CORPORACIÓN UNIVERSITARIA AMERICANA

InGente AMERICANA

ENE-DIC 2022 | VOLUMEN 2 - NÚMERO 2

SELLO EDITORIAL CORUNIAMERICANA

InGente es una publicación científica de periodicidad anual que se desarrolla en los campos del conocimiento de la Ingeniería. Su propósito es propiciar y difundir investigaciones escritas para promover y enriquecer, los múltiples debates que se agitan en torno a las Ingeniería y Tecnología.

Contacto con el equipo editorial:
ingenteamericana@coruniamericana.edu.co
Teléfono:

Guía para autores:

SELLO EDITORIAL CORUNIAMERICANA
Editor
Harold Pérez
Coordinación Sello Editorial
Eva Luna Contreras Mariño
Asistente Editorial
Fabián Márquez Osorio
Administrador OJS
Juan Carlos Miranda Passo
Diagramación y Diseño
Kelly Johanna Isaacs González
Imagen de portada
Pixabay.com

ISSN-e: XXXX XXXX
Colombia

InGente AMERICANA

Presentación

A diario se observan los adelantos vertiginosos de la ciencia y la tecnología, que se plasman, principalmente, con la ayuda de los sistemas de las tecnologías de la información y la comunicación. Las ingenierías son ciencias aplicadas a la solución de problemas, por tal razón son las que influyen a diario en el desarrollo social y económico de una región, nación o el mundo, más aún, se logra con ellas exponer y llevar a la práctica todas sus manifestaciones con innovación e investigación.

La revista Ingente Americana surge como resultado de la responsabilidad y compromiso de la Facultad de Ingenierías y del Centro. De Investigaciones de la Corporación Universitaria Americana de la generación de conocimiento científico, especialmente en la difusión del saber generado por los estudiantes, docentes, directivos, semilleros de investigación e investigadores, conjuntamente con el programa expresado en sus líneas de investigación y sus respectivos proyectos, al igual que la tendencia universitaria de seguir creciendo en todas sus direcciones, y el querer mostrar lo que se gesta dentro del interior y el exterior de ella, donde su proyección social, día a día va sobresaliendo dentro de la comunidad académica.

La Revista es un órgano académico construido para compartir y socializar los resultados producidos por los estudiantes, docentes, directivos, semilleros de investigación e investigadores de la Facultad de Ingenierías y demás comunidades afines que de una u otra manera forjaron el espíritu de propagar las ciencias aplicadas con esplendor, con aras de una mejor corporación y toda su población académica.

El objetivo de la Revista InGente Americana es informar y promover la gestión del conocimiento a través de la investigación, el debate disciplinario y metodológico en los estudios de las ingenierías y las ciencias básicas de la Corporación Universitaria Americana, que a diario se lleva a cabo en su comunidad académica, científica y disciplinaria.

InGente Americana es divulgada de forma digital anualmente, publicando artículos de investigación científica y tecnológica, artículos de reflexión no derivados de los de revisión, artículos cortos, reporte de casos y documento de reflexión no derivado de investigación.

Presentation

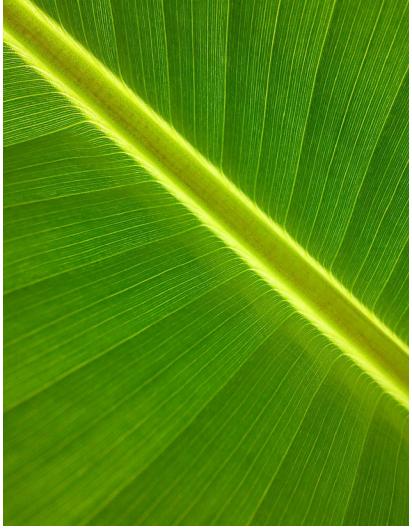
Every day we observe the vertiginous advances in science and technology, which are mainly expressed with the help of information and communication technology systems. Engineering are sciences applied to the solution of problems, for this reason they are the ones that influence daily in the social and economic development of a region, nation or the world, moreover, it is achieved with them to expose and put into practice all its manifestations with innovation and research.

The Ingente Americana magazine arises as a result of the responsibility and commitment of the Faculty of Engineering and the Center. Research Center of the American University Corporation for the generation of scientific knowledge, especially in the dissemination of knowledge generated by students, teachers, managers, research groups and researchers, together with the program expressed in their lines of research and their respective projects, as well as the university trend to continue growing in all directions, and wanting to show what is being generated inside and outside of it, where its social projection, day by day is excelling within the academic community.

The Journal is an academic organ built to share and socialize the results produced by students, teachers, directors, research groups and researchers of the School of Engineering and other related communities that in one way or another forged the spirit of propagating applied sciences with splendor, for the sake of a better corporation and its entire academic population.

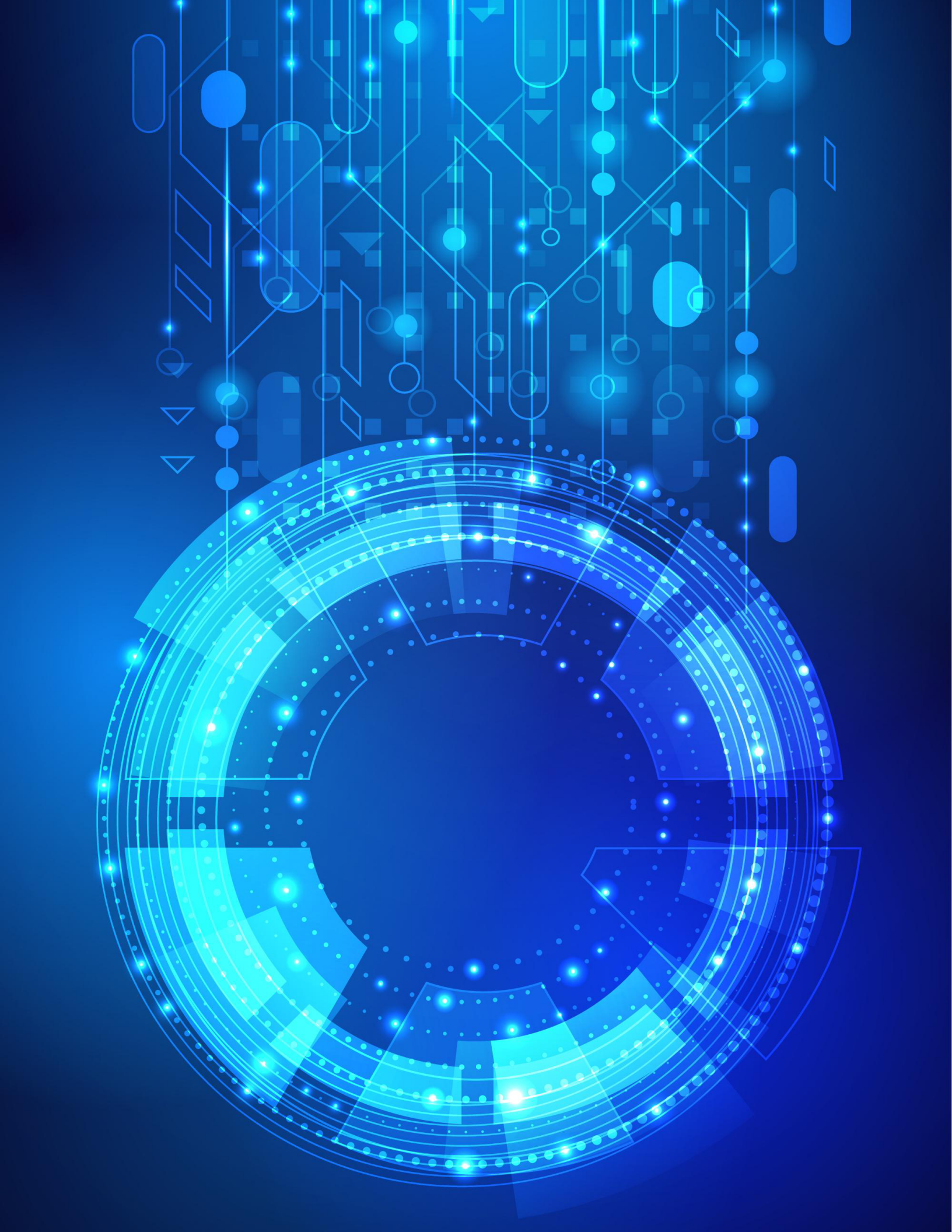
The objective of InGente Americana Magazine is to inform and promote knowledge management through research, disciplinary and methodological debate in engineering studies and basic sciences of the Corporación Universitaria Americana, which is carried out daily in its academic, scientific and disciplinary community.

InGente Americana is published annually in digital form, publishing scientific and technological research articles, reflection articles not derived from review articles, short articles, case reports and reflection papers not derived from research.



Contenido

Artículos de Investigación



Recibido: Oct. 03, 2021 | Aceptado: Ene. 10, 2022

Aplicación de metodología para testing del sistema de información del Dapard para procesos de aseguramiento de la calidad

Application of methodology for testing of the dapard information system for quality assurance processes.

DOI: https://doi.org/10.21803/ingecana.2.2.406

Andrés Agudelo Arboleda[1] · David Alberto García Arango[2] & Frey de Jesús Castro Ramírez[3]

[1]Ingeniería de Sistemas. Corporación Universitaria Americana, agudeloandres0056@coruniamericana.edu.co . [2]Licenciado en Matemáticas y Física. Corporación Universitaria Americana, dagarcia@coruniamericana.edu.co . [3]Ingeniero de Sistemas. Corporación Universitaria Americana, fcastro@coruniamericana.edu.co.

Resumen

Se presenta el desarrollo de un sistema de información que cuenta con un módulo funcional que es el de registro de eventos consulta e integración de todo tipo de información como geográfica documental histórica, (tablas matrices entre otras) de desastres que se presentan en todo Antioquia pero cabe considerar que este sistema no cuenta con sistemas de seguridad de la información, por lo anterior se identifica la aplicación de una metodología que permitan el aseguramiento de la calidad, para la migración de bases de datos ya que esta información no está bien estructurada lo cual dificulta la trazabilidad. Se plantea como elementos finales que es importante contar con protocolos de implementación de seguridad en la plataforma que allí se maneja, la cual también requiere ser más intuitiva para el usuario.

Palabras clave: Aseguramiento De La Calidad, Dapard, Metodología, Sistema De Información, Testing,

Abstract

The development of an information system with a functional module for the registration of events, consultation and integration of all types of information such as geographic and historical documents (matrix tables, among others) of disasters that occur throughout Antioquia is presented, but it should be considered that this system does not have information security systems, therefore the application of a methodology that allows quality assurance is identified, for the migration of databases since this information is not well structured, which hinders traceability. As final elements, it is important to have security implementation protocols in the platform that is managed there, which also needs to be more intuitive for the user.

Keywords: *Quality Assurance, Dapard, Methodology, Information System, Testing,*

Introducción

El sistema de información del DAPARD es un sistema integral con diferentes funciones, pero hay ausencia de lineamientos claros o estructurados en el marco de aseguramiento de la calidad en la realización de próximos módulos. Debido a los problemas presentes, específicamente en el retraso de fechas de entrega y el aumento de errores en el uso de la plataforma se hace de gran importancia realizar la validación de avances en la plataforma junto con sus requerimientos y posibles errores para garantizar el ciclo normal y eficaz del proyecto. En el presente escrito se mencionan los avances en la aplicación de una metodología para la realización de pruebas de software que permita una adecuada gestión de los datos del sistema de información basado en el aseguramiento de la calidad.

MATERIALES Y MÉTODOS

Se genera un paso a paso para la solución de la problemática [1], la cual es:

1. **Identificar Calidad de Producto:** esto implica identificar calidad del servicio y Satisfacción, identificar documentación existente, compromisos del desarrollador, alcance realizados, identificar los datos existentes, recopilar y centralizar la Información, depurar la Base de datos, programar la migración para el sistema de información y realizar pruebas de datos ingresados, funcionamiento y rendimiento.
2. **Definir Políticas informáticas (Internas) para el ingreso de Información:** encontrar el mayor número de issues que pueda tener el sistema de información para gestionar la corrección de estos, demostrar que la aplicación cumple con las especificaciones y requerimientos definidos en la documentación, demostrar la adecuada interacción con las demás aplicaciones y su relación.
3. **Asegurar el correcto funcionamiento de todo el sistema,** frente a un cambio de cualquiera de sus funcionalidades, funcionamiento incorrecto o incompleto, Issues de interface y de accesos a estructuras de datos externas y finalmente identificar problemas de rendimiento.

RESULTADOS

El sistema de información del DAPARD es un software que actualmente está en desarrollo en fases por lo cual es necesario describir una serie de pasos para su evaluación y calidad del producto del software las cuales están regidas por las normas 5415 [2] y 5420 [3].

Básicamente estas cumplen unos procedimientos propuestos en la Norma 5415:

1. **Visión general:** Determina aspectos básicos, definiciones, relaciones provee un marco de trabajo, propósito, requisitos, métricas, tipos de productos.

2. **Planificación y gestión:** Políticas y objetivos, tecnologías a utilizar, roles y responsabilidades, transferencia tecnológica y de conocimiento, apoyo en la gestión del proyecto .

3. **Procedimiento para desarrolladores,** evaluación del software durante el ciclo de vida de desarrollo, identificación de necesidades del usuario, Identificar productos intermedios, Identificar y medir producto internos y externos, uso de indicadores de calidad, proceso de evaluación.

Procedimiento para compradores: requisitos del producto de software a adquirir, especificación de requisitos de compra, preparación de contrato, negociación, control de cambios, evaluación durante la ejecución, aceptación y recibo del producto de software.

4. **Procedimiento para evaluadores,** punto de comienzo para de la evaluación, proceso de evaluación, responsabilidades dentro del proceso de evaluación, especificación de la evaluación, diseño, ejecución y conclusiones de la evaluación, niveles y técnicas de evaluación.

Lo anterior, ajustado a las necesidades de la organización, se puede sintetizar en los resultados de la Figura 1.

DISCUSIÓN

El desarrollo de la aplicación de la metodología posibilita el desarrollo de mejores pruebas de software para la gestión de datos del sistema de información, para esto se caracterizan los procesos relacionados con el aseguramiento de la calidad y seguridad en el sistema de información del DAPARD, identificando las

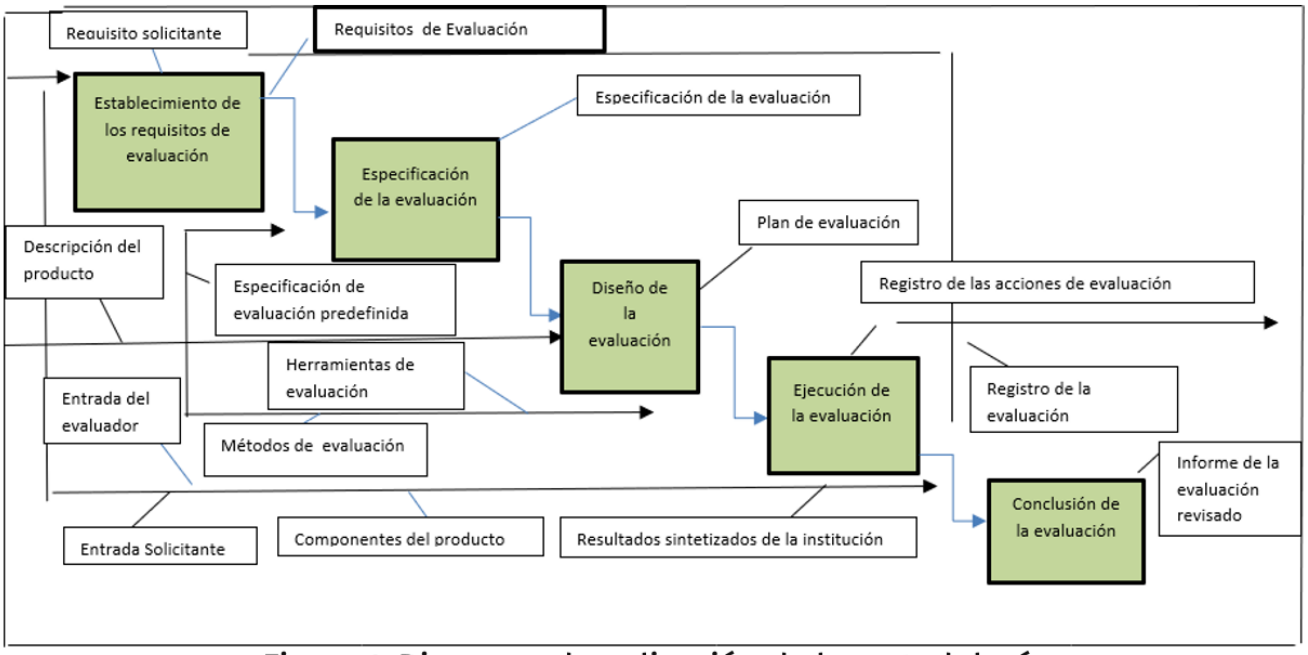


Figura 1. Diagrama de aplicación de la metodología.
Elaboración propia.

rutas o metodologías de mejora para el aseguramiento de la calidad del sistema de información, aplicando pruebas de software para el aseguramiento de la calidad del sistema de información del DAPARD y de esa manera evaluar el desempeño de las metodologías aplicadas en el aseguramiento de la calidad del software tal y como lo propone Palacio Palma et al. [4]. En ese sentido, es fundamental fortalecer procesos que posibiliten mayor integración de pruebas para de esta forma ampliar más el alcance de las soluciones de software requeridas.

CONCLUSIONES

Con la finalización de la aplicación de la metodología se obtuvo un informe de caracterización de los procesos relacionados con la evaluación del sistema de información en plataforma web y se generó un documento de estado del arte de las rutas o metodologías para el aseguramiento de calidad del software. El desarrollo de estas pruebas han permitido un desempeño exitoso de la plataforma como ruta sistémica para el mejoramiento continuo.

REFERENCIAS

[1] DAPARD, Informe - Departamento Administrativo del Sistema para la Prevención, Atención y Recuperación de Desastres de la Gobernación de Antioquia, Medellín: Gobernación de Antioquia, 2014.

[2] ICONTEC, «Tecnología de la Información. Evaluación del producto de Software. Parte 5: procedimiento para evaluadores,» ICONTEC, Bogotá, 2008.

[3] ICONTEC, «Ingeniería de software. Calidad del producto de software. Parte 2: Métricas externas,» ICONTEC, Bogotá, 2007.

[4] E. Palacio Palma, L. Medraño Zúñiga y R. Osorio López, «Desarrollo de una herramienta web que facilite la realización de pronósticos colaborativos en las PYMES de Cali,» ICESI, Cali, 2011.

[5] C. . Gonzalez Beleño, C. . Rodríguez Arias, y A. . Cabarcas Solano, «Calidad de la Gerencia: un análisis bibliométrico», ADGNOSIS, vol. 9, n.º 9, pp. 109–118, dic. 2020.

Recibido: Nov. 25, 2021 | Aceptado: Feb. 18, 2022

Directrices y políticas de firewall

Firewall guidelines and policies

DOI: https://doi.org/10.21803/ingecana.2.2.496

Álex Ávila[1] · Tatiana Echeverría Jiménez[2] · Christian Obando[3] & Carlos Federico Ortiz Zuleta[4]

[1] Docente de la Corporación Universitaria Americana. [2]Docente de la Corporación Universitaria Americana. [3]Ingeniero en electrónica y telecomunicaciones y especialista en seguridad informática hasta2015. E-mail: chrisobib@gmail.com. [4]Administrador de red, Universidad de Antioquia. E-mail: federico.ortiz@udea.edu.co.

Resumen

Los sistemas de información deben estar protegidos por medio de firewalls, estos están diseñados para controlar el tráfico que circula entre las redes privadas y públicas, permitiendo o denegando las peticiones realizadas por las diferentes redes con el objetivo de protegerlas de amenazas. Existen diferentes tipos de firewall que se utilizan dependiendo de las técnicas de filtrado que se deseen implementar, de acuerdo a la pila de protocolos TCP/IP ellos pueden trabajar a nivel de red, de transporte y de aplicación. Un buen diseño en las políticas del firewall, robustece la seguridad de las redes ya que con estas se puede controlar determinados tipos de tráfico de datos.

Palabras clave: Firewall, Políticas Y Directrices, Redes, Seguridad Informática.

Abstract

Information systems must be protected by firewalls, which are designed to control traffic flowing between private and public networks, allowing and denying requests made by the different networks in order to protect them from threats. There are different types of firewalls that are used depending on the filtering techniques to be implemented, according to the TCP/IP protocol stack, they can work at network, transport and application level. A good firewall policy design strengthens network security by controlling certain types of data traffic.

Keywords: *Firewall, Policies And Guidelines, Networks, Computer Security.*

Introducción

En los últimos años las TICs han evolucionado y han cobrado gran importancia a nivel mundial debido a su capacidad para estimular la creatividad, la innovación y transformar el mundo en diferentes entornos. El Ministerio de Tecnologías de la Información y la Comunicación de la República de Colombia en su Boletín trimestral de las TICs – Cifras Primer Trimestre 2013 [1] indica, entre otros, un crecimiento en la penetración de Internet de un 16% con un total de 7.531.670 suscriptores, esta tendencia a la alza se debe, entre otras, a que las TICs nos ofrecen un acceso amplio y ágil a miles de millones de contenidos pero también a recursos humanos valiosos. Internet se ha convertido en un medio fundamental para impulsar el diseño e implementación de servicios que cumplen con las necesidades de las personas y organizaciones en general, pero así mismo ha brindado la oportunidad a personas inescrupulosas de cometer delitos relacionados con la informática y la información, pues cada día hay nuevas redes susceptibles de ser atacadas y nuevos atacantes en potencia. Es por esto que una organización debe tomar conciencia e inquietarse por su seguridad, un mecanismo es la seguridad perimetral.

La seguridad perimetral debe estar diseñada para proteger todos los elementos de una red interna, incluyendo hardware, software e información, no solo de cualquier intento de acceso no autorizado desde internet sino también de ciertos ataques que pueden ser realizados dentro la red. Los firewall son dispositivos o programas que ayudan a controlar las conexiones que pueden iniciar o recibir un computador conectado a la red, este puede ser implementado de acuerdo a las necesidades de las organizaciones, creando políticas específicas de firewall para permitir, limitar y rechazar el tráfico que circula entre las diferentes redes.

