Redes definidas por software (SDN), un nuevo mundo para la seguridad de red

Aguilar Cruz Alvaro Javier.
ajaguilarcruz@gmail.com
Universidad Piloto de Colombia
Marzo de 2015

Resumen— Este artículo muestra dos temas muy importantes, uno de ellos relativamente nuevo como las redes definidas por software (SDN- Software Defined Network), y otro que se enfoca en la seguridad de red. La idea del artículo es dar la información correspondiente de las SDN su funcionamiento, arquitectura, etc. Y basados en la información de las redes definidas por software informar de estrategias para redes seguras tanto virtuales como físicas.

Abstract— This article shows two very important issues, one relatively new as software defined networks (SDN- Software Defined Network), and another that focuses on network security. The idea of the article is to give the corresponding information for SDN operation, architecture, etc. And based on the information of software defined networks inform strategies to secure both virtual and physical networks.

Índice de Términos— Software Defined Network, Seguridad, Arquitectura de red, Topología de red,

I. INTRODUCCIÓN

Últimamente se ha observado como el mundo de las telecomunicaciones y la tecnología de la información avanza, trasformando cada proceso y tecnología utilizada. Estos cambios como el uso increíble de dispositivos móviles, la opción de computación en la nube, Big Data, la virtualización de equipos, sistemas de almacenamiento, todo esto llevando a grandes cambios en el funcionamiento, necesitando así nuevos sistemas para lograr tener un sistema centralizado. Todo ha cambiado pero las redes y su arquitectura desde 1950 no lo hace y todos los cambios generados en telecomunicaciones y las tecnologías de la información nos llevan al proceso de virtualización de redes o más conocidas como SDN.

La red que se tiene actualmente soporta todas las necesidades, pero se ha vuelto muy compleja y poco flexible para evolucionar a la velocidad de las nuevas aplicaciones, y esto no hace pensar en el uso de nuevas tecnologías a nivel de red que pueden ayudar con las futuras necesidades.

Es aquí donde nace como repuesta el uso de una nueva arquitectura de red. Que permita ser menos compleja, más flexible, más eficiente y mucho más económicas. Lo que se conoce como redes definidas por software.

Todo este cambio nos abre un nuevo mundo donde no todos están dispuestos a ingresar, por el temor de la seguridad, sin bien cuando se habla de un sistema virtual se entiende un costo inferior, también se toma como un riego mayor a recibir ataques informáticos, al no tener control total de sus equipos la idea del artículo es poder brindar unas pautas de seguridad indicando que es posible el uso de nuevos sistemas manteniendo un entorno seguro.

II. REDES DEFINIDAS POR SOFTWARE (SDN)

Para abordar el tema de las redes definidas por software es importante conocer un poco del funcionamiento de la arquitectura actual. Para ello se van a dar unas bases de las redes actuales pero sin ir a fondo ya que no es el enfoque de este documento.

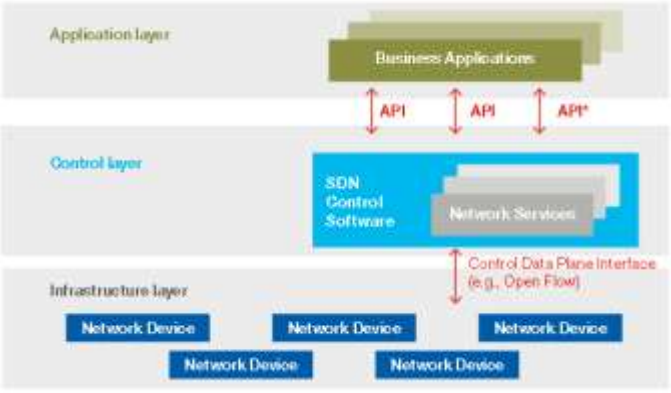
Las redes actuales y más usadas en este momento se enfocan en el modelo OSI y sus equipos más comunes son switch y router. Actualmente para la arquitectura de red se utilizan equipos físicos en las instalaciones de cada compañía y son administrados desde los centros de datos. A groso modo es la arquitectura actual de una red.

Después de conocer un poco de la arquitectura de red actual podemos empezar hablar de las redes definidas por software, el principal cambio que se dio en esta nueva arquitectura es la alteración de la capa de red en el que ocurre control de tráfico. La idea de que una red pueda ser definida por software es que permita separar el plano de control (Software) de los datos, y con esto poder tener redes más programables, atomizadas y flexibles.

