Contents

Seguridad y Gestión del Riesgo en Redes Definidas por Software

Consideraciones sobre la Seguridad en la Infraestructura de Redes SDN.

Fogelbach, Rudiger
rudigerfo@gmail.com
Universidad Don Bosco

García, Melvin A.
melvin.garcia.ardon@gmail.com
Universidad Don Bosco

Gonzalez, Guillermo D.
gda.gonzalez@gmail.com
Universidad Don Bosco.

***Resumen*— La infraestructura de red siempre ha evolucionado en la medida que es requerido por los usuarios y organizaciones que las utilizan. El Internet de las Cosas (IoT) como consecuencia de la consumerización de TI ha demandado una escalabilidad, programabilidad e innovación que la infraestructura de redes convencionales no ha logrado suplir de manera eficiente. Las redes definidas por software (SDN) han surgido como un modelo y arquitectura que puede cumplir con dichas características. Pero se debe tomar en cuenta que la gestión de la seguridad de la información deberá incluir nuevas consideraciones para asegurar dicha infraestructura.**

Keywords*— *Gestión de la seguridad de la información, gestión del riesgo de TI, redes de datos, redes definidas por software, seguridad definida por software, seguridad en redes.

I. INTRODUCCIÓN

Las organizaciones, que mantienen infraestructura de red de gran escala, siguen en busca de arquitecturas que cumplan los requerimientos de las nuevas tendencias tecnológicas. Las redes definidas por software como tecnologías de la información y comunicación se han vuelto un tema de interés que genera grandes expectativas con respecto al cumplimiento de las estrategias organizacionales. Algunos fabricantes y organizaciones han implementado una arquitectura de red definida por software en los ambientes de centros de datos, de igual manera se empieza a incursionar dentro de las arquitecturas de redes perimetrales donde la seguridad definida por software muestra paradigmas interesantes. También se identifican oportunidades para SDN dentro de infraestructura de redes empresarial, en las cuales se busca una reducción de costos operativos y de capital en lo que respecta a la inversión de nueva infraestructura.

El impacto que SDN implica para la seguridad de la información ha sido dimensionado de una manera aislada en varios casos dejando fuera, del Sistema de Gestión de la Seguridad de la Información, el diseño e implementación de dicha infraestructura. El acercamiento desde la perspectiva de la seguridad de la información sobre el diseño e implementación de redes convencionales ha sido llevado en conjunto en la mayoría de los casos por los fabricantes y gestores de la seguridad dentro de las organizaciones, más aún cuando se trata de soluciones de seguridad en la red. Surgen diversos conceptos relacionados a innovaciones tecnológicas como Internet de la Cosas (IoT), Centros de Datos Definidos por Software (SDDC), Infraestructura como servicio (IaaS), Plataforma como Servicio (PaaS), Software como Servicio (SaaS), Computación en la nube y virtualización las cuales son tecnologías que se ven en una u otra medida relacionadas a redes SDN.

En esta tesina se busca inicialmente crear un marco conceptual que cubra una línea base de conocimiento que se debe tener como líderes de la estrategia de TIC, para fortalecer los beneficios que SDN puede traer a las organizaciones. Adicionalmente se busca generar un entendimiento de la arquitectura y componentes que vienen embebidos dentro de SDN para luego entrar en materia de seguridad de la información presentando conceptos como Seguridad Definida por Software (SDS) del cual SDN se ha visto muy beneficiado a nivel de arquitectura, aun no teniendo muchas implementaciones documentadas. Finalmente se busca llevar un acercamiento con respecto a la gestión de la seguridad de la información, que pueda contribuir a las organizaciones a tener una visión más clara dentro de un SGSI para el diseño e implementación de SDN.

II. HISTORIA Y EVOLUCIÓN DE LAS REDES DE DATOS.

A. Reseña historica de redes de datos.

La comunicación ha sido protagonista para la historia de la humanidad, el ser humano se ha ido desarrollando y evolucionando en muchos aspectos con lo que ha contribuido a que la información y las comunicaciones sean un pilar fuerte dentro de este desarrollo.

Nos podemos remontar al siglo XIX [1] que fue cuando se dio origen a las redes de comunicaciones, esto se produjo en los países de Suecia y Francia a principios del siglo mencionado. Con el llamado "Telégrafo Óptico" se dio paso a que los medios telegráficos y telefónicos fueran los principales medios de transmisión a nivel mundial.

Los primeros intentos de transmitir información digital fueron en los años 60 [1], que es cuando comienza la verdadera historia de la red con el establecimiento de las "redes de conmutación de paquetes", que se refiere a la fragmentación de los mensajes que una vez en el destino se ensamblan. Esta "conmutación de paquetes" a través de switches digitales se contrapone a la "conmutación de circuitos" que actuaban mediante switches físicos.

Advanced Research Project Agency (ARPA) como parte del Departamento de Seguridad de Estados Unidos impulsó el desarrollo tecnológico, esto sucedió en el año 1957 [2] al conocer la conmutación de paquetes, pues antes solamente se realizaban pruebas en el Reino Unido y Francia con las cuales se llegaron a crear redes privadas.

La primera red experimental de conmutación de paquetes se usó en el Reino Unido, en los National Physics Laboratories; otro experimento similar lo llevó a cabo en Francia la Societè Internationale de Telecommunications Aeronautiques. Hasta el año 69 esta tecnología no llegó a los Estados Unidos, donde comenzó a utilizarla el ARPA, o agencia de proyectos avanzados de investigación para la defensa. Más delante de la ARPANET surgió la MILNET, red puramente militar, aunque tiene pórticos que la unen a la Internet. ARPANET se convirtió en la columna vertebral de la red, por donde tarde o temprano pasaban todos los mensajes que se dirigen a la Internet [1].

Luego de la evolución de ARPANET, que abarca la primera y segunda generación de la comunicación, nos encontramos con la Tercera Generación que se puede catalogar como la de la "Movilidad" conocida por "Internet de las Personas", continuando por el "Internet de las Cosas" hasta la actualidad, que es considerado como una "Internet Ubicua" o "Internet de Todo", con un gran sistema de cómputo distribuido que soporta el crecimiento o evolución de las tecnologías.

A través de todos los servicios y avances que se conoce como Cuarta Generación, en donde tienen cabida las tecnologías de Virtualización, Cloud Computing y SDN (Software Defined Network), se marca un nuevo horizonte, el cual nos llevará hasta la siguiente etapa de la evolución donde se globalizará y socializará el conocimiento: "La Sociedad del Conocimiento".

B. Internet de la cosas (IoT – Internet of Things)

Hoy en día, el Internet de las Cosas (IoT, por sus siglas en inglés) tiene un gran impacto en la tecnología y las telecomunicaciones, pues del internet actual hacia los cambios que se presentan en esta arquitectura se denota que sufrirá una gran transformación hacia lo que será el Internet del Futuro (FI, según sus siglas en inglés)

IoT abarca un amplio conjunto de tecnologías, hardware y aplicaciones de software cuya rápida evolución y amplio alcance pueden atribuirse a la inclusión de muchas tecnologías maduras existentes como las redes inalámbricas de sensores, RFID y una amplia variedad de soluciones personalizadas y dispositivos inteligentes más nuevos.

La automaticidad permite a los dispositivos actuar de forma independiente, los modelos arquitectónicos que abordan los desafíos como la escalabilidad, distributividad, interoperabilidad y capacidad de programación son la necesidad del ahora.

El Internet de las Cosas representa una gama de dispositivos con alimentación de poder restringida, esencialmente con una conexión a Internet que no requiere altos anchos de banda. La mayoría de estos dispositivos son soluciones personalizadas que inicialmente no fueron diseñados para trabajar en Internet. Adaptar el protocolo IP en dichos sistemas heredados puede ser técnicamente factible y económicamente no-viable; imagine dispositivos que usamos todos los días que tienen inteligencia integrada y son capaces de conectarse a Internet; si esto sucede, podrían ser gestionados desde cualquier lugar en cualquier momento.

La diversidad de los dispositivos móviles en la IoT nos lleva por un flujo lógico a la adopción de la "computación en la nube" por el uso masivo de sensores inteligentes que demandan más recursos y prácticamente esta tecnología tiene un enfoque de conectar cualquier cosa a la internet que es necesaria para hacer frente a los requisitos de gestión distribuida.

El IoT nos brinda nuevas oportunidades y nuevos desafíos, la arquitectura actual es esencialmente basada en conceptos que nacieron en la década de 1950 [3]. Por lo tanto, la arquitectura de redes actual se vuelve compleja y poco flexible, considerándose no escalable para futuras necesidades.

En la actualidad, múltiples profesionales como investigadores, fabricantes y entidades trabajaron en una nueva arquitectura basada en patrones abiertos. Estos nos ofrecen mejoras al ser menos complejos, más flexibles y económicos. Este desarrollo fue creado bajo el concepto de "Redes Programables"

El nuevo mundo del IoT trae complejidad a las redes actuales, que son las redes de misión crítica que precisamente dependen de cuatro factores: disponibilidad, agilidad, flexibilidad y seguridad. Como se puede observar estos cuatro factores tienen una alta relación con la arquitectura de patrones abiertos, pues a estas redes se les llama "Redes de Sensores" y/o "Redes de comunicación entre máquinas" (M2M). Justo aquí es donde se da origen al internet de las cosas (IoT).

En una red convencional el paquete es tratado según el firmware del propietario, cuestión que mantiene con el poder, el dominio y el control de contratación de soporte a las empresas, todos los paquetes son tratados exactamente de la misma manera en una red de estas. Las redes tradicionales que están basadas en protocolos propietarios "aparentemente" abiertos no están preparadas para situaciones críticas de constante cambio y tendrán que adaptarse a este nuevo cambio; cuestión que si es viable con las nuevas tecnologías de IoT.

El auge del IoT, ancho de banda y conectividad han incrementado la complejidad en las redes hasta un punto prácticamente insostenible. Por el crecimiento de ancho de banda, si antes una red tenía cuatro nodos ahora puede tener 4.000. Si esta red de 4.000 nodos requiere 4.000 sistemas de configuración, el grado de complejidad es demasiado grande. Todos los fabricantes vieron que era necesario buscar nuevas estrategias para que la programación no fuera nodo a nodo, sino de una manera centralizada mediante software [4].

Junto con estos beneficios muy reales, sin embargo, hay varias preocupaciones igualmente reales, como la dificultad de aprovisionamiento y mantenimiento de las redes, abordando numerosas amenazas de seguridad para redes.

El IoT posee tres elementos importantes: capacidad, ubicuidad y escalabilidad. La evolución acelerada de los

dispositivos que son cada vez más, permite la interconexión entre el mundo físico y digital, acerca más a que todas las "cosas" se conecten a Internet, lo que permitirá escenarios sin precedentes que marcaran la escalabilidad hacia nuevos límites.

La integración que esto permite, irá alimentando a las aplicaciones de más información relevante, como la información del mundo físico en tiempo real. Esto se vuelve uno de los grandes desafíos para el IoT al crear bases de conocimientos a partir de cantidades enormes de datos en bruto, con lo que se logrará aprovechar la información independientemente del lado que se emite y utilizando de manera más eficiente los recursos.

IoT gestionará en sí, o al menos logrará reducir considerablemente, el grado de la intervención humana requerida. Entre las propuestas que se conocen para reducir la intervención humana en las TIC, existe la denominada tecnología autonómica, esto da lugar a que las funciones del IoT se superpongan con las funcionalidades propuestas por el ciclo autonómico, por ejemplo: el seguimiento, el análisis y la interpretación. Así, la tecnología autonómica parece ser un candidato natural para la gestión del IoT. Sin embargo, el IoT proporciona la información necesaria para alimentar el ciclo autonómico de otros componentes arquitectónicos del FI.

C. Internet de Todo (IoE – Internet of Everything)

La proyección al futuro de IoT brinda inmensas oportunidades, la unión del mundo físico con el digital mejora la experiencia humana y además genera efectividad, baja los costos operativos, soporta la inteligencia entre objetos para sacar mejor beneficios como: ahorro energético, reciclado, optimización de recursos, resultados estadísticos, apoyo para toma de decisiones, interconectividad entre las "cosas", eficiencia y eficacia para nuestro mundo en muchos aspectos.

Sobre dicha proyección a futuro, donde se tienen grandes expectativas de hiper-conectividad de las cosas, se comienza a acuñar el término Internet de Todas las Cosas o Internet de Todo (IoE). Donde todo lo que puede ser modelado para integrarse al mundo digital, tendrá una conectividad a Internet.

En este espacio que se está abriendo se mencionan activos (o cosas) oscuras, que son parte de los activos que actualmente no se encuentran conectados a Internet. Estos activos aunque puedan tener información muy valiosa para las organizaciones y para la sociedad de la información, no generan conocimiento al no estar conectados.

Con IoE se espera tener conectividad de persona, procesos, data, cosas y cualquier activo que pueda aportar información a través de su conectividad, pueda con ello generar conocimiento o, como se especifica dentro de las proyecciones, generar sabiduría.

Aunque en IoT ya se menciona la conectividad de las cosas y de las personas; se vienen sumando procesos y data como cuatro dimensiones separadas. Con IoE se definirá específicamente que estas cuatro dimensiones deberán de estar conectadas entre ellas.

En este momento con las estadísticas actuales, existen varias proyecciones sobre cuantos dispositivos se conectarán al Internet en el 2020 que es cuando se estima que IoE estará en su auge. Cisco Systems (que es la proyección más citada) estima que para este año existirán aproximadamente 50 mil millones de cosas conectadas al Internet.

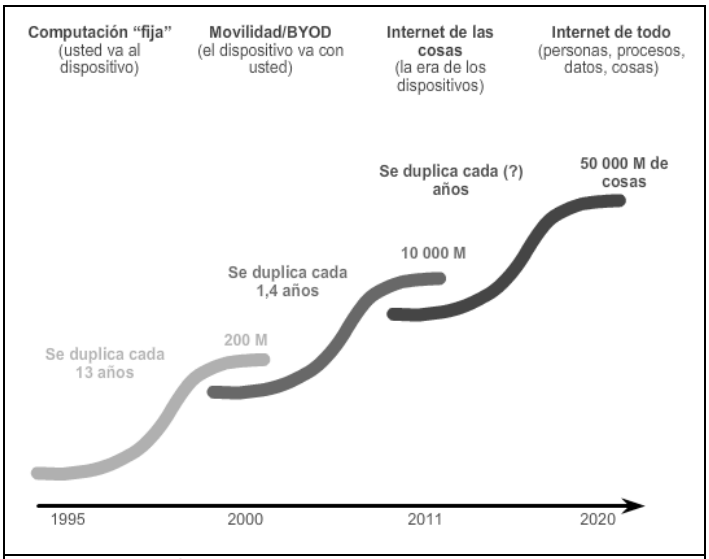

Figura 1. Proyección de cantidad de dispositivos conectados a Internet [5]

Esto se hace en base a las estadísticas que se tiene año con año, donde se calculaba que durante el 2012 existían 8.7 mil millones de objetos globalmente conectados a Internet, y en el 2013 este número excedió los 10 mil millones. [5]

III. COMPUTACION EN LA NUBE E INNOVACION TECNOLOGICA

A. Centros de datos y Virtualización.

Previo a la existencia de los centros de datos como modelo y a todos los componentes que esta reciente forma de despliegue involucra, tales como almacenamiento, procesamiento y memoria, todo esto existía de forma individual y separada en los equipos de los usuarios. Pronto se dieron cuenta que no se trataba de un despliegue escalable, las expansiones en términos de recursos resultaban demasiado costosas. Años más tarde se intentó optimizar este modelo y para cubrir esa creciente necesidad de recursos, se instalaron servidores departamentales los cuales eran básicamente equipos más robustos, centralizados hasta cierto punto y que atendían ahora un entorno más colaborativo.