Este artículo es el resultado de analizar las diferentes tecnologías de firewall, sus capacidades, ventajas y desventajas así como recomendaciones para el establecimiento de políticas de firewall y recomendaciones para seleccionar, configurar, probar, implementar y administrar soluciones de firewall.

TIPOS DE FIREWALL

Existen diferentes tipos de aplicaciones de firewall de acuerdo a las necesidades de filtrado que se desean controlar.

Filtrado de paquetes

Este tipo de firewall tiene un conjunto de reglas estáticas que permiten o bloquean el acceso de tráfico, basado en la información contenida en los encabezados de los paquetes, trabajan a nivel de red y de transporte del modelo TCP/IP, es decir se basa en direccionamiento IP origen-destino y puertos TCP o UDP; tiene una desventaja y es que no detecta el tráfico malicioso.

Firewall de aplicaciones

Trabaja en la capa de aplicaciones del modelo TCP/IP, permite detectar diferentes tipos de ataques

a múltiples niveles, es útil para detectar ataques conocidos como gusanos, spyware, troyanos y bots, esta aplicación es conocida como un sistema de detección y prevención de intrusos (IDS/IPS). La desventaja principal de esta aplicación es que afecta el rendimiento del dispositivo.

Firewall proxy

Actúa como intermediario en ciertos programas, su función es filtrar y reenviar paquetes a nivel de aplicación como TELNET, FTP y HTTP, realiza filtrado de contenidos web controlando el acceso a ciertas páginas desde una red privada, brinda opciones de control de acceso confiable para los protocolos soportados. Esta aplicación reduce el tráfico y mejora la respuesta a solicitudes, ya que permite el almacenamiento en caché de las páginas web más visitadas.

Redes privadas virtuales (vpn)

Los firewall a veces tienen que hacer más que filtrar el tráfico UDP y TCP, también cifra y descifra los flujos de datos de una red protegida y las redes externas, esto implica implementar un red privada virtual, que utiliza protocolos adicionales para cifrar el tráfico, proporcionar autenticación de usuario y proteger la integridad de la información. Es un servicio basado en certificados SSL, que se utiliza para crear túneles VPN cliente/servidor y servidor/cliente, esta flexibilidad permite que las filiales y los trabajadores remotos de una organización, puedan conectarse con seguridad a la red corporativa y realizar las tareas o solicitudes propias de su función.

Control de acceso a la red (car)

Es una aplicación del firewall que revisa los equipos que acceden a la red para comprobar que cumplan con todas las políticas de seguridad, como son actualizaciones de los antivirus, del sistema operativo y de aplicaciones.

Firewall de aplicaciones web

Es una aplicación que permite inspeccionar las peticiones que se puedan realizar sobre una web o una aplicación web, impidiendo que tráfico malicioso alcance la aplicación origen y por lo tanto salvaguardando la información más sensible. Igual que las aplicaciones anteriores se trata de un servicio que complementa a los sistemas tradicionales de seguridad perimetral (firewall), ofreciendo protección a nivel de aplicación donde un firewall tradicional no podría proteger [1].

Unified threat management- utm

Es un gestor unificado de amenazas, básicamente es un firewall que posee múltiples funciones en una misma máquina de seguridad perimetral, algunos de estos servicios son:

- Función de firewall inspección de paquetes.
- Función de VPN
- Antispam
- Antiphishing (falsificación de sitios web)
- Antispyware o Filtrado de contenidos o Antivirus de perímetro
- Detección y prevención de intrusos(IDS/IPS)

Estas funciones adicionales lo hacen un firewall más robusto, que centraliza la administración de las aplicaciones que ayudan a realizar un mejor análisis de datos a nivel de aplicaciones específicas y a la detección de ataques externos.

Actualmente existen diferentes variedades de UTM, unos son llamados open source o de código abierto y gratuito y otros que son soportados por algunos fabricantes, es decir son licenciados [2].

Firewall con ambientes virtuales

Los sistemas de virtualización incluyen la creación de redes virtualizadas como si estuviesen

en una red Ethernet estándar, el tráfico que circula dentro de las redes virtuales no se puede controlar con un firewall externo, pero algunos sistemas de virtualización ofrecen funciones de firewall que se adicionan en el sistema operativo como plugins, y cumplen la función de filtrado de paquetes dentro de las virtualizadas, dándole la seguridad perimetral que necesitan.

Firewall para equipos individuales y redes domésticas

Para dar una buena seguridad a una red, no basta con tener un firewall protegiendo de la red pública, también es necesario tener instalados firewall en las máquinas de escritorio, laptops y servidores, ya que estos ayudarían a protegerlos de ataques internos que no pueden ser filtrados ni detectados por el firewall de perímetro de la red [3].

En el mercado existen muchas aplicaciones gratuitas para esta función, pero las más recomendables son las licenciadas que vienen con los paquetes de antivirus de algunos fabricantes.

Firewall basados en host y firewall personales

Los firewall de host está disponibles como parte del sistema operativo, tales como Windows, Solaris, Linux, BSD y MAC OS X Server, su principal función es controlar el tráfico que circula en su propia red o subred y que no puede ser detectada por el firewall perimetral. Para asegurar mejor los equipos individuales se suelen instalar aplicaciones como antivirus licenciados con funcionalidad de firewall a nivel de aplicación, pero solo para la máquina local [4].

En las redes domésticas también se suele utilizar firewall para proteger las máquinas de la red externa, los más comunes son los llamados router-firewall que tiene funcionalidades anteriormente mencionadas como VPN, filtrado web, ACL y segmentación de red.

FIREWALLS Y ARQUITECTURAS DE RED

Los firewalls son utilizados para diferentes redes con diferentes requisitos de seguridad, tales como Internet y la red interna (LAN) que aloja todos los datos sensibles. Se deben ubicar firewalls donde sus redes y sistemas internos interactúan con las redes y los sistemas externos, y donde los requisitos de seguridad varían entre sus redes internas.

Es importante determinar dónde se deben colocar los firewalls y donde deben estar las redes en relación a los mismos, esto significa normalmente que los firewalls están colocados ya sea como un nodo en la red que divide varias rutas de acceso, o en línea a lo largo de una sola trayectoria.

Los proveedores de firewalls a menudo varían en su terminología para el flujo lógico de tráfico en el firewall. Un firewall toma el tráfico que no se ha comprobado, lo evalúa con la política del firewall, y luego actúa en consecuencia (por ejemplo, pasa el tráfico, lo bloquea o lo pasa con algunas modificaciones). Debido a que todo el tráfico en una red tiene una dirección, las políticas se basan en la dirección en que se mueve el tráfico, el tráfico que aún no ha sido revisado viene del “lado sin protección” del firewall y se está moviendo hacia el “lado protegido.” Algunos firewalls verifican el tráfico en ambos sentidos -por ejemplo, si se establecen para evitar que un tráfico específico de la red LAN salga a Internet. Existen varios tipos de firewall; los firewalls de red que casi siempre son dispositivos de hardware con varias interfaces de red; los firewalls basados en hosts y los firewalls personales que implican software que reside en un solo equipo y protege sólo el mismo, igualmente las aplicaciones de firewall personales que son diseñadas para proteger un equipo en una red pequeña.

Topologías de la red con firewalls

En la Figura 1 se puede ver el gráfico típico de una red de firewall actuando como router El lado sin protección del firewall se conecta a la ruta única con la etiqueta "WAN", y el lado protegido se conecta a tres caminos marcados "LAN1," "LAN2," y "LAN3." El firewall actúa como un enrutador para el tráfico entre el camino de la WAN y los caminos de la LAN. En la figura, uno de los caminos de LAN también tiene un router; algunas organizaciones prefieren utilizar múltiples capas de enrutadores debido a políticas de enrutamiento dentro de la red.

Muchos firewalls tienen una característica denominada DMZ. Las DMZs son útiles a veces para las organizaciones que tienen hosts que necesitan tener un tráfico destinado evadiendo algunas políticas del firewall, pero que requieren que el

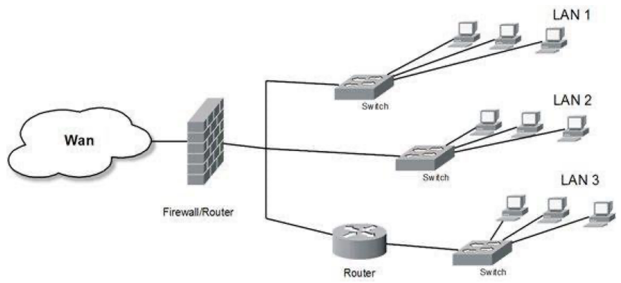


Figura 1. Firewall actuando como router.
Elaboración propia basado en [2]

tráfico procedente de los hosts de otros sistemas en la red si tenga que pasar por el firewall. Es común instalar servidores de cara al público, tales como servidores web y correo electrónico, en la zona desmilitarizada.

Un ejemplo de esto se muestra en la Figura 2, un diseño de red simple de un firewall con una DMZ. El tráfico de Internet entra en el firewall y se dirige a los sistemas en el lado protegido de este o a los sistemas ubicados en la DMZ. El tráfico entre los sistemas de la DMZ y sistemas en la red protegida pasa por el firewall, y puede tener políticas de firewall aplicadas.

En algunas ocasiones se pueden utilizar múltiples firewalls, es decir firewalls redundantes, lo que algunos vendedores ofrecen como firewalls de alta disponibilidad (high-availability firewalls), estos permiten que un firewall pueda hacerse cargo de otro en caso de que el primero falle o se desconecte para mantenimiento.

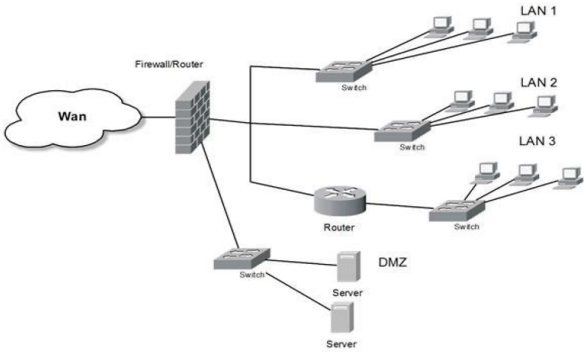


Figura 2. Firewall con DMZ.
Elaboración propia basado en [2].

Los firewalls con alta disponibilidad están desplegados en pares en el mismo lugar en la topología de red, de forma que ambos tienen las mismas conexiones externas e internas. Mientras que los firewalls de alta disponibilidad pueden aumentar la fiabilidad, también pueden presentar algunos problemas, tales como la necesidad de combinar los logs entre los pares de firewalls y puede llevar a posibles confusiones para los administradores al configurar los firewalls (por ejemplo, saber qué firewall está induciendo cambios de política en otro firewall). La Figura 3 presenta un esquema de firewall de alta disponibilidad.

Firewalls actuando como traductores de direcciones de red nat

La mayoría de los firewalls pueden realizar NAT, denominado a veces port address translation (PAT) o network address and port translation (NAPT). A pesar de la creencia popular, NAT no es parte de la funcionalidad de seguridad de un

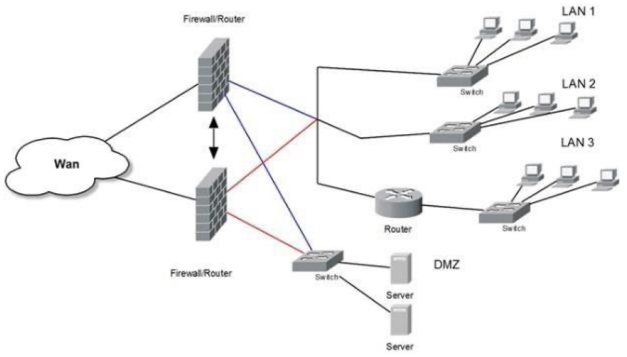


Figura 3. Firewalls de alta disponibilidad.
Elaboración propia basada en [2].

firewall. Típicamente, un NAT actúa como un router que tiene una red con direcciones privadas en el interior y una sola dirección pública en el exterior.

La forma en que un NAT realiza el mapeo varía entre implementaciones, pero casi siempre involucra lo siguiente:

> NAT cambia la dirección origen en cada paquete de salida y, dependiendo del método, también el puerto origen para que sea único. Estas traducciones de dirección se almacenan en una tabla, para recordar qué dirección y puerto le corresponde a cada dispositivo cliente y así saber dónde deben regresar los paquetes de respuesta. Si un paquete que intenta ingresar a la red interna no existe en la tabla de traducciones, es descartado. Debido a este comportamiento, se puede definir en la tabla que en un determinado puerto y dirección se pueda acceder a un determinado dispositivo, como por ejemplo un servidor web.

Arquitectura con múltiples capas de firewalls

Se pueden utilizar varios firewalls dentro de una red, es decir un administrador de red puede querer límites adicionales dentro de la red y el mecanismo para esto es implementar firewalls adicionales. Una situación típica que requiere de múltiples capas de firewalls de red es la presencia de los usuarios internos con niveles de confianza diferentes. Por ejemplo, una organización podría querer proteger sus bases de datos de contabilidad del acceso de usuarios que no forman parte del departamento de contabilidad. Esto se podría lograr mediante la instalación de un firewall en el perímetro de la red (para evitar el acceso general a la red desde Internet) y otro en el perímetro de la red interna que define el límite del departamento de contabilidad. El firewall interno bloquearía el acceso al servidor de base de datos para cualquier persona fuera de la red contable al tiempo que permite el acceso limitado a otros recursos de la red contable. La Figura 4 presenta cómo quedaría este esquema:

> Otro uso típico de los firewalls múltiples dentro de una red puede ser cuando en las organizaciones implementan puntos de acceso inalámbricos específicos dentro de sus redes para uso de los visitantes. Un firewall entre los puntos de acceso y el resto de la red interna, puede impedir que los visitantes accedan a la red local con los mismos privilegios que un empleado. La Figura 5 presenta este esquema.

Hay que tener cuidado cuando se utiliza la combinación de varios firewalls, porque se pueden cometer errores como por ejemplo omitir reglas en el firewall interior considerando que están implementadas en el firewall exterior, esto puede resultar en amenazas para la organización. Una buena práctica es duplicar las directivas de los

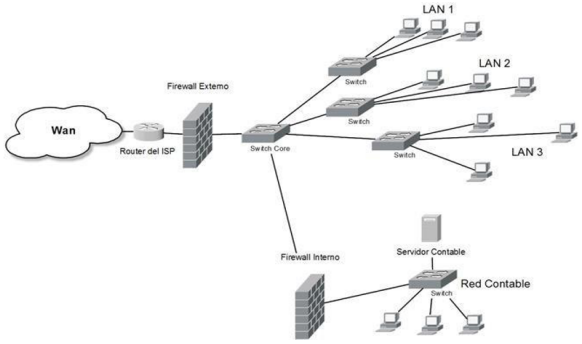


Figura 4. Arquitectura con múltiples capas de firewalls.
Elaboración propia basado en [2].

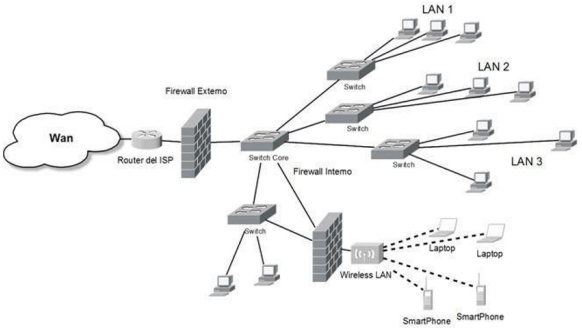


Figura 5. Firewalls múltiples en puntos de acceso inalámbricos. Elaboración propia basado en [2].

firewalls externos que también son relevantes para los firewall internos. Esto puede ser difícil si estos firewalls no son capaces de coordinar sus políticas de forma automática, lo que es probable cuando los firewalls son de diferentes fabricantes. Cuando se tienen varios firewalls puede ser más complicado para el administrador encontrar un error porque tiene que revisar las políticas de cada firewall.

POLÍTICA DE FIREWALL

Las políticas de firewall establecen cómo los firewall deben manejar el tráfico de una red basado en direcciones IP, protocolos, aplicaciones y contenido. Antes de realizar una política de firewall, se debe efectuar un tipo de análisis de riesgos basado en la evaluación de amenazas y vulnerabilidades con el fin de establecer los tipos de tráfico que necesita la organización y cómo deben protegerse [5]. Estas políticas deben considerarse en el plan de seguridad de la organización y deben ser actualizadas a medida que surjan nuevas amenazas.

La función principal de los firewall es la de bloquear todo tráfico entrante y saliente que no haya sido especificado en la política de firewall [6]. Esta práctica conocida como deny by default, reduce tanto el riesgo de ataque como el volumen de tráfico en la red.

Políticas basadas en direcciones ip y protocolos

Las políticas de firewall de una organización, solo deben permitir protocolos IP que sean necesarios, los más comunes son: ICMP, TCP, UDP, ESP y AH, a los demás protocolos se les aplica deny by default. Estos protocolos rara vez pasan entre una red externa y la red LAN de la organización, por lo que deben ser bloqueados en ambas direcciones del firewall [7].

Direcciones ip y otras características ip

Las políticas de firewall solo permiten direcciones IP de origen y destino válido. Las siguientes son recomendaciones para direcciones IP: o Se debe bloquear tráfico con direcciones de origen y destino inválidas, independientemente de la ubicación del firewall.

Se debe bloquear en el perímetro de la red el tráfico de entrada con una dirección de origen inválida o tráfico de salida con destino inválido.

- Se debe bloquear en el perímetro de la red el tráfico entrante con una dirección privada de destino o un tráfico saliente con una dirección de origen.

- Se debe bloquear el tráfico saliente con direcciones de origen inválidas.

- Se debe bloquear el tráfico entrante con dirección de destino del firewall, a menos de que el firewall esté ofreciendo servicios de conexión directa para el tráfico de entrada, por ejemplo, un proxy.

- El tráfico con información de enrutamiento permite a un sistema establecer la ruta que tomarán los paquetes desde su origen hasta su destino, también debe bloquearse o se debe bloquear el tráfico desde fuera de la red que contenga dirección de difusión que se dirija a

la red de la organización.

Los firewalls perimetrales deben bloquear tanto al tráfico que entra a la red como a los host que no deben ser accesibles desde redes externas. De la misma forma, se debe bloquear el tráfico saliente de redes y host de la organización que no deben acceder a redes externas [8].

IPv6

Aunque la longitud y el formato de las direcciones IPv6 son diferentes a las de IPV4, muchas características son similares por lo que los firewall deben funcionar igual para ambos protocolos, por ejemplo, el bloqueo de todo tráfico entrante y saliente que no haya sido especificado en las políticas firewall [9]. En todas las organizaciones ya sea que permitan o no tráfico IPv6, necesita un firewall capaz de filtrar este tráfico con las siguientes características:

- El firewall debe ser capaz de utilizar IPv6 en todas las reglas de filtrado que utilizan direcciones IPv4.

- La interfaz administrativa debe permitir al administrador clonar reglas IPv4 a IPv6 y así facilitar la administración. o El firewall debe ser capaz de bloquear protocolos IPv6 si no se requieren o si se utiliza un firewall para bloquear tráfico IPv6 entrante o saliente, éste firewall necesita reconocer y bloquear cualquier forma de túnel v6 a v4.

Las organizaciones que no utilizan IPv6 deben bloquear todo el tráfico nativo IPv6 en sus firewalls.

TCP y UDP

Los protocolos de aplicación pueden utilizar TCP, UDP o los dos dependiendo del diseño de la aplicación, por ejemplo, la búsqueda de DNS pueden realizarse en el puerto UDP 53 o TCP 53. El firewall escucha normalmente uno o más puertos UDP o TCP por lo que también se hace necesario implementar el método deny by default, aunque se utilizan políticas menos rigurosas que ésta para el tráfico saliente TCP y UDP debido a que muchas organizaciones permiten a sus usuarios acceder a muchas aplicaciones ubicadas en servidores externos [9].

ICMP

ICMP se utiliza por los protocolos de red de bajo nivel para aumentar la velocidad y fiabilidad de las redes. Aunque los ataques suelen utilizar ICMP para manipular el flujo del tráfico de la red, éste también puede ser utilizado para obtener un rendimiento razonable en internet, por lo que el bloqueo de este tráfico genera problemas de rendimiento. Otras políticas permiten el tráfico ICMP saliente pero impiden el entrante evitando el acceso al destino, por ejemplo, el comando ping es importante para realizar diagnósticos de la red, pero los ping entrantes generalmente se bloquean para evitar que los atacantes conozcan la topología de la red de la organización.

Es aconsejable bloquear el tráfico ICMP entrante y saliente en el firewall perimetral excepto cuando la organización necesite hacer uso de ellos. En resumen ICMP no debe ser bloqueado en una organización a menos que las necesidades de seguridad sean mayores que las operacionales [10].

PROTOCOLO IPSEC

La política firewall también debe definir si permite o no IPsec VPNs dentro de la red de la organización. Los protocolos ESP y AH se utilizan en IPsec VPNs, por lo que si se bloquean estos protocolos también lo harán las IPsec VPNs. Para las organizaciones que utilizan IPsec VPN deben bloquear ESP y AH excepto desde y hacia direcciones específicas de la red como las gateways IPsec que son autorizadas para ser el límite de la VPN [11].

POLÍTICAS BASADAS EN APLICACIONES

Las aplicaciones firewall o aplicaciones proxy proporcionan una capa adicional de seguridad para el tráfico de entrada mediante la validación de una parte de éste tráfico antes de llegar al servidor deseado. Estas aplicaciones también ayudan a evitar que el servidor tenga acceso directo con el exterior y a descartar tráfico malicioso antes de que llegue al servidor destino, reduciendo la carga del servidor. Las aplicaciones firewall y proxy se deben implementar cuando no se tiene un servidor capaz de protegerse de ataques [12].

Las aplicaciones firewall pueden presentar problemas si éstos no son lo suficientemente rápidos para manejar el tráfico destinado al servidor, pero si el servidor no posee recursos suficientes para soportar un ataque, estas aplicaciones pueden ser utilizadas como escudos.

Las aplicaciones proxy de salida permiten detectar sistemas que realizan conexiones inapropiadas o peligrosas dentro de la red, por ejemplo, cuando un proxy HTTP filtra contenido puede alertar al usuario que el sitio web visitado envió contenido filtrado. El mayor beneficio de un proxy HTTP no tiene que ver con seguridad sino con la caché de las páginas web para aumentar la velocidad y disminuir el ancho de banda utilizado [7].