Las políticas de tráfico se pueden redefinir rápidamente conforme la empresa lo va requiriendo, en la capa de control sin la necesidad de la configuración de cada switch y de cada router individualmente, esto nos ayuda a poder realizar cambio de manera rápida y efectiva a medida que nuestra organización crece tanto en tamaño, como en tecnologías. Logrando de esta manera la integración de distintos tipos de cambios en cuanto a temas de tecnología logrando el avance en paralelo y no dejando tecnologías obsoletas.

Por lo tanto, fue creado el concepto de redes programables. A partir de esa arquitectura, los elementos de red (routers, switches, firewall, etc.) pasan a tener en su sistema operacional interfaces (APIs) que crearán la posibilidad que aplicaciones no desarrolladas por los fabricantes del hardware interactúen con el plan de control del sistema, tomando decisiones de ingeniería de tráfico basadas en patrones no usuales, tales como: temperatura, costo del link, consumo de energía, entre otros. [1]

A continuación se mostrara la arquitectura lógica de una red definida por software, en donde la inteligencia de la red es lógicamente los controladores de las SDN que mantienen una visión global de la red, con las SDN se podrá tomar un control sobre toda la red desde un único punto, lo que simplifica el diseño de la red.



*API (Application programming interface)

Fig. 1 – Arquitectura de redes definidas por software [2]

Para abordar la visión de separación de plano de datos y de control, se empezó a investigar nuevas arquitecturas para control lógico centralizado. El proyecto 4D, uno de los frutos de estas investigaciones, establecía cuatro capas principales: el plano de datos (data plane), para procesar paquetes basándose en reglas configurables; el plano de descubrimiento (discovery plane), encargado de coleccionar medidas topológicas y del tráfico; el plano de diseminación (dissemination plane), para instalar reglas de procesado de paquetes; y el plano de decisión, que consistía en controladores lógicos centralizados que convertían objetivos a nivel de red en estado de manejo de paquetes. Numerosos grupos de investigación comenzaron el desarrollo de sistemas basados en este enfoque, y en particular, el proyecto Ethane, y su predecesor directo SANE. El despliegue operacional de este proyecto en la universidad de Stanford, comenzó la etapa de creación de Openflow, y en particular, el diseño simple de switch del proyecto Ethane, se convirtió en la base de la API de Openflow. [3]

III. BENEFICIOS DEL SDN

Después de hablar un poco del funcionamiento de las redes definidas por software es importante conocer que beneficios nos puede traer la implementación de este tipo de redes en nuestra compañía, esto es importante ya que al momento de una presentación de nuevas tecnologías frente a una junta directiva en realidad no se le da mucha

importancia a su funcionamiento técnico si no a los beneficios que traerá la implementación de esta tecnología.

El punto primordial a tratar o a mostrar es la reducción de costos, que para una organización es lo más importante. En este caso al momento de realizar la implementación se reducen los costos actuales, en este caso con una infraestructura más sencilla, la utilización de un menor número de profesionales, los costos operacionales de la infraestructura también se reducen, se reduce el costo de cableado al utilizar menos equipos, y reducción en el consumo de energía.

Actualmente los principales problemas con las redes actuales es al complejidad, generada principalmente por la necesidad de protocolos creados para manejar distintas aplicaciones y servicios, actualmente para un cambio es necesario la configuración en diversos niveles en cada componente. Con las redes definidas por software no hay necesidad de usar protocolos ya que los controles no son hechos a nivel de los equipos, y se pueden automatizar procesos que hoy en día se hacen de manera manual, en este caso la complejidad de la red es reducida significativamente. Permitiendo implementaciones mucho más rápidas.

Entrando un poco en el tema que se tratará más adelanté, la seguridad en las redes definidas por software nos pueden garantizar mayor disponibilidad, confiabilidad y seguridad del ambiente ya que se elimina la necesidad de configuración de los equipos de la red, reduciendo riegos de fallas y consecuentes indisponibilidades, que actualmente se presentan por cambios en los equipos de la red.

La implementación de SDN nos permite un control centralizado, permitiendo administrar diferentes proveedores a partir de un punto central.

Una de sus mejores beneficios es la rápida respuesta a los cambios del negocio, con una configuración más simple y control centralizado los administradores de red consiguen adecuar la infraestructura según la necesidad de la organización.

