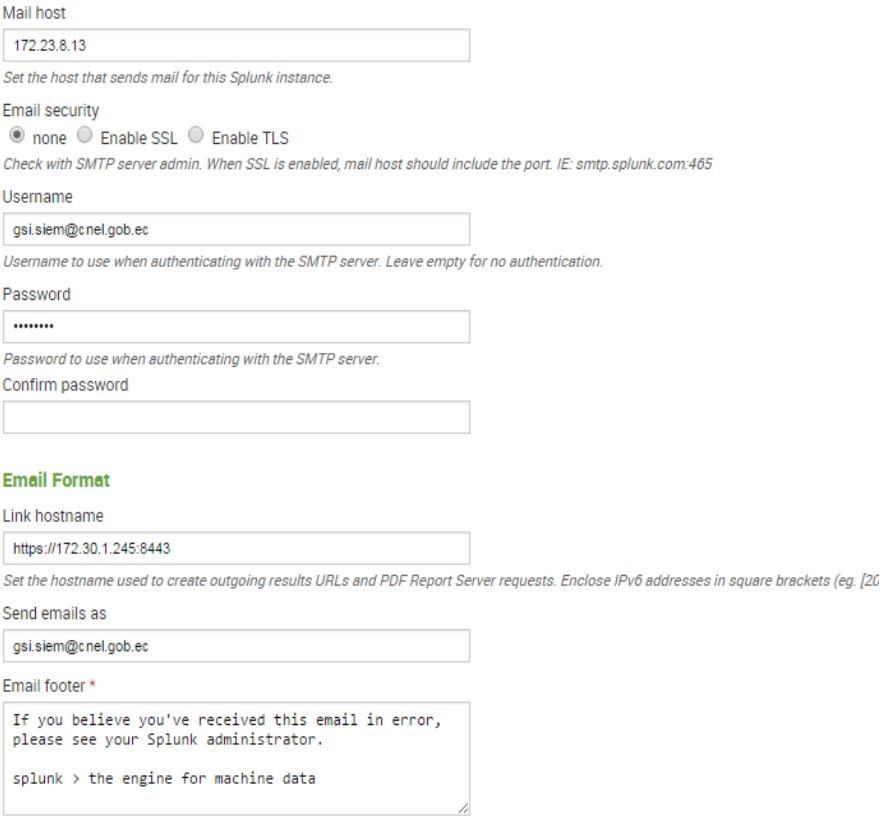

Figura A2.1

Configuración de Indexers.conf

La configuración de los indexes se ha dejado inicialmente por defecto hasta que se evalúe el consumo de espacio por cada index y posteriormente definir los volúmenes de retención

Actualmente la configuración de los indexers está contenida en el app cnel_base_all_indexes y cnel_base_search_volumes dentro del archivo de configuración indexes.conf, esta configuración ha sido desplegada a los indexes mediante el server class all_indexers, tal como se muestra en la figura A2.2.

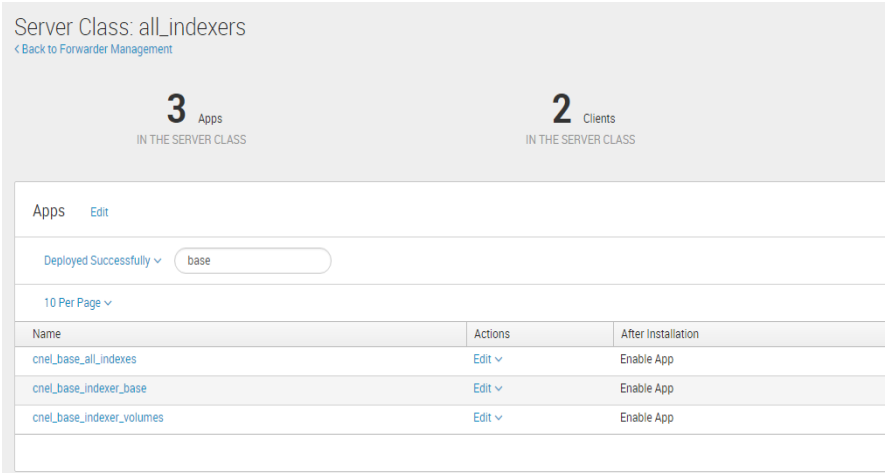

Figura A2.2

Contenido de cnel_base_indexer_volumes/local/indexes.conf

One Volume for Hot and Cold

[volume:primary]

path = /opt/splunk/var/lib/splunk

[volume:secondary]

path = /opt/splunk/var/lib/splunk

Contenido de cnel_base_all_indexes/local/indexes.conf

[main]