Sin embargo, esta variante no tardó en mostrar algunas desventajas, se estaba proveyendo ahora un servicio dedicado y se restringía su uso a una forma local. Debido a que se trataba de servidores dedicados, la potencia de cálculo que existía se centraba en su funcionalidad específica como por ejemplo servidores de correo, servidores de base de datos y demás aplicaciones de TI dentro de la organización.

Por otro lado, estos no eran capaces de satisfacer la creciente carga y las necesidades de un entorno cada vez más participativo, por lo que debieron ser migrados a centros de datos centralizados. Esta nueva concepción de los centros de datos resultaba mucho más factible, se mejoraba en gran medida la gestión del hardware y software, lo que permitía que los usuarios compartieran los recursos. Otro factor importante

era el mantenimiento, el cual se tornaba menos costoso en cuanto a tiempo y dinero.

Se habla ahora de un centro de datos moderno creado desde sus orígenes para elementos computacionales físicamente separados, dentro de un entorno cada vez colaborativo y capaz de atender la siempre creciente demanda de almacenamiento y procesamiento, sin olvidar desde luego las redes que interconectan dichos centros con los usuarios finales.

Uno de los mayores aportes en la evolución de esta industria se dio hace no más de 10 años, cuando una compañía llamada VMWare desarrolló una tecnología interesante, que permitía a un sistema operativo anfitrión ejecutar múltiples sistemas operativos clientes como si se tratase de una aplicación más dentro del anfitrión. Básicamente lo que hicieron fue crear un programa que establece un entorno virtual sobre el que se recrea un ambiente informático real (incluyendo todos sus componentes). Ahora se contaba con una aplicación que lucía esencialmente como otra máquina física, ¿podría alguien imaginar todas las facilidades que esto conllevaría?, quizás no inicialmente, pero el tiempo y la necesidad por atender la creciente demanda de recursos nos mostrarían cómo.

Bien, a este programa que realizaba la tarea de gestionar y supervisar el entorno virtual se denominó hipervisor y fue desde entonces que cambió todo en el mundo IT, ya que significó que ahora el software de servidores podría ser desplegado de una manera más fluida, aprovechando mejor el hardware disponible siendo compartido por aplicativos con funcionalidades diferentes. A partir de entonces, los centros de datos han sido capaces de ejecutar una gran variedad de sistemas operativos de acuerdo a los requerimientos específicos de cada aplicativo y todo desde un entorno virtualizado.

Sistemas Operativos como Windows Server que en despliegues anteriores dominaba una máquina física completa, estaba siendo ejecutado ahora como máquina virtual, en paralelo con otras aplicaciones sobre distribuciones específicas a la medida de las necesidades de los usuarios. Otra de las ventajas que el modelo centralizado ofrecía, en especial a los administradores de la red de interconexión, era la posibilidad de ubicar los nodos de procesamiento no basándose ahora en las máquinas físicas disponibles. Esto permitía un crecimiento dinámico guiado por la demanda de recursos, fue entonces que comenzó la era de la computación elástica.

Dediquemos unas líneas a detallar dicho escenario. En el ahora entorno flexible, los departamentos operativos pueden migrar los servidores físicos a cualquier otro lugar dentro o fuera del centro de datos, únicamente pausando la máquina virtual en el que se ejecutan los servicios o copiando el archivo fuente del hipervisor y ejecutarlo desde otra ubicación. Es aquí oportuno señalar lo ventajoso que resulta utilizar esta técnica cuando se elabora un plan de recuperación ante desastres, ya que lograremos disminuir enormemente los tiempos de puesta en servicio y los tiempos de disrupción de los mismos.

Operativamente hablando, esto es posible implementando nuevas máquinas virtuales a partir de la clonación del archivo fuente en el hipervisor y ejecutándolo de forma local o remota como una nueva instancia. Lo mismo ocurre cuando la demanda por recursos de un servicio crece, puede fácilmente ejecutarse una nueva máquina virtual previamente configurada en base a los requerimientos del servicio y asignarse la instancia para formar parte del arreglo. La misma instancia puede borrarse si con el tiempo la demanda cambia su tendencia y decrece. Esta flexibilidad permite a los operadores de red invertir esfuerzos en optimizar la ubicación de los recursos en los centros de datos, tomando como métrica el requerimiento de energía y climatización.

Resulta entonces evidente el ahorro que significa en términos de mantenimiento, los operadores o las organizaciones podrían entonces prescindir de energía y climatización en ciertos sectores de los centros de datos, si una evaluación previa de la utilización indica que no es necesario tener en servicio dichos equipos. Un factor que no era evidente a simple vista, se fue descubriendo a medida que se utiliza esta técnica, la flexibilidad de este modelo que desde sus orígenes la posicionó como el futuro de las redes convencionales se vio comprometida cuando se decidió evaluar su eficiencia operativa, en términos de maximizar la utilización del procesamiento, almacenamiento, energía y climatización.

Es entonces cuando desarrollan la idea de AWS (Amazon Web Services), y era básicamente pre comprar el equipo con antelación en base a una estimación de crecimiento en la demanda y ponerlo a trabajar aunque no se brindaran servicios propios, entonces hicieron uso de la computación elástica para arrendar dicha capacidad y disponer de ella cuando lo requirieran. Es decir que cuando la demanda interna crecía durante un periodo de tiempo, ellos podían desplazar a los clientes de pequeñas capacidades sub arrendadas y disponer de ella para su propio uso. Desde una perspectiva global, el total de los recursos con el que contaban alcanzaría una utilización cercana al 100% por lo que la puesta en servicio de los nuevos equipos estaría rindiendo frutos siempre. Hoy en día se le conoce como servicios de computación elástica y resulta obvio a que se refiere.

El grado de arrendamiento es otro factor que acompaña esta definición y sencillamente hace referencia a que tanto de la aplicación está siendo compartida. Años más tarde esta definición fue revisada por notables arquitectos de soluciones en la nube y vieron a bien establecer ciertas arquitecturas comunes:

a) Infraestructura como Servicio (IaaS). Infraestructura (cómputo, almacenamiento, red) son compartidos.

b) Plataforma como Servicio (PaaS). Un entorno de desarrollo de aplicaciones es compartido.

c) Software como Servicio (SaaS). Una aplicación es compartida. [6]

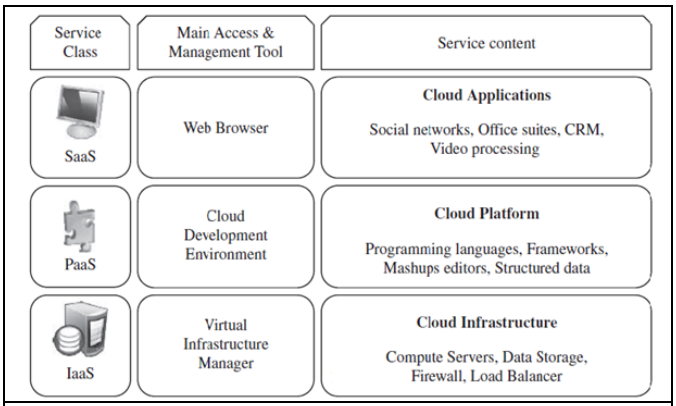

Figura 2. Clase de Servicio [6].

B. Centro de datos definido por Software (SDDC).

Los centros de datos son ahora una de las partes más importantes para las diferentes organizaciones que todavía requieren de manejar una infraestructura propia. Esto requiere que se tenga un nivel de innovación dentro de esta misma infraestructura que esté acompañada por una escalabilidad sin precedentes que requiere mayores niveles de automatización cuando se refiere al crecimiento de la infraestructura.

Los Centros de Datos Definidos por Software se consideran el conjunto de componentes o infraestructura compuesta por el equipo de cómputo, almacenamiento, red y recursos de seguridad que facilitan la implementación rápida y automatizada de servicios utilizando tecnologías de virtualización [7].

Independientemente del tipo de arquitectura que se utilice en las SDN aún se requieren características básicas de conectividad que siempre se han utilizado en las redes de los centros de datos, entre ellas: la segmentación de dominios de broadcast, habilitación de redundancia sin generar enlaces cerrados de reenvío, conectividad, seguridad entre los segmentos de red separados y otros mecanismos más avanzados de seguridad. Por lo que los conceptos que se utilizaban en los centros de datos sobre redes convencionales como: VLAN, agregación de enlaces, Spanning-tree, IP routing, monitoreo de tráfico no deseado son aún elementos o servicios que son requeridos de la infraestructura de red, ya sea virtual, SDN o convencional.

C. Arquitecturas de modelo de servicio en la Nube..

El Cloud Computing se ha vuelto ya una tendencia y presenta una rápida evolución. Ha significado durante los últimos años un cambio importante en la forma en la que se almacenan y ejecutan las aplicaciones ya que posibilita el autoservicio bajo demanda. Cloud Computing proporciona una infraestructura eventualmente ilimitada para almacenar y ejecutar datos y programas, los clientes no necesitan tener su propia infraestructura, únicamente un acceso web.

Iniciemos delimitando los principales modelos de despliegue:

1) Nube Privada. La infraestructura de esta solución sólo opera para una organización y esta puede ser administrada por la organización misma o una tercera parte. Su existencia no se limita de una forma local, pudiendo presentarse fuera de la organización.

2) Nube Comunitaria. Hace referencia a una infraestructura compartida entre varias organizaciones y alberga a una comunidad en específico cuyos intereses comunes son la razón de dicho despliegue. Esta puede ser administrada por las organizaciones involucradas o una tercera parte de común acuerdo. Su existencia se rige de igual forma, local o fuera de ellas.

3) Nube Pública. Es aquella en la que la infraestructura se encuentra disponible al público en general o a un segmento específico y básicamente pertenece al operador que vende los servicios de cloud.

4) Nube Híbrida. Compuesta por dos o más nubes de cualquier tipo, con la particularidad que resulta única para las entidades que participan y se limitan una a la otra. La operación de portabilidad de datos o aplicaciones dentro de esta infraestructura se designa a tecnología propietaria.

D. Software Como Servicio (SaaS).

El modelo más conocido y el servicio líder de adopción más generalizado de cómputo en la nube ha sido SaaS. En un modelo SaaS un operador provee una aplicación para ser usada o comprada bajo demanda. Se puede acceder a las aplicaciones a través de varios clientes (buscadores web, teléfonos móviles, etc.) por los usuarios o clientes. Las aplicaciones no requieren la instalación de un cliente como contraparte, únicamente un buscador u otro agente con conectividad de red. Son varios los factores que contribuyeron al crecimiento en la demanda de este tipo de modelo, entre ellos el acceso generalizado a internet, el incremento en las velocidades de las conexiones, los cortos tiempos de respuesta de las aplicaciones, entre otros.

Pequeñas y medianas empresas están dispuestas a comprar software como servicio y las más solicitadas son: ERP (Enterprise Resource Planning), CRM (Customer Relationship Management) que previamente sólo estaban disponibles en el modelo tradicional de entrega y enfocado solo a grandes compañías. Las licencias tradicionales de software se convirtieron en un punto clave para la reducción de costos incluyendo los subsecuentes gastos en mantenimiento, actualización, operación, etc.

Como cualquier tecnología nueva, un modelo SaaS sufre algunas limitaciones. Uno de los principales retos con las aplicaciones dentro un entorno SaaS es la integración. Las aplicaciones en SaaS típicamente proveen servicios para un área de negocio, como por ejemplo un ERP. Como resultado las compañías están enfrentando serios problemas con la precisión de los datos, la previsión y los procesos de negocio automatizados en donde los datos en tiempo real son requeridos. Algunos proveedores de soluciones SaaS han afrontado el reto de integración desarrollando interfaces de programación de aplicaciones (APIs). Desafortunadamente acceder y gestionar los datos a través de un API requiere cierta codificación y mantenimiento ya que estas interfaces a menudo requerirán modificaciones y actualizaciones. Por otra parte los

APIs han demostrado tener algunas limitaciones, por ejemplo, algunos APIs de servicios web no soportan transacciones multi-registros, lo que significa que la integración de código debe manejar esta lógica.

Otro de los retos que se debe afrontar está relacionado a la ubicación de los datos. Recordemos que los clientes de soluciones SaaS utilizan las aplicaciones para procesar su información de negocio. El problema es que el cliente no conoce donde será almacenada esta información. Debido a normativas de privacidad en varios países, la ubicación de la información es muy importante como parte de la arquitectura de la organización. Por ejemplo, en muchos de los países de la Unión Europea y Sudáfrica, algunos tipos de información no pueden dejar el país, debido al nivel de sensibilidad de esta.

E. Plataforma como servicio (PaaS)

La diferencia más notable entre un modelo SaaS y uno PaaS es que el primero de estos solo organiza aplicaciones completas en la nube mientras que PaaS ofrece una plataforma para ambos tipos, hablamos que existe lugar para aplicaciones en progreso y para completadas o en producción. Aún y cuando se trata de una solución más completa, en el mercado actual todavía se presenta en etapas iniciales. Ciertamente esta resulta una ventaja competitiva en momentos como el actual que presenta una evolución tecnológica tan acelerada y que requiere poner en servicio una aplicación en cortos periodos de tiempo.

PaaS ofrece un ambiente en el que los desarrolladores pueden crear e implementar aplicaciones y en donde no necesariamente estén interesados en conocer cuanta memoria o cuantos procesadores serán requeridos para ejecutar la aplicación. Además pueden ofrecerse múltiples modelos de programación y servicios especializados (como por ejemplo: acceso a la información, autenticación, etc.) como bloques para las nuevas aplicaciones. Un modelo PaaS provee a los desarrolladores un servicio que puede ser usado como un gestor completo del ciclo de desarrollo de software, abarcando desde la planeación hasta el diseño y construcción, lo cual soporta todas las etapas de desarrollo, prueba y mantenimiento.

Las mayores ventajas de un modelo PaaS es que ofrece escalabilidad automática, balanceo de carga y alta tolerancia a fallas. El almacenar información en la nube provee escalabilidad y alta disponibilidad para aplicaciones web pero no soporta consultas complejas. Los desarrolladores deberán entonces diseñar sus programas de acuerdo a estas peculiaridades de NoSQL.

En un modelo PaaS el proveedor entrega cierto control a los desarrolladores para que logren construir aplicaciones por encima de la plataforma, pero ninguna seguridad bajo el nivel de la aplicación como forma de prevenir intrusión a través de la red. Este control aún se establece como un objetivo a futuro para los proveedores de esta solución. Todos los demás detalles son abstractos de cierta manera a los ojos de los desarrolladores. La desventaja de PaaS es que este nivel de abstracción puede beneficiar a los atacantes cuando deciden ejecutar acciones contra la solución.

F. Infraestructura como Servicio (IaaS)

La capa de infraestructura se enfoca en habilitar tecnologías. El modelo IaaS cambia la manera en el que los desarrolladores implementan sus aplicaciones. En lugar de consumir tiempo con sus propios centros de datos o gestionar compañías de hosting, ellos pueden solo seleccionar uno de los proveedores de soluciones IaaS, obtener un servidor virtual, utilizarlo por algunos minutos y pagar únicamente por los recursos que utilizaron. Desde un punto de vista tecnológico el modelo IaaS ha sido el más satisfactorio. En el modelo IaaS, los clientes en la nube usan directamente componentes de infraestructura (almacenamiento, firewalls, redes y otros recursos computacionales) ofrecidos por el proveedor en la nube. La virtualización es la técnica ampliamente utilizada a fin de proveer recursos a la medida de la demanda de los clientes.