IV. MODELOS DE DESPLIEGUE DE SDN

Hay dos modelos: proactivo y reactivo. Cuando un flujo llega a un switch se realiza un mapeo de la tabla de flujos. En el caso de que no se encuentre coincidencia, se envía una petición al controlador para instrucciones más extensas. En modo reactivo, el controlador actúa después de estas peticiones y crea una regla en la tabla de flujos para el paquete correspondiente si es necesario. En modo proactivo, sin embargo, el controlador llena entradas de la tabla de flujos para cada posible coincidencia de tráfico para ese switch, algo parecido con las típicas entradas de tablas de enrutamiento. Además de estos modelos por separados, se puede combinar en una red ambos modelos en forma de un híbrido, para aportar las ventajas de ambos. [4]

V. PROGRAMACIÓN DE REDES SDN

La mayor de las ventajas de las redes definidas por software es la posibilidad de programar las redes y definir procesos.

La mayor parte de la programación de la SDN, reside en las API abiertas northbound y southbound. Las redes definidas por software permiten que la red sea mucha más ágil y flexible, pero esto se debe a la trasformación de la red a una programable permitiendo mayor posibilidad de cambio.

Dentro de los procesos programables dentro de una red definida por software esta la opción de ajustar los flujos, en este caso se centra en Openflow, permitiendo a los controladores de SDN interacción con equipos de red permitiendo controlar el tráfico que fluye ayudando a esta a liberar según la solicitud de la misma.

El Soporte de aplicaciones es otra opción programable, en este caso se preocupa por la coordinación, automatización para desplegar un

gran número de aplicaciones y servicios nuevos, que anteriormente se trabajaba con la configuración de protocolos en los destinos dispositivos de la red. Adicionalmente se pueden manejar las excepciones de la red para medir mejor las necesidades de las aplicaciones.

Por último se puede realizar la programación de las redes para automatizar procesos en donde no se requiere la intervención de un administrador de red, en caso de falla ya que ella estará programada para buscar la solución más efectiva para ser implementada de manera automática, creado una red inteligente.

VI. IDEAS POR FABRICANTE SDN

A continuación se muestran las distintas ideas acerca de redes definidas por software de cada fabricante.

Alcatel: SDN es una herramienta nueva (y distinta) que pretende solucionar unas necesidades que antes no teníamos. Permitirá dimensionar, provisionar y consumir esta plataforma de forma dinámica así como tarificar por consumo y tiempo a imagen de los actuales entornos virtuales de computación. Es importante conocer los problemas reales de los clientes y ver qué puede aportar SDN. La propuesta de valor pasa por definir un entorno de networking y APIs en el que primen la interoperabilidad, la apertura de estándares y la flexibilidad. [5]

Cisco: SDN permite resolver las nuevas necesidades que los clientes tienen, dado que el mundo ha cambiado (movilidad, conectividad…) y aún seguimos operando las redes como hace diez años. Es necesario evolucionar las redes a los requerimientos actuales y resolver el problema de su provisión y gestión. La red, que se encuentra entre las aplicaciones y los usuarios, sabe en cada momento lo que está sucediendo -dónde están los usuarios, la demanda existente, posibles congestiones…-y, utilizando APIs, ha de exponer esa información, para que seamos capaces de explotar dicho conocimiento. [6]

HP: Lo novedoso de SDN es que, por primera vez, tenemos una plataforma que de forma sencilla va a permitir que las aplicaciones programen la red configurándola en tiempo real, en función de los requisitos de conectividad que tengan. De esta forma, la red se alinea con los requisitos de negocio. La propuesta de valor se plantea como un ecosistema abierto, con la generación de aplicaciones y el uso de la red a través de APIs abiertas. Es necesario que no sólo participen los operadores y grandes fabricantes, sino también empresas pequeñas para generar valor porque SDN aporta ventajas extensibles a empresas de todos los tamaños. Por otro lado, es importante aprovechar también las redes ya existentes, para permitir una coexistencia que proteja las inversiones del cliente. [7]