Políticas basadas en la identidad de usuario

La implementación de VPNs permite aplicar en el firewall políticas basadas en la identidad del usuario. IPsec VPN o SSL VPN tienen varias formas para autenticar usuarios como por ejemplo con certificados digitales controlados por cada usuario. Las aplicaciones firewall y proxies pueden permitir o no el acceso a los usuarios en función de la autenticación que hagan los usuarios dentro de éstas aplicaciones. El firewall que permite estas políticas debe ser capaz de registrar tanto la IP del usuario como su identidad [11].

Políticas basadas en la actividad de la red

Estas políticas permiten al administrador del firewall bloquear las conexiones establecidas después de un determinado periodo de inactividad. Las políticas basadas en el tiempo son eficaces para mitigar los ataques causados por inicios de sesión olvidadas por el usuario original [10]. Sin embargo, éstas también pueden ser incómodas para los usuarios que inician conexiones pero no las utilizan con frecuencia.

Planificación e implementación de firewalls

La adopción de un esquema por etapas para la planeación e implementación de firewalls minimiza la probabilidad de ocurrencia de problemas y permite identificar fallas desde el principio. La Figura 6 presenta las etapas, las cuales se detallan a continuación.

Planeación

Esta primera fase del proceso consiste en identificar todos los requisitos que debe tener en cuenta una organización, para determinar el tipo de firewall que implementará para apoyar el cumplimiento de las políticas de seguridad de la organización. Debe partir de una evaluación

Figura 6 – Etapas para la planeación e implementación de firewalls.
Elaboración propia basado en [2]

inicial de riesgos del sistema en todo su conjunto, que considere mínimamente las amenazas y vulnerabilidades, la probabilidad e impacto de ocurrencia y los controles. En esta etapa se deben considerar los siguientes principios básicos:

- Utilizar los dispositivos para lo que están diseñados, un firewall sirve para controlar el flujo entre redes no para proveer servicios web.

- Crear defensa en profundidad, esto es múltiples capas de seguridad, lo cual permite una mejor gestión ya que si una capa se ve comprometida otra puede contener el ataque.

- Analizar las amenazas internas, centrar la atención solo en amenazas externas puede dejar puertas abiertas a los atacantes desde el interior.

- Documentar las capacidades de firewall, estas son las características que afectan positiva o negativamente la planificación y la estrategia de implementación.

Cada red y organización presenta requisitos y condiciones diferentes por lo que requieren soluciones únicas, por lo tanto es importante considerar a la hora de implementar firewalls la expresión "las reglas están hechas para romperse". Al adquirir una solución de firewall las organizaciones deben considerar, entre otras, las capacidades de seguridad, de gestión, de rendimiento, de integración, los medios físicos, las personas y las necesidades futuras.

Configuración

Esta fase incluye todos los aspectos de la configuración de la plataforma del firewall, incluyendo la instalación de hardware y software, configuración de políticas, configuración de logs y alertas, y la integración del firewall en la arquitectura de red.

- Configuración e instalación de hardware y software: los firewall se deben fortalecer para minimizar el riesgo de vulnerabilidades y proteger el sistema contra accesos no autorizados. Algunos elementos a tener en cuenta son: instalación de los últimos parches y actualizaciones y consolas de administración remota, configuración de cuentas de administración, inhabilitación de servicios de gestión como SNMP y sincronización de relojes. Adicionalmente los requisitos medioambientales recomendados para el producto como temperatura, humedad, espacio, energía, etc., y el espacio debe ser físicamente seguro para evitar que personas no autorizadas accedan.

- Configuración de políticas: el conjunto de reglas describe cómo funcionará el firewall e implementa la política de firewall de la organización por lo tanto debe ser lo más específico posible. Los detalles de la creación de conjunto de reglas varían según el tipo de firewall y productos específicos, sin embargo se debe tener claro el tipo de tráfico requerido por las aplicaciones de la organización, incluyendo los protocolos.

- Configuración de logs y alertas: Los logs son un paso crítico en la prevención y recuperación de fallas, así como para asegurar que se han establecido las configuraciones de seguridad adecuadas en el firewall. Un log adecuado puede proporcionar información vital para responder a los incidentes de seguridad. También se deben configurar las alertas en tiempo real para notificar cuando se produzcan eventos importantes en el firewall. Las notificaciones pueden incluir modificación o desactivación de las reglas de firewall, reinicios del sistema, espacio en discos y otros eventos operacionales.

Pruebas

Antes de la implementación de nuevos firewalls es necesario realizarles pruebas para asegurarse de que funcionan correctamente. Estas deben realizarse en redes aisladas de producción y

deben tratar de replicar las de producción lo más exactamente posible, incluyendo la topología y el tráfico de red que viajaría a través del firewall. Para las pruebas deben tenerse en cuenta aspectos como la conectividad, los conjunto de reglas, la compatibilidad con aplicaciones, administración, logs, el rendimiento, la seguridad de la aplicación, interoperabilidad de componentes, sincronización de políticas y algunas características adicionales como VPNs y capacidades antimalware.

Implementación

- Luego de finalizar las pruebas y resolver todos los problemas, la siguiente fase es la implementación, la cual se debe realizar en conformidad con las políticas de la organización. Previo a esto se debe informar a los usuarios o propietarios de sistemas sobre la nueva implementación para que ellos puedan evaluar el impacto en sus sistemas; todos los cambios necesarios deben ser coordinados como parte de la implementación del firewall. La política de seguridad global de la organización debe incluir la política de seguridad expresada en la configuración del firewall y todos los cambios deben integrarse con los procesos de gestión de la configuración de la organización.

- Para el despliegue de varios firewalls, incluyendo firewalls personales o en múltiples dependencias, se debe considerar un enfoque gradual o por etapas y la realización de un programa piloto, especialmente para identificar y resolver los problemas de las políticas en conflicto. Esto proporcionará a los administradores la oportunidad de evaluar el impacto de la solución de firewall y resolver los problemas antes de la implementación en toda la empresa.

- La conexión de un firewall implica no solo incluirlo en la topología de red sino integrarlo con otros elementos de la red que van a interactuar con él. Esto es, integrarse en la estructura de enrutamiento de la red, implicando en algunos casos sustituir routers, cambiar tablas de enrutamiento de otros routers de la red de la organización para gestionar la incorporación del nuevo dispositivo, aún para los que utilizan enrutamiento dinámico, cambios de configuración de los switches, entre otros.

Gestión

Esta última fase es la de mayor duración, pues la gestión incluye el mantenimiento de la arquitectura, las políticas, el software, y los otros componentes de la solución. En esta etapa: (1) Se deben actualizar las políticas con las nuevas amenazas y los cambios de requisitos que ocurran. (2) Se debe monitorear el rendimiento de los componentes del firewall para asegurar que se identifican y se tratan con tiempo los posibles problemas de los recursos. (3) Por otra parte, los logs y las alertas también deben ser controlados continuamente para identificar amenazas –exitosas y no exitosas- que se realizan en el sistema. (4) Se deben ejecutar pruebas periódicas para comprobar que las reglas del firewall están funcionando como se espera.

Además, (5) las políticas y los conjuntos de reglas del firewall se deben respaldar con regularidad en los múltiples formatos que se requieran. (6) Como los cambios en los conjuntos de reglas del firewall o en las políticas mismas impactan en la seguridad se debe integrar con el proceso formal de gestión de la configuración. (7) Se debe mantener un log asociado con el firewall que incluya todas las decisiones frente a las políticas y los cambios.

(8) Siempre que sea posible, los conjuntos de reglas se deben documentar con comentarios sobre cada regla específica. (9) Se deben utilizar

las restricciones sobre quién puede realizar cambios en el conjunto de reglas, y sobre las direcciones desde las que los administradores pueden hacer tales modificaciones.

Con el tiempo los conjuntos de reglas pueden hacerse cada vez más complejos debido al ingreso de nuevas reglas, esto se puede originar por el ingreso de nuevos usuarios, hosts o simplemente nuevos requisitos de negocio. El mantenimiento servirá tanto para identificar reglas obsoletas como para identificar nuevas necesidades de las políticas que se deben agregar al firewall.

Las mejores prácticas de NIST 800-41 indican que la política firewall se debe revisar a intervalos regulares para que esos hallazgos no ocurran en las auditorías de seguridad, o, peor aún, sólo en casos de emergencia. Cada revisión debe incluir una evaluación detallada de todos los cambios desde la última revisión, quien lo realizó y las circunstancias sobre las que lo hizo. Personas diferentes al equipo que revisan periódicamente las políticas deben realizar una revisión con el objetivo de obtener una visión externa del cumplimiento de los objetivos de seguridad. Debe hacerse uso de las herramientas de diagnóstico que traen algunos firewall con el objetivo de buscar cosas como reglas redundantes o reglas que faltan y que son ampliamente recomendables.

Las pruebas de penetración, que permiten evaluar la seguridad global del perímetro de la red son un mecanismo recomendado, estas pruebas se pueden utilizar para comprobar que un conjunto de reglas del firewall está funcionando según lo previsto Deben ser usadas como complemento a las auditorías.

CONCLUSIONES

La seguridad perimetral en las redes de datos de cualquier organización es de vital importancia, ya que con ella se minimizan los riesgos que vulneran los sistemas de información y la información misma. Los firewall cumplen este papel puesto que se encargan de controlar el tráfico de datos entre la redes privadas e internet y lo puede realizar en las capas de red, transporte y aplicación del modelo TCP/IP, dependiendo del tipo que se desee implementar, sin embargo se sabe que estos dispositivos por si solos no son la solución a la implementación de seguridad en una red, se requieren delimitar claramente las políticas para que realmente cumpla con su objetivo.

El firewall puede trabajar en cualquier topología de red que se desee proteger, con unas buenas políticas de firewall que controlen el tráfico y un buen control por direccionamiento IP y que estén alineadas con las políticas de seguridad de la información de la organización. En general, debe encajar en el diseño de una red actual, sin embargo, una organización puede cambiar su arquitectura de la red al mismo tiempo que se implementa un firewall como parte de un programa de actualización de seguridad en general

Diferentes arquitecturas de red comunes conducen a opciones muy diferentes de dónde ubicar un firewall, por lo que una organización debe evaluar qué arquitectura le funciona mejor para sus objetivos de seguridad. En algunos entornos, ubicar un firewall detrás de otro puede conducir al objetivo de seguridad deseado, pero en general estas múltiples capas de firewalls pueden ser problemáticas [11].

Si un firewall perimetral tiene una DMZ, tenga en cuenta cuales de los servicios orientados hacia el exterior deben ejecutarse desde la zona desmilitarizada y cuales deben permanecer en el interior de la red.

Para robustecer el firewall nos podemos

apoyar en sistemas de prevención y detección de intrusos (IDS/IPS) que trabajan en la capa de aplicación, estos ayudan a detectar el software malicioso que pueden vulnerar las aplicaciones de las organizaciones.

Para la implementación de un firewall es aconsejable realizar una planificación acorde a las necesidades de la red, realizar la configuración de las políticas del firewall, hacer pruebas que identifiquen posibles fallas y por último, gestionar el mantenimiento de la aplicación para mantenerlo en buen funcionamiento.

REFERENCIAS

[1] NEXICA. Aplicaciones más seguras y rentables. [En línea]. Disponible en: http://www.nexica.com/es/firewallaplicaciones

[2] FORTINET. Protecting your network from viruses. [En línea]. Disponible en: http://docs.fortinet.com/cb/html/index.html#page/FOS_Cookbook/UTM/cb_utm_av_basic_db.html

[3] SOPHOS UTM Home edition. [En línea]. Disponible en: http://www.sophos.com/es-es/products/freetools/ sophos-utm-home-edition.aspx

[4] Á. Gomez Vieites. Enciclopedia de la seguridad informática. Cap 4 Los aspectos técnicos para implantar las medidas de seguridad en las redes. RA-MA. 2011.

[5] NSS labs. Next Generation Firewall (NGFW). V5.3. Disponible en: https://www.fortinet.com/lat/products/next-generation-firewall

[6] R. Bustamante. Seguridad en Redes. Universidad Autónoma de Hidalgo. Disponible en: http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/do cumentos/Seguridad%20en%20redes.pdf

[7] K. Scarfone, P. Hoffman. Guidelines on firewall and policy. V1. National Institute of Standard and TechnologyNIST. 2009.

[8] R. Ziegler. Firewalls Linux Guía Avanzada. Prentice Hall. Disponible en: http://hack.dk/~dvc/doc/Prentice.Hall.-.Firewalls.Linux.(libro-book-espa%C3%B1ol).%5Bwww.elbuscaelinks.com%5D.pdf

[9] R. Hunt. Internet/Intranet firewall security - policy, architecture and transaction services. 1998.

[10] PALO ALTO NETWORKS. Protección contra botnets con el firewall de nueva generación. The network security company. Disponible en: http://www.exevi.com/doc/PAN_WP_BotNet_ES.pdf

[11]ELSEVIER. Formal security policy implementations in network firewalls. 2012. Computers & Security. Disponible en: http://www.deepdyve.com/lp/elsevier/formalsecurity-policy-implementations-in-network-firewalls-A6AwrNm6ne

Recibido: Oct. 12, 2021 | Aceptado: Ene. 10, 2022

Elaboración de concentrado para tilapia roja *"Oreochromis sp"* a base de desechos obtenidos de las centrales de abasto de Medellín

Preparation of concentrate for red tilapia "Oreochromis sp" based on waste obtained from Medellín's central supply centers.

DOI: https://doi.org/10.21803/ingecana.2.2.399

Carlos Mario Acosta Feria[1], Jorge Luis Pérez Pérez[2], Laura Isabel Bedoya Corrales[3], Albeiro Hernán Suarez Hernández[4]

[1]Estudiante de Ingeniería Industrial. Corporación Universitaria Americana, acostacarlos2091@coruniamericana.edu.co.. [2]Estudiante de Ingeniería Industrial. Corporación Universitaria Americana, jorgelperez2011@hotmail.com, perezjorge4913@americana.edu.co. [3]Ingeniera Mecánica. lauraisabel.bedoya@gmail.com. [4]Ingeniero Industrial, MSc. Calidad y Productividad. orieblazeraus@gmail.com

Resumen

El presente artículo brinda generar una nueva alimentación para peces, particularmente para la Tilapia Roja "Oreochromis sp", a partir de los residuos vegetales que son producidos en las centrales de abastos, los cuales están provocando daños al medio ambiente por su crecimiento en los vertederos; por ello se busca por medio de este concentrado, brindar a la dieta mejores oportunidades en costo, cantidad de vitaminas, minerales, ácidos grasos los cuales son importantes para el crecimiento de los peces, proporcionando un mejoramiento en la tabla nutricional con el fin de obtener un producto de mejor calidad por tamaño, textura y color, aspectos que son importantes para el consumo humano.

La idea de elaborar un nuevo concentrado surgió de mitigar los desechos que se generan a diario, y darle un mejoramiento al concentrado que actualmente se les brinda a los alevinos, ya que se encuentra alimentación no balanceada y retraso en su crecimiento que están proporcionando afectación para el desarrollo, lo que conlleva no suplir la demanda que está creciendo por este alimento.

Para llevar a cabo el desarrollo de la nueva dieta alimenticia es necesario realizar estudios estadísticos, pruebas en laboratorio de medición y observación, identificando el adecuado comportamiento de los alevinos, lo cual se busca adaptar especificaciones técnicas que generen confiabilidad en las personas que se dedican a la labor de la piscicultura en Medellín.

Palabras clave: Concentrado; Centrales de Abastos; Residuos Vegetales; Tilapia Roja.

Abstract

The present research thesis offers to generate a new fish feed, particularly for the Red Tilapia "Oreochromis sp", from the vegetable residues that are produced in the central supply plants, which are causing damage to the environment by their growth in the landfills; Therefore, this concentrate seeks to provide the diet with better opportunities in cost, quantity of vitamins, minerals, fatty acids which are important for the growth of fish, providing an improvement in the nutritional table in order to obtain a better quality product in terms of size, texture and color, aspects that are important for human consumption.

The idea of developing a new concentrate arose to mitigate the waste that is generated daily, and to improve the concentrate that is currently provided to the fry, since there is an unbalanced diet and delayed growth that is affecting their development, which leads to not supplying the growing demand for this food.

To carry out the development of the new food diet, it is necessary to carry out statistical studies, laboratory tests of measurement and observation, identifying the adequate behavior of the fry, which seeks to adapt technical specifications that generate reliability in the people who are dedicated to the work of fish farming in Medellin.

Keywords: *Concentrate, Food Processing Plants, Vegetable Residues, Red Tilapia.*

Introducción

En la actualidad, Colombia cuenta con un gran potencial piscicultor, el cual puede llevarse a futuro como una alternativa viable de ingresos dentro del Agro. Para el total de las variedades de peces utilizadas en el país para el consumo humano, la producción nacional en el 2011 fue de 82.733 toneladas, de las cuales más de la mitad correspondió a las tilapias roja, proyectándose como uno de los alevinos con mayor consumo en el país [1]. Su crecimiento rápido genera que la fabricación de alimentos con mejor calidad se realice de manera eficaz y eficiente, pensando en la salud de los animales y del hombre para brindar una confiabilidad y certeza, con el fin de que siga creciendo el consumo de pescado. Así mismo permitirá convertirse para la acuicultura una buena alternativa comercial, y lograr disminuir los sobrecostos y productos de bajo rendimiento.

Como alternativas de aprovechamiento sostenible para el alimento de los peces, los residuos vegetales pueden ser utilizados como materias primas y destinarlos a la fabricación de alimentos [2], ya que se generan en las centrales de abastos 75 toneladas de desechos cada 24 horas y son considerados alimentos con componentes que aportan una gran cantidad de vitaminas, minerales y ácidos grasos importantes para el crecimiento, textura, peso y sabor a los peces que puedan adquirirla [3], mitigando el manejo inadecuado de los residuos y evitando que genere mayor contaminación en los rellenos sanitarios. Adicionalmente, se pretende generar crecimiento, sostenibilidad e innovación en la acuicultura del país, a través del impacto ambiental positivo en el aprovechamiento de estos residuos en diferentes ámbitos, al bajo costo y a su alta disponibilidad.

La presente investigación tiene como propósito diseñar un modelo de alimento integrado para tilapia roja “Oreochromis sp” a partir de los residuos de las centrales de abastos de la ciudad de Medellín, con el fin de determinar los atributos de calidad en la Tilapia roja por el alimento formulado, como color, tamaño y textura, transformando los residuos en un alimento y así, mitigar los daños que ocasionan los residuos, aprovechando sus características, como vitaminas y minerales que ayudan a una producción de un concentrado, bajo la sostenibilidad, innovación y aspectos naturales para la nueva dieta.

MATERIALES Y MÉTODOS

Formulación del concentrado

La materia prima se obtuvo de los desechos de la central de abastos de Medellín, en la cual se seleccionaron papa, plátano, zanahoria y hueso cerdo. Para la formulación se analizaron las siguientes composiciones:

- Dieta experimental 1: 30% Papa – 30% Plátano – 40% Zanahoria.
- Dieta experimental 2: 30% Hueso de Cerdo – 25% Papa – 25% Plátano – 20% Zanahoria
- Dieta experimental 3: 60% Hueso de Cerdo – 15% Papa – 15% Plátano – 10% Zanahoria.

La metodología de producción del concentrado se adaptó de Maya [4]. La materia prima se tritura en un molino MTN QJH C12A, para luego ser remojados en hipoclorito de concentración del 13% por media hora, para luego dejarlo escurrir en un colador. Posteriormente, es secada en un horno WGL (b) a una temperatura de 40°C por un tiempo de 12 horas, excepto el hueso de cerdo que requiere 60°C por su alto contenido de humedad. Después de estar seca la materia prima se pulveriza, para luego juntar todos los componentes con aglomerante; y finalmente hacer la granulación del concentrado. Cuando está lista la granulación se ingresa al horno a una temperatura de 40°C por 12 horas para obtener la granulación seca y empacarla.

Prueba en Peces

Se verifican las propiedades de los vegetales seleccionados a partir de la influencia en los atributos de calidad de los peces. Estas materias primas contienen nutrientes importantes para aportar un adecuado desarrollo a los peces, por lo tanto, se realizaron ensayos para analizar el desarrollo de los alevinos, donde se tomaron 20 peces como muestra, con diferentes porcentajes de los componentes mencionados anteriormente.

Se evaluó el desarrollo de los peces a través de las siguientes pruebas:

- Color: Se logró obtener resultados a partir de las investigaciones realizadas y por la comparación que se realizaba con peces que ya estaban formados y listos para el consumo. El control que se realizaba era cada 3 días por medio de un acuario acondicionado para los peces de prueba.

- Tamaño: Se determinó utilizando un medidor de peces, a partir de las mediciones que se realizaban cada 8 días, se analizaron las cantidades de los componentes que se debían tener en cuenta para mejorar.

- Textura: Se determina mediante observaciones realizadas cada 8 días, donde se observa que el pez tenga piel clara y brillante y la carne sea firme al tocarlo.

RESULTADOS

En la Figura 1 se muestra el diagrama de flujo general correspondiente al proceso de fabricación de los concentrados experimentales.

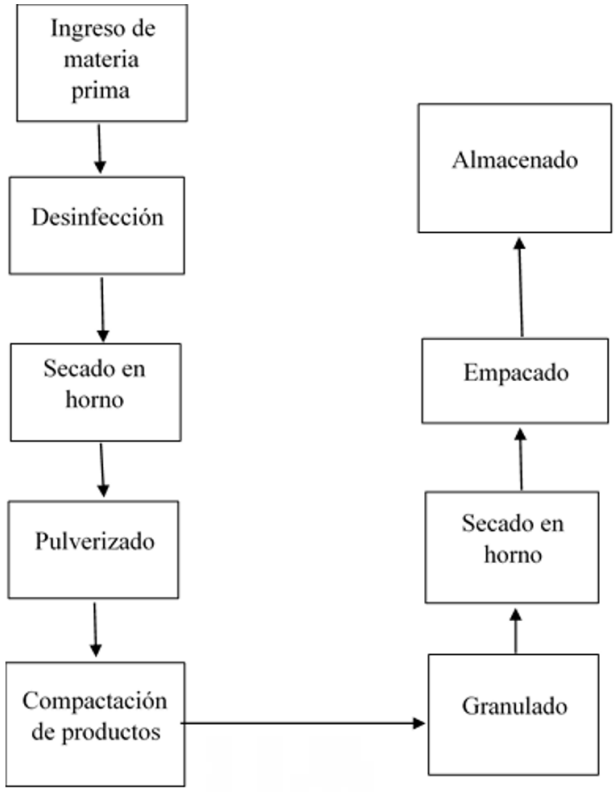


Figura 1. Diagrama de flujo general para la fabricación del concentrado
Elaboración propia.