La idea básica de la técnica de virtualización es que los recursos de una computadora física puedan ser particionados en recursos lógicos y re-organizados en múltiples máquinas virtuales. Por ejemplo, los sistemas operativos pueden ser establecidos para ejecutarse de forma múltiple, virtualizando imágenes para correr simultáneamente a fin de maximizar la eficiencia. Las redes también pueden virtualizarse, así el ancho de banda disponible puede ser particionado en canales separados, reduciendo la complejidad de la red y mejorando la capacidad de gestionar la red completa. La virtualización de almacenamiento permite la puesta en común de muchos recursos de almacenamiento así toda la capacidad disponible es asignada y gestionada de forma centralizada. [8]

IV. REDES DEFINIDAS POR SOFTWARE

A. Antecedentes de las redes SDN.

En los tiempos en que se iniciaba el desarrollo del Internet y de las grandes redes corporativas la descentralización, desde el punto de vista de diseño de red, se fue convirtiendo en algo deseable. De cierta manera el mantener una infraestructura descentralizada genera tolerancia a fallas, pudiendo aislar problemas específicos a un punto o sector determinado de la infraestructura de la red. De igual manera este acercamiento dentro del diseño de redes resultó conveniente desde la perspectiva del rendimiento de la red, obteniendo rápidos aumentos de anchos de banda y densidad de puertos adicionando dispositivos independientes.

Pero a pesar de las ventajas, también se fue determinando que las redes y su arquitectura se vuelven más complejas y rígidas. Aunque esta complejidad y rigidez realmente se marcaban dentro de la lógica de control y la administración de la red, cuando la red escala o incrementa su capacidad, la configuración y administración se ven sujetas a fallas como parte misma de la gestión y configuración.

Adicionalmente se demarca una falta de innovación con respecto a las redes de datos convencionales. Esto debido a que los planos de control y administración están sujeto a la investigación y desarrollo que realizan un número determinado de fabricantes que aun utilizando soluciones abiertas, ofrecen soluciones con un hardware que no se podía desacoplar del sistema operativo ya que formaban parte de un solo equipo,

incluyendo en algunas ocasiones un software de control especializado para la administración y configuración de los equipos de red, conformando todo esto por un único y simple elemento que se requería dentro de la infraestructura de red.

Desde otra perspectiva, la falta de innovación no necesariamente se generaba por la utilización de protocolos cerrados o propietarios que podría generar problemas de interoperabilidad entre distintos fabricantes, ya que todos los fabricantes utilizan también protocolos abiertos con los que se pueden mantener la interoperabilidad de los elementos siendo aún de distintos fabricantes. Es la perspectiva financiera donde se genera un detrimento inherente a la innovación, ya que dentro de las organizaciones se deben de manejar ciclos de retorno de mayor plazo cuando buscan cubrir los costos de capital y costos operativos dentro de un nuevo proyecto de renovación, mejora o reemplazo de la infraestructura de red.

Finalmente esta falta de innovación resulta en una red que requiere de equipos cada vez más especializados para administrar, aplicar y ejecutar políticas de red y políticas de seguridad que cubran las necesidades de las organizaciones. Resultando en la adición de equipos de hardware y software cada vez más especializados para reforzar las mismas políticas de red y seguridad. Es en este punto donde la infraestructura de red crece adicionando equipos cortafuegos (firewalls), sistemas de prevención o detección de intrusos (IDS/IPS), balanceadores de carga u optimizadores de tráfico WAN. Teniendo cada uno de estos equipos su propia unidad de procesamiento física, un sistema operativo y aplicaciones correspondientes.

Por todas las desventajas que se van encontrando, comenzaron muchos detractores de las redes convencionales, a buscar nuevas formas de implementar las redes de datos. La primera visualización que se tenía, es que todo el poder de procesamiento y decisiones de reenvío que se manejaba de manera individual en cada equipo se podría centralizar, reduciendo significativamente los costos de implementación, de operación y mantenimiento, teniendo dispositivos más económicos únicamente para el reenvío que no requerían un poder de procesamiento alto ya que este se contenía y manejaba en un plano de control centralizado.

Los primeros pasos que se dieron en esta dirección los tomaron dos ingenieros de Standford desarrollando el protocolo Open-Flow que posibilitó inicialmente la separación del reenvío de la data y el control de dicho reenvío. Este protocolo que se desarrolló como un protocolo abierto fue retomado por la ONF (Open Networking Foundation) que fue fundada por un conglomerado de organizaciones, las cuales se definieron finalmente como la autoridad de estandarización de Open-Flow y que busca finalmente proveer un soporte comercial a dicho protocolo y sus tecnologías inherentes de implementación.

B. Definiciones generales de SDN.

Las redes de datos o redes de computadoras pueden ser divididas en tres planos de acuerdo a su funcionalidad. El plano de datos, el plano de control y plano de administración (o gestión). Esta separación se puede determinar de acuerdo a las diferentes funciones que cada plano sostiene.

El primer plano, que se define como el plano de data, realmente se podría denominar el plano de envío o reenvío, ya que es en este paso donde efectivamente se conmutan los datos (tramas, paquetes, datagramas) transmitiéndoles a través de la red desde un nodo hacia otro. El segundo plano, el plano de control, representa realmente los protocolos que son utilizados para poder alimentar las diferentes tablas de enrutamiento o reenvío que se utilizan finalmente en el plano de datos. Finalmente el tercer plano, plano de administración; es donde se incluye cualquier servicio basado en software que se utiliza para administrar o configurar remotamente la funcionalidad del plano de control

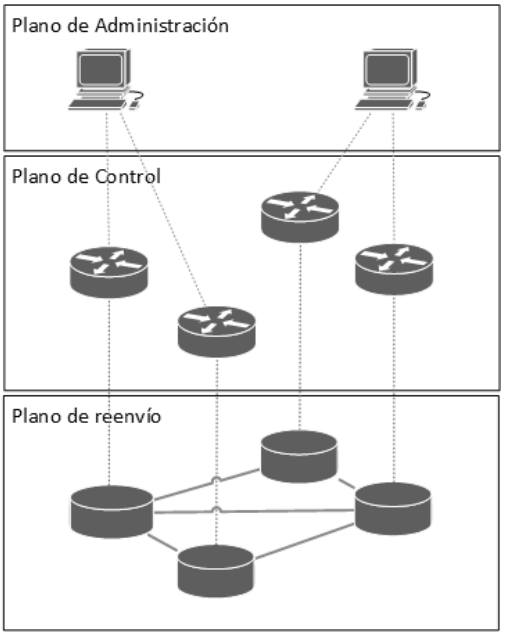

Figura 3. Funcionalidad de planos de red

[6] Definen inicialmente SDN como un acercamiento arquitectural que optimiza y simplifica la operación de las redes entrelazando la interacción entre las aplicaciones, los servicios y dispositivos de red. Siendo esto de cierta manera independiente de la implementación, refiriéndose a ambientes físicos o virtuales, pero siempre considerando un equipo centralizado orquestador que realiza las mediaciones y facilita las comunicaciones entre los dispositivos o elementos de red que requieren interactuar con las aplicaciones y aplicaciones que requieren interactuar con los elementos de red.

Dentro de esta definición caben sin duda muchos conceptos que forman, de cierta manera, parte de SDN, pero que desde hace un tiempo muchos fabricantes han venido acuñando como términos o como técnicas de diseño o incluso como formas de ofrecer nuevos servicios. Entre estos podemos mencionar conceptos como redes programables, redes virtuales, redes inteligentes, redes orientadas al servicio, redes orientadas al contenido entre otros términos que finalmente se pueden o no reducir a una infraestructura de red que independientemente de la arquitectura provee una conectividad entre dispositivos que

finalmente permite el nacimiento de la sociedad de la información.

Por otro lado, [9] buscan definir sin tanta ambigüedad lo que se debería de entender cómo una red definida por software, resultando como conclusión no una definición específica sino cuatro características básicas que se pueden encontrar en toda red SDN.

1) Los planos de control y data se separan.
La funcionalidad de control es removida de los dispositivos de red, el cual se convierte en un elemento de reenvío de datagramas (plano de datos)

2) Las decisiones de reenvío se realizan en base a flujos y no en base a destinos.
El flujo es definido de manera general por un conjunto de valores dentro de los campos (específicos de los encabezados) de las tramas, paquetes o datagramas y por un conjunto de acciones o instrucciones respectivamente. Dichos valores esperados en los campos de un encabezado determinado son los que conforman el criterio de filtro para la toma de decisiones de reenvío.

3) La lógica de control se mueve a una entidad externa.
Dicha entidad se puede denominar controladora SDN o Sistema Operativo de Red (NOS, Network Operating System). Dicha controladora es una plataforma de software que opera sobre un hardware de servidor (físico o virtual), que provee los recursos y abstracción esencial para facilitar la programación o configuración de los equipos de reenvío o conmutadores considerando una perspectiva de una red abstracta y centralizada a nivel lógico. Su propósito finalmente no difiere mucho del de cualquier sistema operativo.

4) El software de aplicación que opera sobre el Sistema Operativo de Red (NOS)
Es lo que convierte a la red en una red programable, que finalmente interactúa directamente con los dispositivos del plano de data.

De las cuatro características anteriores, la última resulta una de las características fundamentales de una red SDN. Pero en su totalidad todas las características ofrecen varios beneficios a nivel operativo, de diseño y escalabilidad dentro de la infraestructura de red. Incluso ONF define dichas características como parte del desarrollo e implementación de Open-Flow.

Específicamente en la centralización de la lógica de control, se obtiene una simplificación de las modificaciones de las políticas de la red, que la hace incluso menos propensa a errores. Adicionalmente un programa de control puede generar reacciones de acomodación a cambios como falsos positivos sin modificar o dejando intactas las políticas de alto nivel. Además, en base a la centralización de la lógica de control, también se puede considerar que en dicha controladora se contiene información o conocimiento global de la red de datos, que finalmente contribuye al desarrollo de funciones servicios y aplicaciones de red más sofisticadas.

Adicionalmente [9] definen la existencia de tres abstracciones fundamentales (no características) de una red SDN que bajo cualquier arquitectura que se busque implementar se mantienen.

1) Abstracción de Reenvío (conmutación)
La abstracción de reenvío debería de permitir cualquier comportamiento de reenvío (enrutado o conmutado) de acuerdo a lo especificado por la controladora o el programa de control dentro de la aplicación de la red. Para esto, OpenFlow resulta la herramienta o forma de dicha abstracción de reenvío, considerando OpenFlow como un driver de un dispositivo dentro de un sistema operativo. Donde dicho Sistema Operativo se consideraría la aplicación dentro de la controladora (Plano de Control) y el dispositivo se consideraría el equipo de reenvío (Plano de Data)

2) Abstracción de Distribución.
Esta abstracción específicamente contribuye a que el problema de un control distribuido se vea como un problema lógicamente centralizado. En este caso, en esta abstracción se da origen a la controladora, que inicialmente debe de aplicar los comandos de control que los dispositivos de reenvío ejecutan, como también se debe de encargar de la recolección de información de estados de los dispositivos de reenvío, tanto de los enlaces como los dispositivos de red en sí.

3) Abstracción de Especificación.
Esta abstracción, define el comportamiento de la red esperado que es aplicado por la sistema operativos de la red (NOS) o por la aplicación de la red. Esto se logra a través de los mismos lenguajes de programación de la red que abstraen las configuraciones que la misma aplicación realiza sobre un modelo de red resumido y simplificado, concluyendo en una configuración física para la misma red que es vista globalmente por la controladora SDN.

En la siguiente figura, se ven los planos y su abstracción implícita que menciona Kreutz.

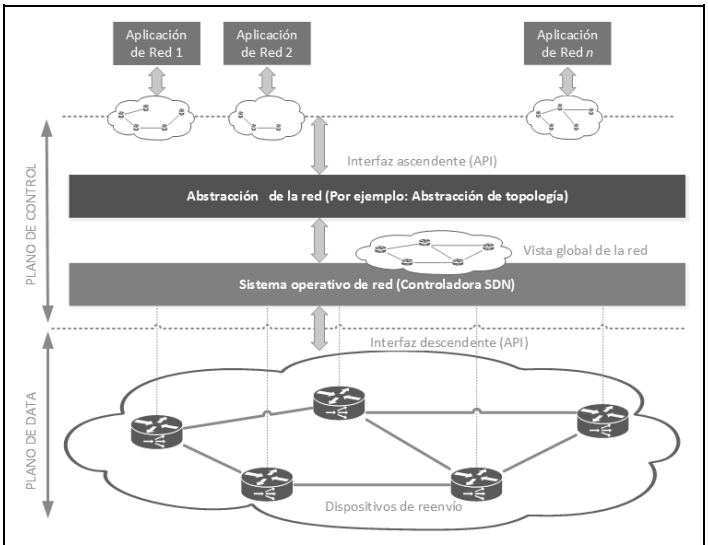

Figura 4. Abstracciones Fundamentales de la arquitectura de SDN.

Considerando que SDN finaliza la conjunción que se ha mantenido durante años del plano de control y el plano de data, que ha convertido la innovación y mejoras en la red en algo prácticamente imposible, se puede ver como la implementación de dispositivos intermedios que elimina la implementación de modelos centralizados de control. Esto se puede adicionar a los puntos de control o funciones especializadas que se puede agregar dentro de los despliegues realizados, considerando que elementos como Sistemas de Detección o Prevención de Intrusos o Firewalls pueden incorporarse como mecanismo de control en dicho plano, dejando el plano de data sin la necesidad de tener mayores características o especificaciones de hardware/software para dicho despliegue.

Esto es lo que se muestra en la siguiente figura donde se realiza una comparativa de una red convencional y una red SDN.

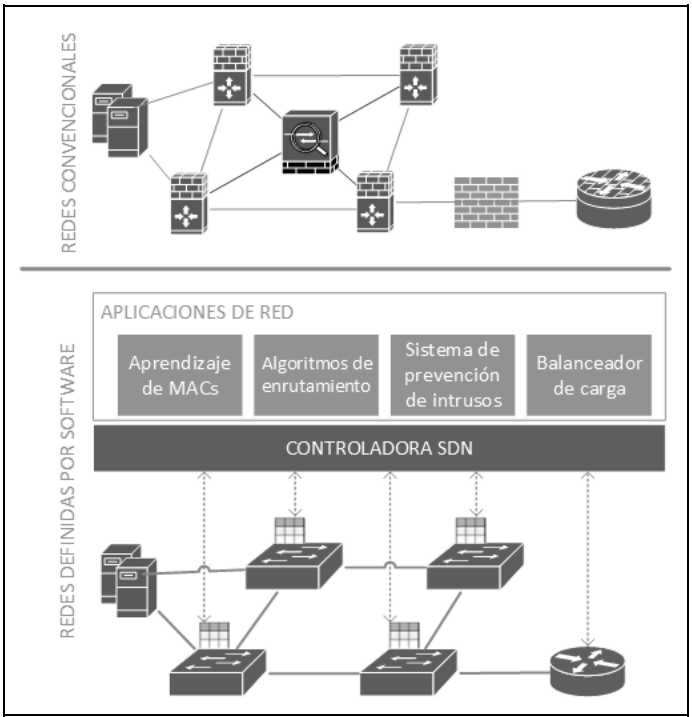

Figura 5. Redes tradicionales versus SDN.

Esto trae muchas ventajas, que se pueden expandir de acuerdo a los requerimientos de las organizaciones, pero que se pueden resumir en las siguientes:

Aplicaciones o servicios específicos esperados de la red, se vuelven simples programas, ya que la abstracción provista por la plataforma de control y el lenguaje de programación de red pueden ser compartidos para otras implementaciones.

- Todas las aplicaciones toman ventaja de la misma información o vista global de la red, lo que concluye en decisiones sobre las políticas más consistente y efectivas, mientras que se pueden reutilizar los módulos de software del plano de control
- Dichas aplicaciones pueden tomar acciones, como re-configurar dispositivos de reenvío, desde cualquier parte de la red. Por lo que la ubicación de alguna funcionalidad no debe de ser precisada dentro de la estrategia.
- La integración de las diferentes aplicaciones se vuelve más coherente. En este caso, se puede combinar secuencialmente la decisión de balanceo de carga previo a la decisión de la política de enrutamiento. Como parte de la decisión y aplicación de la política de la red, esto se pudiese cambiar de acuerdo a la misma estrategia definida.