Juniper: en realidad muchos de los conceptos de SDN no son nuevos. La cuestión es que seguimos "obligando" a los sistemas y aplicaciones a entender el lenguaje de los elementos de la red. Es necesario pasar a una arquitectura software de abstracción en la que el Controlador se encargue de procesar el lenguaje de la red. SDN nos permitirá preocuparnos del "qué" en vez del "cómo", poder automatizar la manera en que se implementan las cosas frente a la necesidad de lo que necesitamos conseguir. La propuesta de valor busca la simplicidad y una mayor agilidad en la interacción con la red. [8]

VII. SEGURIDAD EN REDES

Actualmente la seguridad de redes se basa en el uso de dispositivos y configuraciones específicamente se utilizan firewall y antivirus, con el trascurso del tiempo se ha podido determinar que no solo con el uso de estos dispositivos se puede mantener una red segura, aunque para muchas organizaciones aún se basa su sistema de seguridad en firewall, suponiendo que con el solo uso de este equipo en la red se mantendrá seguro.

Los firewall son dispositivos muy robustos que me permiten mantener mi red aislada, pero no tienen nada que hacer en el caso de usar ingeniería social,

el firewall en un sistema que se ubica entre dos redes y que ejerce una política de seguridad, específicamente se encarga de proteger una red confiable de una no confiable, en el caso de cualquier organización una red externa como lo es internet o redes de otras organizaciones que tienen contacto con la nuestra, la idea es limitar los accesos que no se permiten protegiendo mi red, esto lo puede hacer en los dos sentidos desde adentro hacia afuera y viceversa.

Las principales desventajas de los firewall es que se limita a configuraciones dadas por un administrador, el firewall no es inteligente. Esto genera que cualquier hueco que no se tape cualquier atacante lo pueda explotar se es descubierto esto deja nuestra red expuesta.

Cuando se habla de seguridad en redes se debe tener en cuenta la arquitectura de la red y los equipos usados, es importante conocer que servicios se van usar para así mismo poder realizar configuración seguras para cada uno de los servicios y aplicaciones a utilizar, en el caso de redes se empieza a diseñar la seguridad desde el momento en el que se diseña la red.

Actualmente se tiene configuraciones propias dentro de los equipos de red que permiten tener un control y seguridad mínima en la red, pero que son útiles al momento de proteger nuestro sistema. Es muy común la utilización de restricción por MAC en una red wireless, pero no es la única opción de proteger nuestra red, por ejemplo se puede limitar la conexión a cierta cantidad de funcionarios los cuales autentican por medio de LDAP, tanto los funcionarios como las equipos que se conectan tienen asignados grupos correspondientes para realizar la conexión limitando el uso de la red a personas específicas.

En las redes actuales se pueden realizar configuraciones que nos ayudaran a tener un control de los equipos que se conectan. Es el caso de la configuración de bloqueos de conexión por medio de la configuración de un port-security para evitar que cualquier movimiento en la red. Esto se implementa como prevención a conexión de equipos que permitan la conexión de personas no autorizadas a la red, por medio de dispositivos como Access Point, etc. Con esta configuración se logra un control por parte del administrador, aunque no es muy productiva, ya que se requiere realizar movimientos de equipos en la organización generan mayor carga sobre el administrador para habilitar las conexiones.

Dentro de las configuraciones propias de los equipos se pueden definir contraseñas y tipos de conexión normalmente se habilitan conexiones por medio SSH o telnet para la administración de estos equipos, la idea es no dejar configuraciones de fábrica del router para evitar accesos no autorizados. Lo ideal al momento de configurar el acceso de administradores a la red es no habilitar telnet ya que es una conexión en claro, lo recomendable para una conexión de administradores es por medio de SSH cifrando la clave logrando así un poco más de confianza en la personas que acceden a los equipos. Adicionalmente se puede realizar la conexión con el usuario de red, dando los permisos por directorio activo y bloqueando la conexión del equipo por medio de usuario local cuando se encuentre conectado a la red el equipo al cual se desea acceder.

Lo más importante al momento de implementar una red es la seguridad de la misma, es importante tener en cuenta lo nombrado anteriormente, y que para una seguridad óptima se requiere desde el diseño de red tener en cuenta las distintas variables y cambio de la red, es decir, debemos tener en cuenta aplicaciones y servicios que se utilizaran y realizar un cálculo en el diseño mayor para un posible crecimiento del mismo, para evitar entrar en conflicto con nuevas configuraciones y perder seguridad implementada desde el diseño.