En la Tabla 1 se muestran las dietas utilizadas con los parámetros que se tuvieron en cuenta a la hora de la formulación, analizando por semana el crecimiento, peso y textura de los peces, de acuerdo a la cantidad de alimento que se le proporcionó, observando por meses la eficiencia de cada dieta.

TABLA 1.

FORMACIONES ANALIZADAS CON SUS PARÁMETROS DE DISCUSIÓN

Dieta experimental 1: 30% Papa – 30% Plátano – 40% Zanahoria	**Incremento por Semana**	**Peso (g)**	**Cantidad de Siembra**	**Alimento diario**	**Textura**
semana 0	0	2	15	0,78	Elástico
semana 1	8,8	10,8	15	4,21	Elástico
semana 2	9,1	19,9	15	7,76	Elástico
semana 3	9,4	29,3	15	11,43	Elástico
semana 4	9,7	39	15	15,21	Elástico
Dieta experimental 2: 30% Hueso de Cerdo – 25% Papa – 25% Plátano – 20% Zanahoria	**Incremento por Semana**	**Peso (g)**	**Cantidad de siembra**	**Alimento Diario**	**Textura**
semana 5	10,16	39	14	14,20	Elástico
semana 6	10,61	49,61	14	18,06	Elástico
semana 7	11,08	60,69	13	20,51	Suave
semana 8	11,56	72,25	13	24,42	Suave
semana 9	12,05	84,3	13	28,49	Suave
Dieta experimental 3: 60% Hueso de Cerdo – 15% Papa – 15% Plátano – 10% Zanahoria.	**Incremento por Semana**	**Peso (g)**	**Cantidad de Siembra**	**Alimento Diario**	**Textura**
semana 10	12,71	84,3	13	28,49	Suave
semana 11	13,37	97,67	13	33,01	Suave
semana 12	13,97	111,64	10	29,03	Suave
semana 13	14,67	126,31	10	32,84	Firme
semana 14	15,37	141,68	10	36,84	Firme
semana 15	16,12	157,8	10	41,03	Firme
semana 16	16,87	174,67	10	45,41	Firme
semana 17	17,62	192,29	10	50,00	Firme
semana 18	18,42	210,71	10	54,78	Firme
semana 19	19,32	230,03	10	59,81	Firme
semana 20	20,12	250,15	10	65,04	Firme

Dieta experimental 3: 60% Hueso de Cerdo – 15% Papa – 15% Plátano – 10% Zanahoria.	Incremento por Semana	Peso (g)	Cantidad de Siembra	Alimento Diario	Textura
semana 10	12,71	84,3	13	28,49	Suave
semana 11	13,37	97,67	13	33,01	Suave
semana 12	13,97	111,64	10	29,03	Suave
semana 13	14,67	126,31	10	32,84	Firme
semana 14	15,37	141,68	10	36,84	Firme
semana 15	16,12	157,8	10	41,03	Firme
semana 16	16,87	174,67	10	45,41	Firme
semana 17	17,62	192,29	10	50,00	Firme
semana 18	18,42	210,71	10	54,78	Firme
semana 19	19,32	230,03	10	59,81	Firme
semana 20	20,12	250,15	10	65,04	Firme

Las exigencias nutricionales de los alevinos son iguales a la de las tilapias en términos cualitativos, sin embargo, en términos cuantitativos, las exigencias son mayores en peces jóvenes que en adultos [5] [6].

Los resultados indican que la dieta experimental 3, es la que aporta mayor ganancia de peso, en la cual los peces obtienen de 250 g a 300 g y un tamaño de 20 cm, logrando conseguir este peso en un periodo de 5 meses; así mismo se observa que es una alimentación lenta a comparación de los alimentos que se comercializan tradicionalmente que ganan peso de 400 a 450 g en 6 meses, sin embargo podría compensarse con los bajos costos de la materia prima con respecto a la alimentación tradicional. Adicionalmente, se brinda una alimentación alternativa que no utiliza conservantes ni acelerantes químicos.

Por otra parte, se observó que para obtener una pigmentación adecuada de la piel a la de la tilapia roja, es necesario cultivarlos en estanques de aguas tratadas, ya que en las muestras que se obtuvieron se realizó en estanques experimentales donde eran pequeños y de agua pura, sin cloro y no tenía oxigenación constante, lo que fomentó la decoloración de los peces dejándolos más blancos. Igualmente, el tamaño del estanque debe ser adecuado a los kilogramos a cultivar ya que, si son bastantes peces, el roce entre ellos hace que se les quite las escamas y se corten entre ellos.

En contraste con la investigación, algunos investigadores [7], insertaron cáscaras de naranja en la alimentación para tilapia, determinando que la harina de cáscara de naranja tiene parámetros importantes que aportan un alto valor de calcio y proteína cruda, indicando que el tratamiento propuesto brinda una tendencia bien marcada de incremento de peso y ganancia diaria de peso. Por lo tanto, un subproducto como lo es la cáscara de naranja representa una buena alternativa para la realización de dietas alimenticias, ya que permiten disminuir los costos de producción en la elaboración de las raciones para tilapia.

Así mismo, en la investigación utilización de la pulpa de café en la alimentación de alevinos de tilapia roja [8], tuvieron en cuenta los parámetros de peso y ganancia diaria de peso, donde la pulpa de café deshidratada ayuda a obtener un peso adecuado de acuerdo a los requerimientos de muchos centros de alevinaje, por lo que brinda porcentajes de supervivencia buenos, especificando el 2% de mortalidad. Igualmente, las dietas donde se utiliza la pulpa de café son más económicas, demostrando una factibilidad para obtener una producción de bajo costo.

CONCLUSIONES

La formulación de la nueva dieta alimenticia genera un 75 % de ahorro en los costos de producción y un 30 % menos de crecimiento en los peces, aunque se destaca que es una dieta artesanal que brinda componentes totalmente naturales, por la composición nutricional de la papa, plátano y zanahoria son favorables para ser utilizadas en la alimentación de la tilapia roja. Se determinó que para mejorar el parámetro de peso y crecimiento en los peces es necesario aportar una proteína que constituya una ganancia significante de peso diario y ayude a la disminución de tiempo de cultivo, en esta investigación se tomó el hueso de cerdo que es un alimento fácil de conseguir y de bajo costo.

Finalmente, se concluye que el tratamiento propuesto para los peces aporta calidad en el cultivo del producto final, generando confiabilidad en el sector, mostrando peces aptos para el consumo humano, adicional demuestra ganancias ya que en la actualidad los residuos son fáciles de conseguir y generan un impacto positivo al medio ambiente.

REFERENCIAS

[1] M. Merino, S. Bonilla y F. Bages, «Diagnóstico del estado de la acuicultura en Colombia» RM Gráficos, 2013.

[2] G. Jaramillo Henao y L. M. Zapata Márquez, «Aprovechamiento de los residuos sólidos orgánicos en Colombia» 2008. [En línea]. Disponible en: http://tesis.udea.edu.co/bitstream/10495/45/1/AprovechamientoRSOUenColombia.pdf.

[3] R. Rodríguez Ramírez, «La central de abastos “ José Maria Jiménez “ de Saltillo, Coahuila. Evolución y perspectivas de la distribución de frutas y hortalizas.,» 06 2008. [En línea]. Disponible en: http://repositorio.uaaan.mx:8080/xmlui/bitstream/handle/123456789/3598/T16713%20%20RODRIGUEZ%20 RAMIREZ,%20 ROSALVA%20TESIS.pdf?sequence=1.

[4] S. Maya Henao, «Procesos de producción de alimentos balanceados - Planta de Concentrados Colanta Itagüí,» 2016. [En línea]. Disponible en: http://repository.lasallista.edu.co/dspace/bitstream/10567/1492/1/Procesos_Produccion_Alimentos_balanceados_COLANTA.pdf.

[5] J. Pokniak, «Nutrición de peces,» TecnoVet,3:2. Facultad de Ciencias Veterinarias y Pecuarias, Universidad de Chile, 1997.

[6] D. Torres Novoa y V. Hurtado Nery, «Requerimientos nutricionales para Tilapia del Nilo (Oreochromis niloticus),» Orinoquia - Universidad de los Llanos - Villavicencio, Meta, 2012.

[7] M. Moreno, J. Hernández, R. Rovero, A. Tablante y L. Rangel, «Alimentación de tilapia con raciones parciales de cáscaras de naranja,» CYTA Journal of food, pp. 29-33, 2009.

[8] E. Castillo, Y. Acosta, N. Betancourt, E. Castellanos, A. Matos, V. Cobos y M. Jover, «Utilización de pulpa de café en la alimentación de alevines de tilapia roja,» Aquatic, 2002.

Recibido: Oct. 3, 2021 | Aceptado: Ene. 22, 2022

Implementación de mejora en el proceso de empaque del banano: caso aplicado en finca de Urabá (Antioquia)

Implementation of improvement in the banana packing process: case applied in Urabá farm (Antioquia).

DOI: https://doi.org/10.21803/ingecana.2.2.400

Anderson Manuel Trespalacio González[1]

[1]Ingeniero Industrial, Magister en Administración. Corporación Universitaria Americana. amtrespalacio@americana.edu.co

Resumen

El presente trabajo tiene como objetivo identificar las posibles dificultades en el proceso de empaque del banano desarrollado por la finca Kalamary, ubicada en el Urabá Antiqueño, con el fin de implementar mejoras en el proceso de forma que se pueda ofrecer un mejor rendimiento en la planta y aumentar la producción en la finca.

Para lograr este propósito, fue realizado un trabajo de campo en el que se obtuvo información preliminar del proceso, con la que posteriormente se realizó una simulación base que reflejó la realidad del proceso de empaque del banano. Por último, se realizó una simulación final en la cual se implementaron las mejoras, evidenciando un aumento en el rendimiento productivo de la finca Kalamary.

Palabras clave: Empaque; Banano; Simulación; Procesos.

Abstract

The objective of this work is to identify the possible difficulties in the banana packing process developed by the Kalamary farm, located in Urabá Antiqueño, in order to implement improvements in the process so as to offer a better yield in the plant and increase the farm's production.

To achieve this purpose, field work was carried out to obtain preliminary information on the process, which was later used to carry out a basic simulation that reflected the reality of the banana packing process. Finally, a final simulation was carried out in which the improvements were implemented, showing an increase in the productive yield of the Kalamary farm.

Keywords: *Packaging, Banana, Simulation, Processes, Simulation*

Introducción

Colombia ha tenido una relativa y buena tradición como productora y exportadora de banano, ocupando el cuarto país exportador mundial, alcanzado una producción de 100,4 millones de cajas de 18 kilos de fruta en el 2014 [1], proporcionándole a la agroindustria un papel importante para la economía del país.

La producción de banano ha venido expandiendo sus cultivos representando innovaciones para el proceso de producción, dando pie a realizar producciones con calidad para una comercialización segura y apta para el consumo humano, lo que lleva aportar estándares relevantes cada día para lograr ser líder en el mercado y lograr superar países como Ecuador, Costa Rica y Guatemala [1].

Por tal motivo se desarrolló una simulación del proceso de empaque del banano, mediante la recopilación de información y análisis que se pudo obtener en la visita a la finca Kalamary ubicada en el Urabá Antioqueño, donde se lograra obtener información de los tiempos y métodos en los cuales se ejecutan las actividades, y aplicarlas en las áreas donde se identificaron fallas, como el transporte de la fruta, control y manejo del inventario, aplicación de químicos, bandas transportadoras y el pesaje del banano.

La importancia de realizar una implementación de mejoras en el proceso de producción surge a partir de lo observado en el trabajo de campo en lo que se identifica que se puede mejorar la cantidad de fruta que se transporta desde la finca al embarcadero con destino a Europa y que se verá reflejado en un aumento de la utilidad de la operación.

La simulación pretende tener en cuenta unas mejoras significativas que disminuirán el tiempo de ejecución de las actividades en las que se identifiquen mayor oportunidad de mejora y por lo cual se quiere seguir una metodología mixta, en la cual se realizarán observaciones del proceso, tomando en cuenta los tiempos en que se ejecutan las actividades en la finca, forma de trabajo de los operarios y necesidades de la finca.

MATERIALES Y MÉTODOS

La realización de un estudio de simulación requiere la ejecución de una serie de actividades y análisis que permitan sacarle el mejor provecho [2].

A continuación, se mencionan los pasos básicos para realizar un estudio de simulación.

Definición del sistema: En esta etapa es necesario conocer el sistema a modelar, para ello se requiere saber qué origina el estudio de simulación. Es por eso qué en este paso vamos a describir las áreas que componen la planta de empaque de banano.

Modelo de simulación base: Una vez que se ha definido y descrito las áreas que componen la planta se procede a realizar un modelo no formal, a pesar de que no se cuenta con una información estadística en este paso se usará la creatividad para

Figura 1. Descripción de metodología.
Elaboración propia a partir de [2]

realizar un modelo que refleje la realidad y tener una idea base de cómo quedaría la simulación.

Recolección y análisis de datos: Aquí se realiza la recopilación de datos estadísticos de las variables aleatorias del modelo, en esta etapa se debe definir la información que es útil para la distribución de probabilidad, Aquí se analizarán los datos, tiempos y se analizaran si requieren pruebas de bondad y ajuste.

Generación del modelo preliminar: En este paso se realiza la integración de la información recolectada y el análisis de datos obtenidos, luego se procede a realizar las relaciones matemáticas, relaciones lógicas, distribuciones y al tener estas actividades listas el modelo estará listo para sus primeras corridas.

Verificación del modelo: Cuando se den las primeras corridas al modelo se dará una verificación a los datos y distribuciones para detectar posibles fallas y poder comprobar que los parámetros usados en la simulación funcionen correctamente, algunas de las fallas que surgen posiblemente son debido a error humano u operaciones que requieren de mucha programación o distribuciones de probabilidad difícil de programar.

Análisis de sensibilidad: Una vez se tengan los resultados de los dos procesos de simulación del actual y del mejorado, se procede a realizar una revisión para comparar y determinar la diferencia entre las dos simulaciones y poder dar resultados más claros.

Documento final: Cuando se realice el análisis de sensibilidad, ya se procede al paso final que es reunir toda la documentación final, dicha documentación debe estar complementada por los modelos de simulación realizados, resultados, distribuciones, alcances y limitaciones, la recopilación de toda esta información mencionada nos permitirá obtener un informe más claro y se podrá sacar conclusiones y dar recomendaciones.

Cosecha: Es el proceso que inicia desde el momento del corte de los racimos hasta su transporte a la empacadora, e implica un conjunto de procedimientos para conservar en última instancia las características esenciales de la fruta hasta su consumo final, en el banano, la cosecha hace referencia a las labores de corte del racimo, el cual consiste en separar de las plantas madres todos aquellos racimos que cumpla con los requisitos exigidos para el mercado objeto o hayan alcanzado el índice de madurez comercial. El proceso de corte se inicia con la labor del puyero, que es la persona que identifica a los racimos que estén dentro de las especificaciones de corte alcanzado, luego procede a hacer un corte en forma de “V” en la planta para doblarla El corte se debe hacer en el tercio superior de la planta, para

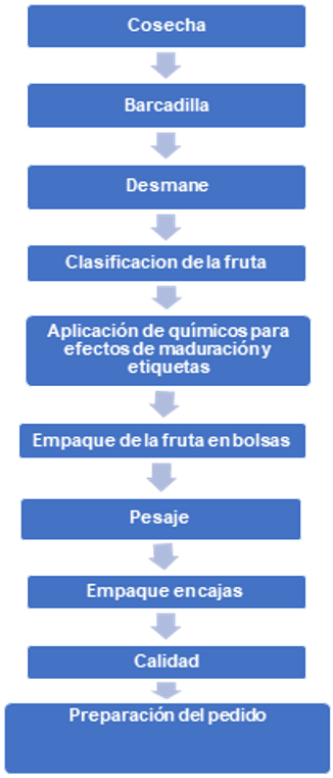


Figura 2. Descripción del proceso de empaque del banano. Elaboración propia.

que al doblarla el racimo no se golpee con el suelo o el pseudotallo de la planta. Esto se realiza con herramientas bien afiladas (machete y puya). El colero o recibidor debe recibir el racimo una vez la planta se dobló, este se puede recibir en una cuna o almohada y transportarlo a la empacadora, ya sea por cable vía o en su defecto en la misma cuna.

Cable vías: Este sistema debe estar diseñado de tal manera que permita la facilidad del tránsito del operario dentro de él y de los racimos, así mismo en un sentido práctico. Debe tener una altura aproximada de 2.10 metros sobre la superficie y sujetado por arcos de tubo galvanizado o madera inmunizada, colocados entre 8 y 10 metros para su mayor resistencia y durabilidad. El cable debe estar constituido por una varilla de aproximadamente 7/16 de pulgada de diámetro y con una resistencia de 100 kg por Mm para no correr el riesgo de ruptura

Área de barcadilla: Es la encargada de recibir la fruta que viene del campo, apenas se corta los racimos de banano estos son guindados en serie en una cadena la cual es jalada por un operario desde el punto de recolección de la fruta hasta el área de barcadilla o "bodega de la fruta recolectada" en este área también se puede evidenciar el tiempo que tiene la fruta esto lo hacen por medio de una bolsa de colores que son amarradas en la parte superior del racimo, en la siguiente área con esta misma bolsa hacen el conteo de racimos cortados y llevan el control del inventario.

Área de desmane: Medición de la fruta y control de inventario: inicia con una inspección detallada de la fruta en la empacadora, observándose el calibre, largo, presencia de maltratos de campo y verificación de la edad del racimo. Posteriormente se procede a desmanar se corta las manos de banano dejando así el mero vástago y dividir las manos en clúster de acuerdo a las especificaciones del mercado, se procede a un lavado de la fruta en tanques con muy buenas condiciones higiénicas y con una solución de agua, alumbre y algún floculante para impedir la adherencia del látex en la fruta, con personal idóneo y capacitado, por último se le retira la bolsa de color con la que viene identificada cada racimo y se hace conteo para llevar control de inventario.

Clasificación de la fruta: En esta área se le hace una clasificación de la fruta donde se divide ya sea en pequeña, mediana o grande dependiendo el destino de exportación, además se le hacen un corte más pulido al cogollo de la mano de banano, también es donde se retira la fruta que no cumple con las especificaciones y se ubica en canecas para envío nacional, luego de cumplir con la debida clasificación es sumergida nuevamente en la alberca y dirigida a la siguiente área.

Aplicación de químico y etiquetas: En esta área ya se retira la fruta de los tanques con agua y se ubican en bandejas de acuerdo al tamaño

de la fruta, y se procede a la aplicación de un químico para evitar efectos de maduración antes del tiempo, dicho químico es aplicado manualmente con una brocha sobre la mano de banano, adicionalmente se asigna una etiqueta a cada mano de banano y se procede al área de empaque.

Empaque de la fruta en bolsas: En esta área se ingresa cada mano de banano en bolsas dicha bolsa ya vienen con una verificación adecuada que da la seguridad que la fruta va llegar a su destino libre de cualquier plaga o enfermedad y en buenas condiciones para el consumo humano.

Pesaje: Aquí se pesa las unidades para ser empacadas en la caja, el peso debe estar entre los 20 y 21 kilogramos no puede estar por fuera de los rangos debido a que esto puede causar multas o daño en la fruta y si no está entre los rangos el operario encargado debe cambiar manos de banano hasta encontrar el peso adecuado.

Empaque de las manos de banano en cajas: Es una de las fases finales, aquí se ubican las manos de banano dentro de las cajas de una forma adecuada para garantizar la calidad de la fruta y de esta manera obtener una buena imagen para la empresa.

Calidad: En esta última fase antes de la preparación de pedido se escogen algunas muestras para hacer inspección de calidad, que el empaque haya quedado bien y verificar que todo vaya bajo las normas establecidas, esto con el fin de buscar un progreso y un crecimiento de la empresa porque sabemos que un producto con calidad es ganancia y prestigio para el negocio.

Preparación de pedido: La fase final, se ubican las cajas sobre las estibas y se prepara el despacho, además se le asigna etiqueta y por cada mula enviada hasta el puerto van, ejemplo: 18 pallets, de 48 cajas [3].

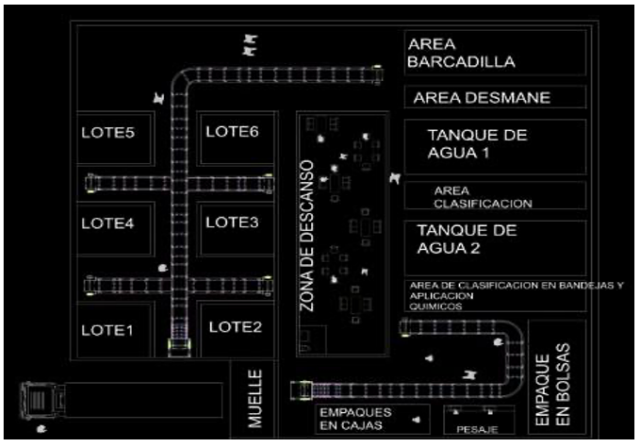


Figura 3. Layout finca Kalamary.

Elaboración propia.

En la actualidad se cuenta con una serie de software que pueden ayudar a la toma de decisiones en temas muy diversos. La facilidad que brinda la utilización de esta herramienta para dar soluciones a problemáticas complejas ha hecho que se desarrollen y mejoren los programas de simulación mostrando una significada capacidad para dar análisis relevantes e interpretaciones importantes [4]. La simulación que se realizó es una simulación de eventos discretos que es el conjunto de relaciones lógicas, matemáticas y probabilísticas que componen el proceder del sistema bajo estudio cuando se presenta un evento determinado [5].

Teniendo claro lo que el tipo de simulación que se realizó, se elaboró el modelo en el software PROMODEL, útil para simular y experimentar con los procesos de sistemas existentes sin que éstos se alteren [6]. Esta técnica es ubicada típicamente dentro de la Ingeniería Industrial cobra importancia para simular el comportamiento real del proceso de empaque del banano en la finca, con lo cual se cumple con la metodología propuesta, por lo que se muestra las locaciones, entidades y recursos utilizados en la simulación.