homePath = volume:primary/defaultdb/db

coldPath = volume:secondary/defaultdb/colddb

thawedPath = $SPLUNK_DB/defaultdb/thaweddb

[history]

```
homePath   = volume:primary/historydb/db
coldPath   = volume:secondary/historydb/colddb
thawedPath = $SPLUNK_DB/historydb/thaweddb

[summary]
homePath   = volume:primary/summarydb/db
coldPath   = volume:secondary/summarydb/colddb
thawedPath = $SPLUNK_DB/summarydb/thaweddb

[_internal]
homePath   = volume:primary/_internaldb/db
coldPath   = volume:secondary/_internaldb/colddb
thawedPath = $SPLUNK_DB/_internaldb/thaweddb

# For version 6.1 and higher
[_introspection]
homePath   = volume:primary/_introspection/db
coldPath   = volume:secondary/_introspection/colddb
thawedPath = $SPLUNK_DB/_introspection/thaweddb

[_audit]
homePath   = volume:primary/audit/db
coldPath   = volume:secondary/audit/colddb
thawedPath = $SPLUNK_DB/audit/thaweddb
```

```
[_thefishbucket]
homePath   = volume:primary/fishbucket/db
coldPath   = volume:secondary/fishbucket/colddb
thawedPath = $SPLUNK_DB/fishbucket/thaweddb

# SPLUNKBASE APP INDEXES

[iseries]
homePath = volume:primary/iseries/db
coldPath =  volume:secondary/iseries/colddb
thawedPath = $SPLUNK_DB/iseries/thaweddb

[netflow]
homePath   = volume:primary/netflow/db
coldPath   = volume:secondary/netflow/colddb
thawedPath = $SPLUNK_DB/netflow/thaweddb

# Windows

[windows]
homePath   = volume:primary/windows/db
coldPath   = volume:secondary/windows/colddb
thawedPath = $SPLUNK_DB/windows/thaweddb

[wineventlog]
```

```
homePath   = volume:primary/wineventlog/db
coldPath   = volume:secondary/wineventlog/colddb
thawedPath = $SPLUNK_DB/wineventlog/thaweddb

[perfmon]
homePath   = volume:primary/perfmon/db
coldPath   = volume:secondary/perfmon/colddb
thawedPath = $SPLUNK_DB/perfmon/thaweddb

[msad]
homePath   = volume:primary/msad/db
coldPath   = volume:secondary/msad/colddb
thawedPath = $SPLUNK_DB/msad/thaweddb

[winevents]
homePath   = volume:primary/winevents/db
coldPath   = volume:secondary/winevents/colddb
thawedPath = $SPLUNK_DB/winevents/thaweddb

# Nix

[os]
homePath   = volume:primary/os/db
coldPath   = volume:secondary/os/colddb
thawedPath = $SPLUNK_DB/os/thaweddb
```

```
[firedalerts]
homePath   = volume:primary/firedalerts/db
coldPath   = volume:secondary/firedalerts/colddb
thawedPath = $SPLUNK_DB/firedalerts/thaweddb

# ES

[ioc]
homePath   = volume:primary/ioc/db
coldPath   = volume:secondary/ioc/colddb
thawedPath = $SPLUNK_DB/ioc/thaweddb

[access_summary]
homePath   = volume:primary/access_summary/db
coldPath   = volume:secondary/access_summary/colddb
thawedPath = $SPLUNK_DB/access_summary/thaweddb

[access_summary2]
homePath   = volume:primary/access_summary2/db
coldPath   = volume:secondary/access_summary2/colddb
thawedPath = $SPLUNK_DB/access_summary2/thaweddb

[audit_summary]
homePath   = volume:primary/audit_summary/db
```

```
coldPath   = volume:secondary/audit_summary/colddb
thawedPath = $SPLUNK_DB/audit_summary/thaweddb

[audit_summary2]
homePath   = volume:primary/audit_summary2/db
coldPath   = volume:secondary/audit_summary2/colddb
thawedPath = $SPLUNK_DB/audit_summary2/thaweddb

[endpoint_summary]
homePath   = volume:primary/endpoint_summary/db
coldPath   = volume:secondary/endpoint_summary/colddb
thawedPath = $SPLUNK_DB/endpoint_summary/thaweddb

[endpoint_summary2]
homePath   = volume:primary/endpoint_summary2/db
coldPath   = volume:secondary/endpoint_summary2/colddb
thawedPath = $SPLUNK_DB/endpoint_summary2/thaweddb

[session_start]
homePath   = volume:primary/session_start/db
coldPath   = volume:secondary/session_start/colddb
thawedPath = $SPLUNK_DB/session_start/thaweddb

[session_end]
homePath   = volume:primary/session_end/db
```

```
coldPath   = volume:secondary/session_end/colddb
thawedPath = $SPLUNK_DB/session_end/thaweddb

[traffic_center_summary]
homePath   = volume:primary/traffic_center_summary/db
coldPath   = volume:secondary/traffic_center_summary/colddb
thawedPath = $SPLUNK_DB/traffic_center_summary/thaweddb

[traffic_center_summary2]
homePath   = volume:primary/traffic_center_summary2/db
coldPath   = volume:secondary/traffic_center_summary2/colddb
thawedPath = $SPLUNK_DB/traffic_center_summary2/thaweddb

[whois]
homePath   = volume:primary/whois/db
coldPath   = volume:secondary/whois/colddb
thawedPath = $SPLUNK_DB/whois/thaweddb

[network_summary]
homePath   = volume:primary/network_summary/db
coldPath   = volume:secondary/network_summary/colddb
thawedPath = $SPLUNK_DB/network_summary/thaweddb

[network_summary2]
homePath   = volume:primary/network_summary2/db
```

```
coldPath   = volume:secondary/network_summary2/colddb
thawedPath = $SPLUNK_DB/network_summary2/thaweddb

[network_summary3]
homePath   = volume:primary/network_summary3/db
coldPath   = volume:secondary/network_summary3/colddb
thawedPath = $SPLUNK_DB/network_summary3/thaweddb

[proxy_center_summary]
homePath   = volume:primary/proxy_center_summary/db
coldPath   = volume:secondary/proxy_center_summary/colddb
thawedPath = $SPLUNK_DB/proxy_center_summary/thaweddb

[proxy_center_summary2]
homePath   = volume:primary/proxy_center_summary2/db
coldPath   = volume:secondary/proxy_center_summary2/colddb
thawedPath = $SPLUNK_DB/proxy_center_summary2/thaweddb

[risk]
homePath   = volume:primary/risk/db
coldPath   = volume:secondary/risk/colddb
thawedPath = $SPLUNK_DB/risk/thaweddb

[notable]
homePath   = volume:primary/notable/db
```

```
coldPath   = volume:secondary/notable/colddb
thawedPath = $SPLUNK_DB/notable/thaweddb

[notable_summary]
homePath   = volume:primary/notable_summary/db
coldPath   = volume:secondary/notable_summary/colddb
thawedPath = $SPLUNK_DB/notable_summary/thaweddb

[cim_summary]
homePath   = volume:primary/cim_summary/db
coldPath   = volume:secondary/cim_summary/colddb
thawedPath = $SPLUNK_DB/cim_summary/thaweddb

[xtreme_contexts]
homePath   = volume:primary/xtreme_contexts/db
coldPath   = volume:secondary/xtreme_contexts/colddb
thawedPath = $SPLUNK_DB/xtreme_contexts/thaweddb

[threat_activity]
homePath   = volume:primary/threat_activity/db
coldPath   = volume:secondary/threat_activity/colddb
thawedPath = $SPLUNK_DB/threat_activity/thaweddb
```

```
# CUSTOMER INDEXES

[stream]
homePath   = volume:primary/stream/db
coldPath   = volume:secondary/stream/colddb
thawedPath = $SPLUNK_DB/stream/thaweddb

[huawei]
homePath   = volume:primary/huawei/db
coldPath   = volume:secondary/huawei/colddb
thawedPath = $SPLUNK_DB/huawei/thaweddb

[kaspersky]
homePath   = volume:primary/kaspersky/db
coldPath   = volume:secondary/kaspersky/colddb
thawedPath = $SPLUNK_DB/kaspersky/thaweddb

[endpoint]
homePath   = volume:primary/endpoint/db
coldPath   = volume:secondary/endpoint/colddb
thawedPath = $SPLUNK_DB/endpoint/thaweddb

[oracle]
homePath   = volume:primary/oracle/db
coldPath   = volume:secondary/oracle/colddb
```

```
thawedPath = $SPLUNK_DB/oracle/thaweddb

[oracle_db]
homePath   = volume:primary/oracle_db/db
coldPath   = volume:secondary/oracle_db/colddb
thawedPath = $SPLUNK_DB/oracle_db/thaweddb

[apache]
homePath   = volume:primary/apache/db
coldPath   = volume:secondary/apache/colddb
thawedPath = $SPLUNK_DB/apache/thaweddb

[jboss]
homePath   = volume:primary/jboss/db
coldPath   = volume:secondary/jboss/colddb
thawedPath = $SPLUNK_DB/jboss/thaweddb

[tomcat]
homePath   = volume:primary/tomcat/db
coldPath   = volume:secondary/tomcat/colddb
thawedPath = $SPLUNK_DB/tomcat/thaweddb

[elastix]
homePath   = volume:primary/elastix/db
coldPath   = volume:secondary/elastix/colddb
```

thawedPath = $SPLUNK_DB/elastix/thaweddb

[sophos]

homePath = volume:primary/sophos/db

coldPath = volume:secondary/sophos/colddb

thawedPath = $SPLUNK_DB/sophos/thaweddb

Captura de Información

La captura de información dependerá de la fuente de los logs. Se debe conocer previamente la ruta de donde se desea capturar los logs, o donde ejecutar el script para recuperar los datos. Posteriormente se debe crear o utilizar una app existente para configurar el archivo inputs.conf para monitorear la información. Recordar que los inputs.conf que se desea desplegar hacia otras instancias de Splunk (Indexers o Forwarders) deben colocarse en la ruta /opt/Splunk/etc/deployment-apps/ **[7].**

Ejemplo Monitoreo iseries:

En la carpeta /opt/Splunk/etc/deployment-apps/iseries_input/local se encuentra el archivo de configuración inputs.conf con el siguiente contenido:

[monitor:///home/splunk/AUDMLG*]

index = iseries

sourcetype = dspjrn:5

host = SICO_MLG

[monitor:///home/splunk/AUDLRS*]

index = iseries

sourcetype = dspjrn:5

host = SICO_LRS

[monitor:///home/splunk/AUDSTD*]

index = iseries

sourcetype = dspjrn:5

host = SICO_STD

[monitor:///home/splunk/AUDEOR*]

index = iseries

sourcetype = dspjrn:5

host = SICO_EOR

[monitor:///home/splunk/AUDMNB*.]

index = iseries

sourcetype = dspjrn:5

host = SICO_MAN

En este archivo se está especificando el nombre de los archivos que se espera encontrar y dependiendo de la estructura del nombre se asigna un host.