VIII. SEGURIDAD EN REDES DEFINIDAS POR SOFTWARE

Siempre que se habla de cambio de tecnologías

todas las organizaciones tienden a desconfiar un poco, se desconfía por la estabilidad, el costo y la seguridad que no es un tema nuevo pero que si desde hace poco tiempo se tiene en cuenta al momento de realizar cambios de sistemas o tecnologías, es por ello que lo que se quiere mostrar es como las redes definidas por software aunque son una tecnología nueva pueden tener una estructura de seguridad definida.

Las redes definidas por software llevan su capa de control a un controlador SDN dedicado encargado de gestionar la red, funciones y servicios tanto de redes virtuales y físicas. En los sistemas de seguridad se ofrece un mayor nivel de análisis, monitores y control de tráfico de manera centralizada y esto ayudara con la prevención de ataques en la red.

Gracias a la estructura de las redes definidas por software se puede realizar un monitoreo centralizado, permitiendo tener un control y realizar el seguimiento y análisis de información que pasa por la red, que anteriormente se podría tener con capturas SPAN o port mirror, esto ayuda a la disminución de equipos y configuración ya que con las SDN tengo un control centralizado.

La ventaja de utilizar redes definidas por software para la seguridad de redes es la posibilidad de usar su utilidad de control centralizado para así mismo lograr centralizar la seguridad de red, es de aquí donde nace otro concepto como lo son las SDM que es monitoreo definido por software, logrando utilizar cierta cantidad de recursos para la seguridad y de manera efectiva y central dentro de los mismos equipos de red sin necesidad de tener en cuenta los servicios y protocolos.

Las redes definidas por software a partir de su llegada ha surgido términos referentes a su funcionamiento y la seguridad no podría quedarse atrás. Es de allí donde nace el concepto de SDS que no es más que seguridad definida por software y de igual manera de las SDN nos permite implementar y automatizar procesos como la detección de intrusos y otros controles de seguridad de la red con software.

La seguridad definida por software nos ofrece la posibilidad de mejorar la seguridad de nuestra organización.

Algunos de los beneficios que nos brindan las SDS son los siguientes:

Permite a las empresas organizar grupos y sistemas de seguridad específicos (por ejemplo, con políticas para hosts, aplicaciones y entidades de red similares) que cruzan las fronteras físicas y lógicas y han demostrado ser difíciles de manejar con cualquier apariencia de eficiencia.¨

Facilita dominios de seguridad dinámicos para móviles, nube y en todos los sistemas de redes empresariales tradicionales, permitiendo a las organizaciones montar y desmontar sistemas a voluntad y, al mismo tiempo, ser capaces de hacer cumplir consistentemente las políticas de seguridad en todos los ámbitos, independientemente del momento y la ubicación de estos sistemas.

Ofrece una mejor integración con otras tecnologías definidas por software que las empresas ya pueden tener instaladas (por ejemplo, SDN) para moverse hacia una automatización más holística para tecnologías de seguridad tales como prevención de intrusiones, gestión de identidad y acceso, prevención de pérdida de datos y geolocalización.

Enfoca la inteligencia a un nivel superior en el software en lugar de en el hardware, lo que puede permitir que los arquitectos empresariales y a los administradores de seguridad enfocarse en las políticas y no en mantener los sistemas corriendo en un nivel inferior. [9]

La seguridad de red por medio de SDN no ayuda con la prevención de ataques, a continuación nombro algunos de los ataques más comunes y como las redes definidas por software no ayuda a controlarlos, uno de los ataques más comunes son los ataques de denegación de servicios, estos ataques consisten en lograr por medio de grandes

paquetes TCP (Ping de la muerte), por medio de la programación de la red podría actuar como la primera línea defensa buscando patrones particulares con un volumen de paquetes de una solo fuente o distintas fuentes, previniendo este tipo de ataques.

Los ataques a aplicaciones o servicios, los cuales son los dirigidos a servicios web con series de peticiones HTTP particulares, los dispositivos SDN pueden identificar, registrar y descartar estas peticiones. Otro tipo de ataque común es el de llenar las tablas de estado de los dispositivos de la red, pero con las redes definidas por software puedo identificar esta falla por medio de tiempo y límites de conexión. Como se puede observar las SDN nos permiten tener mayor control de nuestro sistema y se pueden automatizar procesos convirtiendo nuestra red en un sistema de detección de primer nivel.

Así como todas las tecnologías tienen fallas que deben ser tratadas para brindar mayor seguridad las redes definidas por software no son la excepción.