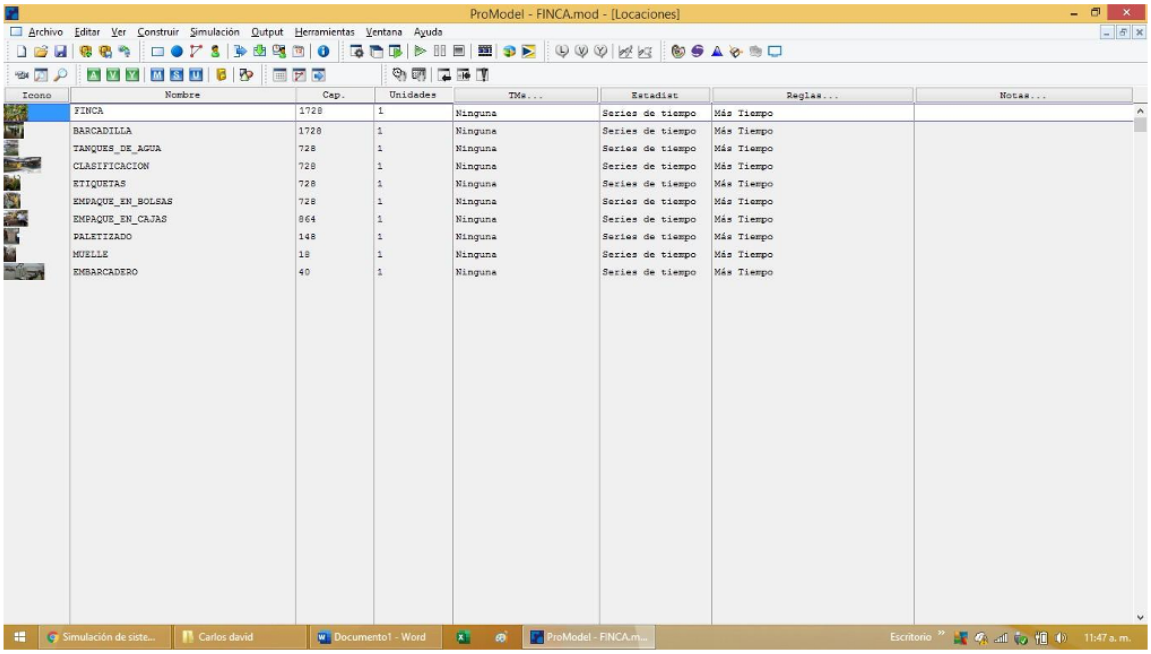


Figura 4. Locaciones del modelo.
Elaboración propia.

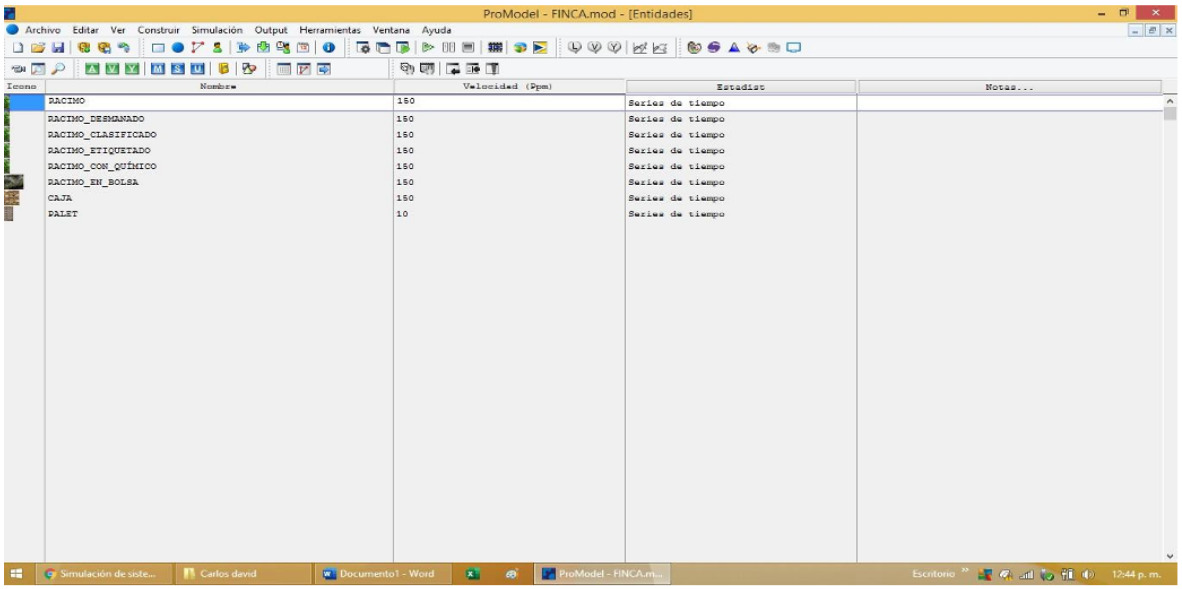


Figura 5. Entidades del modelo.
Elaboración propia

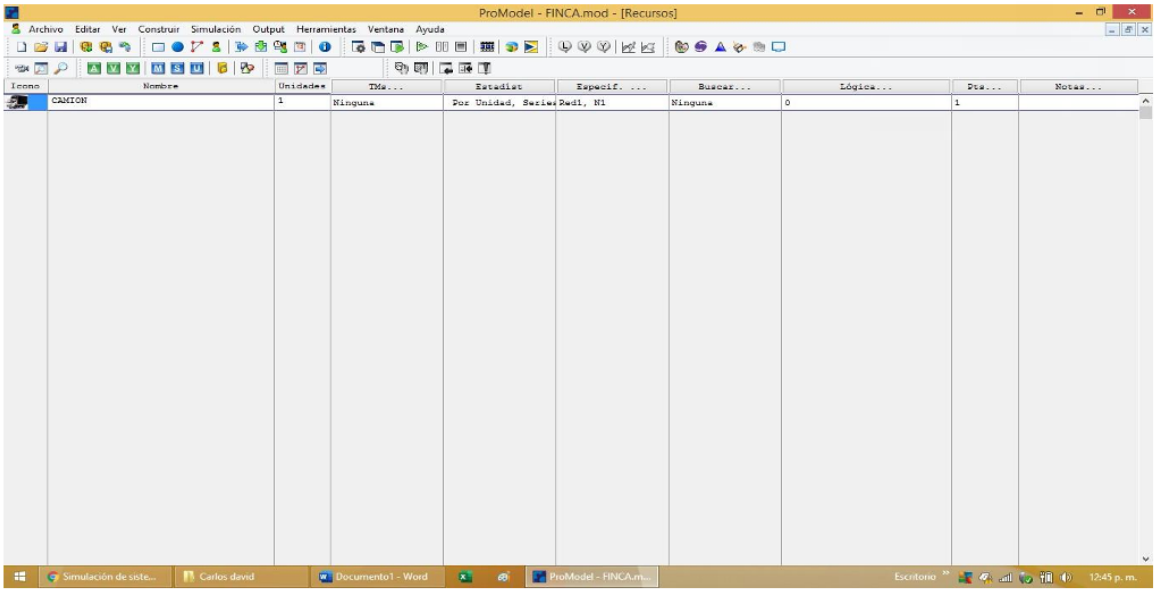


Figura 6. Recursos del modelo.
Elaboración propia.

Para realizar la simulación se consideró las mejoras implementadas para que el proceso de empaque del banano sea más eficiente, es de resaltar que cada mejora está asociada a las dificultades encontradas en el proceso y que fueron identificadas en el trabajo de campo y que se espera mejore el rendimiento de la planta. A continuación, se describen las mejoras implementadas y se describe cuál es la dificultad puntual a solucionar:

Transporte de la fruta: Es el proceso que inicia desde el momento del corte de los racimos hasta su transporte a la empacadora, actualmente esta labor es ejecutada por un grupo de trabajo llamado cuadrillas y cada cuadrilla la componen un colero, un puyero y 2 garrucheros. El colero es el encargado de llevar el racimo hasta los cables y los garrucheros jalan por medio de los cables vías los 24 racimos que se llevan en cada viaje hasta el área de barcadilla.

La mejora consiste en que los cables vías queden automatizados por medio de un motor y poleas los cables se muevan automáticamente [7]. Con esta mejora se pueden obtener beneficios como lo son: Optimización de tiempo, reducción de la fuerza bruta del operario, alta calidad del producto transportado, garantía de transporte sin importar las condiciones del clima o del terreno, no compactación del suelo, aumento de la capacidad, entre otros.

Control de inventarios: Luego de realizar el desmane se procede a realizar el control de inventarios esto lo hacen contando cada bolsa de color que trae amarrada el racimo en la parte superior esta actividad es ejecutada por un operario.

Con el fin de tener mayor claridad y rapidez en este área se propone la asignación de una etiqueta a cada racimo en el campo, para cuando llegue a la planta de empaque pueda ser registrado por medio del código de barras con unas pistola láser [8], beneficios esperados son: Mayor claridad y

manejo de inventario de la materia prima, el margen de error es muy bajo al momento de estar contabilizando, incremento en la rapidez del conteo de racimos, mejora la competitividad, mejor control sobre la entrada y salidas de productos, seguridad alimentaria, entre otros.

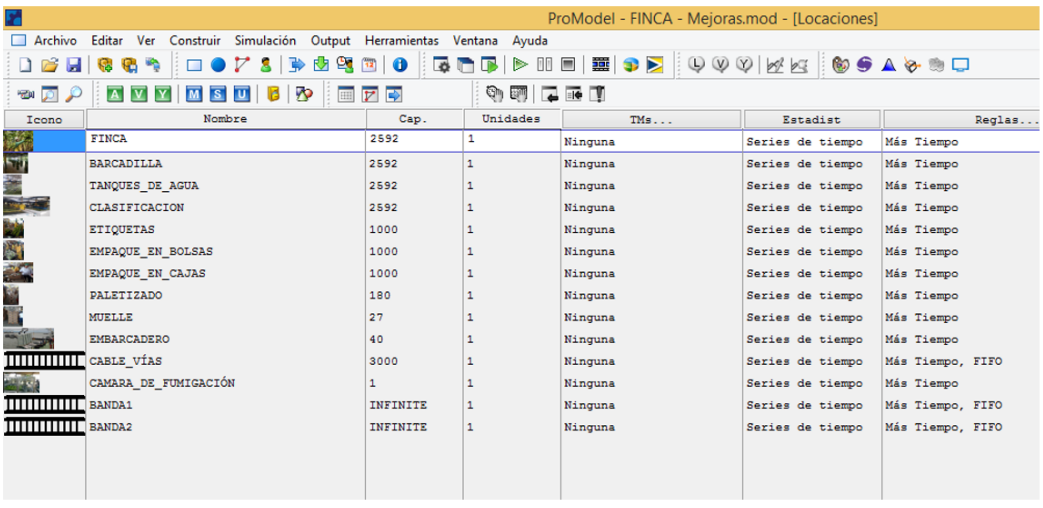
Aplicación de químicos: En esta área se realiza la clasificación de la fruta en canastas para la aplicación de etiquetas y un químico en el cogollo de cada mano de banano para evitar efectos de maduración, en el momento el químico es aplicado manualmente por dos operarias con una brocha.

Se instaló una cámara de fumigación, se utiliza para fumigar frutas, con posibilidad de automatizar 100% el sistema eliminando el operador ya que un sensor detectará el ingreso de la bandeja de fruta y automáticamente se iniciara la fase de fumigación, posibilidad de incluir el sistema de bombeo y tanque de almacenamiento de producto con agitador, los beneficios esperados son: Permite realizar una fumigación uniforme, permite controlar exactamente la dosificación del producto a aplicarse, la cámara encierra la aspersión protegiendo la salud del operador y aprovecha 100% el producto a aplicarse, reduce el rechazo en exportaciones ya que mejora la calidad del producto, optimización de tiempo, aumento de capacidad, entre otros.

Bandas transportadoras: Actualmente la planta cuenta con unas bandas de rodillos en madera algo muy empírico y el recorrido de las bandas empieza desde el área de clasificación hasta el muelle.

Se hizo la instalación bandas automatizadas, es un sistema de transporte continuo formado por una banda continua que se mueve entre tambores, la banda es arrastrada por la fricción de sus tambores que a la vez este es accionado por un motor, adicionalmente las bandas llevan un sistema integrado de pesaje “cintas transportadoras pesadoras” y así omitir el proceso de peso con el que se cuenta actualmente, los beneficios esperados con este sistema de bandas son: Es posible la carga y descarga en cualquier punto del recorrido, aumenta la capacidad de producción, permite el transporte a mayor rapidez, no altera el producto transportado, permite un proceso más continuo, el pesaje del producto es más rápido y confiable, mejor manejo de la higiene, reduce personal, entre otras.

A continuación, se procede a realizar la segunda simulación incluyendo las mejoras en el implementadas en el proceso de empaque del banano, en las que se agregan 3 locaciones respecto al modelo base, las cuales se pueden apreciar en las últimas 3 posiciones.



Icono	Nombre	Cap.	Unidades	TMs...	Estadist	Reglas...
	FINCA	2592	1	Ninguna	Series de tiempo	Más Tiempo
	BARCADILLA	2592	1	Ninguna	Series de tiempo	Más Tiempo
	TANQUES_DE_AGUA	2592	1	Ninguna	Series de tiempo	Más Tiempo
	CLASIFICACION	2592	1	Ninguna	Series de tiempo	Más Tiempo
	ETIQUETAS	1000	1	Ninguna	Series de tiempo	Más Tiempo
	EMPAQUE_EN_BOLSAS	1000	1	Ninguna	Series de tiempo	Más Tiempo
	EMPAQUE_EN_CAJAS	1000	1	Ninguna	Series de tiempo	Más Tiempo
	PALETIZADO	180	1	Ninguna	Series de tiempo	Más Tiempo
	MUELLE	27	1	Ninguna	Series de tiempo	Más Tiempo
	EMBARCADERO	40	1	Ninguna	Series de tiempo	Más Tiempo
	CABLE_VÍAS	3000	1	Ninguna	Series de tiempo	Más Tiempo, FIFO
	CAMARA_DE_FUMIGACIÓN	1	1	Ninguna	Series de tiempo	Más Tiempo
	BANDA1	INFINITE	1	Ninguna	Series de tiempo	Más Tiempo, FIFO
	BANDA2	INFINITE	1	Ninguna	Series de tiempo	Más Tiempo, FIFO

Figura 7. Locaciones del modelo propuesto – modelo base.
Elaboración propia

Como con las mejoras realizadas no se agrega un proceso adicional en el empacado del banano, es decir, las entidades del modelo propuesto se conservan como en el modelo base, por esta razón no fue necesario crear nuevas entidades, sin embargo, se agrega un recurso adicional que será el Auxiliar de inventario, persona encargada de hacer la lectura del código de barras, como se aprecia a continuación.

Recursos

Icono	Nombre	nidade:	TMs...	Estadist	Especif. ...
	CAMION	1	Ninguna	Por Unidad, $	Red1, N1
	AUXILIAR_DE_INVENTARIO	3	Ninguna	Por Unidad, $	Red1, N3, Rtn

Figura 8. Recursos del modelo propuesto.

Elaboración propia

Luego de implementar las mejoras propuestas en el modelo base se decide correr la simulación, teniendo en cuenta el mismo tiempo de operación, es decir, los 6 días de trabajo (48 horas que es el reloj de la simulación) para poder comparar respecto al modelo base.

RESULTADOS

Con base a la visita realizada a la finca Kalamary en el Urabá, Antioqueño, se pudo hacer una simulación base elaborada en el software PROMODEL, esta simulación representa la realidad en cuanto al proceso de empaque debido a que arroja los resultados reales en cuanto a la capacidad de producción en 48 horas de operación, que corresponden al reloj de la simulación.

TABLA 1.

RESULTADOS DE LA SIMULACIÓN BASE

ENTIDAD	CANTIDAD/DÍA
RACIMOS	1728
CAJA	864
PALET	18

El reloj de la simulación corresponde a 6 días de trabajo en jornadas de 8 horas cada día, obteniendo los siguientes resultados en la simulación base.

Dichos resultados se pueden apreciar mejor en la siguiente imagen, que corresponde a una toma de pantalla al finalizar la simulación.

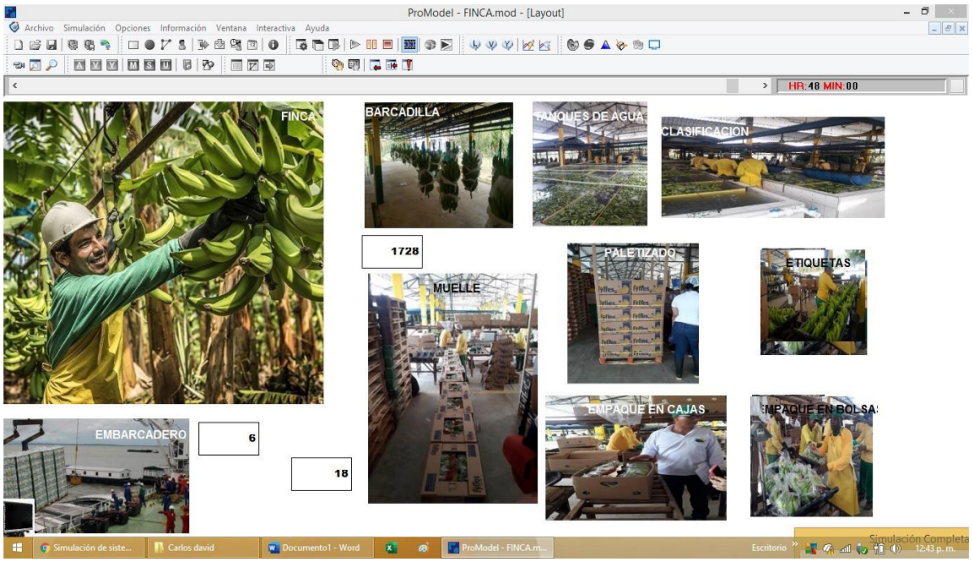


Figura 9. Modelo de la operación en la finca Kalamary – modelo base.

Elaboración propia

Estos resultados corresponden a un día de operación en la finca, cabe resaltar que los 18 palets que se generan al finalizar el día son enviados en un camión carpado cuya capacidad corresponde precisamente a la misma cantidad de palets. De esta forma podemos inferir que:

- 2 racimos conforman una caja
- 48 cajas conforman un palet
- 18 palets conforman un viaje

Con las mejoras realizadas se ejecuta el nuevo modelo, teniendo en cuenta las especificaciones de cada mejora propuesta como se explicó anteriormente, obteniendo los siguientes resultados:

TABLA 2.
RESULTADOS DE LA SIMULACIÓN CON MEJORAS

ENTIDAD	CANTIDAD/DÍA
RACIMOS	2592
CAJA	1296
PALET	27

Este resultado corresponde a un día de operación en la finca, teniendo en cuenta que las condiciones iniciales se mantienen, es decir, 2 racimos conforman una caja y 48 cajas conforman un pallet, como muestra la imagen 7 ahora se van a producir 27 palets en la operación de un día.

DISCUSIÓN

Como resultados del modelo base estamos cumpliendo con los valores preliminares obtenidos del trabajo de campo y que se pueden apreciar en la imagen 6, si hacemos lectura de los contadores ubicados en las áreas de barcadilla, muelle y embarcadero.

Los valores arrojados en el modelo base cumple con los datos de producción de 6 días de trabajo (reloj de la simulación) lo que evidencia que el modelo base representa la realidad, por lo que no se considera necesario hacer un análisis estadístico para hacer una validación del mismo.

Los resultados obtenidos de las dos simulaciones muestran un aumento en la producción de la simulación con las mejoras implementadas respecto a la simulación base, este aumento se ve reflejado en un beneficio económico que impacte directamente en la utilidad de la operación del empaque de banano en la finca kalamary, así se trae un balance del mes de Agosto de 2014, con los resultados obtenidos en las dos simulaciones, podremos evidenciar la utilidad actual y la utilidad esperada con las mejoras aplicadas.

TABLA 3.
UTILIDAD DE LA FINCA KALAMARY CON LA PRODUCCIÓN ACTUAL.

Mes	Días	cajas x día	Costo de producción x unidad	Precio de venta x unidad	Destino: España
junio	1	864	$ 17.600	$ 50.000	
Mes	**Días**	**Cajas x mes**	**Costo de producción x mes**	**Total de ventas x mes**	**Utilidad**
junio	24	20736	$ 364.953.600	$ 1.036.800.000	$ 671.846.400

Teniendo en cuenta los costos por unidad y el precio de venta, se hace el mismo ejercicio con los datos que arroja la simulación con las mejoras propuestas, así:

TABLA 4.
UTILIDAD DE LA FINCA KALAMARY CON LA PRODUCCIÓN DE LA SIMULACIÓN PROPUESTA.

Mes	Días	cajas x día	Costo de producción x unidad	Precio de venta x unidad	Destino: España
junio	1	1296	$ 17.600	$ 50.000	
Mes	**Días**	**Cajas x mes**	**Costo de producción x mes**	**Total, de ventas x mes**	**Utilidad**
junio	24	31104	$ 547.430.400	$ 1.555.200.000	$ 1.007.769.600

Se puede apreciar que la finca Kalamary con la implementación de las mejoras obtiene una utilidad de $1.007.769.600, muy significativo teniendo en cuenta que para el ejercicio del mes de agosto obtuvieron $671.846.400.

CONCLUSIONES

Luego de la visita a la finca Kalmary se puede resaltar la importancia que tiene la ingeniera industrial en la región, debido a que en dicha visita se pudo identificar diferentes procesos bastante relacionados con la carrera como lo son, la producción, logística, optimización de tiempo, implementación de nuevos métodos, seguridad en el trabajo, inventarios etc...

Después de realizar las simulaciones en el software PROMODEL, se concluye que las diferencias entre las dos muestran un gran aumento en la capacidad de la planta, se puede pasar de una producción de 18 pallets en 8 horas de trabajo a una producción de 27 pallets en las mismas 8 horas de trabajo, lo que significa un aumento del 50% de la producción.

Las mejoras implican una redistribución del personal operativo de la finca, debido a que en las operaciones de transporte de la fruta, control de inventarios y aplicación de químicos se requiere menos mano de obra para realizar las actividades propias de esas áreas mientras que en las áreas de empaques y paletizado hubo aumento en la mano de obra debido a que la simulación nos muestra que fue necesario empacar más cajas para producir la cantidad de pallets esperada, por lo que las mejoras no tiene un impacto social significativo, debido a que no se generó desempleo y no hubo resistencia a los cambios propuestos porque los operarios están capacitados para realizar cualquiera de las labores operativas de la finca.