Para continuar se debe desplegar la configuración a las instancias deseas. En este caso se están recibiendo los archivos en el xx.xx.xx.xx. En la interfaz gráfica de Splunk ir a Settings > Forwarder Management

En caso de no existir se debe crear un Server Class:

- Escoger la pestaña Server Class

- Escoger un nombre para el Server Class, como se muestra en la figura A2.3

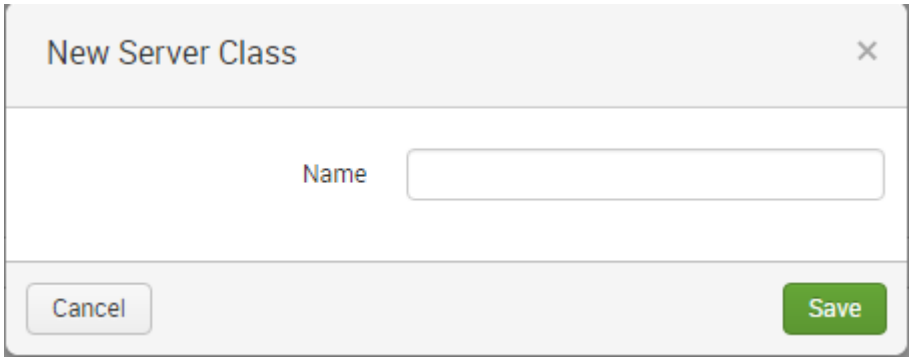

Figura A2.3

- Una vez creada, seleccionar las apps y los clientes a los que se desea desplegar la configuración, como se muestra en la figura A2.4.

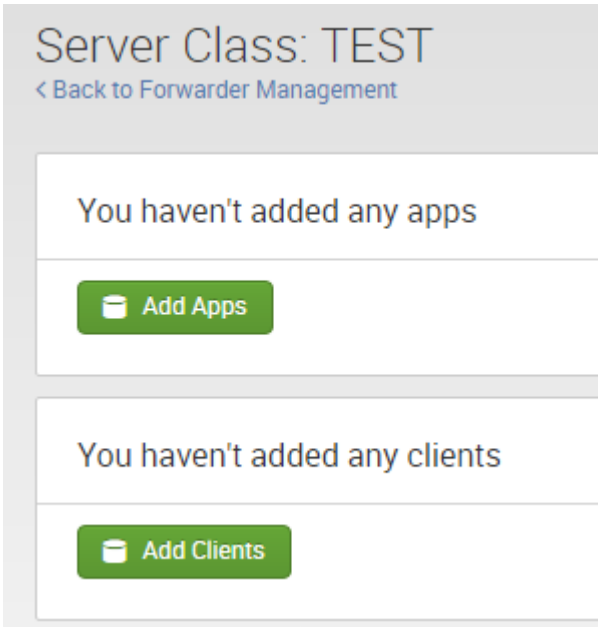

Figura A2.4

Para la configuración del iseries existe el server class cnel_iseries, como se muestra en la figura A2.5.

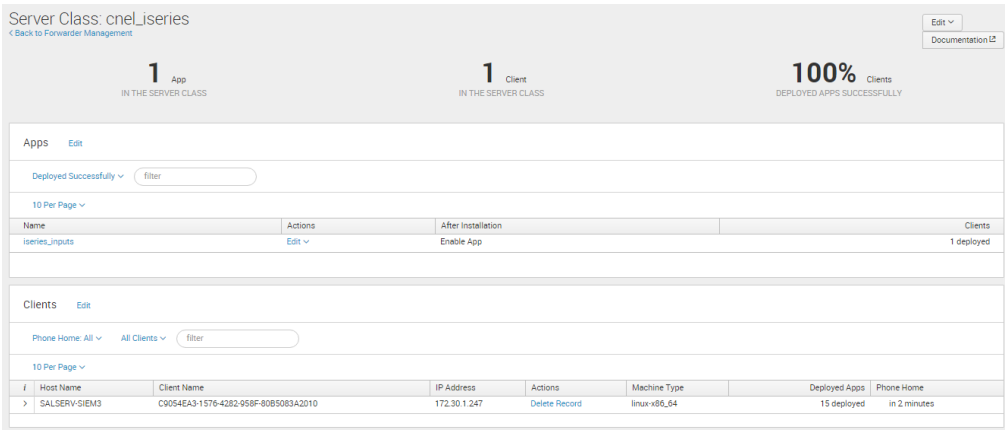

Figura A2.5

Para confirmar que el app se desplegó apropiadamente se puede revisar el cliente y verificar que exista la ruta /opt/Splunk/etc/apps/iseries_input/local. Dentro de esta ruta existe el archivo inputs.conf qe debe contener la misma información que se creó en el servidor.

Ejemplo Monitoreo Linux:

Los add-on (apps de configuración) que vienen por defecto o se descargan de splunkbase.splunk.com también se deben desplegar, en este ejemplo se tiene el add-on para sistemas *nix que se desea desplegar, como se muestra en la figura A2.6.

Para desplegar el add se debe:

- Copiar el app (directorio) *Splunk_TA_nix_inputs* en la ruta /opt/Splunk/etc/deployment-apps
- Ingresar a la interfaz gráfica y utilizar un Server Class para desplegar la configuración. El server Class utilizado ahora es *all_nix*

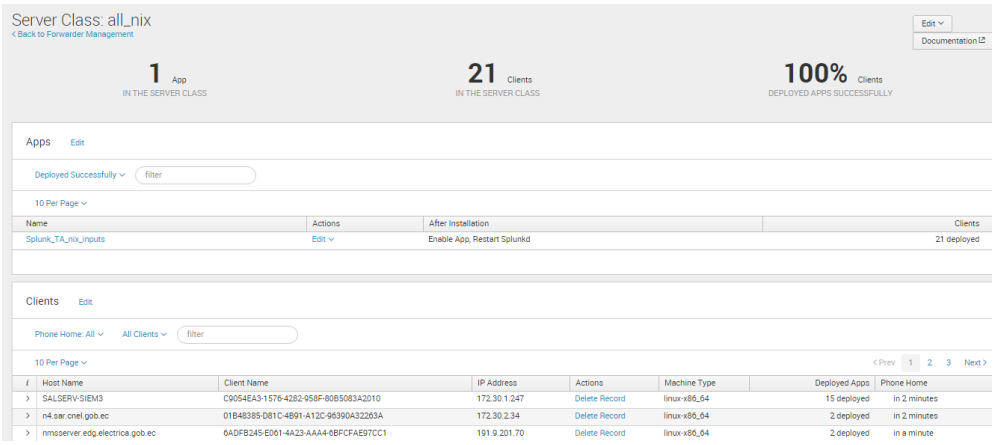

Figura A2.6

- En el server class se debe incluir la app *Splunk_TA_nix_inputs* y todos los clientes de Splunk que son Linux. Seleccionar el filter by machinne type, como se muestra en la figura A2.7.