C. Componentes de SDN.

Los componentes que se encuentran en una red SDN difieren mucho de una red convencional aunque se trate de una red de las mismas dimensiones involucrando los mismos planos (data, control y administración). Esto en relación a la función determinada. En la mayoría de casos, la referencia central para determinar los componente de una red SDN se definen en el protocolo Open-Flow, pero existen fabricantes que dan mantenimiento a protocolos propietarios específicos que definen componentes distintos pero con funciones similares.

De cualquier manera, la premisa básica de poder generar interoperabilidad genera que la mayoría de fabricantes den el seguimiento, dentro de su ruta estratégica sobre arquitecturas, a los estándares abiertos y a los componentes que se definen en dichos estándares. Dentro de estos componentes se tienen los siguientes:

1) Dispositivo de Reenvío (FD – forwarding device):

Es el dispositivo específico del plano de data, que puede ser basado en software o basado en hardware para poder realizar operaciones básicas dentro de la red. Los dispositivos de reenvío tienen un conjunto de instrucciones completamente definidas también conocidas como reglas de flujo, que se utilizan para tomar acciones sobre los datagramas (paquetes o tramas) que entran por las interfaces de los dispositivos.

Entre este conjunto de instrucciones se pueden ver por ejemplo, el reenvío de un paquete por una interfaz/puerto específico, descartar el paquete, reenviar el paquete a la controladora o reescribir el encabezado del mismo. Dichas instrucciones se definen por las interfaces descendentes, conocidos como “south-band interfaces” que se ampliaran más adelante.

De acuerdo a las implementaciones, las instrucciones que se envían desde la interfaz descendente alimentan una base de información de reenvío que puede ser un símil a una simple tabla que indica una condición de coincidencia y una interfaz de salida para dicha coincidencia. Como una comparativa en redes convencionales se podría abstraer a una red de conmutación capa 2 Ethernet a una tabla de direcciones MAC y un puerto de salida. El switch únicamente revisará dicha tabla comparando la MAC destino y reenviará la trama por el puerto correspondiente. Lo mismo pasaría en un router con su Base de Información de Reenvío (FIB – Forwarding Information Base) donde en base a una dirección de red destino hace el envío correspondiente por una interfaz donde se encuentre el router

adyacente que servirá como puerta de enlace para esa red o a un dispositivo final conectado a la interfaz de red.

Vale aclarar que los elementos de decisión específicos se encuentran en otros planos dentro de SDN, y los elementos de envío solamente realizan o ejecutan el reenvío del datagrama, paquete o trama en base a los elementos de decisión que ya recibieron por la interfaz descendente.

2) Plano de Data (DP – Data Plane)

Los dispositivos de reenvío son interconectados a través de distintos canales o medios, siendo estos cables, hilos de fibra o medios inalámbricos. Adicionando estos elementos de interconectividad física junto con los dispositivos de reenvío, se conforma el plano de data. Desde una vista comprensiva, es prácticamente la infraestructura física que interconecta los dispositivos finales que requieren conectividad. Se debe de tomar en cuenta que al hacer referencia al Plano de Data, se comprende el conjunto de todos los dispositivos de reenvío, y no únicamente un dispositivo de reenvío aislado. Esto es importante tomarlo en cuenta, ya que en SDN el comportamiento de los dispositivos de reenvío específicos puede ser diferente, y el tratamiento que se le dé a un tráfico específico puede variar dependiendo del dispositivo de reenvío por el que dicho tráfico esté atravesando.

Individualizando los dispositivos de reenvío que se interconectan a través de distintos tipos de medios, se debe de conocer que hay algunos servicios específicos de pequeña escala que en algunas implementaciones de SDN se pueden proveer en el Plano de Data. Pudiendo ser algo más que una decisión de reenvío de datagrama, se puede implementar un filtrado básico con control de acceso o incluso una política de QoS, como por ejemplo "policing" que resulta algo más específico de una interfaz manejando porcentajes específicos de encolamiento (queuing) de acuerdo al tipo de tráfico. Incluso en algunas implementaciones se maneja cifrado IPSEC directamente en este plano. Esto depende mucho del nivel de abstracción que la implementación de la red SDN mantenga.

3) Interfaz descendente (SI – South-bound Interface)

Dicha interfaz está conformada por una Interfaz de Programación de Aplicación (API – Application Programming Interface) que es la Interfaz descendente que define el conjunto de instrucciones dentro de los dispositivos de reenvío. La interfaz descendente (SI) define el protocolo de comunicación o la forma de interacción entre los dispositivos de reenvío y los elementos del plano de control.

En otras palabras, dicha interfaz es un conector entre el plano de datos y el plano de control. Siendo conectores definidos específicamente por un protocolo. Dentro de estos conectores se pueden mencionar los siguientes.

a) OpenFlow,

b) ForCES,

c) Protocol-Oblivious Forwarding (POF)

Estos conectores son los que se instalan en los equipos de reenvío y en la controladora para que estos puedan activar la interfaz descendente correspondiente.

4) Plano de Control (CP – Control Panel)

Este es el conjunto de elementos que programan a los dispositivos de reenvío a través de la interfaz descendente. El plano de control se puede considerar como la unidad de procesamiento central de la red. Los elementos del plano de control consisten en la controladora y la aplicación de control lógico, que en la mayoría de los casos se ve como una única entidad dentro de las definiciones de SDN.

Dentro del Plano de Control es donde se establece el conjunto especifico de información que se deberá utilizar para la creación de las tablas de reenvío que finalmente son aplicadas o utilizadas por los dispositivos de reenvío dentro del plano de data. Como por ejemplo en el caso de utilizar una red que requiere enrutamiento utilizando el protocolo OSPF (Open Shorest-Path First), será en la controladora donde se establecerá la información que se requerirá para mantener la tabla de topología del área correspondiente además de mantener dicha tabla actualizada. Este mismo conjunto de información definido se utilizaría para mantener la Base de Información de Ruteo (RIB – Routing information base) que se mantendría en la controladora misma.

De igual manera dentro del Open Flow se define que la Base de Información de Ruteo (RIB) que es mantenida por el mismo Plano de Control a través de la misma información establecida, es la que finalmente mantiene la Base de Información de Reenvío (FIB – Forwarding Information Base) que por lo general se mantiene de una manera paralela tanto en el Plano de Data como en la controladora.

Es importante aclarar que dicha Base de Información de Ruteo (RIB) puede ser generada a través de programación específica, programación por observación de la red misma, o incluso puede ser construida por la información que se obtenga de otras instancias de Plano de Control con el que se mantiene comunicación. Es decir que dicha base no se construye únicamente a través del uso de uno o varios protocolos de enrutamiento, sino también a través de programación específica o una combinación de protocolos de enrutamiento y programación

Otra aclaración importante que se debe de hacer en este punto, es que dentro del Plano de Control no se habla únicamente de enrutamiento de capa 3 (Capa de Red del modelo OSI), si no que se puede determinar específicamente sobre el encabezado de que capa se deberá de verificar para realizar el reenvío dentro del dispositivo de envío. Este pudiese ser en base al direccionamiento específicos de capa 2 como puede ser la dirección MAC que define IEEE 802.

Independientemente de dicha funcionalidad en el plano de control, luego de la evolución que se ha venido dando en las redes convencionales, es cada vez menos común encontrar una red de capa 2 que se extienda a una gran cantidad de dispositivos o en ubicaciones extendidas, debido a los mismos problemas inherentes que se generan dentro de topologías de este tipo. Por esto mismo mucha de la información de referencia e implementaciones que se hacen de SDN, mantienen una controladora y un plano de control de capa 3. Pero no es necesariamente en base al direccionamiento capa 3 que se realiza el reenvío.

5) Interfaz ascendente (NI – North-bound Interface):

La interfaz descendente es prácticamente una Interfaz de Programación de Aplicación (API) que se encuentra dentro del sistema operativo de red y que se utiliza para el desarrollo de aplicaciones. Esta interfaz abstrae a un alto nivel los conjuntos de instrucciones de bajo nivel que son usadas por la interfaz descendente.

6) Plano de Administración (MP – Management Plane):

Este plano lo comprende el conjunto de aplicaciones que utilizan las funciones ofrecidas por la interfaz descendente, para implementar en la red la lógica de control y la lógica de operación. Esto incluye aplicaciones tales como enrutamiento, cortafuegos, balanceadores de carga, monitoreo, entre otros. Básicamente, la aplicación de administración define las políticas de la red, que son convertidas a las instrucciones descendentes específicas que son las que finalmente programan el comportamiento de los dispositivos de reenvío.

7) Corredor de Red Definida por Software (Broker SDN):

Dentro de la terminología de SDN, se han incluido nuevos términos, entre estos el Corredor de SDN, que se define en determinadas implementaciones, donde se busca habilitar nuevas Interfaces de Programación de Aplicación que interactúa de manera bi-direccional entre la red y la aplicación, que funciona como un corredor o intermediario entre estos componentes. Con este nuevo intermediario, se obtiene una red más orientada a la programabilidad y con mayores facilidades de adaptación a las necesidades de la organización.

8) Superposición de red definida por software (Overlay SDN):

Este se refiere a una implementación, donde la red de borde es programada de una manera interactiva para que se puedan manejar túneles entre los hipervisores y las redes conmutadas. Este acercamiento se ha visto mucho dentro de centro de cómputo virtualizados. Estos túneles que tienen una terminación dentro de switches (conmutadores) virtuales y en equipos físicos que finalmente actúan como puertas de enlaces para una red ya instalada. Esta las profundiza más Kreutz en su publicación [9].

D. OpenFlow.

Open Flow, se define como un protocolo emergente y abierto de comunicaciones que permite a un servidor de software determinar el camino de reenvío de paquetes que debería seguir en una red de switches [10].

En la era del "Mainframe de la Informática" se integraron las aplicaciones, sistemas operativos y hardware; todos estos eran proporcionados por proveedores exclusivos y casi únicos que frenaban la innovación que se podía llegar a dar. Ahora, en nuestros tiempos se conoce que OpenFlow surgió como parte de estandarizar las tecnologías emergentes y fue la ONF (Open Networking Foundation) que se plasmó ese objetivo y la cual fundó la primera versión del protocolo, a los que se unieron otras organizaciones para desarrollo de este.

Para que se pueda llevar a cabo la arquitectura de SDN se necesitan dos requisitos: la arquitectura lógica común en todos los dispositivos (switches, routers, etc.) y el protocolo seguro entre SDN y los dispositivos; OpenFlow cubre esos dos requisitos. Este controlador de SDN debe de comunicarse con todos los conmutadores que sean compatibles con OpenFlow [11]

En muchos casos la gente usa indistintamente los términos SDN y OpenFLow; para aclarar esta situación, SDN se refiere a la arquitectura mientras que OpenFlow es el protocolo usado entre el controlador y la infraestructura de red.

En términos simples, un controlador habla este lenguaje (OpenFlow) para comunicarse con hardware compatible. OpenFlow es un protocolo de red abierto diseñado para gestionar y direccionar tráfico de red en equipos que pueden ser diferentes fabricantes. Como cualquier otro lenguaje, OpenFlow maneja su propio vocabulario, el cual es usado entre el controlador y la infraestructura.

Todos los mensajes intercambiados en el protocolo OpenFlow pueden dividirse en 3 grandes grupos [12]:

S. Mensajes del controlador al switch.

Estos mensajes son iniciados por el controlador y son usados para gestionar los switches o para obtener información de ellos. Estos pueden ser de seis tipos:

- Lectura de estado: Usado por el controlador para leer los contadores de acuerdo al flujo, al puerto o de acuerdo a los contadores de colas,
- Modificación de estado: Comúnmente usado para agregar, borrar o modificar flujos en la tabla de flujo del switch.
- Envío de paquete: Usado para enviar paquetes a través de un puerto particular del switch.
- Solicitudes y respuestas de barrera. Usadas para recibir notificaciones de las operaciones completadas por el switch. Si una solicitud de barrera es recibida desde una controladora en un switch, el switch debe completar todas las tareas pendientes que tiene antes de recibir dicha solicitud. Esto crea una barrera en el switch de manera que pueda saltar a la siguiente tarea. Una vez completa las tareas, envía una respuesta de barrera de regreso a la controladora e inicia el trabajo sobre las siguientes tareas.
- Características: Esta solicitud es una característica del switch luego de asegurar que la conexión es establecida entre la controladora y el switch. El switch responde solo a la controladora con las características y capacidades que puede soportar.
- Configuración: Usada por la controladora para conseguir y establecer los parámetros de configuración en el switch.

b. Mensajes asíncronos: Este mensaje entrega al switch una oportunidad de comunicarse libremente con la controladora sin solicitud de permiso. Es aquí donde el switch puede informar a la controladora sobre paquetes descartados o interfaces caídas. Estos se clasifican en 4 tipos:

- Estatus de puerto: Cualquier cambio en el estado del puerto es enviado a la controladora. Este no incluye

únicamente caídas del puerto, si no también cambios en el estado de Spanning-Tree.

- Paquetes entrantes: Este mensaje es enviado a la controladora solo si hay un paquete entrando al switch que no coincide con ninguna de las entradas de la tabla de flujo. Lo que implica que debe ser enviado a la controladora, o en otro caso que el paquete coincide con una regla que especifica que el paquete tiene que ser enviado a la controladora.
- Remover del flujo: Cualquier flujo de entrada agregada a la tabla de flujo que ha excedido el tiempo de espera y un valor de temporizador asociado a él. Si una de estas condiciones se cumple, el mensaje "Remover del flujo", es enviado desde el switch hacia la controladora.
- Error: Este mensaje es enviado desde el switch a la controladora para informar de un error.

c. Mensajes simétricos: Estos mensajes son bidireccionales y son enviados por la controladora al switch o viceversa sin solicitud de permiso, por ejemplo: solicitudes de HELLO o ECHO. Estos mensajes manejan acuse de recibo.

- HELLO: Mensaje que se intercambia entre el switch y la controladora al momento de la inicialización.
- ECHO: Mensaje que obliga al receptor a responder de recibido. Estos mensajes se utiliza para conocer la latencia de la conexión entre el switch y la controladora.
- Fabricante: Mensaje que provee una manera estandarizada para que los switches puedan informar a la controladora sobre funcionalidades adicionales que el mismo pueda ofrecer. Este mensaje también es utilizado para prueba de nuevas funcionalidades.

Ahora que conocemos los mensajes, podemos revisar su intercambio y analizar cómo opera el protocolo.

La conexión entre la controladora y el switch es establecida utilizando una dirección IP y es asegurada utilizando TLS (Transport Layer Security). La conexión es iniciada por el switch utilizando la dirección IP de la controladora y el puerto TCP 6633. El switch y la controladora se autentican mutuamente para intercambiar certificados. Tan pronto la conexión es establecida, mensajes HELLO son enviados en ambos dispositivos, este mensaje también contiene la versión más reciente del protocolo OpenFlow que cada componente puede soportar. Este se utiliza para establecer la versión que ambos usaran que representa la menor versión compatible.

En caso que la versión más baja compatible no pueda operar entre la controladora y el switch, un mensaje de error es enviado conteniendo los detalles de la falla y terminación de la conexión.

Una vez establecida la versión del protocolo, la controladora solicita al switch información sobre sus funcionalidades. Un paquete de "Features Request" es enviado al switch. Este responde con sus funcionalidades y capacidades, esto es seguido por una solicitud de configuración "Get Configuration Request". A través de este la controladora informa al switch sobre su configuración.

Existen otras solicitudes como:

- Solicitud de estadísticas, "Stats Request".
- Estatus de puerto, "Port Status"

Lo último que requiere la controladora es conocer la ubicación del switch para que pueda dirigir el tráfico correctamente. Esto se realiza utilizando LLDP (Link Layer Discovery Protocol). La controladora crea un paquete LLDP y solicita al switch que replique ese mensaje a través de todos sus puertos. Existe una regla ya configurada por la controladora que todos los paquetes LLDP sean enviados de regreso a la controladora. Cuando el switch envía los paquetes LLDP, los switches vecinos reciben estos paquetes y los envían de regreso a la controladora. De esta manera la controladora hace el descubrimiento de la topología de la red.