Como recomendaciones, se sugiere que estas empresas productoras de banano puedan mejorar los procesos por medio de la optimización de tiempo, automatización de procesos, aumentar la capacidad, etc; con el fin de conseguir nuevos clientes y poder aumentar su utilidad y ofrecer un producto de mayor calidad.

AGRADECIMIENTOS

Corporación universitaria Americana sede Medellín, quien fue la institución patrocinadora de la pasantía experiencia Golfo de Urabá. A los administradores de la finca Kalamary, por el acompañamiento en el proceso de la investigación.

REFERENCIAS

[1] Sectorial Grupo Inercia Valor, «Récord en Producción de Banano en Colombia,» 2014.

[2] O. R. R. G. L. P. P. H. M. B. y. L. V. V. Bernardino Candelaria Martínez, «Application of simulation models in agricultural research and planning, a review,» Tropical and subtropical agroecosystems, vol. 14, 2011.

[3] H. G. R. L. E. C. B. Eduardo García Dunna, «Simulación y análisis de sistemas con Promodel,» PEARSON, Monterrey, 2006.

[4] G. Salazar, «Tips en cosecha y postcosecha de banano» 2013.

[5] D. A. C. D. Lilia Teresa Bermúdez Correa, «Hacia el uso de la simulación como herramienta para el análisis de proyectos de inversión» 2011.

[6]A. E. A. G. E. I. C. Rosa Imelda Garcia Chi, «Uso de la herramienta de software promodel como estrategia didáctica en el aprendizaje basado en competencias de simulación de procesos y servicios,» TECTZAPIC, vol. 1, 2015.

[7]C. SA, 2015. [En línea]. Disponible en: https://web.constructecsa.com/pagina.php?c=65.

Recibido: May. 14, 2021 | Aceptado: Nov. 03, 2021

Importancia de la alimentación animal en el sector agroindustrial

Importance of animal feed in the agro-industrial sector

DOI: https://doi.org/10.21803/ingecana.2.2.401

César Augusto Quintero Serna[1]

[1]Ingeniero Químico. Especialista en Alta Gerencia con Énfasis en Calidad. Magister en Administración. Corporación Universitaria Americana.
Correo Electrónico: cquintero@americana.edu.co

Resumen

El proceso productivo de los alimentos balanceados para animales, hace parte de una cadena de actividades que van desde la producción e importación de las materias primas hasta los resultados de la explotación animal. En Colombia la manufactura de alimentos balanceados para animales ha crecido a niveles que superan la producción promedio de la Industria manufacturera y que hacen del sector agroindustrial uno de los más influyentes en la economía del país. Con el crecimiento de la agroindustria se espera cumplir los requerimientos de alimentación humana en el territorio nacional que son insuficientes para lograr una población bien nutrida. Con un enfoque mundial sobre producción más limpia, las políticas de control ambiental, y el uso de la biomasa como fuente de alimentación alternativa a la convencional; la Industria de alimentos balanceados es una de las mejores alternativas de inversión que permiten aprovechar los subproductos de molinerías de arroz, de maíz, subproductos de los ingenios de azúcar como la melaza, el afrecho de cebada y levadura en las cervecerías, la carne, cuero, sebo, pre mezclas vísceras, harinas de sangre, plumas y huesos de los subproductos animales. Todos aquellos subproductos o residuos del proceso industrial que impactan el entorno de manera negativa. El poder disponer de estos subproductos para la alimentación animal, ayuda a mejorar el impacto ambiental y a darle una valoración a un residuo del cual se desconocían sus propiedades, y que hoy día se vende a precios razonables para ser usados de manera productiva en la alimentación animal.

Palabras clave: Subproducto; Nutrición; Biomasa; Manufactura.

Abstract

The production process of animal feed is part of a chain of activities ranging from the production and importation of raw materials to the results of animal exploitation. In Colombia, the manufacture of animal feed has grown to levels that exceed the average production of the manufacturing industry and make the agro-industrial sector one of the most influential in the country's economy. With the growth of the agroindustry, it is expected to meet the human food requirements in the national territory, which are insufficient to achieve a well-nourished population. With a global focus on cleaner production, environmental control policies, and the use of biomass as an alternative food source to the conventional one; the balanced feed industry is one of the best investment alternatives that allow taking advantage of the by-products of rice mills, corn mills, sugar mill by-products such as molasses, barley bran and yeast in breweries, meat, leather, tallow, pre-mixed viscera, blood meal, feathers and bones of animal by-products. All those by-products or residues of the industrial process impact the environment in a negative way. The availability of these by-products for animal feed helps to improve the environmental impact and to give a value to a waste whose properties were unknown, and that today is sold at reasonable prices to be used productively in animal feed.

Keywords: *By-product, Nutrition, Biomass, Manufacturing.*

Introducción

En Colombia la producción de alimentos para animales hace parte de una economía de empresas tipo oligopolio, debido a que la participación en el mercado se concentra en muy pocas empresas que son especializadas en esta producción a través del uso de negocios de economías de escala, desarrollo de infraestructuras, mejoras logísticas, tecnología de punta, innovación, desarrollo de nuevos productos, implementación tecnológica en laboratorios etc. La mayoría de los cereales utilizados en la industria agropecuaria son importados, debido a su valor comercial en el mercado mundial, entre los cuales tenemos el maíz, la soya y sus subproductos, el sorgo, el trigo; también se cuentan con productos más especializados como los aminoácidos sintéticos, la hemoglobina, los subproductos de origen animal como las harinas de carne y de pescado; todo ello requiere tener una gran infraestructura en el manejo de puertos, buques, comercio exterior, logísticas de transporte y de almacenamiento al interior del país que garantice un rendimiento en el manejo de las materias primas, efectividad de las negociaciones en la bolsa de valores a través de los commodities, manejo en el cambio de la tasa representativa de la moneda de origen (TRM), garantizando la mejor negociación que pueda dar rentabilidad al negocio.

La demanda en Colombia de los alimentos balanceados para animales la determinan las familias en el consumo de alimentos para mascotas, y los consumidores que hacen parte de la explotación animal, que son intermediarios entre los productores de alimentos balanceados y el consumidor final de leche, huevos, carne etc [1].

La entidad gubernamental que regula el sector agropecuario en Colombia es el ICA “Instituto Colombiano Agropecuario”, quienes a través de la resolución 1056 de 1996 y las PBFA, establece las directrices para el manejo adecuado en las plantas productoras relacionadas con los alimentos balanceados para animales. De allí se resalta la participación del Químico Farmacéutico, Ingeniero de Alimentos, Zootecnista e Ingeniero Industrial y otros profesionales involucrados en temas de negociación de las materias primas, producción, comercialización, nutrición, que hacen parte del proceso industrial en las principales empresas de alimentos concentrados y en los negocios relacionados como empresas de aceites, de caña de azúcar, despojo de ganado entre otros; para todos ellos, se ha decidido escribir este libro de conocimiento general de tipo académico aplicable en la industria de alimentos balanceados para animales, que sirva de herramienta de control para la toma de decisiones basadas en la experiencia y en estudios serios aplicados en el sector agropecuario; y de esta forma poder aportar al crecimiento del campo Colombiano y la alimentación humana.

MATERIALES Y MÉTODOS

Anteriormente los molinos harineros impulsados por agua de los arroyos, molían cereales destinados para el consumo humano; de esta forma se generaban residuos que se disponían en terrenos alejados, en ríos, o simplemente se quemaban en lugares cercanos a

las fábricas, ya que en aquel entonces no se tenía una regulación estricta en el control ambiental. Se desconocía del uso de muchos subproductos como la semilla de algodón, cascarilla de soya y cascarilla de café que solo se utilizan como abono. La industria, entendiendo el poder nutricional de los subproductos, empezó a utilizarlos de manera potencial en las formulaciones de los alimentos balanceados. Sin embargo, el papel del nutricionista era usar aquellos ingredientes de fácil consecución cuyo costo fuera manejable en términos de conservación, transporte, disponibilidad y resultados beneficiosos en la formulación de alimentos para animales. Entre los valores nutricionales a tener en cuenta en los desperdicios estaban las vitaminas, minerales, grasas, fibras y proteínas para la producción de leche, huevo, carne de diferentes especies [2].

Con el tiempo el sector agropecuario se fue desarrollando de manera más tecnificada, consolidándose de esta forma la base para la masificación en la producción de la alimentación animal. A continuación se resaltan los aspectos más relevantes:

- Se establecen las garantías en valores nutricionales de alimentos para las diferentes líneas de producción y comenzando en el sector avícola.

- Se desarrolla de manera técnica el análisis proximal discriminando los alimentos en humedad, proteína, grasa, fibra y cenizas, dándole un enfoque más objetivo a la formulación de los alimentos balanceados para animales.

- Se crean alimentos especializados a partir de premezclas y aditivos aplicados a la Edad y Función del animal, tanto para el ganado y la avicultura; por ejemplo, para el caso de los caballos se requería un alimento específico en energía para suplir el requerimiento que éste tenía en el transporte de carga para la época.

- Las integraciones entre las empresas productoras de alimentos balanceados y las empresas explotadoras de animales en el sector avícola o lechero, migrando hacia las zonas que permitan disminuir costos en transporte de los alimentos. De esta manera comienza a ser un reto importante las alternativas logísticas en las compañías.

- La creación de tecnologías que hacían más eficientes los procesos, a través de equipos de producción de economía de escala que permitía bajar el costo de los concentrados. Entre estas tecnologías tenemos: los molinos de martillos, procesos de la pre molienda y la post molienda, las mezcladoras con capacidad de 3 a 8 toneladas/hora, equipos especializados en la recepción de las materias primas, paletizadoras automáticas con sistemas de acondicionamiento más eficientes, sistemas de extrusión para alimentos para mascotas, alimentos flotantes para peces, adición de líquidos por peso y no por volumen mejorando su precisión, generador de vapor instantáneo. Con la implementación tecnológica y la automatización en estos procesos durante los años setenta y ochenta, se logran bajar costos por mano de obra.

- La construcción de plantas especiales para elaboración de premezclas, producción de peces, laboratorios especializados en bromatología, y microbiología.

- La evolución de algunos subproductos como: harina de semilla de algodón en Estados Unidos, gluten de maíz, residuos grasos y desperdicios de carne que antes se usaban como fertilizantes. La mezcla de melaza con alimentos balanceados, las

harinas de linaza y de alfalfa para ganado, la harina de hueso para pollos y cerdos, el suero de leche y las harinas de pescado para cerdos en la etapa de pre iniciación, la torta de soya como fuente principal de proteína, la urea como fuente sintética para rumiantes, la grasa animal como fuente importante de energía, la harina de plumas por su alta digestibilidad, los aminoácidos sintéticos, los pigmentos, los Inhibidores de hongos, los saborizantes, y los preservantes entre otros.

- Aportes desde la industria química en síntesis de la urea, de las vitaminas, del ácido fólico, de los antibióticos y los promotores de crecimiento, en la metionina como aminoácido sintético, y los antioxidantes para las grasas.

PLANTA DE ALIMENTOS BALANCEADOS PARA ANIMALES

Factibilidad

El primer paso para la construcción de una planta para alimentos balanceados para animales es tener en cuenta el nivel de factibilidad de la planta. Para ello se debe hacer los siguientes estudios:

Estudio de mercadeo

La actividad de mercadeo y ventas se inicia con el conocimiento del mercado, sus necesidades, deseos y temores, presentes en los diferentes segmentos productivos. A partir de ello se genera el portafolio de productos que respondan a los requerimientos de la genética moderna. Los planes de alimentación se diseñan y adaptan de forma flexible a los diferentes nichos, tanto para explotaciones tecnificadas como semi tecnificadas. Esto genera gamas de productos a los que se asignan precios diferenciales según sus costos de materia prima, fabricación, empaque y operación. Además, se tiene en cuenta la posición competitiva de la compañía y las posibilidades que ofrece el mercado para manejar la rentabilidad a favor de la empresa, dentro de un marco de excelente relación costo beneficio para el cliente. De otro lado se define la estructura de canales de distribución que permita acercar el producto al cliente de la forma más rápida, eficiente y eficaz. Los procesos de comunicación que apoyan todos estos procesos se dividen en publicitarios, promocionales y de fuerza de ventas. Por último, se debe apoyar el desarrollo empresarial de los clientes, mediante el servicio de asesoría técnica por parte de la empresa, y que, además, pueda monitorear el desempeño de los productos en campo, retroalimentando y permitiéndo se mantener a la vanguardia en nutrición animal. Otros procesos como la programación de ventas, el estudio de créditos, la atención de quejas y reclamos, son realizados dentro del engranaje de la operación [3].

Entre los aspectos relevantes a incluir en este estudio está:

- Se debe incluir el mercado meta que se quiere atender como: la explotación avícola, porcícola, ganadera, piscícola, equinos, caninos, cunicultura o cualquier otra línea sobre la cual se quiere trabajar en la planta.

- Definir el sistema de abastecimiento tanto de materias primas como la distribución del producto terminado, verificando su cercanía a sectores agroindustriales como molinos, trilladoras, Ingenios, mataderos, o granjas que bajen costos por la logística y que represente una sinergia tanto para la empresa como para el cliente.

- Obtener información relevante de la población, como su cultura en la región, nivel demográfico, nivel de empleo, grado de escolaridad, o cualquier información

que sea importante para caracterizar al cliente que hará parte de la empresa.

- Definir los requerimientos del cliente en la zona, de acuerdo al tipo de suelo, al clima, al mercado, a la logística de transporte, a los requerimientos técnicos de la explotación específica etc. Todo este análisis conlleva a vender la solución a un problema que se traduce en beneficios para el negocio del cliente, generando de esta forma fidelidad y confianza con la compañía y que al final se traduce en nuevas ventas.

- Establecer los canales de distribución: Distribuidoras, clientes directos o autoconsumo y los mecanismos de acercamiento a dichos canales.

- Estudiar el precio de la competencia y el volumen de participación en el mercado que se pretende alcanzar y los mecanismos de participación, que pueden ser a través de un modelo agresivo para quitar participación o hacer parte de un modelo participativo en un mercado desabastecido.

- Definir el factor diferenciador de la compañía que puede ser por calidad, precio, asistencia técnica, velocidad de respuesta, reconocimiento de marca; todo ello para entrar a competir en el mercado del sector agropecuario.

Estudio de localización

Establecer la mejor ubicación que disminuya costos para la compañía y garantiza abastecimiento de materias primas y de producto terminado a los clientes. Es definir si se quiere estar cerca a los puertos, para disminuir costo de fletes por transporte de las materias primas y tener disponibilidad inmediata de las mismas; o cerca a los clientes para atender el mercado meta de manera inmediata. Evaluar los tipos de vías de acceso, para adquirir las materias primas y/o ventas de producto terminado; las cuales pueden ser vías férreas, carreteras, ríos, vías marítimas o por aire. Análisis de los servicios públicos, como agua, energía, tipo de combustible a utilizar para la producción del vapor en la planta, cuyas alternativas pueden ser: carbón, ACPM, gas o electricidad; y evaluar la facilidad de adquisición de estas fuentes de energía para evitar desabastecimiento y a su vez paros por falta de combustible. Evaluar velocidad de respuesta de la comunidad para prestar atención a desastres en casos de emergencias o siniestros y definir los sistemas de comunicación como internet, celulares, teléfonos fijos que permitan conectividad con el cliente, los proveedores, el personal de la empresa, autoridades, la comunidad en general e incluso el cliente [4].

Estudio técnico

Definir el tipo de infraestructura que se desea obtener, que puede ser la construcción de una planta nueva, o adecuación de una planta existente que esté en proceso de venta. Definir el área del terreno, teniendo en cuenta la posibilidad de expansión en caso de crecimiento en volumen de ventas con miras hacia el futuro. Establecer el tiempo máximo del proyecto para comenzar a producir, hacer el análisis de costo beneficio, definir si se va a utilizar tecnología de punta con equipos nuevos o se van a rescatar equipos que han estado en uso; seleccionar el personal a laborar en la construcción de la obra. Implementar los sistemas de información apropiados, aplicar los requerimientos gubernamentales para la selección del personal a trabajar en la zona y el cumplimiento de todos los aspectos legales con las entidades gubernamentales, como el ICA, la DIAN, el ministerio de justicia y del interior, para el control de sustancias químicas controladas por estupefacientes, el registro de la cámara de comercio ante los organismos del estado, permisos

para la construcción ante planeación municipal o departamental etc.

Estudio financiero

Hacer análisis de cuál sería la inversión, y su retorno de acuerdo a los costos presupuestados. En cuanto tiempo sería dicho retorno a la inversión y como su financiación, cuál sería el valor económico agregado de este proyecto, y si es viable o no financieramente. Implementar y hacer seguimiento a Indicadores financieros que permitan evaluar la viabilidad del proyecto. Estos indicadores pueden ser:

- Valor presente neto (VPN)
- Tasa interna de retorno (TIR)
- Período de recuperación de capital (PRC)
- Rentabilidad contable media (RCM)
- Índice de rentabilidad (IR)
- Valor económico agregado (EVA)
- Beneficio anual uniforme equivalente (BAUE)
- Costo anual uniforme equivalente (CAUE)

Diseño de la planta

Se deben conocer las materias primas a usar dentro de la formulación para adecuar los equipos, tolvas, silos, y bodegas de almacenamiento que requieran una infraestructura especial; como el caso de la melaza que requiere ser almacenada aproximadamente a 3 metros por debajo del piso para garantizar su descarga por gravedad, o las especificaciones de los tanques metálicos con control de temperatura para almacenamiento de sebo o aceite de palma. Diseñar la logística de recibo de las materias primas, las cuales pueden ser mediante sistema de rastrillo o descarga por plataforma volcadora. Se debe tener conocimiento de las cantidades en toneladas proyectadas de los materiales a almacenar para el diseño de los tanques, de las tolvas, de la capacidad hora de la peletizadora, del molino y la mezcladora para evitar errores por el sobre dimensionamiento o sub dimensionamiento en el proyecto [5].

Es importante conocer la promesa de venta al cliente y los requerimientos de entes de regulación gubernamentales como el ICA o secretaría de salud para la garantía de calidad del producto que permita diseñar el proceso para cumplir con los parámetros de control establecidos.

La planta debe estar diseñada de tal forma que tenga la posibilidad de expandirse en el tiempo sin parar el proceso productivo, y poder crecer de manera escalonada a medida que el mercado lo demande. Esto quiere decir que debe ser flexible a la hora de incrementar su capacidad instalada en todos los ámbitos del proyecto sin generar traumas.

Se debe contar con el plan maestro que administre y controle la capacidad de procesamiento, almacenamiento, los diagramas de flujo, planos, distribuciones de instalaciones y equipos, la descripción del proceso productivo, costos de mano de obra, equipos y materiales para que sea conocido por los líderes de los procesos y poderlos hacer partícipes de las mejoras en los detalles del proceso de implementación [6].

Proceso de operación

El proceso de operación de las empresas de concentrados para animales, comienza desde la negociación de las materias primas hasta la satisfacción del cliente final en su proceso de explotación animal. Durante este proceso de

operación se tendrán en cuenta cada una de las etapas que allí participan como son Recepción de Materias Primas, Almacenamiento de Materias Primas, Proceso de Dosificación, Proceso de Molienda, Proceso de Mezclado, Proceso de Peletizado, Proceso de Extrusión.

RESULTADOS

De acuerdo al análisis anterior vemos como en Colombia, aún existen empresas pequeñas, que aún fabrican sus alimentos balanceados para animales de una manera muy rústica, sin tener en cuenta todas las variables que afectan su producción, poniendo en riesgo la salud de los animales, y con niveles de producción ineficientes e ineficaces. Es por ello que es importante producir los alimentos balanceados para animales de una manera técnica que le permita rentabilidad tanto al productor del alimento como a la industria de Explotación Animal. Hay una necesidad grande en Colombia en los pequeños productores en términos de tecnificar su conocimiento para que se mantengan en el mercado de una manera competitiva.

DISCUSIÓN

Hoy en Colombia las grandes empresas del sector agropecuario hacen parte de un oligopolio que hace que su participación en el mercado sea casi de un 60%-70% en la venta de alimentos balanceados, y así su nivel de crecimiento y participación en el mercado cada vez es mayor. Es por ello que se requiere apoyar a los pequeños productores de alimentos balanceados con conocimiento, con infraestructura y recursos para que se mantengan y poder tener un equilibrio económico en este sector [7].

CONCLUSIONES

1. Las Empresas de Alimentos Balanceados para Animales tienen un impacto económico importante en el PIB del país.

2. Hoy en día se requieren profesionales con alto conocimiento en Nutrición Animal, procesos productivos, logísticos, uso eficiente de materias primas, que permitan hacer más eficientes el sector agropecuario.

3. Si bien el sector agropecuario en lo que tiene que ver con la producción de la alimentación animal está concentrado en unas pocas empresas. Son muchas las empresas relacionadas en el sector que deben ser impactadas en términos de inocuidad, tecnología, conocimiento que le ayuden a mejorar sus procesos productivos.

4. Hoy en día la alimentación animal va de la mano de la alimentación humana. Una cosa no puede coexistir sin otra, ya que el primer eslabón de la alimentación humana es la alimentación animal, para tratar de cumplir con los requerimientos mínimos necesarios de alimentar a la sociedad.

REFERENCIAS

1] J.O.L. King. Introducción a la zootecnia. Editorial Acribia, Zaragoza España, 1981.

[2] W. H. Peters. Ganadería productiva, Editorial Hispanoamericana, México, 1947.

[3] M.E. Ensminger. Zootecnia general., B. Aires, Editorial El Ateneo, 1973.

[4] L. A. Maynard. Nutrición animal. 7ed. México. Editorial Mc Graw Hill, 1988.

[5] W.G. Pond. Fundamentos de nutrición y alimentación de los animales. 2ed. México. Editorial Uthea Wiley, 2002.

[6] W. Bechtel. The effect of the crust on the staling of bread. Oxford. Editorial Academic Press, 1953.

[7] S. Herbert. Sensory evaluation practices. City California. Editorial Academic Press 1985.

Recibido: Dic. 13, 2021 | Aceptado: Mar. 22, 2022

Redes sociales: atracción y riesgo para jóvenes

Social networks: attraction and risk for young people

DOI: https://doi.org/10.21803/ingecana.2.2.403

Yeiler Alberto Quintero Barco[1]

[1] Especialista en Seguridad de la Información. Fundación Universitaria María Cano, yeileralbertoquinterobarco@fumc.edu.co.