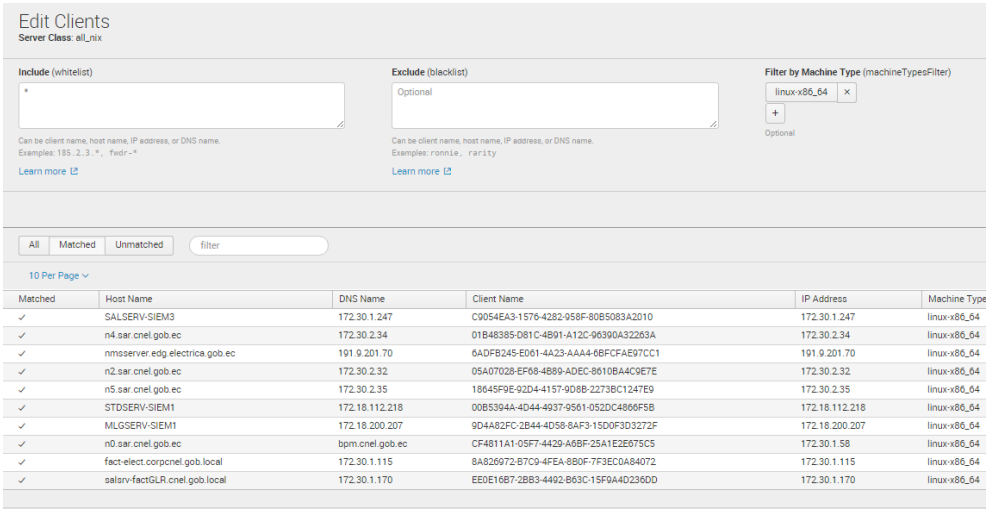

Figura A2.7

Integración con Active Directory

Para que los usuarios del Active Directory puedan usar su cuenta de dominio en Splunk, deben realizarse una conexión hacia el grupo o los grupos que contengan los usuarios que van a usar la herramienta, como se muestra en la figura A2.8, A2.9 y A2.10.

- Ir a Settings > Access control

- Luego seleccionar Authentication method
- Seleccionar External Authentication Method:LDAP
- Dar click en LDAP Settings
- NEW
- Y completar los datos según indique el Administrador del Diretorio Activo

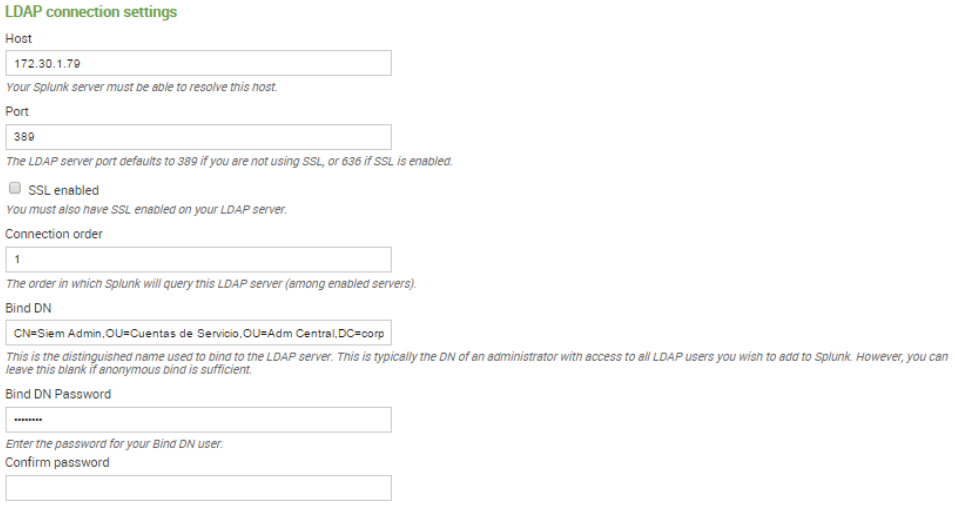

Figura A2.8

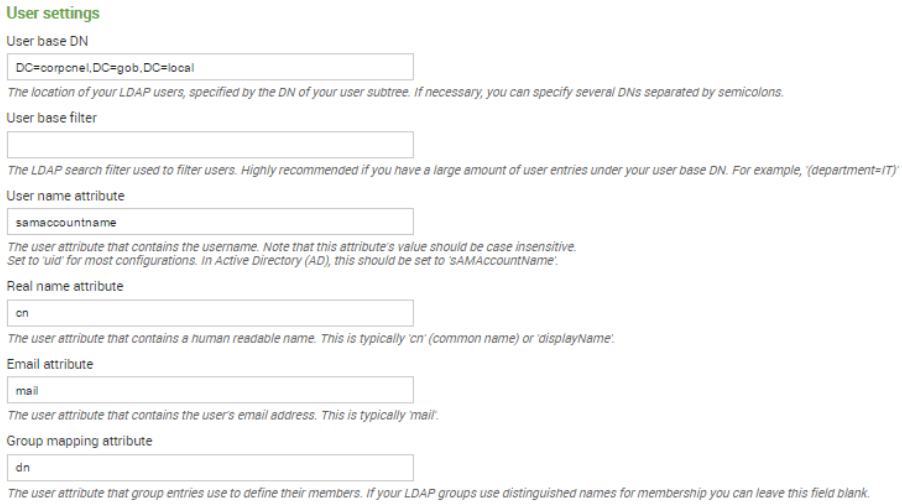

Figura A2.9

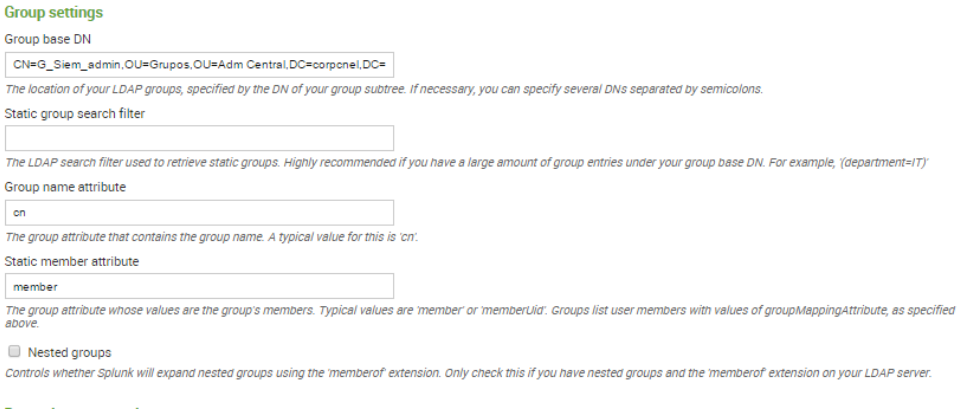

Figura A2.10

Una vez comprobada la conexión, se podrá hacer el mapeo con los roles de usuario que existan en Splunk.