Luego de completado este proceso, se procesan solicitudes y respuestas de ECHO entre el switch y la controladora.

En caso de desconexión entre el switch y la controladora debido a una falta de respuesta a una solicitud de ECHO o a una sesión TLS vencida o cualquier otra razón, el switch trata de buscar una o más controladoras de respaldo. El orden en que el contacto es realizado no está especificado por OpenFlow.

En caso que el contacto con la controladora falle, el switch debe reiniciar su conexión TCP con la controladora y pasa a modo de emergencia. En este modo el switch depura todas las entradas de la tabla de flujo, excepto por las que se encuentran marcadas con un bit de emergencia. Una vez se restablece la conexión, la tabla de flujo de emergencia sigue siendo utilizada, es decisión de la controladora depurar la tabla completamente agregando entradas nuevas o solo agregar las entradas faltantes.

Si un paquete viene de un host conectado al switch, el switch verifica si existe una coincidencia en la tabla de flujo y de no existir tal coincidencia el paquete es enviado a la controladora. El switch envía este paquete encapsulado en OpenFlow hacia la controladora. La controladora devuelve una solicitud de ARP a la que se espera una respuesta para el ingreso del flujo a la tabla correspondiente. [13]

La figura siguiente muestra la arquitectura de OpenFlow, esta se ejecuta sobre la capa de SSL (Security Socket Layer) que está entre la comunicación del controlador SDN y los dispositivos compatibles con OpenFlow. [11]

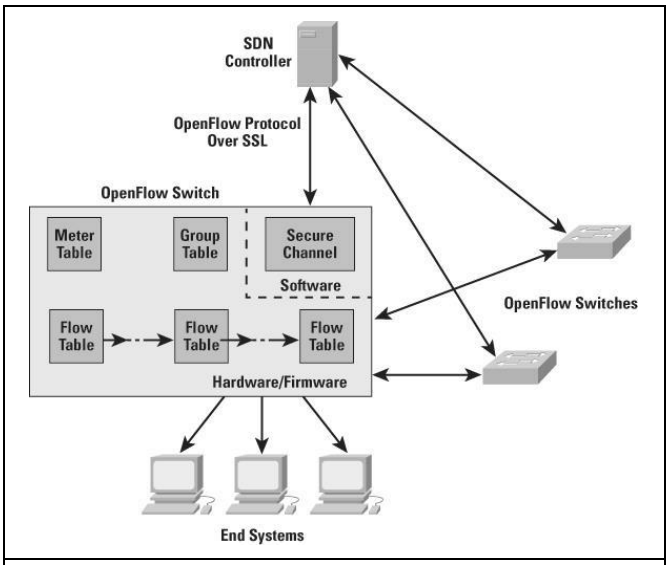

Figura 6. Operación de OpenFlow

El elemento común que se encuentra en los dispositivos como los switches y routers son las tablas de flujo (table-flow), OpenFlow ofrece controlar esto mediante su protocolo abierto. Prácticamente esto se enfoca a los reenvíos de paquetes que en los dispositivos tradicionales se tenía control de ello; ahora con OpenFlow el "controlador" se encarga de eso de forma más eficiente.

OpenFlow contiene tres tipos de tablas en su arquitectura lógica, estas son:

- Flow Table: compara los paquetes entrantes y le especifica las funciones a realizar.
- Group Table: puede desencadenar una o más acciones para los flujos.
- Meter Table: puede realizar diferentes acciones para el rendimiento del flujo.

Podemos observar las entradas de las tablas de flujo que pueden ser manipuladas en un switch de OpenFlow [14].

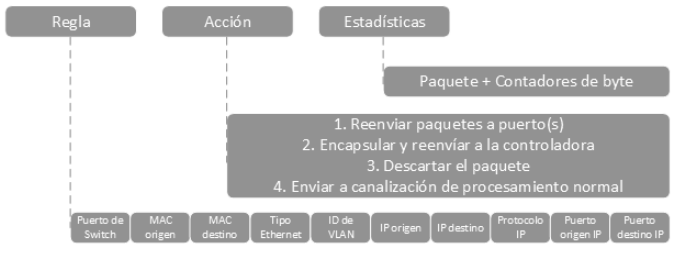

Figura 7. Entradas de la tabla de flujo.

Action set, es una lista de acciones asociadas a un paquete que se acumula mientras que el paquete es procesado por cada tabla y es ejecutado cuando el paquete sale del pipeline (tubería de proceso). Las instrucciones son de cuatro tipos [11]

- Direct packet through pipeline: La instrucción Goto-Table dirige el paquete a una tabla lejos a lo largo de la tubería. La instrucción Meter dirige el paquete a un meter específico.
- Perform action on packet: Las acciones pueden ser realizadas en el paquete cuando se hace coincidir con una entrada de tabla.
- Update action set: Combinar acciones especificadas en el conjunto de la acción actual de este paquete en este flujo, o borrar todas las acciones del conjunto de acciones.
- Update metadata: Un valor de metadatos puede estar asociada con un paquete. Se utiliza para transportar información de una tabla a otra.

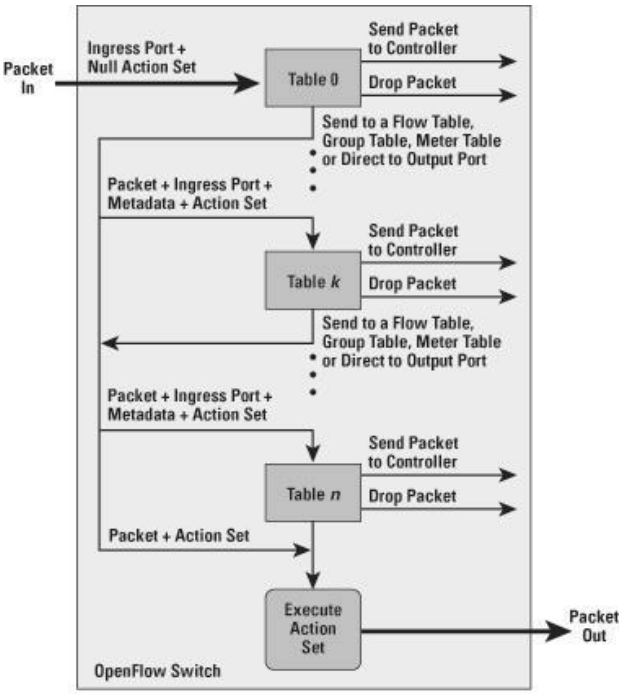

Figura 8. Flujo de paquetes a través del switch OpenFlow

SDN y OpenFlow brindan un enfoque poderoso para la gestión de redes complejas y críticas con exigencias a demanda y el crecimiento constante de las estructuras de red, aun así pueden interactuar con las redes existentes y sabiendo la tendencia que están marcando para el futuro.

Los problemas que se presentan en la gestión de las redes hoy en día se vuelven tareas más difíciles entre más grande es la empresa y la red, con OpenFlow y SDN se ha permitido la virtualización de las redes, que mejora enormemente la administración y la gestión de redes complejas. Aunque existe una complejidad y dificultad en construir estas redes, por lo que no se verá el cambio tan inmediato a estas tecnologías.

V. SEGURIDAD DE LA INFORMACIÓN

A. Seguridad Definida por Software (SDS)

La Seguridad Definida por Software (SDS o SDSec, conocido por sus siglas en inglés) es un nuevo término que está en evolución, está formado por un conjunto de aplicaciones que utilizan el concepto de SDN, también utiliza dispositivos de seguridad virtualizada que indica el próximo paso a la Red de Funciones de Virtualización (NFV, conocido por sus siglas en inglés)

Este enfoque NFV en palabras breves asume que casi todo el hardware y los sistemas especializados que participan en las operaciones de red, como los IDS/IPS, se transformaran en dispositivos virtuales que se ejecutan en una plataforma de hardware independiente. Además, está diseñado para consolidar y entregar los componentes de red necesarios para apoyar una infraestructura totalmente virtualizado incluyendo servidores virtuales, almacenamiento e incluso otras redes.

Ahora, se sabe que el concepto SDN fue originalmente diseñado para empoderar a las aplicaciones en la ejecución de reglas de reenvío sofisticadas y, por consiguiente estrategias de seguridad. A pesar de que esta es una de las ventajas más significativas presentadas por SDN a la seguridad de la red, también introduce nuevos objetivos para ataques potenciales. La seguridad debe ser garantizada, incluso a nivel del plano de control.

El objetivo principal en el despliegue SDN es proteger la disponibilidad, integridad y privacidad de todos los recursos y la información conectados, en la terminología de seguridad informática llamados “activos”.

Hay varios atributos clave de seguridad de red definida por software [15]

Abstracción: La abstracción de la seguridad se aparta de los paradigmas de seguridad física como cortafuego de estado de puerto o sniffers pasivos reemplazándolos por un conjunto de controles flexibles, en forma de políticas que toman la cobertura de manera virtualizada o física sobre los activos. Abstracción es la función para establecer modelos de seguridad comunes, los cuales pueden ser implementados de manera automatizada y repetitiva sin la preocupación inherente de las capacidades de recursos de hardware.

Automatización: Las políticas de seguridad de los activos deben de apegarse a las re-implementaciones o modificaciones que se hacen sobre los mismos. Dicha automatización elimina la amenaza inherente sobre el error de administrador (o error humano, ya que la seguridad definida por software puede garantizar que ningún activo pueda ser creado o introducido a la infraestructura sin haber sido colocado, de manera automática, dentro de una zona de confianza. Controles basados en roles aseguran que no solo los administradores con privilegios adecuados pueda realizar modificaciones. La automatización de SDS también implica una reacción ante un evento anómalo de seguridad que se puede ejecutar a gran velocidad, con alertas y poniendo en cuarentena de manera instantánea como la política indica. En contraste la seguridad tradicional todavía relega o depende fuertemente de la detección manual y acciones del administrador.

Escalabilidad y flexibilidad: Se eliminan las dependencias de un hardware físico, implica que la seguridad puede ser implementada sobre la escala apropiada para cada huésped de virtualización, creciendo el alcance y logrando los requerimientos del negocio. Debido a que se trata únicamente de software, la política de seguridad es elástica y puede ser extendida a través de un clúster o un centro de datos. Esto también significa que la seguridad está disponible bajo demanda.

Control de Orquestación: SDS está diseñado para un rango de controles de seguridad de la red (Detección y prevención de intrusos, gestión de vulnerabilidades, segmentación de red, herramientas de monitoreo, y otras) dentro de un único controlador para la inteligencia, análisis y ejecución. Fuentes ilimitadas de entradas de seguridad pueden ser canalizadas dentro de un sistema de orquestación orientada a la política, mejorando grandemente la certeza de la data y acción operadora. La orquestación es crítica para el éxito del reforzamiento del cumplimiento, como todos los estándares de cumplimiento dictan una variedad de controles para las especificaciones. Lograr este nivel de orquestación en centros de datos con seguridad basada en hardware aislado resulta complejo y costoso, en la medida que es difícil encontrar distintos dispositivos de seguridad que utilicen los mismos lenguajes y que no tengan una controladora única analizando sus datos de entrada.

Portabilidad: En un centro de datos gobernado por Seguridad Definida por Software los activos contienen sus configuraciones de seguridad en la medida que estos escalan o sufren modificaciones. El personal de ITSec (Seguridad de TI) y NETSec (Seguridad de Red) pueden configurar inicialmente y luego dejar que se administre por sí misma.

Visibilidad: Por tratarse de un software y residiendo en una infraestructura virtualizada, la Seguridad Definida por Software mejora dramáticamente la visibilidad de la actividad de la red. Los administradores de red y el personal de seguridad pueden detectar comportamientos anómalos que pueden pasar desapercibidos con dispositivos físicos, logrando de esta manera proteger con un nivel más alto de exactitud.

Estas características son exclusivas de SDS por lo que son difíciles de alcanzar con los dispositivos de seguridad tradicionales.

En estos últimos años las empresas han sido cada vez más firmes con el movimiento de aplicaciones de misión crítica y sensible al rendimiento de la “nube”, mientras que al mismo tiempo muchas nuevas aplicaciones móviles, sociales, y de análisis son desarrollados y operados directamente en las plataformas de computación en la nube. Estos dos movimientos están ralentizando el cambio de la propuesta de valor de computación en la nube y de la reducción de costos a la agilidad y optimización simultánea.

Nos encontramos en la era de la virtualización en la prestación de servicios en la nube. La gestión de centros de datos es muy compleja y se dificulta con las redes tradicionales, ya que no son lo suficientemente flexibles.

La libertad de movimiento que posee SDN permite una mejor seguridad y control de todas las áreas de la red y

nuestros sistemas. La capacidad de tener un control centralizado permite a los administradores realizar cambios con eficiencia, por ejemplo: Si ocurriese una filtración de malware se puede actuar rápidamente en limitar que se propague hacia switches o routers, así como se puede modular el tráfico y QoS de paquetes de manera más segura. En las redes convencionales de hoy en día pueden contar con esa capacidad pero no se tiene la velocidad y eficiencia para intervenir o asegurar la red.

El paradigma de flujo es ideal para el procesamiento de la seguridad, ya que ofrece un modelo de conexión de extremo a extremo orientada a servicios que no está atado por las restricciones de enrutamiento tradicionales [16].

B. Conceptos de la seguridad de la información

Al hablar de seguridad de la información no se debe de caer en la confusión de estar hablando acerca de seguridad informática, puesto que la seguridad de la información va más allá del medio informático y se refleja más en la privacidad de la información del individuo; es más, puede manifestarse en diferentes formas.

La información es centralizada y se maneja a través de la tecnología, pues para la organización posee un gran valor y un gran poder; por eso representa un alto riesgo. La información se puede clasificar como: crítica, valiosa, sensible y poderosa.

Según diferentes fuentes de información dan a conocer los conceptos de seguridad de la información:

"La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma." [17]

"La seguridad de la información tiene como objeto los sistemas, el acceso, uso, divulgación, interrupción o destrucción no autorizada de información. Los términos seguridad de la información, seguridad informática y garantía de la información son usados frecuentemente como sinónimos porque todos ellos persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información." [17]

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización [18].

1) Triada de la seguridad y servicios

La información es el activo más importante o uno de los más importantes de la organización, por esta razón se debe prestar mucho interés por protegerla y velar por su seguridad; con esto aseguramos la continuidad y desarrollo de la organización.

Por ende, entre mayor sea la información mayores serán los riesgos o amenazas de seguridad, por lo que se debe realizar una eficiente gestión; esto se logra con los principales pilares que son: confidencialidad, integridad y disponibilidad

a) Confidencialidad

La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

b) Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. Es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

c) Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. La disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

d) Autenticación o autentificación

Es la propiedad que permite identificar el generador de la información.

e) No repudio

Un servicio que proporciona pruebas de la integridad y origen de los datos.

2) Protocolos de Seguridad de la Información

Son un conjunto de reglas que gobiernan dentro de la transmisión de datos entre la comunicación de dispositivos para ofrecer confidencialidad, integridad, autenticación y el no repudio de la información. Se componen de:

a) Criptografía

b) Lógica (Estructura y secuencia).

c) Identificación (Autenticación).