Analistas de McAfee señalan que, aunque las redes definidas por software (SDN) fueron desarrolladas en un intento por simplificar las redes y hacerlas más seguras, también abren agujeros de seguridad potenciales, especialmente en las conexiones entre los controladores y los elementos de red.

Hoy en día, la seguridad en la red tiene como objetivo evitar la entrada de malware, lo que aumenta la complejidad de la red y dificulta su gestión. En este sentido, las redes definidas por software pueden ayudar a proporcionar una mayor seguridad sin aumentar los dolores de cabeza a la hora gestionar redes virtuales complejas en centros de datos, aunque también pueden aumentar los riesgos.

Expertos de McAfee señalan que las SDN pueden aumentar la seguridad a través del enrutamiento de tráfico, a través de un sistema de prevención de intrusiones y firewall de próxima generación central, así como mediante la reprogramación y la reestructuración dinámica de una red que está sufriendo un ataque distribuido de denegación de servicio.

Las redes definidas por software también pueden proporcionar capacidades tales como la cuarentena automática de un punto final o red que haya sido infectada con malware. [10]

IX. CONCLUSIONES

Como se sabe la tecnología cada vez avanza más rápido, en los dos sentidos tanto en la mejora y compatibilidad con en la parte negativa, para los hackers y crackers permitiendo que ellos también avancen al ritmo de nuevas tecnologías, es importante que cada especialista de seguridad informática continúe en aprendizaje tanto de las nuevas tecnologías que se pueden usar como de los nuevos intentos de ataques para esos servicios, las redes definidas por software son un claro ejemplo del avance que lleva la tecnología permitiendo centralizar nuestra red, pero llevando a que sea el punto central de ataques. Lo importante de la tecnología es no dejar que ella nos tome ventaja sino tratar de pasarla y siempre pensar a futuro para poder mantener cada dispositivo seguro y cada vez más alejado de los atacantes informáticos.

REFERENCIAS

[1] Cómo el nuevo universo trazado por las redes definidas por software impactará en los negocios. Available: http://www.la.logicalis.com/globalassets/latin-america/advisors/es/advisor_sdn.pdf

[2] Arquitectura de SDN (software defined network). Available: http://www.la.logicalis.com/globalassets/latin-america/advisors/es/advisor_sdn.pdf

[3] Feamster N., Rexford J., Zegura E. "The Road to SDN: An intellectual history of programmable networks" Available: http://queue.acm.org/detail.cfm?id=2560327, 30 de diciembre de 2013.

[4] OpenFlow: Proactive vs Reactive. Available: http://networkstatic.net/openflow-proactive-vs-reactive-flows/

[5] SDN: las redes al servicio de las necesidades del negocio Available: http://www.aunclicdelastic.com/sdn-las-redes-al-servicio-de-las-necesidades-del-negocio/

[6] SDN: las redes al servicio de las necesidades del negocio Available: http://www.aunclicdelastic.com/sdn-las-redes-al-servicio-de-las-necesidades-del-negocio/

[7] SDN: las redes al servicio de las necesidades del negocio Available: http://www.aunclicdelastic.com/sdn-las-redes-al-servicio-de-las-necesidades-del-negocio/

[8] SDN: las redes al servicio de las necesidades del negocio Available: http://www.aunclicdelastic.com/sdn-las-redes-al-servicio-de-las-necesidades-del-negocio/

[9] Seguridad definida por software: ¿El futuro de la seguridad de red? Available: http://searchdatacenter.techtarget.com/es/consejo/Seguridad-definida-por-software-El-futuro-de-la-seguridad-de-red 10 de diciembre de 2014.

[10] Las Redes Definidas por Software abren agujeros de seguridad potenciales, advierte McAfee. Available: http://www.pcworld.com.mx/Articulos/31285.htm 7 de enero 2014.

RECONOCIMIENTO

Agradezco a cada una de las personas que contribuyeron con la información referente, a los fabricantes de nuevas tecnologías, Cisco, Juniper, Alcatel por la información encontrada sobre sus avances en la tecnología, a cada uno de mis profesores por el aprendizaje continuo y nutritivo en los diferentes temas.

Autor

Alvaro Javier Aguilar Cruz
Ingeniero Electrónico y Telecomunicaciones
Universidad Piloto de Colombia
2015