Resumen

En la presente investigación aplicada, se digitaliza la toma de asistencia, mejorando la eficacia y eficiencia de dicha toma, mediante el uso de dispositivos biométricos conectados a una base de datos soportada en una plataforma diseñada específicamente para dicha tarea brindando una herramienta adecuada de control y consulta, tanto para docentes, como estudiantes y demás miembros del cuerpo académico competentes para acceder a la información que se almacena automáticamente y en tiempo real, al reportar la asistencia en el lector de huella dactilar ubicado en el lugar de la asesoría definido por el personal encargado. Este proyecto mejoró la calidad en el proceso de toma de datos de asistencia a las asesorías de los proyectos integradores por parte del docente a los alumnos, los que deberían ocupar un lugar asignado según días y horas correspondientes. Con la presente investigación aplicada, se logró facilitar el registro mediante lectores de huellas digitales, implementados y soportados sobre tecnología innovadora, adecuadamente programada para tal finalidad, brindar un índice superior de confianza en cuanto a la veracidad de la información ingresada y en el momento de consulta, ya que es muy difícil falsificar una huella digital esto daría un grado mayor de confianza en la información.

Palabras clave: Procesos de capacitación; Servicio postventa; Implementación; estandarización.

Abstract

In the present applied research, the attendance taking was digitized, improving the effectiveness and efficiency of said taking, through the use of biometric devices connected to a database supported on a platform specifically designed for said task, providing an adequate control tool and consultation, both for teachers, students and other members of the competent academic body to access the information that is stored automatically and in real time, when reporting attendance in the fingerprint reader located in the place of counseling defined by the staff in charge. This project improved the quality of the data collection process of assistance to the consultancies of the integrative projects by the teacher to the students, who should occupy an assigned place according to the corresponding days and hours. With the present applied research, it was possible to facilitate registration through fingerprint readers, implemented and supported on innovative technology, properly programmed for this purpose, providing a higher level of confidence in terms of the veracity of the information entered and at the time of registration. consultation, since it is very difficult to falsify a fingerprint, this would give a greater degree of confidence in the information.

Keywords: *training processes, after-sales service, implementation, standardization.*

Introducción

Las redes sociales son plataformas creadas para hacer relaciones y contactar personas que ya conocíamos o para entablar nuevas relaciones, es nuestro deber garantizar y preservar la integridad de los adolescentes en internet, esto solo se logra generando una Cibercultura que permita que cada uno de ellos tome conciencia y empiece a entender el gran riesgo que se corre al hacer cualquier tipo de publicación de manera desmedida o entablar relación con cualquier tipo de personas, también el entregar información confidencial a alguien simplemente porque nos generó un alto grado de confianza.

Las redes sociales son plataformas de comunicación e interacción con mucha fuerza en nuestros jóvenes ya que permiten manejar todo tipo de información ya sea Video, Imágenes, Audios, Texto, donde ellos pueden subir y ver todo este tipo de información, todo esto hace de las redes sociales un lugar muy atractivo para ellos.

En este documento se tiene un marco teórico donde se sustenta nuestro trabajo, se habla sobre los delitos y riesgos que actualmente se encuentran en las redes sociales, presentando información de algunos delitos que han venido tomando fuerza en Colombia y el Mundo, se toman algunos casos reales para dar a conocer por qué debemos darle suma importancia al uso de las redes sociales, luego se plantea una discusión entre los riesgos y delitos de tal manera que podamos analizar el impacto y al final se dan posibles soluciones que busquen mitigar el riesgo de materialización de dichos delitos y conclusiones de del problema.

MATERIALES Y MÉTODOS

Hoy en día se ha venido dando un gran salto a nivel de comunicación e interacción entre personas, se da un notable cambio en las formas de relacionarnos. Los jóvenes de estos tiempos ya no buscan realizar encuentros en parques, Bibliotecas, Centros comerciales, etc. Sino que ahora se utiliza como entorno de encuentro la Web. Actualmente existen diversos tipos de redes sociales, cada una de ellas especializada en un área de interés particular, en el caso de YouTube, esta se especializa en la publicación de Videos, Instagram es especializada en el manejo y publicación de imágenes y fotografías, pero existe Facebook que permite entablar relaciones más cálidas por ser una red especializada en el manejo de relaciones interpersonales, se piensa que en la actualidad son más de Mil Millones de usuarios que utilizan esta red social como medio de comunicación e interacción interpersonal, “La Hipótesis del Cerebro Social” de Dunbar dice que la relación observada entre el tamaño relativo del neocórtex y el tamaño de los grupos sociales se debe a la necesidad de mantener la compleja estructura de relaciones que posibilita la coexistencia estable de los grupos [1], dicha hipótesis al parecer se confirma desde los estudios neurobiológicos que se han realizado. Lo que indica que las redes sociales son estructuras naturales a la forma de ser del hombre, ya que dicho entorno nos permite desarrollar las necesidades que buscamos como seres sociales.

Las redes sociales son “comunidades virtuales”. Es decir, plataformas de Internet que

agrupan a personas que se relacionan entre sí y comparten información e intereses comunes. Este es justamente su principal objetivo: entablar contactos con gente, ya sea para reencontrarse con antiguos vínculos o para generar nuevas amistades. Pertenecer a una red social, le permite al usuario construir un grupo de contactos, que puede exhibir como su "lista de amigos". Estos amigos pueden ser amigos personales que él conoce, o amigos de amigos. A veces, también, son contactos que se conocieron por Internet.

El primer antecedente de red social se remonta a 1995, cuando un ex estudiante universitario de los Estados Unidos creó una red social en Internet, a la que llamó classmates.com (compañeros de clase.com), justamente para mantener el contacto con sus antiguos compañeros de estudio. Pero recién dos años más tarde, en 1997, cuando aparece SixDegrees.com (seis grados.com) se genera en realidad el primer sitio de redes sociales, tal y como lo conocemos hoy, que permite crear perfiles de usuarios y listas de "amigos".

A comienzos del año 2000, especialmente entre el 2001 y el 2002, aparecen los primeros sitios Web que promueven el armado de redes basados en círculos de amigos en línea. Este era precisamente el nombre que se utilizaba para describir a las relaciones sociales en las comunidades virtuales. Estos círculos se popularizaron en el 2003, con la llegada de redes sociales específicas, que se ofrecían ya no sólo para reencontrarse con amigos o crear nuevas amistades, sino como espacios de intereses afines.

Al año 2009, más de 850 millones de personas en todo el mundo, estaban en alguna Red Social. ¿Cómo se distribuyen los usuarios entre las diferentes redes? Las dos más populares, como dijimos, atraen a la gran mayoría: Facebook: 400 millones, en la Argentina existen más de 7 millones de usuarios de Facebook, MySpace: 274 millones, Twitter: 105 millones, hi5: 80 millones, Tagged.com: 70 millones, Orkut: 67 millones, Linkedin: 43 millones, Flickr: 32 millones, Fotolog: 20 millones, Sónico: 17 millones, DevianART: 9 millones.

La mayoría de quienes están en alguna red social son jóvenes. El 80 por ciento de los usuarios de redes sociales en todo el mundo, tiene entre 12 y 30 años. Y la frecuencia de uso entre los adolescentes (12 a 19) es muy alta: El 50% de los Jóvenes visita la red día por medio, El 30% de los Jóvenes visita la red a diario, El 20% de los Jóvenes visita la red una vez por semana [2].

El uso de las redes sociales ha permitido que los jóvenes desarrollen relaciones más cálidas con otras personas, lo que los lleva a tener confianza al sentirse en su zona de confort, generando así un aumento en las posibilidades de ser afectado a través del uso de técnicas de ingeniería social que lo llevarían a entregar información que podrían utilizar en su contra.

En los últimos años por el gran crecimiento y uso tecnológico ha aumentado la aplicación y uso de estas para desarrollar los delitos informáticos como un modo de actuación delincuencial en contra de los jóvenes, siendo estos la población más vulnerable dentro del ciberespacio.

Los delitos informáticos vienen siendo utilizados para utilizar delitos normales en contra de la población joven, entre estos tenemos chantaje, fraude, hurto y acoso sexual entre otros. En Colombia debido a este tipo de delitos se decidió incluir modificaciones en el código penal donde se penalicen estas conductas ilícitas realizadas a través de medios tecnológicos. La forma como se generan los delitos, el entorno utilizado y la población objeto de ataques, hacen muy difícil detectar a los ciberdelincuentes, lo que hace que aumenten este tipo de delitos.

Según datos estadísticos suministrados por el Sistema de Información, Estadístico, Delincuencial

y Contravencional de la Policía Nacional deja entrever que los delitos informáticos que afectaron a los niños, niñas y adolescentes han presentado un incremento considerable especialmente las amenazas, que en lo corrido del presente año se han reportado 17 casos comparado con el mismo período del año anterior que no se presentaron denuncias por este delitos, seguido la extorsión y el hurto de información.

Los delitos que han cobrado fuerza en contra de los jóvenes son el ciberacoso o cyberbullying que es el uso de información electrónica y medios de comunicación que está contenida en el correo electrónico, redes sociales, blogs, mensajería instantánea, mensajes de texto, teléfonos móviles y websites, para acosar, intimidar o amedrentar a una persona con comentarios difamatorios, degradantes y agresivos. También está el Grooming, considerada como una nueva forma de acoso y abuso hacia jóvenes mediante redes sociales y grupos de chat donde el atacante le hace creer a su víctima que es alguien de su misma edad y gustos para después lograr la confianza de la víctima y así poder lanzar su ataque con un nivel de efectividad alto, a estos se les suma el Sexting que no es más que promocionarse a través de imágenes en ropa interior o mostrando sus atributos con el fin de conseguir la mirada de todos, con esto terminan siendo objeto de ataques por parte de los Ciberdelincuentes.

Estudios de la Policía Nacional de Colombia muestran que el comportamiento que optan por tomar los jóvenes víctimas de estos ataques nos permiten tener la posibilidad de identificar y detectar a una víctima de estos delitos. Los jóvenes víctimas tienden a presentar agresividad con las personas con las que se relacionan en su entorno, pierden el interés por navegar en la web, se encierran dejando de ser sociables, sufren de estrés y duermen poco [3].

El uso de sitios web de medios sociales es una de las actividades más comunes de los niños y adolescentes de hoy en día. Cualquier sitio web que permite la interacción social se considera un sitio de redes sociales, incluyendo los sitios de redes sociales como Facebook, MySpace y Twitter; sitios de juegos y mundos virtuales, como Club Penguin, Second Life, y los Sims; sitios de video como YouTube; y blogs. Tales sitios ofrecen a los jóvenes de hoy un portal para el entretenimiento y la comunicación y han crecido exponencialmente en los últimos años. Por esta razón, es importante que los padres sean conscientes de la naturaleza de los sitios de medios sociales, teniendo en cuenta que no todos ellos son ambientes saludables para los niños y adolescentes. Los pediatras están en una posición única para ayudar a las familias a entender estos sitios y para fomentar el uso saludable y urge a los padres para supervisar los posibles problemas con el acoso cibernético, "Facebook depresión," sexting, y la exposición a contenido inapropiado [4].

Delitos

Grooming

Es aquella "situación de extorsión, que se produce on line entre un individuo a un niño, para que, bajo amenazas o coacciones, éste acceda a sus peticiones de connotación sexual principalmente, y que usualmente tienen lugar mediante la utilización de una webcam o, a través del programa de chat del ordenador, llegando incluso a concertar acuerdos para materializar el abuso [5].

Ciberacoso o Ciberbullying

Es el uso y difusión de información lesiva o difamatoria en formato electrónico a través de medios de comunicación como el correo electrónico, la mensajería instantánea, las redes sociales, la mensajería de texto a través de teléfonos o dispositivos móviles o la publicación de vídeos y fotografías en plataformas electrónicas de difusión de contenidos [5].

Sexting

El Sexting es un abuso mediante TIC que incluye un elemento sexual, cosa que se hace ya evidente en el nombre que proviene de una unión entre sex (sexo) y texting (comunicación mediante mensajes de texto o SMS). [5]

Sextorsion

Es una forma de explotación sexual en la cual una persona es chantajeada con una imagen o vídeo de sí misma desnuda o realizando actos sexuales, que generalmente ha sido previamente compartida mediante sexting. La víctima es coaccionada para tener relaciones sexuales con alguien, entregar más imágenes eróticas o pornográficas, dinero o alguna otra contrapartida, bajo la amenaza de difundir las imágenes originales si no accede a las exigencias del chantajista.

Phishing

Suplantación de identidad es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Pornografía Infantil

Es toda aquella representación visual y real de un menor desarrollando actividades sexuales explícitas; esto es, en donde aparezca contacto sexual (incluyendo el genital-genital, oral-genital, anal-genital u oral-anal entre menores o un adulto y un menor), brutalidad, masturbación, desarrollo de conductas sádicas o masoquistas o exhibición lasciva de los genitales o el área púbica de un infante [5].

Casos reales

Se suicida joven canadiense de 17 años por violación y acoso cibernético por un grupo de jóvenes.

Rehtaeh Parsons, una joven de Cole Harbour, una pequeña localidad a unos mil 800 kilómetros al este de Toronto, murió por las heridas que sufrió al intentar suicidarse el 4 de marzo.

La familia de Parsons denunció que la joven fue violada cuando tenía 15 años por un grupo de 4 jóvenes. Pocos días después del ataque, alguien empezó a distribuir por Internet una foto de la violación entre sus compañeros de colegio.

La policía nunca presentó cargos contra los jóvenes por falta de pruebas, pero Parsons sufrió un constante acoso cibernético, desde proposiciones de relaciones sexuales con desconocidos hasta insultos, lo que la obligó a cambiar de colegio y la sumió en una profunda depresión [6].

Delincuentes asesinan a joven contactada por Facebook

A principios de septiembre, Ana María Chávez se contactó con dos hombres por la red social Facebook. Por varios días, los sujetos entablaron múltiples conversaciones con la joven, situación que le generó confianza a Ana María, quien aceptó luego de un tiempo verse con ellos. A mediados del mismo mes, la joven fue vista por los dos hombres en Quinta Paredes. Testigos cuentan que la vieron ingresar a un apartamento con dos personas, pero luego los vieron salir del lugar sin la compañía de Chávez.

Según investigaciones de la Sijín, se trata de una organización dedicada a contactar personas por Facebook para luego citarlos y efectuar robos [7].

Niña de 12 fue violada por un “amigo” de las redes sociales

Una niña de 12 años fue abusada brutalmente por un hombre a quien conoció a través de las redes sociales. De acuerdo a los datos, la víctima y el depravado, se habían conocido hace unas semanas y se encontraron en tres oportunidades, en las dos primeras solo hablaron, pero en la tercera la niña fue abusada sexualmente por el degenerado que ya se encuentra con orden de captura.

El depravado ganó la confianza de la niña y la volvió a invitar por tercera vez el 21 de agosto pasado con la excusa de tomar unos helados juntos, la menor accedió a la invitación y el joven fue a buscarla a bordo de una motocicleta, pero no la llevó precisamente a una heladería, sino que a un reservado.

Allí empezó a seducirla y ante la negativa de la víctima, la forzó a sacarse la ropa y la violó brutalmente [8].

Una niña de 10 años creó un exitoso grupo en Facebook para humillar a una compañera de clase, Romina Perrone, estudiante de 10 años en un colegio bonaerense, tuvo que sufrir que una compañera de clase crease un grupo en Facebook dando razones para odiarla. Llegó a sumar más de cinco mil fans y pese a los esfuerzos de la madre de Romina, Facebook se negaba a eliminarlo [9].

La acosaron hasta provocar su muerte (e incluso después) Nueve adolescentes (siete de ellos, chicas) fueron juzgados en 2010 por acosar y maltratar física, psicológicamente y a través de móviles y de Internet a una compañera de escuela, inmigrante irlandesa. Phoebe Prince, de 15 años, fue acosada, humillada y agredida durante tres meses por algunos compañeros del instituto hasta que no pudo aguantarlo más y se suicidó ahorcándose. El acoso, de hecho, siguió online tras su muerte. El grupo de adolescentes que se sentaba en el banquillo la insultaba a voces en los pasillos del colegio, en la biblioteca, en la cafetería o en el camino de vuelta a casa. La llamaban día tras día puta irlandesa y zorra, la empujaban, le tiraban cosas, le quitaban los libros de la mano y le mandaban mensajes de SMS con amenazas [10].

DISCUSIÓN

Las redes sociales son definitivamente excelentes plataformas, que van con la metodología de este mundo cambiante y lleno de atracciones, permitiéndonos acortar brechas y establecer relaciones que conducen a la creación de nuevas ideas de negocios, trabajos colaborativos, implementación de nuevas soluciones empresariales, el problema o más bien el punto a tener en cuenta es el uso, es ahí donde se está fallando ya que no se le está dando el uso apropiado debido a que se están usando todas las bondades ofrecidas ahí para darles un uso inapropiado el cual está generando todo tipo de malas experiencias e infortunios que han logrado materializar todo tipo de delitos, delitos que afectan profundamente a la población joven.

Cada uno de los delitos que se materializan a través de las redes sociales tiene un componente particular que debe ser analizado por nosotros para poder detectar cada acción que nos pueda llevar a la materialización de estos, así podemos estar con un pie adelante y poder prevenir a nuestros jóvenes de dichos ataques.

Al hacer un análisis de la situación que se presenta con el uso que los jóvenes le están dando a las redes sociales y ver la cantidad de delitos que día a día se materializan se ve la necesidad de generar estrategias que busquen mitigar el alto riesgo que se corre por parte de los jóvenes en las redes sociales, siendo este un mundo lleno de oportunidades de crecimiento. Las atracciones que traen consigo las redes sociales han permitido que estas se conviertan en el entorno donde converge

la delincuencia, esto les ha permitido tener un mayor nivel de acceso a las personas a través de su información, información que está siendo publicada sin control ni prevención alguna.

De acuerdo a lo estudiado se proponen algunas soluciones que ayudarían a mitigar dicho riesgo, entre estas tenemos las siguientes:

Se deben realizar jornadas de sensibilización a padres y jóvenes que permitan que estos entiendan la importancia de hacer un uso controlado y adecuado de dicho espacio, para evitar incurrir en conductas inapropiadas o ser víctima de algún tipo de delito.

Generar estrategias informativas que permitan que los jóvenes puedan realizar denuncias sin que se sientan amenazados o en riesgo de sufrir algún tipo de daño, nuestro deber es preservar la integridad de nuestra población joven.

Generar políticas y controles que busquen la judicialización de muchas conductas inadecuadas en las redes sociales.

Establecer controles con el manejo de información por parte de los jóvenes en las redes sociales, de tal manera que se mitigue el riesgo de caer en manos de los ciberdelincuentes.

Hoy en día es muy fácil crear una cibercultura que permita mantener un nivel de uso sano en las redes sociales.

CONCLUSIONES

Por parte de nuestros jóvenes, es nuestro deber lograr conseguir que ellos entiendan que cada acción que realizan mediante la web les afectará en su vida futura, ya sea para bien o para mal. Si logramos que de cada 10 jóvenes que usan las redes sociales 1 entienda la importancia de hacer un buen uso podremos lograr rápido el cambio que nos llevara a una cibercultura de buen uso en la web

En estos tiempos es muy común encontrarnos con jóvenes que manejan poca interacción con las personas de su núcleo familiar, llevándolos a ser personas solas, con poco sentido social, introvertidos, esto es un punto al que no se le está prestando la atención requerida ya que no hemos visualizado sus consecuencias futuras.

Las redes sociales nos presentan un futuro con muchos beneficios, pero con la posibilidad de encontrarnos con un entorno oscuro lleno de peligros, donde los ciberdelincuentes estarán acechando a esos jóvenes desprevenidos y confiados que usan la red de forma indebida.

Es fundamental incluir y contar con los padres en el proceso de sensibilización y generación de una cibercultura sana y apropiada para tener jóvenes educados en un mundo lleno de sorpresas. Hay algunos aspectos que están generando conflictos en nuestros jóvenes al usar las redes sociales entre estos podemos mencionar el mal uso que se le está dando a las redes sociales, donde los jóvenes la están utilizando como el trampolín de su popularidad; tenemos también el abuso y este tiene que ver con el tiempo que nuestros jóvenes permanecen conectados en la red, estas están sobrepasando el tiempo en que deberían estar conectados y están publicando información sensible de su vida y por último la adicción, nuestros jóvenes están sintiendo que deben permanecer conectados y al no tener la posibilidad de estar conectados esto les genera un caos al no poder conectarse a continuar con una rutina virtual que han venido generando a través de los días, esta adicción puede terminar ligada con otro tipo de problemas.

REFERENCIAS

[1] D. Reig y L. Vilchez, Los jóvenes en la era de Hiperconectividad, Madrid: Albadalejo, 2013.

[2] Ministerio de Educación Argentina, Los Adolescentes y las Redes Sociales, Buenos Aires: Escuela y Medios, 2010.

[3] G. Y. Liliana, «Delitos Informáticos,» Observatorio del Delito, p. 3, 2013.

[4] A. A. o. Pediatrics, «Informe clínico-El impacto de los medios sociales en los niños, adolescentes y familias,» Ame- rican Academy of Pediatrics, pp. 800-804, 2011.

[5] A. C. Padilla, «EL NUEVO DELITO DE GROOMING DEL ARTÍCULO 183 BIS DEL CÓDIGO PENAL,» 2014.

[6] Agencias, «http://www.zocalo.com.mx,» 2013. [En línea]. Available: http://www.zocalo.com.mx/seccion/articu-lo/protestas-en-canada-tras-suicidio-de-joven-que-fue-ciberacosada-1365702858.

[7] E. espectador, «http://www.elespectador.com,» 2009. [En línea]. Available: http://www.elespectador.com/noti-cias/bogota/articulo169551-delincuentes-asesinan-joven-contactada-facebook.

[8] D. Jornada, «http://diariolajornada.com,» 2014. [En línea]. Available: http://diariolajornada.com.py/v6/nina-de-12-fue-violada-por-un-amigo-de-las-redes-sociales.

[9] Ciberbullying, «https://ciberbullying.wordpress.com,» 2010. [En línea]. Available: https://ciberbullying.wor- dpress.com/2010/06/10/argentina-vigilara-el-ciberbullying-discriminatorio-en-las-redes-sociales-de-inter- net/.

[10] E. Mundo, «Ciberconvivencia,» 2010. [En línea]. Available: https://ciberconvivencia.wordpress.com/2010/04/07/ comienza-el-juicio-contra-los-acosadores-de-phoebe-prince-la-joven-inmigrante-que-se-ahorco-en-los-ee- uu/.