VI. SEGURIDAD DE LA INFRAESTRUCTURA DE RED.

Si bien una red definida por software centraliza ciertas funciones de control a través de una interfaz que nos permiten agilizar enormemente su operación y maximizar la escalabilidad del entorno de comunicación no significa que la capa física varía mucho en comparación a las redes tradicionales, incluso no se habla de implementaciones separadas sino más bien de un servicio sobre la arquitectura tradicional y ciertos requerimientos adicionales, que generalmente incluyen dispositivos conectados a la red, programas y archivos que soportan las operaciones de red. Las funciones de control en SDN se llevan a cabo a través de una terminal de control y de software especializado de comunicación. Así podemos establecer algunos de los controles que son recomendables mantener para este tipo de implementaciones:

a) Las acciones de control deberán realizarlas operadores técnicamente capacitados.

b) Debe garantizarse la segregación de funciones para la ejecución de las mismas y estas deben rotarse periódicamente siempre que sea posible.

c) El software de control de redes debe restringir el acceso del operador para que incluso los perfiles de mayor grado tengan funcionalidades limitadas hasta cierto punto.

d) Debe habilitarse en el software de control de red la funcionalidad de permitir el almacenamiento de registros de acceso y ejecución para mantener la evidencia o pistas que puedan ser requeridas en un proceso de auditoría.

e) Los registros de acceso y ejecución deben ser revisados periódicamente para detectar cualquier actividad no autorizada en la operación de la red.

f) Las normas de operación de la red deben ser documentadas, comunicadas y estar a disposición de los operadores. Estas deberán revisarse periódicamente para garantizar su aplicabilidad ante cambios en el entorno.

g) Se recomienda efectuar análisis periódicos para asegurar el equilibrio de la carga de trabajo, respuesta rápida y eficiencia del sistema.

h) Se debe aplicar técnicas de cifrado de datos para proteger los mensajes y que estos no puedan ser revelados durante su transmisión. Estos procesos deberán incluirse por etapas, siempre y cuando se asegure que dicha inclusión no altera el tratamiento del riesgo.

Para mejorar el control, mantenimiento y uso de la infraestructura de red, deben recopilarse los registros de los dispositivos de control de red, firewalls y terminales. Estos registros deben almacenarse hasta donde el análisis de costos previo de mantenimiento de pistas de auditoría lo permita, ya que obviamente el costo que significa almacenar y analizar los registros debe ser considerado. Estos costos, además de recursos económicos incurren en horas de cómputo para el procesamiento de los archivos y horas hombre para el análisis de estos.

Otro factor que aporta cierto grado de seguridad a la infraestructura como tal, es el inventario dinámico de equipos y/o terminales ya que cuando se realizan tareas de correlación de eventos como etapa posterior a un plan de recuperación ante desastres es importante conocer quien utiliza cada equipo.

Los requerimientos que anteceden están más orientados a facilitar la práctica del gobierno de TI. Uno de los modelos utilizados para este proceso es ITIL, cuya meta principal es el respaldo de la gestión de recursos como sistemas de información a través del uso de acuerdos de niveles de servicios.

A. Seguridad en entornos LAN.

Una de las funciones de las redes de área local es la de facilitar el almacenamiento y la recuperación de los programas y datos usados por un conjunto de personas. El software y las prácticas orientadas a escenarios de infraestructura local están enfocados a garantizar los servicios de seguridad de estos programas y datos. Desafortunadamente la mayoría de software en entornos LAN proporciona un nivel bajo de seguridad. Así podemos enumerar algunos de los riesgos asociados al uso de entornos LAN:

a) La pérdida de integridad de los datos y de los programas debido a cambios no autorizados.

b) No puede garantizarse el control de versionamiento por lo que no puede asegurar la protección de los datos vigentes, esto debido a la manipulación simultánea de la información.

c) La limitada verificación de usuarios y el establecimiento de conexiones externas expone los activos.

d) Infecciones debidas a virus, gusanos y otras amenazas.

e) La violación de acuerdos de licenciamiento entre clientes y proveedores de software debido al uso de copias sin licencias o un número excesivo de ellos.

f) El acceso ilegal simulando ser un usuario legítimo en la LAN.

g) Sniffing, como forma de rastrear información aparentemente no importante, por parte de usuarios internos y que posteriormente puede ser usada para realizar ataques.

h) Spoofing, que se refiere a usuarios internos suplantados a través de la reconfiguración de direcciones de red para pretender que se trata de una dirección diferente.

i) Usuarios internos obteniendo acceso para la manipulación y/o destrucción de los registros de acceso y auditoría.

Las medidas de seguridad en entornos LAN dependen en muchas ocasiones del software, de la versión y de la forma en la que se implementó. Algunas de las funcionalidades administrativas de seguridad que están disponibles son:

- Determinación de la propiedad de los programas, archivos y almacenamiento.
- Limitar el acceso a modo solo lectura.
- Bloqueo de registros y archivos para prevenir que se lleven a cabo actualizaciones simultáneas.
- El cumplimiento de los procedimientos de autenticación o identificación de usuarios a través de un usuario y una contraseña, incluyendo las reglas relacionadas a la longitud, complejidad, formato y frecuencia de cambio de las contraseñas.
- El uso de IPSec como protocolo de cifrado para tráfico local.

El uso de estos procedimientos de seguridad implica el aumento en las tareas administrativas para su implementación y mantenimiento. Debido a la ausencia de estos procesos la administración de la red se torna inadecuada, proporcionando acceso global debido a que el soporte administrativo es limitado. Otra práctica recomendable para el aseguramiento del entorno es la documentación para evaluar la evolución del

mismo. Regularmente esta documentación debe incluir: La topología de la LAN y el diseño de la red, el administrador y/o propietario de la LAN, las funciones que desempeña el administrador y/o propietario, grupos de usuarios, aplicaciones informáticas usadas, procedimientos y normas relativas al diseño de la red, soporte, perfiles de acceso y seguridad de la información.

Riesgos y problemas en entornos LAN.

Las funciones administrativas y de control disponibles con el software de red suelen ser limitadas. Los proveedores de software y los clientes de estos han reconocido la necesidad de proveer funcionalidades adicionales que proveen cierto grado de diagnóstico para identificar la causa de los problemas cuando el comportamiento de la red no es el usual. Hasta hace poco el uso de Logon-Ids y de contraseñas con facilidades de administración se han convertido en un estándar.

Las funcionalidades para otorgar permisos de lectura, escritura y ejecución para los archivos y los programas son opciones disponibles solo con algunas versiones de sistemas operativos de red pero rara vez se encuentran en las bitácoras de una LAN. Afortunadamente, las nuevas versiones de software de red ofrecen un mayor número de estas funcionalidades de control y administración.

Las LAN pueden representar una forma de computación descentralizada. El procesamiento local descentralizado provee el potencial para un entorno informático más sensible, sin embargo, las organizaciones no siempre dan la oportunidad de desarrollar eficientemente al personal para encarar los problemas técnicos, operativos y de control que representa la tecnología asociada a las LAN. Como resultado de ello, a los operadores locales de estas redes, les falta la experiencia, la pericia y el tiempo para manejar con efectividad estos entornos.

Cada implementación de redes incluye diversas alternativas de medios de comunicación, protocolos, hardware, técnicas de transmisión, topología y software de gestión que vuelven a cada una de ellas única. Son precisamente estos factores los que dificultan el implementar estándares de gestión, operación e incluso auditoría. Por ello cuando ocurren problemas, los costos de resolverlos suelen ser sustanciales.

Para los usuarios legítimos dentro de una LAN, la principal preocupación es la funcionalidad, dejando de lado cualquier atributo adicional. Dentro de una LAN bien estructurada los usuarios promedio se tornan incapaces de evaluar si la tecnología utilizada es la adecuada o si el software está instalado y documentado de forma correcta o si se han incluido las suficientes medidas de seguridad. En este entorno, simple, las evidencias o pistas de auditoría son consideras hasta que un problema se presenta.

B. Seguridad en entornos Cliente – Servidor..

Estos entornos comúnmente contienen numerosos puntos de acceso. La mayor parte de los administradores no comprende a totalidad los procedimientos de seguridad requeridos en estos escenarios específicos, incluso desconocen que estos se encuentran más expuestos que un entorno de procesamiento de mainframe por ejemplo. La mayor parte de los sistemas que utilizan el método cliente-servidor emplea técnicas distribuidas, lo que conlleva un mayor riesgo de acceso a los datos y a las funcionalidades de procesamiento.

En un entorno cliente-servidor existen muchas rutas de acceso, ya que los datos de aplicación pueden residir en cualquiera de estas dos entidades. Por ello debe verificarse cada una de estas rutas de forma individual a fin de asegurar que no hayan quedado exposiciones sin verificar. Existe numerosas técnicas de control para un entorno cliente-servidor, dentro de las que podemos mencionar:

- Inhabilitar la unidad de almacenamiento que se utiliza para la inicialización del sistema, asegurando el acceso a las aplicaciones o a los datos en entornos cliente-servidor. Las estaciones de trabajo sin la unidad de inicialización, impiden que el software de control de acceso pueda ser evadido ya que en caso que ocurra, vuelve a las estaciones de trabajo vulnerables a accesos no autorizados. A la vez se asegura los archivos de arranque o de carga para así evitar que evadan los comandos de registro de entrada.
- Los dispositivos utilizados para el monitoreo de la red pueden utilizarse para inspeccionar la actividad de usuarios conocidos o desconocidos. Estos dispositivos a menudo logran identificar las direcciones de clientes, permitiendo finalizar las sesiones de forma proactiva, esto también permite encontrar evidencia de accesos no autorizados. Pero la confianza de esta técnica radica en el administrador mismo, ya que si este no mantiene estos dispositivos la herramienta se volverá inútil.
- Técnicas de cifrado pueden ayudar a proteger la información sensible de accesos no autorizados.
- Los sistemas de autenticación pueden proporcionar a un entorno cliente-servidor las facilidades lógicas que permiten diferenciar a los usuarios.
- El uso de software de control de acceso a nivel de aplicación y la delimitación de usuarios en grupos funcionales permite restringir el acceso, limitando las operaciones solo a las que el perfil tiene permitido.

C. Seguridad en Internet.

La naturaleza misma del internet lo hace muy vulnerable a ataques de todo tipo. Se habla de un sistema global basado en TCP/IP que permite interconectar redes heterogéneas públicas y privadas. Este fue diseñado inicialmente para permitir el intercambio de información, datos y archivos de una forma lo más libre posible y actualmente tiene mayor injerencia en fines comerciales. Es esto lo que plantea ciertos problemas de seguridad a las organizaciones que buscan proteger sus activos de información. Algunos atacantes buscan invadir la privacidad de los demás y tratan de adentrarse en las bases de datos que contienen información sensitiva o husmear en la información a medida que esta recorre la red, es por ello que se vuelve una prioridad entender los riesgos y los factores de seguridad que se necesitan para asegurar que se cuente con los controles mínimos en caso que se requiera conectar una red a internet.

El protocolo IP está diseñado específicamente para el direccionamiento y enrutamiento de los paquetes de datos a

través de una red, este no garantiza la entrega de los paquetes y mucho menos presenta evidencia de la entrega, es por ello que estas funcionalidades se buscan en otros protocolos para proveer los servicios de seguridad a este nivel.

Para establecer controles efectivos de seguridad para internet, una organización debe poner especial atención en desarrollar controles enfocados en un marco de seguridad para sistemas de información, a partir del cual se puedan implementar y soportar estos con el fin de brindar seguridad sobre internet. Regularmente el proceso de selección de dicho marco conlleva el definir las reglas que la organización seguirá para controlar el uso de este recurso a través de políticas corporativas y procedimientos específicos.

Por ejemplo, podemos restringir el uso de internet a quienes tengan necesidades del negocio, definir qué conjunto de recursos estarán disponibles para los usuarios externos y establecer las redes de confianza para la organización. También puede establecerse un conjunto de reglas que traten sobre la clasificación de la sensibilidad o criticidad de los recursos corporativos de información. Así conoceremos qué información se permitirá que esté disponible para su uso en internet y el nivel de seguridad que consideraremos para los recursos corporativos.

A partir de estas evaluaciones lograremos establecer directrices específicas para estas circunstancias. Así se podrá definir cómo debe configurarse el sistema operativo, que servicios de internet deben ser bloqueados para el uso por parte de usuarios externos con los que no se tiene una relación de confianza, así como definir de qué forma el sistema estará protegido por firewalls. Entro los procesos que logran dar soporte a estos controles tenemos:

- Evaluaciones periódicas del riesgo asociadas con el desarrollo y rediseño de aplicaciones web basadas en internet.
- Campañas de entrenamiento sobre seguridad para los empleados de acuerdo a sus niveles de responsabilidad.
- Estándares que regulen las arquitecturas de firewalls a utilizar en la implementación.
- Estándares que regulen las arquitecturas de IDS e IPS a utilizar en la implementación.
- Gestión de incidentes y respuesta ante la detección, contención y recuperación.
- Administración de las configuraciones para mantener el control de los criterios básicos de seguridad ante cualquier cambio.
- Empleo de técnicas de cifrado de información para garantizar la integridad de esta en su camino a través de la red.
- Monitoreo de las actividades o usos no autorizados de internet y la debida notificación a los usuarios finales sobre incidentes de seguridad gestionados por el equipo de respuesta ante emergencias generadas en el entorno informático [19]

D. Firewalls.

Los firewalls pueden ser una forma efectiva de proteger un sistema local o una red de sistemas de ciertas amenazas de seguridad, al mismo tiempo que proporciona acceso al mundo exterior a través de redes WAN e Internet. La necesidad de esta funcionalidad está relacionada directamente al hecho que la conectividad a internet dejó de ser una opción para las organizaciones y pasó a ser un bien esencial para la operación de estas. Hoy en día es una necesidad el acceso a internet y este no puede ser provisto directamente por sus propias redes LAN, así requerirán servicios de conectividad a través de un proveedor.

Si bien es cierto que dicho acceso provee de una amplia gama de beneficios a la organización, también permite al mundo exterior alcanzar nuestra red local e interactuar con los bienes organizacionales. Mientras sea posible, para disminuir este impacto podemos proveer a las estaciones de trabajo y servidores de ciertas premisas que fortalezcan la seguridad, como por ejemplo protección contra intrusos, pero al cabo de un tiempo nos daremos cuenta que no son lo suficiente y en algunos casos no resultan costo-efectivas.

Evaluemos un escenario específico, consideremos una red con cientos o incluso miles de hosts ejecutando diferentes versiones de sistemas operativos; cuando una vulnerabilidad en una de estas distribuciones es descubierta cada uno de los equipos que resultan potencialmente afectados deberán ser actualizados para corregir este problema. Esta operación requerirá un método escalable de gestión y ciertas funciones agresivas de parchado de sistemas y esto forma parte de los requerimientos cuando decidimos adoptar mecanismos de seguridad basados en hosts. Ante todo esto, el implementar un firewall será visto como complementario y no tanto como alternativa.

En cuanto a la ubicación estratégica de un firewall, regularmente se inserta entre el equipo de red y el acceso a internet para establecer un enlace de control en una de las direcciones del tráfico y en el sentido opuesto figura como perímetro. La función de este perímetro será proteger a los equipos de red de ataques basados en internet además de establecer un punto único de validación de seguridad, controles y futuros requerimientos o auditorías. Técnicamente el firewall puede conformarse por un único equipo o un conjunto de ellos que operan para desarrollar la función mencionada.

En resumen, un firewall provee una capa adicional de defensa que aísla los equipos o sistemas internos de redes externas. Enumeremos algunas de las características de un firewall para reforzar nuestra concepción de estos:

a) Todo el tráfico entrante o saliente debe pasar a través del firewall. Esto se logra bloqueando físicamente todos los accesos a la red local y permitiendo únicamente vía el firewall y es en esta etapa en donde diversas configuraciones pueden tomar lugar.

b) Sólo el tráfico autorizado debe ser permitido a pasar y es definido como autorizado por la política local de seguridad, también en este punto puede desarrollarse una gran cantidad de políticas basadas en diversas métricas.

c) El firewall idealmente es inmune a penetraciones, esto implica el uso de técnicas de refuerzo de sistemas o "harderning" y teniendo como base un sistema operativo seguro. Algunas entidades especiales hacen requerimientos estrictos en cuanto a sistemas confiables para albergar el firewall.