Al final las configuraciones quedaran almacenadas en el archivo authentication.conf, que se encuentra en la ruta /opt/splunk/etc/system/local del servidor principal, que contine:

[authentication]

authSettings = Active Directory

authType = LDAP

[Active Directory]

SSLEnabled = 0

anonymous_referrals = 1

bindDN = CN=Siem Admin,OU=Cuentas de Servicio,OU=Adm Central,DC=corpcnel,DC=gob,DC=local

bindDNpassword = 1AHJ+RDLvxdVl9A==

charset = utf8

emailAttribute = mail

groupBaseDN = CN=G_Siem_admin,OU=Grupos,OU=Adm Central,DC=corpcnel,DC=gob,DC=local

groupMappingAttribute = dn

groupMemberAttribute = member

groupNameAttribute = cn

host = xx.xx.xx.xx

nestedGroups = 0

network_timeout = 20

port = 389

realNameAttribute = cn

sizelimit = 1000

timelimit = 15

userBaseDN = DC=corpcnel,DC=gob,DC=local

userNameAttribute = samaccountname

[roleMap_Active Directory]

admin = G_Siem_admin

Configuración Enterprise Security

Instalación de Splunk Enterprise Security

1. Descargar Enterprise Security de la url: splunkbase.splunk.com, Como se muestra en la figura A2.11
2. Utilizar el buscador para encontrar el instalador y descargar.

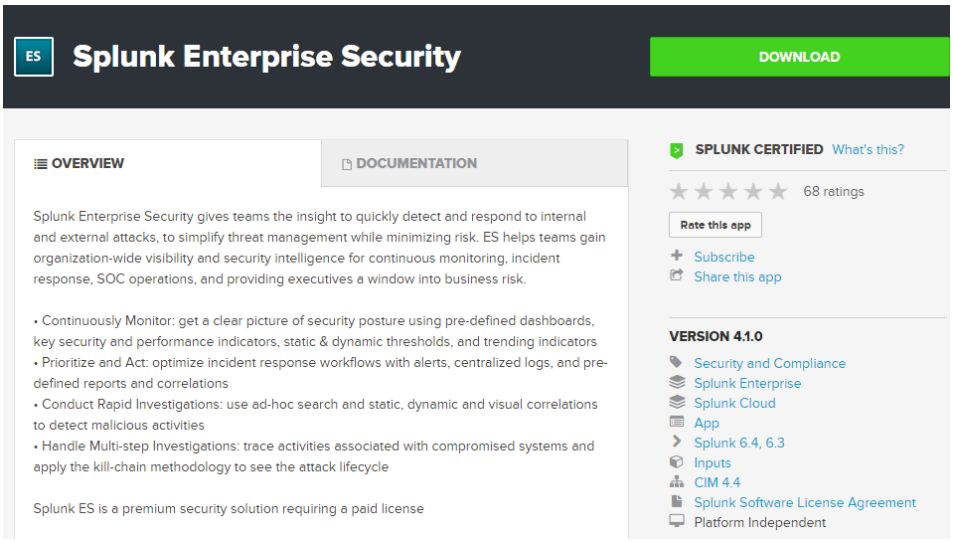

Figura A2.11

3. Para poder realizar la descarga se deben utilizar las credenciales de CNEL EP.
4. El archivo que resulte del final de la descarga debe estar en una máquina que tenga acceso usando el browser al Search Head de la solución Splunk Enterprise.
5. Ingresar a Splunk Enterpise como Administrador.
6. Para instalar Splunk Enterpise Security se debe ingresar al administrador de apps, como se muestra en la figura A2.12.

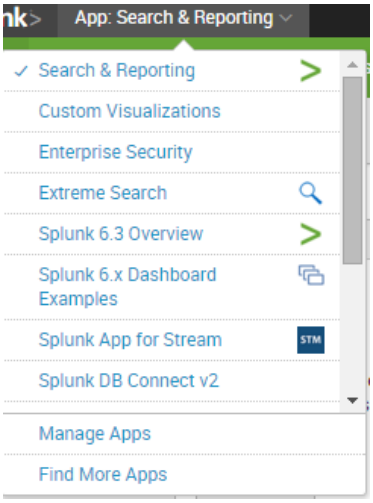

Figura A2.12

7. Seleccionar Install App from file y seleccionar el archivo que se descargó previamente.
8. Seleccionar Upload para comenzar la instalación
9. Una vez que termina la carga del archivo aparcera una opción para iniciar el Setup
10. Seleccionar Start
11. Automáticamente aparecerá un wizard que guiara cuales add –ons se desea utilizar, en CNEL están habilitado los siguientes add-on:
    DA-ESS-AccessProtection
    DA-ESS-EndpointProtection
    DA-ESS-IdentityManagement
    DA-ESS-NetworkProtection
    DA-ESS-ThreatIntelligence
    SA-AccessProtection
    SA-AuditAndDataProtection
    SA-EndpointProtection
    SA-IdentityManagement
    SA-ldapsearch
    SA-NetworkProtection

SA-threat_activity_drilldown
SA-ThreatIntelligence
SA-UEBA
SA-Utils
Splunk_SA_CIM
Splunk_SA_ExtremeSearch
Splunk_TA_flowfix
Splunk_TA_flowfix_input
Splunk_TA_nix
Splunk_TA_oracle
Splunk_TA_ueba
Splunk_TA_windows
TA-DNSServer-NT6
TA-DomainController-NT6

12. La lista de estos add-ons y el resto de apps instaladas se encuentran en el Search Head en la ruta:

    /opt/splunk/etc/apps

13. Una vez terminada la selección se debe reiniciar el servicio de Splunk para que los cambios tomen efecto.

    NOTA: El app de Splunk Enterprise Security solo se instala en el Search Head. Para que los indexers trabajen en conjunto se deben desplegar los add-on via deployment server

Configuración de Splunk Enterprise Security

Despliegue de configuraciones

Mediante la utilización del deployment server se ha realizado el despliegue de la información de Splunk Enterprise Security hacia las distintas instancias de la solución.
Se realizó el envío utilizando server clases. Las Apps desplegadas fueron las siguientes, como se muestra en la figura A2.13:
Splunk_TA_flowfix

Splunk_TA_nix

Splunk_TA_oracle

Splunk_TA_windows

TA-DNSServer-NT6

TA-DomainController-NT6

Previamente estas apps debieron ser copiadas en la ruta:

/opt/splunk/etc/deployment-apps/

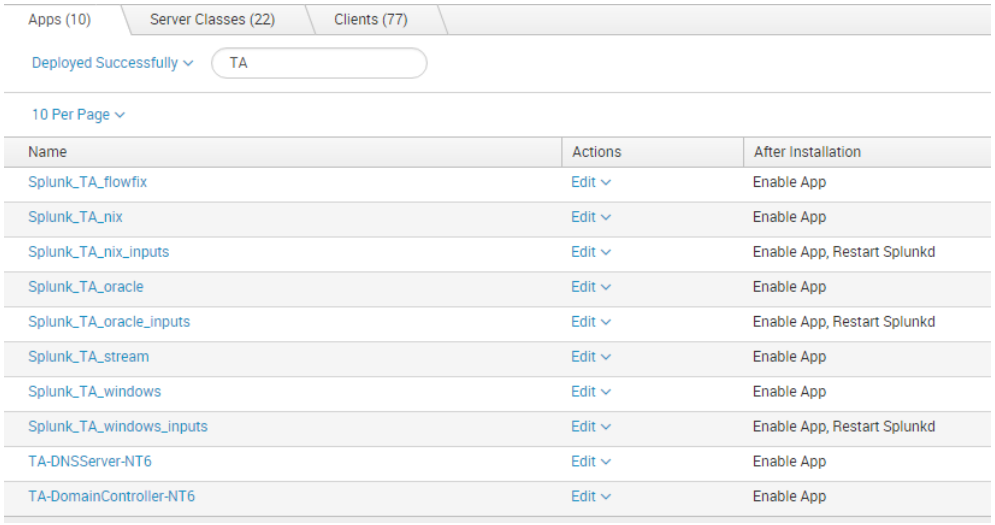

Figura A2.13

Se utilizó el siguiente Server Class para enviar las configuraciones a los indexadores, como se muestra en la figura A2.14:

all_indexers

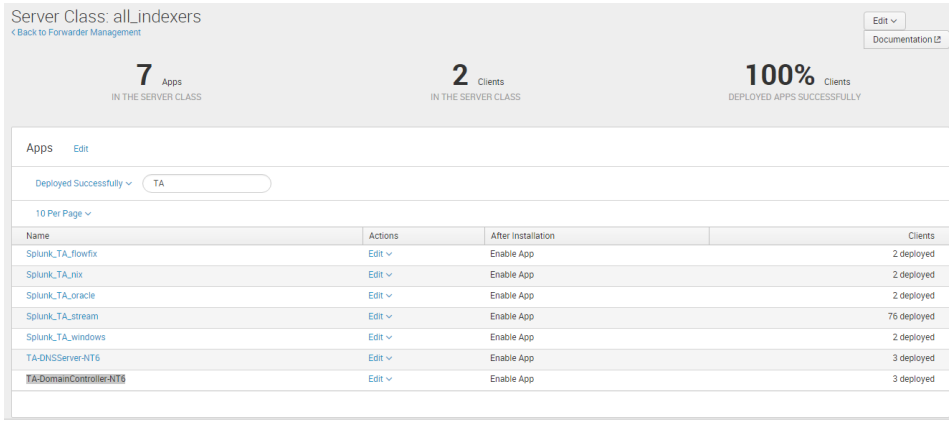

Figura A2.14

Tener en cuenta que este mismo Server Class incluye otros add-on de varias configuraciones personalizadas.

También utilizando los Server Class se desplegaron las configuraciones de inputs hacia los distintos agentes, entre ellos:

all_nix
all_oracle
all_windows

Tener en cuenta que este mismo Server Class incluye otros add-on de varias configuraciones personalizadas.
También se debe considerar que algunas de las apps fueron separadas para mejorar la distribución de los archivos de configuración. Las apps que tengan una terminación _**inputs** son exclusivamente creadas para ser enviadas a las fuentes de información, que en la mayoría de los casos son los colectores. Las que tienen la terminación _**props** fueron creadas para realizar labores de transformación y serán enviadas a los indexadores
Ejemplo:
Splunk_TA_nix
Splunk_TA_nix_inputs
Splunk_TA_oracle
Splunk_TA_oracle_inputs

Configuración de Usuarios

Se ha dejado la configuración por defecto, todos los usuarios del grupo de Active Directory G_Siem_Admin tienen el rol de ess_analyst. Para cambiar esta configuración se debe acceder a las opciones de Map Group en las configuraciones de acceso, como se muestra en la figura A2.15.

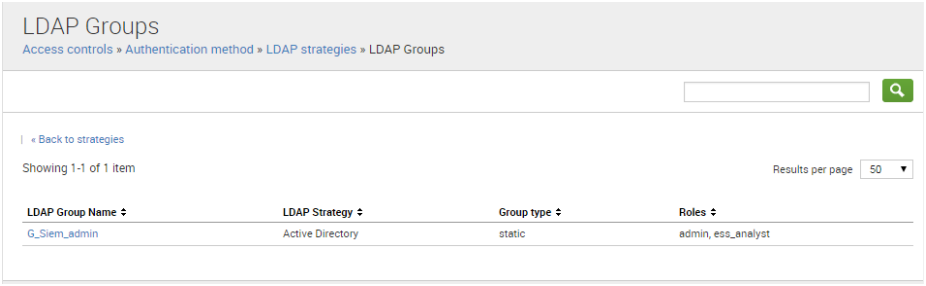

Figura A2.15

Configuración de Modelos de Datos

Se definió que los siguientes modelos de datos sean acelerados por periodos de un mes:

Application State
Authentication
Certifies
Change Analysis
Domain Analysis
Email
Incident Management
Intrusion Detection
Malware
Network Resolution
Network Sessions
Network Traffic
Performance
Risk Analysis
Splunk Audit logs
Threat Intelligence
Ticket Management
Update
Vulnerabilties

Web

Para Seleccionar los modelos de datos a acelerar se selecciona, como se muestra en la figura 2.16 y 2.17: Settings > Data Models. Luego en la opción Edit > Edit Acceleration

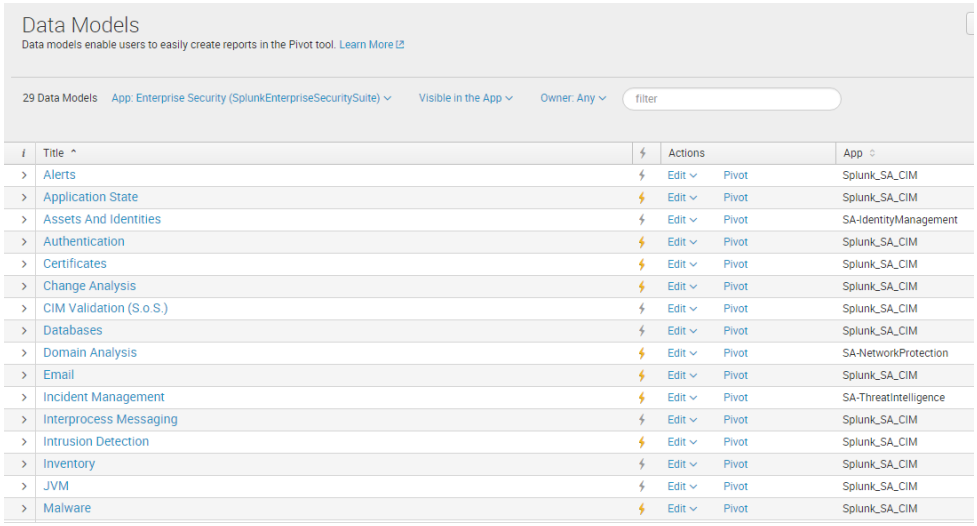

Figura A2.16

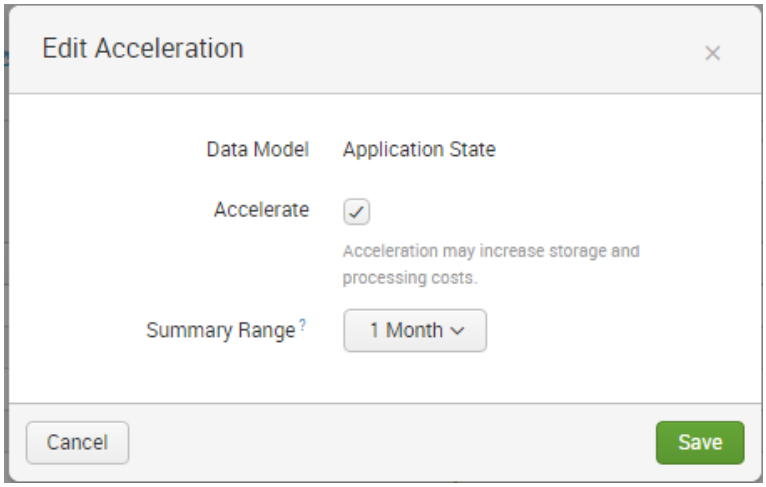

Figura A2.17

Los cambios realizados en las configuraciones serán almacenados dentro del archivo de configuración datamodels.conf, que a su vez está almacenado en la carpeta de la app que lo crea. La mayoría de los modelos que usan el app Splunk_SA_CIM.