Para desarrollar las tareas anteriores, el firewall, hace uso de técnicas básicas las cuales le permiten llevar a cabo el control de acceso y el cumplimiento de las políticas de seguridad. Algunos sostienen que los firewalls originalmente se enfocaban en la técnica de control de servicios pero hoy en día son capaces de aplicar cualquiera de las siguientes:

- Control de servicios: Determina el tipo de servicio de internet al que se puede tener acceso, ya sea entrante o saliente. En esta el firewall debe filtrar el tráfico en base a direcciones IP, protocolos, puertos y debe a la vez proveer servicio proxy que reciba e interprete cada solicitud de servicio antes de dejarla pasar.
- Control de direcciones. Determina la dirección en la que una solicitud de servicio es iniciada y permitida a fluir a través del firewall.
- Control de usuarios. Controla el acceso a cierto servicio de acuerdo a que usuario está intentando ingresar. Esta función es regularmente aplicada a usuarios locales, es decir, dentro del perímetro. Esta operación debe también ser aplicada al tráfico entrante (de usuarios externos) que luego requerirán algún tipo de autenticación, como IPSec por ejemplo.
- Control de comportamiento. Controla cómo un servicio en particular es usado.

Los firewalls también tienen ciertas limitaciones, a continuación enumeramos algunas:

- El firewall no puede proteger contra ataques que sobrepasan el firewall (bypass).
- El firewall no puede proteger a los sistemas de amenazas internas como un empleado disgustado o uno que colabore con atacantes externos.
- Una red LAN inalámbrica insegura tiene acceso disponible desde fuera de la organización. Un firewall interno que separa porciones de la red organizacional no puede garantizar las comunicaciones inalámbricas entre los sistemas locales en diferentes lados del firewall interno.
- Diversos dispositivos móviles (Laptops, PDAs, USBs) pueden ser usados e infectados una vez estando fuera de la red luego usarse internamente propagando así una amenaza [20].

E. Sistemas de detección de Intrusos (IDS) y prevención (IPS).

La detección de intrusos, en términos de seguridad informática, se refiere al proceso de monitorear los equipos y toda la actividad de red relacionada con los activos tecnológicos para analizar ciertos eventos en busca de señales o muestras de intrusión en los sistemas. El objetivo principal de buscar por accesos no autorizados es alertar a los administradores de cualquier brecha o vulnerabilidad en los sistemas.

1) IDS.

Un sistema de detección de intrusos se diseña para monitorear tanto la actividad de red interna como externa e identificar cualquier patrón sospechoso que pueda indicar un ataque a nuestra red o los sistemas mismos, por parte de alguien intentando comprometer nuestros activos. IDS es considerado como una forma de monitoreo pasivo ya que su función es advertir de la actividad sospechosa llevándose a cabo, no prevenir que ocurra. Un IDS esencialmente revisa los datos y el tráfico de red para identificar ataques, amenazas y vulnerabilidades. Un IDS puede así responder a un evento sospechoso de una de muchas maneras, como por ejemplo mostrando una alerta, registrando el evento o incluso localizando al administrador. En algunos casos un IDS puede inducir a la reconfiguración de la red para reducir el efecto de futuras intrusiones.

Un IDS específicamente busca por actividad que resulte sospechosa o eventos que puedan ser el resultado de un virus, un worm o gusano, o un hacker y esto se logra a partir del conocimiento de firmas de ataques o firmas de intrusión documentados al igual que operan los antivirus. Así un IDS será capaz de notificar sólo ataques conocidos contenidos en las firmas.

Existen varias maneras en las que se pueden categorizar un sistema IDS, en base a su operación hablamos de:

a) Detección de abuso vs. Detección de anomalías. El IDS analiza la información que obtiene del monitoreo de la actividad en la red y lo compara con una extensa base de datos de firmas de ataques. Básicamente busca en esa base por un ataque específico que ya ha sido documentado previamente, al igual que lo hacen los sistemas antivirus. El software de detección será tan bueno como lo sea la base de datos de firmas de intrusión contra la que se compare la información obtenida.

b) Sistemas pasivos vs. Reactivos. La diferencia esencialmente radica en que un IDS como sistema pasivo detecta una potencial brecha de seguridad, registra la información y señala el resultado, mientras que un IDS como sistema reactivo responde a la actividad sospechosa cerrando la sesión del usuario o reprogramando el firewall para bloquear el tráfico proveniente de dicha fuente.

c) Basados en red vs. Basados en host. Un sistema de detección de intrusos puede ser una solución basada en red o basada en host. Uno basado en red, también llamado NIDS a menudo es un dispositivo de hardware independiente que incorpora capacidades de detección. Técnicamente su implementación incluye la instalación de sensores en varios puntos a través de la red o también puede lograrse con software instalado como un sistema conectado a la red el cual deberá analizar los paquetes entrando y dejando la red. Un sistema de detección basado en host, conocido como HIDS no ofrece detección en

tiempo real pero si se configura adecuadamente puede lograrse una buena aproximación.

El desempeño dependerá del tamaño de la red y del número de hosts que requieran la operación de detección; generalmente NIDS resulta una solución más barata de implementar requiere menos administración, pero no resulta tan versátil como HIDS. Un factor que no debemos olvidar es asegurar el acceso a internet y el ancho de banda para que estos sistemas actualicen periódicamente la base de datos de firmas de intrusión con las que se tengan disponibles hasta la fecha.

Es importante en esta etapa mencionar que no es lo mismo un firewall a un IDS y es un error común confundirlos y hasta pretender que uno puede sustituir al otro. Un IDS difiere de un firewall a que este último busca intrusiones a fin de detenerlos, mientras que el firewall limita el acceso entre redes para prevenir la intrusión pero no señala un ataque desde dentro de la red. Un IDS evalúa la intrusión sospechosa y una vez que se llevó a cabo indica su aparición. Un IDS no reemplaza a un firewall o a un antivirus. Debe ser considerado como una herramienta a utilizar en conjunto con los demás productos de seguridad para incrementar así la seguridad a nuestros activos tecnológicos.

2) IPS.

Un sistema de prevención de intrusos es en definitiva el siguiente nivel de seguridad tecnológica, el cual es capaz de proveer seguridad a todos los niveles, desde el núcleo del sistema operativo hasta paquetes de red. Este provee políticas y reglas para el tráfico de red junto a un IDS para alertar a los administradores de sistemas y administradores de red de la presencia de tráfico sospechoso pero permitiéndole a ellos establecer las acciones al ser notificados de ello. Mientras un IDS informa de un potencial ataque un IPS hace el intento de detenerlo. IPS tiene la capacidad de prevenir ataques basado en las firmas de intrusión a conocidas, pero también ciertos ataques desconocidos debido a que incorpora una base de datos que le dice cómo actuar ante ataques desconocidos, en cierta medida como comportamientos genéricos antes dichas acciones. Aunque un IPS puede ser visto como una combinación de un IDS y un firewall de capa de aplicación, IPS es generalmente considerado como la siguiente generación de un IDS [21]

VII. Gestion de la Seguridad de la Información en Redes definidas por software.

Como parte de un sistema de gestión de seguridad de la información (SGSI), siempre se deben de definir una estrategia para una adecuada planificación, implementación, monitoreo y mejora de una política de la seguridad de la información integrando los controles adecuados para el aseguramiento de la infraestructura de TI. La relevancia que tiene la infraestructura de red para una organización y en general una red definida por software debe de seguir dicha estrategia. De acuerdo a la Norma ISO/IEC 27001:2005 y la Norma ISO/IEC 27001:0213 (que es la más reciente) hay muchos ítems o actividades que se deben de completar con respecto a la implementación del SGSI [22]

Muchas de las etapas definidas dentro de las normas hacen referencia con la parte organizacional y de gestión en general del SGSI para la finalización del Sistema de Gestión y Política de la Seguridad de la Información. Pero la gestión del riesgo y definición de elementos a tomar en cuenta dentro de una auditoría, que se ve contenida en dichas normas, toma relevancia cuando se busca realizar un cambio dentro de la infraestructura de red, aún más dentro de la transición de una red convencional a una red SDN.

Por lo anterior se establece que solo una parte, de cada una de las fases, se debe de tomar en cuenta ya que la aplicabilidad dentro del SGSI para una infraestructura de red SDN no debe de considerar todo el cúmulo de actividades que se tienen en ambas versiones de la ISO (2005 y 2013), sino más bien tomar en cuenta únicamente las que tienen relevancia dentro de las cuales se consideran los siguientes ítems y actividades.

- Metodología de evaluación de riesgos
- Inventarios de activos
- Identificar amenazas y vulnerabilidades
- Identificar impactos
- Análisis y evaluación de los riesgos
- Definir plan de tratamiento de riesgos
- Implementar plan de tratamiento de riesgos
- Implementar los controles

Cada una de las tareas, se puede ubicar en determinadas fases, las que se apegan en distinta medida al ciclo de Deming. Planificación, Ejecución, Monitoreo y Mejorar (Planear, Hacer, Monitorear y Actuar). Aunque en la más reciente versión, ISO27001:2013 se ha disminuido el énfasis a dicho ciclo, se puede notar que todas las tareas anteriormente listadas hacen referencia a gestión de riesgos de los sistemas de TIC y Auditoría de TIC. Inclusive en ambas normas se ha mantenido la gestión del riesgo y los controles como un pilar fundamental para la gestión de la seguridad de la información y en general de un SGSI.

A. Gestión de Riesgos en una red SDN.

1) Metodología de evaluación de riesgos.

Como se establece inicialmente dentro de la ISO 27001, se debe de seleccionar una metodología que se utilizara para la gestión y evaluación de riesgos. Lo que se define dentro de la norma es que esto parte de la fase de planificación, donde la metodología que se decida utilizar, se debe de tener clara y bien definida para que la misma puede ser utilizada para toda la infraestructura de TI y no una específica por el tipo de Infraestructura (Redes, servidores, almacenamiento, etc.).

Esto es realmente parte de lo que se define dentro del alcance del SGSI, considerando que la ISO 27001 no identifica una metodología como parte de su estándar se debe de considerar la utilización de cualquiera de las metodologías disponibles que se apegue más a las necesidades organizacionales.

Dentro de los más populares se pueden mencionar Mehari, Magerit, NIST800-30 y Guía de Gestión de Seguridad de Microsoft. Estos cuatro fueron evaluados y comparados por [23] considerando que en ninguno de estos marcos se encuentra una deficiencia o mejora por sobre dichas metodologías para que sea considerado como un marco más idóneo para evaluación del riesgo de la infraestructura de red SDN. Ya que todas las metodologías se consideran independientes de la infraestructura que se considera evaluar.

2) Identificación de activos..

La identificación de activos con respecto a la conectividad que se mantiene en redes convencionales y redes SDN, puede resultar parecido sin importar el tipo de red por sobre la cual se requiere realizar el análisis y gestión del riesgo. Esto considerando que la ubicación y el componente tienen una funcionalidad similar, como es el caso de los dispositivos de reenvío en comparación con los equipo de comunicación convencionales (router, switches, firewalls, etc.) que mantienen una ubicación física similar, siendo dispositivos intermedios que interconectan a través de distintos medios los dispositivos finales.

Otro elemento que se identifica dentro de la red SDN es el plano de gestión que mantiene el control, monitoreo y gestión frente al administrador de dicha infraestructura. Esta infraestructura es independiente, utilizando elementos separados (del mismo o diferente fabricante) y normalmente en redes convencionales de escala corporativa tiene una infraestructura homóloga o prácticamente igual a la que se podría tener en una red SDN. Este es realmente el centro de monitoreo y gestión que ya se maneja en los denominados Centros de Operación de Red (NOC), que en lo único en que diferencia de SDN, es que puede de cierta medida simplificar la cantidad de dispositivos y procesos a gestionar generando capacidades de valor agregado dentro de la gestión misma.

Pero hay componentes que únicamente se pueden identificar en una red SDN como la controladora, que es la que mantiene la comunicación con los dispositivos de reenvío a través de las interfaces descendentes (como Openflow) como ya se ha aclarado en capítulos anteriores. Las controladoras son un activo centralizado o semi-distribuido en múltiples centro de datos para generar redundancia. Incluso en este caso el mismo protocolo de conexión de interfaz descendente y ascendente se puede identificar como un activo de la infraestructura de red SDN.

En base a lo anterior se identifican únicamente los activos por su función dentro de la arquitectura de SDN, sin considerar ubicación física, cantidad u otras consideraciones que normalmente atiende a esta fase de identificación, considerando de igual manera la importancia o valoración del componente dentro de la operatividad de la arquitectura, considerando únicamente tres valores (bajo, medio o alto)

Componente	Valoración
Dispositivo de reenvío	Baja
Interfaz descendente	Media
Controladora	Alta
Interfaz ascendente	Media
Dispositivo de administración.	Alta

Tabla 1 – Identificación de Activos

Se debe de tener en cuenta que dicha apreciación debe de realizarse en cada organización y la anterior es solamente una referencia para identificar una metodología de gestión riesgo genérica que se puede considerar dentro de una red SDN.

3) Identificación de amenazas e identificación de impactos.

Cualquier infraestructura de red por su alta relevancia como activo en general de la infraestructura de tecnologías de la información y comunicación, resulta ser un activo siempre muy perseguido por los atacantes viéndose fácilmente expuesto a amenazas y vulnerabilidades sin importar necesariamente el tipo de organización. Incluso cuando se materializa alguna amenaza u ocurre un evento disruptivo sobre toda la infraestructura de TIC de una organización, parte de las primeras acciones de recuperación que se realizan van orientadas a la infraestructura de red para habilitar los servicios de TI que la organización considere críticos para su operación.

Como parte de la identificación de riesgos, se deben de considerar las amenazas y vulnerabilidades de redes SDN de cada uno de sus componentes y en general de la arquitectura. [8] Ya han mencionado algunos de estos vectores de riesgo que son considerados una amenaza para este tipo de infraestructuras. Sin dejar de lado las ventajas que traen las redes SDN con respecto a la seguridad de la información, se deben de considerar alguno riesgos identificados que pueden ser específicos Por lo anterior es importante validar si la amenaza o riesgo no sea algo ya existente en un tipo de red de datos.

Dentro de las amenazas que pueden explotar vulnerabilidades intrínsecas en redes SDN se pueden dilucidar dos bajo el entendimiento de la arquitectura y su operación:

a) La programabilidad de la red. A pesar de ser uno de las partes intrínsecas de SDN, se debe de comprender que la habilidad de controlar la infraestructura de red a través de un software, la hace vulnerable al mismo nivel que lo es el lenguaje de programación, el sistema operativos y cualquier otro sistema que se utilice e involucra el desarrollo e implementación de dicha programabilidad.

b) La centralización de la controladora. El cerebro de la red no solamente puede resultar como un punto único de falla de acuerdo a la implementación que se realice, si no también que es un punto donde el acceso autorizado o no

autorizado al sistema conlleva un control potencial e inequívoco de la totalidad de la infraestructura de la red.

Por lo anterior se puede considerar que dentro del dimensionamiento de las redes SDN en diferentes planos, se pudiesen considerar planos alternos como el plano de falla (falla de una persona, infraestructura, proveedor u otras) y el plano de ataque. Considerando que estos planos ahora podrían resultar parte de una arquitectura de red innovadora y adaptable a cambios pero también con vulnerabilidades adicionales en las que la separación de los planos de control y reenvío no posibilitaba.

Dentro de las dos premisas anteriores y en base a la investigación realizada por [9] se han reconocido siete vulnerabilidades, o como también le denominan siete vectores de amenazas que parecen ser parte del tipo de arquitectura que se propone en SDN.

a) Vector de Amenaza 1: Flujos de tráfico falso.