El archivo contiene lo siguiente:

```
[Updates]
acceleration = true
acceleration.manual_rebuilds = true

[Web]
acceleration = true
acceleration.manual_rebuilds = true

[Performance]
acceleration = true
acceleration.manual_rebuilds = true

[Splunk_Audit]
acceleration = true
acceleration.manual_rebuilds = true

[Ticket_Management]
acceleration = true
acceleration.manual_rebuilds = true

[Vulnerabilities]
acceleration = true
acceleration.manual_rebuilds = true

[Application_State]
acceleration = 1
acceleration.manual_rebuilds = 1
```

```
[Authentication]
acceleration = 1
acceleration.earliest_time = -1mon
acceleration.manual_rebuilds = 1

[Certificates]
acceleration = 1
acceleration.earliest_time = -1mon
acceleration.manual_rebuilds = 1

[Change_Analysis]
acceleration = 1
acceleration.earliest_time = -1mon
acceleration.manual_rebuilds = 1

[Network_Traffic]
acceleration = 1
acceleration.earliest_time = -1mon
acceleration.manual_rebuilds = 1

[Network_Sessions]
acceleration = 1
acceleration.earliest_time = -1mon
acceleration.manual_rebuilds = 1

[Network_Resolution]
acceleration = 1
acceleration.earliest_time = -1mon
acceleration.manual_rebuilds = 1

[Malware]
```

acceleration = 1
acceleration.earliest_time = -1mon
acceleration.manual_rebuilds = 1

[Intrusion_Detection]
acceleration = 1
acceleration.earliest_time = -1mon
acceleration.manual_rebuilds = 1

[Email]
acceleration = 1
acceleration.earliest_time = -1mon
acceleration.manual_rebuilds = 1

Para verificar el estado de la aceleración de los modelos de datos, ingresar al app de Splunk Enterprise Security > Audit >Data Model Audit, como se muestra en la figura 2.18.

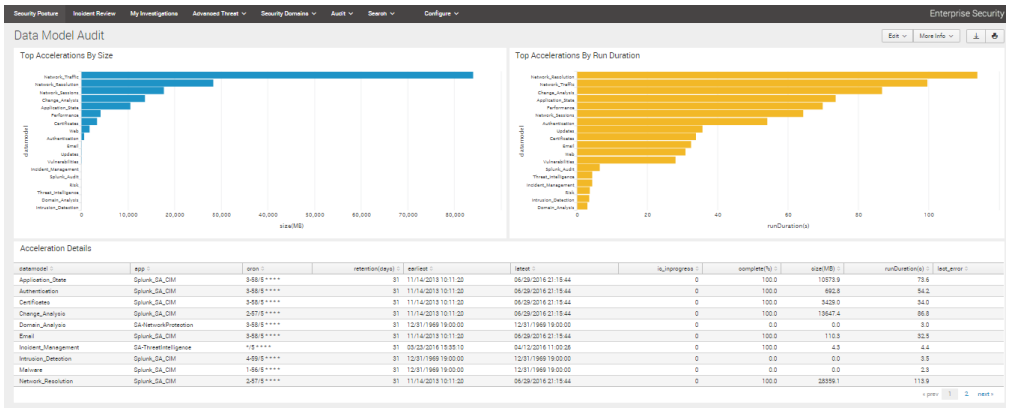

Figura A2.18

Ingreso de Data Personalizada a Splunk Enterprise Security[1]

Para que el ingreso de cualquier fuente de información a Splunk Enterprise Security debe ser los que se denomina CIM Compliant. Que sea CIM Compliant quiere decir que la información que es capturada por Splunk debe cumplir con los estándares de los modelos de datos que vienen con la herramienta. Tener en cuenta que aunque un modelo de dato no haya sido acelerado, la información que entra a ese modelo de datos aun es utilizada para Enterprise Security.

Los modelos de datos que vienen en Splunk Enterprise Security se muestran en la Tabla 31:

Data Model	
Alerts	Application State
Assets And Identities (ES)	Authentication
Certificates	Change Analysis
Databases	Domain Analysis (ES)
Email	Incident Management (ES)
Interprocess Messaging	Intrusion Detection
Inventory	Malware
Java Virtual Machines	Network Resolution (DNS)
Network Sessions	Network Traffic
Performance	Risk Analysis (ES)
Splunk Audit Logs	Threat Intelligence (ES)
Ticket Management	Updates
Vulnerabilities	Web

Tabla 31

Cada modelo de datos contiene una serie de campos que son utilizados por Enterprise Security. La mayoría de las apps que son creadas por Splunk y se encuentran en Splunk.base.com son compatibles con los modelos de datos. Para verificar esto se debe revisar a un lado las propiedades del app antes de descargar y verificar si en CIM compatible, como se muestra en la figura A2.19.

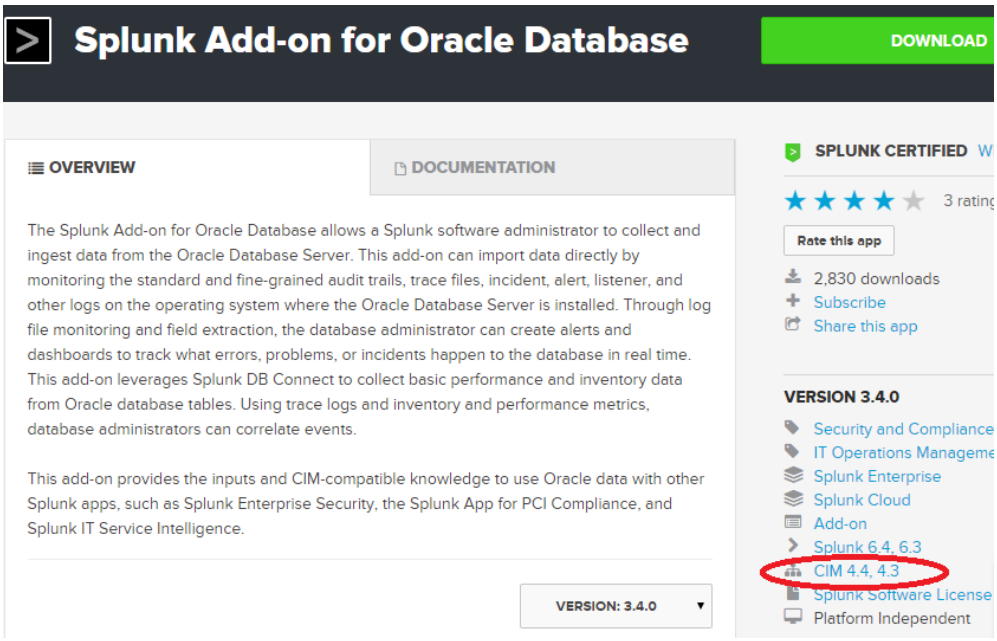

Figura A2.19

Cuando no existe un app, o el app no es compatible, se debe transformar el sourcetype de manera que cumpla con los estándares del modelo al que se requiera incluir la información.

Ejemplo:

En el caso de los dispositivos de red huawei, se hizo para esta información ingrese al modelo de datos de Network Traffic. El modelo de Network Traffic solo permite los campos que se muestran en la Tabla 32:

Campo	Tipo de Dato	Valores Permitidos
Action	string	allowed, blocked,dropped, unknown
App	string	*
Bytes	number	*
bytes_in	number	*
bytes_out	number	*
Cannel	number	*
Dest	string	*
dest_bunit	string	*
dest_category	string	*
dest_interface	string	*
dest_ip	string	*
dest_mac	string	*
dest_port	number	*
dest_priority	string	*
dest_translated_ip	string	*
dest_translated_port	number	*
dest_zone	string	*
direction	string	inbound, outbound,unknown
Duration	number	*
Dvc	string	*
dvc_bunit	string	*
dvc_category	string	*
dvc_ip	string	*
dvc_mac	string	*
dvc_priority	string	*

dvc_zone	string	*
flow_id	string	*
icmp_code	string	*
icmp_type	number	0 a 254
Packets	number	*
packets_in	number	*
packets_out	number	*
Protocol	string	*
protocol_version	string	*
response_time	number	*
Rule	string	*
session_id	string	*
Src	string	*
src_category	string	*
src_interface	string	*
src_ip	string	*
src_mac	string	*
src_port	number	*
src_priority	number	*
src_translated_ip	string	*
src_translated_port	number	*
src_zone	string	*
Ssid	string	*
Tag	string	*
tcp_flag	string	SYN, ACK, FIN, RST, URG, PSH.
transport	string	tcp, udp, unknown
Tos	string	*

Ttl	number	*
User	string	*
user_bunit	string	*
user_category	string	*
user_priority	string	*
vendor_product	string	*
Vlan	string	*
Wifi	string	*[2]

Tabla 32

Se deberá tomar un grupo de logs e identificar que valores son válidos para que sean utilizados por el modelo de datos.

A partir de esto se modifica el props.conf y tranforms.conf para que se ajuste al modelo de datos.

props.conf

```
[huawei_firewall]
SHOULD_LINEMERGE = false
TRUNCATE = 1000
TIME_PREFIX = ^
TIME_FORMAT = %FT%T%z
MAX_TIMESTAMP_LOOKAHEAD = 25
SEDCMD-0 = s/\.$//

EXTRACT-0 = interzone-(?<src_zone>\w+)[^-]+-(?<dest_zone>\w+)\S+
(?<direction>\w+)
REPORT-0 = huawei_firewall
FIELDALIAS-00 = source_ip as src
FIELDALIAS-01 = source_ip as src_ip
FIELDALIAS-02 = source_port src_port
```

FIELDALIAS-03 = destination_ip as dest
FIELDALIAS-04 = destination_ip as dest_ip
FIELDALIAS-05 = destination_port as dest_port
LOOKUP-0 = cnel_huawei_vendor_product sourcetype
LOOKUP-1 = cnel_huawei_firewall_actions category_sub
LOOKUP-2 = cnel_huawei_transports number as protocol

transforms.conf
[cnel_huawei_vendor_product]
filename = cnel_huawei_vendor_product.csv

[cnel_huawei_firewall_actions]
filename = cnel_huawei_firewall_actions.csv

[cnel_huawei_firewall_traffic_actions]
filename = cnel_huawei_firewall_traffic_actions.csv

[cnel_huawei_transports]
filename = cnel_huawei_transports.csv

[huawei_firewall]
REGEX = ^(?:\S+){4}(?<dvc>\S+) %%\d+(?<category>[A-Z]+)\/\d+\/(?<category_sub>[A-Z]+)
Como se puede apreciar, en el transform.conf tambien se ha utilizado para invocar algunos lookups. Los lookups deben almacenarse dentro de la carpeta lookups al mismo nivel de donde está la carpeta local, como se muestra en la figura A2.20

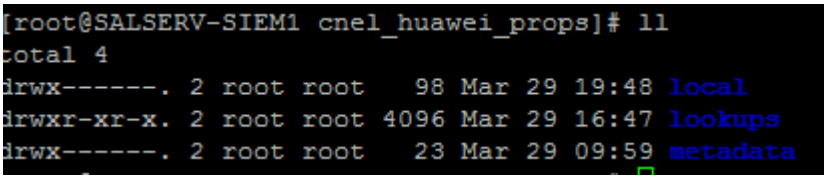

Figura A2.20

Los lookups en este caso nos van a servir en los casos que los campos esperan valores predeterminados. Como por ejemplo el campo action (mirar los valores predeterminados en la tabla superior)

cnel_huawei_firewall_actions.csv
category_sub,action
POLICYPERMIT,allowed
POLICYDENY,blocked
SAPOLICYPERMIT,allowed
SAPOLICYDENY,blocked

La primera columna siempre va a contener el nombre de los campos. La primera fila se referirá a los valores que se encuentran en el log original, y la segunda fila es el valor que el modelo de datos está esperando.

Una vez concluida la transformación del log, para que sea compatible con los modelos de datos, se debe crear un eventtype para que incluya la información nueva que hemos transformado. Dentro de nuestra carpeta local creamos el archivo eventtypes.conf con la siguiente información:
eventtypes.conf
[huawei_network_traffic]
search = index=huawei sourcetype=huawei* category_sub=*POLICY* OR category_sub=TRAFFIC

Luego se debe incluir un tag para que el modelo de datos, de ahora en adelante, tome la nueva fuente de datos. Cada modelo de datos tiene especificado cuales son los tags, que se requieren para incluir nuevos datos.
Para conocer cuáles son los tags correspondientes al modelo de datos Network Traffic, ir a Settings > Data Models > Network Traffic y verificar en la descripción los tags, como se muestra en la Figura A2.21.

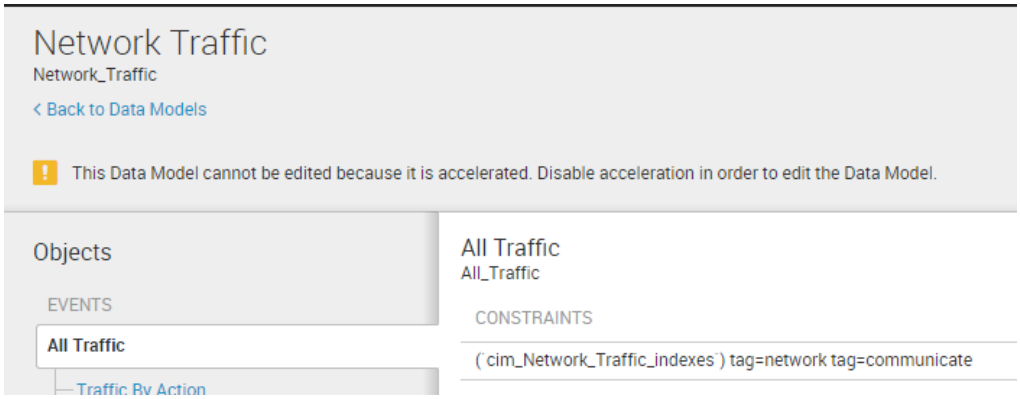

Figura A2.21

En este caso los tags son network y comunícate.

Para crear los tags a la información que acabamos de formatear dentro de la carpeta local se crea un archivo tags.conf con la siguiente información:

tags.conf

[eventtype=huawei_network_traffic]

network = enabled

communicate = enabled