Este es uno de los ataques que puede ser lanzado o visto como un ataque de denegación de servicio, llenando las tablas dinámicas de reenvío los switches o dispositivos de reenvío (Switches OpenFlow) agotando los recursos del switch para reenviar tráfico o incluso agotar recursos de la controladora. No necesariamente se puede explotar dicha vulnerabilidad con un dispositivo final controlado por un atacante o usuario malicioso, si no también por un dispositivo final o de un dispositivo de reenvío que no está funcionando correctamente. Para este tipo de vulnerabilidad se puede considerar que no existe un control específico de autenticación, como se podría hacer en un red convencional, ya que si asume que el atacante tiene acceso o privilegios a los planos superiores puede identificar puertos, usuarios o direcciones físicas de las tarjetas de red (MAC) para generar un tráfico que cumpla con los requisito de validez siendo aún un tráfico falso (no deseado).

b) Vector de Amenaza 2: Ataque sobre las vulnerabilidades de los switches o dispositivos de reenvío.

Esta amenaza se puede potencializar rápidamente utilizando un único switch siendo el mismo controlado por un usuario malicioso o un atacante haciéndose pasar uno de los dispositivos conectado a la controladora maestra, logrando así detener el reenvío de tráfico valido, o demorar el reenvío o incluso logrando clonar o reenviar copias no autorizadas del mismo tráfico a otro dispositivo con el objetivo de robar información dentro de la misma infraestructura de red. Teniendo el control de dicho switch incluso se pudiese generar una sobrecarga de una controladora o de los switches adyacentes o vecinos a nivel de capa 2 potencializando más el riesgo de materialización de dicha amenaza.

c) Vector de Amenaza 3: Ataque sobre las comunicaciones de Plano de Control o Interfaz Descendente.

Dentro de los protocolos que se utilizan para la comunicación de mensajes entre el plano de reenvío y el plano de control, se conocen muchos protocolos no solamente de comunicación en sí, si no también protocolos de cifrado para asegurar el tráfico que existe entre la controladora y los dispositivos de reenvío. TLS/SSL es uno de los protocolos que actualmente se utilizan para garantizar esta confidencialidad del mensaje de control incluyendo a la infraestructura necesaria de PKI que el mismo protocolo requiere, para cifrar los mensajes que se envían por la interfaz descendente. Pero ya es conocido que TLS/SSL [24] por varios artículos e investigaciones al respecto que la infraestructura PKI y TLS/SSL no tiene totales garantías de seguridad para cifrado de la comunicación.

Dentro de cualquier protocolo, algoritmo o infraestructura que se tenga para cifrar la comunicación entre la controladora y los dispositivos de reenvío, se debe de considerar que esta comunicación es tan segura como el eslabón más débil dentro de todo el sistema. En este caso específico, logrando el descifrado de los mensajes de la interfaz descendente, se puede ganar el acceso no autorizado al plano de control o al panel de reenvío dentro del cual se puede alterar la confidencialidad, integridad y disponibilidad de la información o tráfico que circula por la infraestructura de red SDN.

d) Vector de Amenaza 4: Ataque sobre las vulnerabilidades en las controladoras.

Este es una de las amenazas que podría causar un mayor riesgo sobre toda la infraestructura de red SDN. Una controladora que este fallando o manipulada por un atacante compromete inmediatamente toda la infraestructura de red. Dentro de la controladora se deben de mantener controles de seguridad, constantes endurecimientos de seguridad y otra cantidad de medidas necesarias para poder garantizar que la controladora no se vea comprometida por una vulnerabilidad.

Se debe de tener en cuenta que este uno de los componente que al ser más críticos dentro de la red, resultan más atractivos para los atacantes que quieran comprometer la seguridad de la información de una organización, y no solamente la infraestructura de red. En este caso, todos los protocolos, lenguajes de programación, imágenes de sistema operativo, copias de recuperación y cifrado que se pueda mantener deberá de ser protegido para que no vea vulnerado dicho componente. Pero nuevamente, la controladora podrá asegurarse como tanto se asegure el eslabón más débil dentro de toda la cadena que conforma el sistema de la misma.

e) Vector de Amenaza 5: Falta de mecanismos de confianza entre la controladora y la aplicación de administración.

La comunicación entre el plano de control y el plano de administración que se lleva a través de la Interfaz ascendente (north-bound interface) y sus respectivos protocolos contienen controles y mecanismos de autenticación u otros elementos necesarios para establecer dicha comunicación de manera segura, evitando que se generen el no repudio, confidencialidad, integridad manteniendo de igual manera la disponibilidad de la misma comunicación. En este caso un atacante o un dispositivo mal configurado pueden generar una administración no deseada de la red, enviando programaciones específicas a la controladora que puedan poner en riesgo la seguridad de la información que baja por la red.

f) Vector de Amenaza 6: Explotación de las vulnerabilidades de la estación de trabajo dentro del plano de administracion.

El plano de administración que es donde se definen finalmente las políticas y el dispositivo final que genera las directrices y son comunicadas a través de la interfaz ascendente, se puede ver comprometida a la explotación de vulnerabilidades intrínsecas de su sistema operativo y software de aplicación que se utilice para la generación del rol de administración. Este puede ser otro punto donde un atacante puede buscar el control total de la red a través del control de estas estaciones de trabajo de administración.

Dentro de la abstracción de SDN y OpenFlow podría parecer que estas quedan fuera del alcance de definición de la arquitectura de una red definida por software, ya que las estaciones o computadoras que utilicen los administradores dentro del plano de administración realmente trabajan de manera independiente, pero debe de tomarse en cuenta ya que finalmente es una de las puertas que se tienen para generar el control de la red.

g) Vector de Amenaza 7: Falta de herramientas confiables de análisis forense y recuperación.

La recuperación de una red SDN como parte de su arquitectura se ha vistos como un tema de auto-recuperación, ya sea que se trate de incidente disruptivo, un incidente de la seguridad de la información u otro tipo de incidente. Esto debido a la misma programabilidad, que se puede tener en la red y que genera directrices de acomodamiento automatizados para la misma recuperación. Pero de igual manera se debe de tener claro que muchas de las investigaciones forenses, bitácoras de incidentes o incluso base de lecciones aprendidas requiere que se mantenga una información confiable sobre la recuperación o manejo de un incidente.

Si dentro de la abstracción del plano de administración y del plano de control se generan acomodamientos de la infraestructura, se debe de tener claro que las instrucciones o cambios realizados por el elemento automatizado puede que contenga información equivocada o errónea respecto a las medidas que realmente se ejecutaron

4) Análisis y evaluación de los riesgos.

Para realizar un análisis y evaluación de los riesgos, se debe de tener en cuenta que se debe de seguir la metodología específica y que se debe de definir como parte de la planificación del SGSI o específicamente dentro de la política de seguridad de la información de la organización en sí. En este caso, se definen una metodología genérica y de matrices para el análisis y evaluación del riesgo considerando los posibles impactos a la infraestructura de red directa y únicamente, en lugar de considerar toda una infraestructura de TIC (como debe de realizarse en un ambiente organizacional).

Adicionalmente, se debe de considerar que la probabilidad de que alguno de los vectores de riesgo se materialice, considerando dentro de esto la probabilidad del mismo. Se debe de asumir la existencia de medidas de aseguramiento intermedias y que los posibles ataques explotan las vulnerabilidades que se consideran más atractivas desde el punto de vista de un atacante. Por lo que prácticamente todas las probabilidades de ocurrencia oscilaran por objetivos de análisis dentro del 0%, 25%, 50%, 75% y 100%.

Dentro de esta metodología genérica se debe de realizar inicialmente una matriz de vector de amenaza contra los activos para poder dimensionar el impacto estimado de materialización de acuerdo a la valoración previa que se ha realizado del activo.

Vector de Amenaza	**Activo del Vector**
Vector 1	Dispositivo de reenvío
Vector 2	Dispositivo de reenvío
Vector 3	Interfaz descendente
Vector 4	Controladora
Vector 5	Interfaz ascendente
Vector 6	Dispositivo de administración
Vector 7	Controladora / Dispositivo de Administración

Tabla 2 – Matriz Amenazas/Activos

Considerando la matriz anterior se facilita la validación del impacto del vector en base a una matriz de probabilidad contra impacto. Los impactos son identificados como alto, medio o bajo en base a la matriz de colores también definida dentro de la identificación de activos.

Matriz de riesgo e impacto	**Probabilidad de ocurrencia**				
	0%	**25%**	**50%**	**75%**	**100%**
Vector 1	Bajo	Bajo	Bajo	Medio	Alto
Vector 2	Bajo	Bajo	Bajo	Medio	Alto
Vector 3	Bajo	Bajo	Medio	Medio	Alto
Vector 4	Bajo	Medio	Alto	Alto	Alto
Vector 5	Bajo	Bajo	Medio	Alto	Alto
Vector 6	Bajo	Bajo	Medio	Alto	Alto
Vector 7	Bajo	Bajo	Bajo	Medio	Alto

Tabla 3 – Matriz de Riesgo e Impacto

5) Implementar plan de tratamiento de riesgos e Implementar los controles.

De acuerdo a la gestión del riesgo se determina que la implementación de ciertas medidas que se pueden tomar para mantener SGSI y la seguridad de la información en general

dentro de la infraestructura de TIC y en este caso de la red SDN. Se debe de tener en cuenta que hay medidas o soluciones específicas dentro del diseño e implementación de una red SDN que se puede mantener para dar un tratamiento a los riesgos previamente identificados antes de poner en operación la red.

La replicación dentro de la infraestructura, la diversidad de fabricantes, habilitación de mecanismo de confiabilidad de los mensajes de interfaces descendentes y ascendentes, el aseguramiento de todos los componentes en general de la red y la actualización de parches son elementos que siempre se deben de tener en cuenta para una red definida por software. Estos elementos no son ajenos en su mayoría al aseguramiento de una red convencional.

VIII. Conclusiones

Las redes definidas por software como parte de las recientes innovaciones tecnológicas, han tenido en cierta medida una lenta adopción. El desconocimiento de la arquitectura de las redes SDN y su operación, sumado a una falta de estrategia con respecto a la gestión del riesgo dentro del Sistema de Gestión de Seguridad de la Información puede llevar a una implementación de SDN inadecuada, poniendo en riesgo en general la seguridad de la información.

Pero si la gestión del riesgo dentro del sistema de gestión de la seguridad de la información se tiene una estrategia clara y alineada con las metas organizacionales, la decisión de la implementación de una red SDN no trae mayores inconvenientes que cualquier red convencional. Incluso, cualquier tecnología sin importar los componentes u protocolos que incluyan puede ser dimensionada si es adecuada para la organización si las ventajas y desventajas que estas puedan traer, pueden ser sopesadas a favor de la estrategia de la organización.

En base a esta investigación, se ha visto con claridad que si se deben de considerar ciertos componentes adicionales en lo que respecta a la seguridad de la información cuando se habla de SDN versus redes tradicionales. Pero también es claro que con una adecuada gestión del riesgo, las organizaciones se pueden beneficiar de una reducción de costos de capital y operativos y reducción de costos de oportunidad por innovación al implementar redes definidas por software.

IX. References

[1] J. Merelo, "GeNeura Team," Jueves Marzo 1995. [Online]. Available: http://kal-el.ugr.es/internet/section3_2.html. [Accessed 23 Agosto 2015].

[2] B. Denissse, "Slideshare," 09 Marzo 2013. [Online]. Available: http://es.slideshare.net/biancaDenissse08765/origen-y-evolucion-de-las-redes.

[3] "Cómo el nuevo universo trazado por las redes definidas por software impactará en los negocios," *Logicalis*, 2014.

[4] N. Figuerola, "SDN redes definidas por software," *Wordpress*, 2013.

[5] Cisco, «Cisco's Technology News Site,» Cisco, 29 Julio 2013. [En línea]. Available: http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342. [Último acceso: 2015 Agosto 2015].

[6] T. D. Nadeau and K. Gray, SDN: Software Defined Networks, Chapter6. Data Center Concepts and Constructs., O´REILLY, 2013.

[7] V. Törhönen, Designing a Software-Defined Datacenter, Tampereen: TAMPERE UNIVERSITY OF TECHNOLOGY, 2014.

[8] E. Savolainen, «Cloud Service Models,» de *Seminar – Cloud Computing and Web Services*, Helsinki, 2012.

[9] D. Kreutz, F. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky y S. Uhlig, «Software-Defined Networking: A Comprehansive Survey,» de *Towards Secure and Dependable* , Lisboa, 2014.

[10] Community, «Wikipedia,» Wikipedia, 28 Mayo 2015. [En línea]. Available: https://es.wikipedia.org/wiki/OpenFlow. [Último acceso: 23 Agosto 2015].

[11] W. Stallings, «Software-Defined Networks and OpenFlow,» *The Internet Protocol Journal*, vol. 16, nº 1, 2013.

[12] V. Tiwari, "Chapter 6 - Openflow - Protocol Details," in *SDN and OpenFlow for beginners with hands on labs*, Northville, 2013.

[13] V. Tiwari, «Chapter 7 - OpenFlow in action,» de *SDN and OpenFlow for beginners with hands on labs*, Northville, 2013.

[14] «SDx Central,» SDx Central, 2015. [En línea]. Available: https://www.sdxcentral.com/resources/sdn/what-is-openflow/. [Último acceso: 23 Agosto 2015].

[15] Catbird, «CATBIRD,» CATBIRD, [En línea]. Available: http://www.catbird.com/software-defined-security/software-defined-security-sds-defined. [Último acceso: 24 Agosto 2015].

[16] B. Prasad, Security Issues in Software Defined Networking, Bengali: Jadavpur University, 2014.

[17] Community, «Wikipedia,» Wikipedia, 28 Mayo 2015. [En línea]. Available: https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n. [Último acceso: 23 Agosto 2015].

[18] «ISO 27000.es,» ISO 27000.es, 2012. [En línea]. Available: http://www.iso27000.es/sgsi.html. [Último acceso: 23 Agosto 2015].

[19] ISACA, Manual de preparación al Examen CISA, Florida: ISACA, 2008.

[20] W. Stallings, Cryptography and Network Security, New York: Pearson, 2013.

[21] V. Beal, «Intrusion Detection (IDS) and Prevention (IPS)

Systems,» 15 Julio 2005. [En línea]. Available: http://www.webopedia.com/DidYouKnow/Computer_Science/intrusion_detection_prevention.asp. [Último acceso: 23 Agosto 2015].

[22] ISO / IEC, "Information technology — Security techniques — Information security management systems — Requirements," ISO / IEC, 2013. [Online].

[23] A. Syalim, Y. Hori y S. Kouichi, «Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide,» de *Browse Conference Publications > Availability, Reliability and ... Help Working with Abstracts*, Fukuoka, 2009.

[24] S. J. Vaughan-Nichols, «FREAK: Another day, another serious SSL security hole,» ZDNet, 3 Marzo 2015. [En línea]. Available: http://www.zdnet.com/article/freak-another-day-another-serious-ssl-security-hole/. [Último acceso: 23 Agosto 2015].

Acerca de los autores.

Fogelbach, Rudiger (San Salvador, 8 de Abril de 1986), Ingeniero en Telecomunicaciones, de la Universidad Don Bosco y egresado de la Maestría en Seguridad y Gestión del Riesgo Informático de la misma universidad.

Actualmente desempeñándose como Ingeniero de diseño de infraestructura de telecomunicaciones dentro del sector financiero, contando con más 5 años de experiencia el área de consultoría, diseño e implementación de arquitecturas empresariales.

García, Melvin A. (San Salvador, 14 de Julio de 1986); Ingeniero en Telecomunicaciones de la Universidad Don Bosco y egresado de la maestría en Seguridad y Gestión de Riesgos Informáticos de la misma universidad.

Actualmente desempeñándose como Ingeniero de Optimización de redes móviles en un proveedor de servicios de telecomunicaciones por más de 4 años.

González, Guillermo D. (San Salvador, 29 de Abril de 1984); Ingeniero en Ciencias de la Computación de la Universidad Don Bosco y egresado de la Maestría en Seguridad y Gestión de Riesgos Informáticos de la misma universidad.

Actualmente desempeñándose como Administrador de redes con experiencia de más de tres años en el sector gubernamental.