Recibido: May. 19, 2021 | Aceptado: Oct. 22, 2021

SDN el futuro de las comunicaciones

SDN The Future of Communications

DOI: https://doi.org/10.21803/ingecana.2.2.404

Yeiler Alberto Quintero Barco[1]

[1]Especialista en Seguridad de la Información. Fundación Universitaria María Cano, yeileralbertoquinterobarco@fumc.edu.co.

Resumen

Las Redes definidas por software (SDN) es una tecnología que permite el diseño y la administración de las redes de una forma dinámica. Aunque esta tecnología tiene el concepto de ser nueva en este mundo de la tecnología, si se puede afirmar que el SDN tiene una larga historia de esfuerzos para hacer que las redes de ordenadores pudieran llegar al punto de ser programables. Por tal motivo, este artículo, tiene como finalidad hablar sobre la historia que ha enmarcado el SDN y mirar cual es el futuro de la misma con respecto a las grandes empresas donde se maneja grandes flujos de datos más comúnmente llamados data centers, por último, se hace una pequeña discusión de los temas abordados al inicio de este artículo.

Palabras clave: SDN; Comunicaciones; Tendencias; Redes de datos.

Abstract

Software Defined Networking (SDN) is an exciting technology that enables the design and management of networks in a dynamic way. Although this technology has the concept of being new in this world of technology, it can be stated that SDN has a long history of efforts to make computer networks to the point of being programmable. For this reason, this article aims to talk about the history that has framed the SDN and look at what is the future of it with respect to large enterprises where large data flows are handled more commonly called data centers, finally, a small discussion of the issues addressed at the beginning of this article is made.

Keywords: *SDN, Communications, Trends, Data networks.*

Introducción

Hoy en día las organizaciones buscan tecnologías y arquitecturas que les permitan manejar una infraestructura de red con su constante crecimiento y que a su vez está conectada con las marcadas tendencias en materia tecnológica, SDN se ha convertido en una tecnología que permitirá realizar manejo de grandes volúmenes de datos con altos estándares de calidad, lo cual genera gran expectativa y mucho interés por parte de las organizaciones, permitiendo así cumplir con las estrategias de comunicación planteadas al interior de cada organización.

La llegada de nuevas tecnologías y aplicaciones se convierten en un factor que genera un aumento significativo del tráfico y del volumen de información que transita en la red, teniendo en cuenta que así también aumenta la necesidad de dar soporte a esa información, contando con grandes servidores, estos con mayor capacidad de almacenamiento y procesamiento de la información, esto quiere decir, que si se tiene un crecimiento en la red, definitivamente los elementos y todo lo que esté en su entorno también crecerá.

En el presente artículo se hace un análisis de las redes SDN y el futuro que tiene dicha tecnología en las comunicaciones de hoy en día. Este artículo cuenta con las siguientes secciones: un marco teórico que reúne información pertinente para dar soporte a la discusión y análisis que se planteará más adelante, una sección de discusión y análisis que busca plantear la importancia de dicha tecnología y finalmente unas conclusiones sobre la importancia de dicha tecnología.

MATERIALES Y MÉTODOS

El nacimiento de las aplicaciones en tiempo real, el video streaming; la masificación de las redes sociales, la introducción del cloud computing y muchos otros servicios, han dado como resultado el crecimiento exponencial del tráfico que circula por la red. A pesar de ello, se continúan utilizando las mismas tecnologías que hace cincuenta años y los avances en cuanto a nuevas formas de comunicación y tratamiento de la información son casi inexistentes. Se ha intentado cubrir cada necesidad con la creación de protocolos, que dicho sea de paso toman mucho tiempo en ser estandarizados. Si bien se ha dado una solución temporal a todos los requerimientos que demanda el mercado, ésta no representa una solución global al verdadero problema, la carencia de métodos de comunicación más eficientes. En consecuencia se plantea la necesidad de cambiar la forma de comunicación de las redes, en la cual se le proporcione mayor inteligencia a la misma [1]. Cada vez más se ven involucradas las nuevas tecnologías y aplicaciones que permiten que el entorno evolucione de manera notable, esto marca el gran crecimiento de flujo de información en la red, lo que obliga a mejorar la infraestructura de red que se tiene en las organizaciones.

Sin embargo, el mercado de telecomunicaciones y tecnología de la información está pasando por un momento de gran transformación. El crecimiento explosivo del uso de dispositivos móviles y de las redes sociales, la adopción cada vez más frecuente de computación en nube y, en un futuro próximo, el uso masivo de sensores inteligentes en los más variados dispositivos, conectando prácticamente cualquier cosa a la red (creando la llamada "Internet de las Cosas" o IoT ("Internet of Everything"), han proporcionado nuevas oportunidades de negocios. Sin embargo, al mismo tiempo, ha traído enormes desafíos a los profesionales de telecomunicaciones y tecnología de información. Así, y entre los principales desafíos, está la modernización de las redes de telecomunicaciones [2]. Los desafíos a los que se enfrentan los profesionales de telecomunicaciones van directamente asociado al crecimiento de las redes, que a su vez se da por el uso masivo y aparición de nuevas tecnologías.

Las redes de telecomunicación en su evolución han operado a través de dispositivos intermedios que transportan datos desde un origen hasta un destino. Cada dispositivo de red es independiente y visualiza la red a partir de mensajes enviados y recibidos en sus interfaces interconectadas, su simplicidad de operación ha permitido el desarrollo y expansión de las redes de datos e internet, sin embargo, la funcionalidad es cerrada, osificada y depende de los aportes que realicen los fabricantes y los desarrollos de los estándares internacionales. A partir de las problemáticas aprendidas con las redes tradicionales y la necesidad de plataformas que soporten nuevos servicios surgen esfuerzos para dar impulso a la evolución de las telecomunicaciones, estas tecnologías de nueva generación buscan usar características tales como virtualización, ingeniería de tráfico, control de acceso, procesamiento intermedio, aislamiento, seguridad entre otros para apoyar servicios emergentes como lo son la computación en la nube y los sistemas distribuidos [3].

Las arquitecturas tradicionales están teniendo complicaciones a la hora de satisfacer todos los requerimientos de las empresas, carriers y los usuarios finales. En ese contexto, SDN (Software Define Network) se presenta como un estándar para cubrir estas necesidades y promete una transformación completa de las arquitecturas de red como conocemos en la actualidad. Software Define Network (SDN) es una arquitectura de red emergente, donde el control es desacoplado de la función forwarding y permite ser programable. Esta migración del plano de control permite abstraer a las aplicaciones y los servicios de la red de la infraestructura base, permitiendo que éstos manejen la red como una identidad lógica o virtual [4].

Las redes de computadoras suelen ser construidas a partir de un gran número de dispositivos de red tales como routers, switches y numerosos tipos de dispositivos intermedios (middleboxes) (es decir, dispositivos que manipulan el tráfico para fines distintos de reenvío de paquetes, tales como un firewall) con muchos protocolos complejos implementados en ellos. Los operadores de red son responsables de la configuración de políticas para responder a una amplia gama de eventos de red y aplicaciones, tienen que transformar manualmente estos-políticas a nivel alto en comandos de configuración de bajo nivel mientras se adapta a las condiciones cambiantes de la red y a menudo necesitan para llevar a cabo estas tareas muy complejas con acceso a herramientas muy limitadas. Como resultado, la gestión de la red y la optimización del rendimiento es bastante difícil y por lo tanto, propensa a errores. El hecho de que los dispositivos de red son cajas negras habitualmente integradas verticalmente exacerba el desafío que operadores y administradores de red se enfrentan. Otro reto casi insuperable al

que profesionales e investigadores de la red se enfrentan ha sido referido como “la osificación de Internet”. Debido a su enorme base de despliegue y el hecho de que se considera parte de la infraestructura crítica de nuestra sociedad (al igual que el transporte y las redes de energía), Internet se ha convertido en extremadamente difícil para evolucionar tanto en términos de su infraestructura física, así como sus protocolos y el rendimiento. Sin embargo, como las aplicaciones y servicios de Internet actuales y emergentes se vuelven cada vez más complejos y exigentes, es imperativo que Internet sea capaz de evolucionar para hacer frente a estos nuevos retos [5].

Las redes de nueva generación, NGN, actualmente son punto de convergencia de tecnologías que por muchos años han ofrecido servicios de telecomunicaciones y se han propagado por el mundo. Redes que fueron pensadas para perdurar en el tiempo e imponerse como estándares, hoy son poco usadas, tal es el caso deX.25, ATM, Frame Relay, entre otras. Un motor preponderante en la innovación y futuro de las redes de telecomunicaciones son las universidades y grupos líderes en investigación. Ellos están explorando nuevas estrategias para hacer las LAN y WAN del mañana más fáciles de manejar, más seguras y potentes, capaces de operar sobre diferentes tecnologías bajo el concepto de convergencia y buscando cambiar el modo de controlarlas; una de estas nuevas formas son las ya nombradas SDN [6].

DISCUSIÓN

Con los grandes avances en materia de comunicaciones es importante comenzar a estudiar las nuevas tendencias que buscan mejorar el reenvío de información y el manejo del flujo de información al interior de las redes, pensar en SDN y todo lo que trae para este mundo en materia de comunicaciones es un gran acierto ya que, con la separación de los planos de control y de datos permite tener redes autónomas al permitir poder desarrollar aplicaciones que ayuden a mejorar su administración.

Así pues, el poder ofrecer una red centralizada, programable y que se pueda administrar dinámicamente con el fin de responder a las necesidades cambiantes de las empresas, puede generar aspectos positivos en función de la red centralizada como lo es la programación directa, la administración centralizada, la reducción del CapEx, la reducción del OpEx, el entrego ágil y flexible de la información y algo que es muy importante para la organización el cual es la adaptación de la innovación en la organización.

Dicho de otra manera, para los data centers es de suma importancia contar con los nuevos desarrollos y aplicaciones que trae consigo la tecnología SDN permitiendo mejorar su rendimiento a través de desarrollo de aplicaciones que busquen mejorar el flujo de datos al interior de la red, mediante políticas y configuraciones que ayudan incluso a reducir el consumo de energía en los data centers.

Todo esto tendrá una mejor evolución en la manera en que la industria se complementa con la academia, a través de investigaciones lideradas por los grupos de investigación y sus semilleros, pensando desde ahí en la manera como se desea que esta tecnología evolucione para hacer del tráfico de datos en la red una operación más eficiente, esto mediante el desarrollo de aplicaciones que busquen optimizar el uso de las redes y sus dispositivos de internetworking.

Cabe resaltar que con el crecimiento de la red todo lo que esté asociado a esta, definitivamente también crecerá, es por eso que desde ya se debe pensar en cómo evolucionar de la mejor manera, esto sin generar problemas en el rendimiento de la red.

Definitivamente factores como la virtualización de servidores, la necesidad que presentan las organizaciones para adaptarse a los constantes cambios del negocio, el hecho de que los usuarios requieran acceder a su información y servicio desde cualquier lugar ponen a las SDN en un plano de suma importancia para que evolucionen las redes y estas se adapten a las tendencias marcadas que presenta el mundo en materia de comunicación hoy en día.

Las SDN surgen como una tecnología que busca introducir la virtualización de redes de una manera eficiente, permitiendo que se programe el plano de control centralizando dicho proceso y dándole mejor manejo al flujo de datos, esto debido a la separación de los planos de control y de datos.

CONCLUSIONES

Las SDN hacen parte de las innovaciones en materia de tecnologías, pero estas están siendo adoptadas de manera muy lenta por parte de las organizaciones debido a que es una tecnología muy nueva en el mundo de las comunicaciones, a esto se le suma que aún hay pocas instituciones realizando investigaciones en este campo lo que genera cierto desconocimiento a pesar de que ya grandes empresas decidieron crear la ONF (open network foundation) y a través de esta se vienen adelantando múltiples trabajos de investigación que ayudarán a incorporar dicha tecnología de manera más eficiente en las organizaciones. Las instituciones universitarias deben comenzar a desarrollar investigaciones en materia de SDN que ayuden a mejorar las aplicaciones que dicha tecnología trae consigo.

Se debe pensar en la migración hacia las SDN como un proceso normal a pesar de que esto se tome algún tiempo para que los proveedores y usuarios se adapten a dicha tecnología debido a que es una tecnología muy nueva y todo cambio tiende a generar caos, esto nos pone a pensar en el proceso de sensibilización para lograr que dicha adopción se convierta en un proceso menos traumático para los involucrados.

REFERENCIAS

[1]L. I. B. López, PROPUESTA DE ESCENARIOS VIRTUALES CON LA HERRAMIENTA VNX PARA PRUEBAS DEL PROTOCOLO OPENFLOW, Madrid, 2013.

[2]J. N. L. P. F. H. D. D. C. S. Luís Minoru Shibata, «Cómo el nuevo universo trazado por las redes definidas por software impactará en los negocios,» Advisor, pp. 1-16, 2014.

[3]H. R. J. Leonardo, «INFORME GUÍA TEÓRICO-PRÁCTICA SOBRE REDES DEFINIDAS POR SOFTWARE PARA LA UNIVERSIDAD TECNOLÓGICA DE PEREIRA,» UNIVERSIDAD TECNOLÓGICA DE PEREIRA, Pereira, 2015.

[4]C. Spera, «Software Defined Network: el futuro de las arquitecturas de red» Logicalis Now, pp. 42-45, 2013.

[5]M. M. X.-N. N. K. O. y. T. T. Bruno Astuto A. Nunes, «A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks,» HAL, pp. 1-17, 2014.

[6]B. G. D. Felipe, « Openflow: El protocolo del futuro» pp. 61-72, 2013.

Recibido: Ago. 4, 2021 | Aceptado: Ene. 10, 2022

Seguridad a nivel de enlace de datos en el modelo de interconexión de sistemas abiertos (OSI)

Security at the data link level in the Open Systems Interconnection Model (OSI)

DOI: https://doi.org/10.21803/ingecana.2.2.405

Christian Obando I[1], Martín Vásquez V[2]

[1] Ingeniero en electrónica y telecomunicaciones y especialista en seguridad informática hasta 2015. E-mail: chrisobib@gmail.com. [2] Ingeniero informatico

Resumen

Las redes de comunicaciones pueden llegar a prestar una innumerable cantidad de servicios en una organización que van a permitir satisfacer las necesidades más importantes de ésta, ayudándola con el cumplimiento de sus objetivos organizacionales con mayor eficiencia, sin embargo, la falta de implementación de seguridad de la información en sus dispositivos informáticos, puede causar una gran desventaja para dichos objetivos. La capa dos del modelo OSI se considera una de las más importantes en el flujo de la información ya que de ella prácticamente parte la comunicación con el resto de las capas de este modelo, por lo que se ve la necesidad de estudiar los ataques informáticos a esta capa e implementar técnicas que permitan mejorar la seguridad en dicha capa.

Palabras clave: Seguridad informática; Modelos de referencia, Protocolos, Redes, Dispositivos de red; Medios de transmisión.

Abstract

Communications networks can provide an innumerable amount of services in an organization that will allow it to satisfy its most important needs, helping it to fulfill its organizational objectives more efficiently.
in their computing devices can cause a great disadvantage for these objectives. Layer two of the OSI model is considered one of the most important in the flow of information, since it is practically the starting point for communication with the rest of the layers of this model, so there is a need to study computer attacks on this layer and implement techniques to improve security in this layer.

Keywords: *Computer Security, Reference Models, Protocols, Networks, Network Devices, Transmission Media.*

Introducción

Los sistemas informáticos sin importar sus características tecnológicas hardware, como por ejemplo el procesador con su capacidad de procesamiento de la información, al conectarse a una red de comunicaciones, como es el internet, es vulnerable a cualquier ataque informático ya que la forma como acceden y transmiten información en este tipo de redes no depende de esas características tecnológicas sino del medio de transmisión, y principalmente de la estructura en la cual los datos viajan de un dispositivo a otro. Esta estructura es igual para todos los dispositivos conectados y de hecho es ésta la que permite comunicar todos los dispositivos informáticos no solo localmente sino a nivel mundial. Esta estructura es conocida como el modelo de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection). Este modelo fue creado por la Organización Internacional para la Normalización (ISO, International Organization for Standardization) en 1984 para solucionar la incompatibilidad que existía entre redes a la hora de comunicarse una con otra [1]. En la figura 1 [2] se puede observar el modelo de referencia OSI.

Desafortunadamente, las siete capas que componen a este modelo han sido objeto de muchos ataques informáticos con el fin de robar información u ocasionar percances en algún servicio de la red informática.

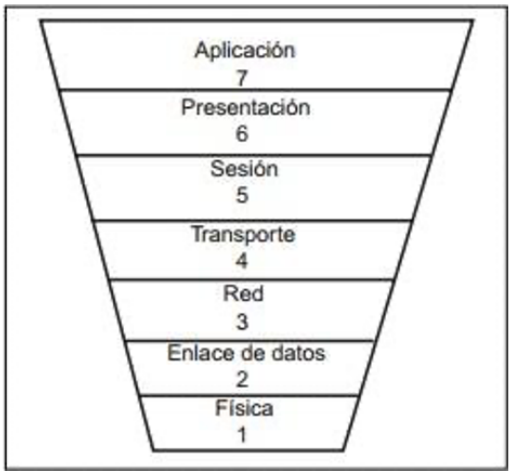


Figura 1. Modelo OSI

Este artículo es el resultado de analizar las diferentes capas del modelo OSI e identificar los ataques informáticos más relevantes que afectan a este modelo y por ende a una red de comunicaciones. El análisis detectó que la capa dos correspondiente a la de enlace de datos es una de las capas que mayor cantidad de ataques recibe por considerarse erróneamente, por algunos administradores de red, que no es importante o que no existen mecanismos de seguridad que la protejan o simplemente por falta de conocimiento de tecnologías que pueden asegurar esta capa tan importante del modelo OSI, de hecho un ataque en la capa dos podría llegar a causar el efecto dominó como se afirma en [3] el cual consiste en vulnerar esta capa y desde ella vulnerar las capas superiores que la siguen pudiendo llegar a ser catastrófico para la red de una organización.

Capa 2: Enlace de datos

Como se ha dicho con anterioridad el modelo OSI posee 7 capas, cada una de ellas cumple una determinada función en el proceso de transmisión de información desde un dispositivo origen hasta otro destino; en cada una de estas capas la información se procesa de manera diferente y tienen su propia forma de nombrar a sus unidades de datos como se indica a continuación [4]:

- Capa 1: bits
- Capa 2: tramas
- Capa 3: paquetes
- Capa 4: Segmentos
- Capa 5: SPDU (Session Protocol Data Unit)
- Capa 6: PPDU (Presentation Protocol Data Unit)
- Capa 7: APDU (Application Protocol Data Unit)

En general, en cada una de las capas la información se maneja como Unidad de Datos de Protocolo (PDU, Protocol Data Unit). Estas PDU permiten el intercambio de la información de una capa a otra, sin embargo, solo la capa homóloga será capaz de interpretar esa información, dicho de otro modo, la capa 2 de un dispositivo destino, solo puede interpretar la información que le es enviada de la capa 2 de un dispositivo origen, este tipo de comunicación es conocida como par a par [5].

Funciones de la capa 2

La tarea primordial de la capa de enlace de datos es la de corrección de errores y el control de acceso al medio. Esta capa en un dispositivo destino, hace que los bits provenientes de un dispositivo origen se transformen en tramas las cuales se transmitirán en forma secuencial hacia la siguiente capa. En sentido contrario a la comunicación, cuando los paquetes de datos llegan a la capa de enlace de datos, éstos empiezan a ubicarse en tramas, que vienen definidas por la arquitectura de red que se está utilizando (como Ethernet, Token Ring, etc.). Esta capa se encarga de desplazar los datos por el enlace físico de comunicación hasta el dispositivo destino, e identificar cada computador incluido en la red de acuerdo a su dirección física o también conocida como dirección de Control de Acceso al Medio (MAC, Media Access Control) la cual viene codificada en la Tarjeta de Interfaz de Red (NIC, Network Interface Card). La capa de enlace de datos también se asegura de que las tramas enviadas por el medio físico se recibieron sin error alguno mediante la adición de un campo en la trama llamado Chequeo de Redundancia Cíclica (CRC, Cyclical Redundancy Check), el cual básicamente es un valor que se calcula tanto en el origen como en el destino. Si los dos valores de CRC son iguales, significa que la trama se recibió correcta e íntegramente, y no recibió error alguno durante su transmisión [6].

Es también en esta capa donde se debe evitar que un transmisor muy rápido sature con datos a un receptor lento [7]. Finalmente, esta capa va a preparar los paquetes de la capa de red para ser transmitidos en el medio de transmisión.

Formato de trama de la capa 2

Como se mencionó anteriormente, el tipo de trama que se genera en la capa de enlace de datos dependerá de la tecnología de red que se está utilizando, como Ethernet, Token Ring o FDDI.

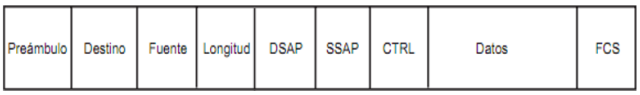


Figura 2. [7] trama Ethernet 802.2.

Preámbulo: Bits de alternación (1 y 0) que indican que se ha enviado una trama.

Destino: La dirección MAC destino

Fuente: La dirección MAC origen

Longitud: especifica el número de bytes de datos incluidos en la trama

DSAP: Punto de Acceso al Servicio de Destino (Destination Service Access Point)

SSAP: Punto de Acceso al Servicio de Origen (Source Service Access Point)

CTRL: Control Lógico de Enlace

Datos: en este segmento, la trama mantiene los datos que se han enviado o se van a enviar.

FCS: Secuencia de Comprobación de la Trama (Frame Check Sequence) el cual contiene el valor CRC de la trama. Como se puede observar, esta trama básicamente se compone de un encabezado que la describe, de los datos que la incluyen y de la información referente a la capa de enlace de datos (como los DSAP y SSAP), que no solo definen el tipo de trama que se trata (Ethernet en este caso) sino que también contribuyen a que la trama llegue a la computadora destino [2].

Dispositivos de red de la capa 2

Entre los dispositivos de red que se encuentran en la capa de enlace de datos encontramos: tarjetas de red o NIC, hub, bridge y el switch, siendo este último el objeto de estudio en este artículo ya que de todos los dispositivos presentes en esta capa, éste es el que actualmente más se utiliza en las redes de las organizaciones y por otro lado este dispositivo es el único de los cuatro que evolucionó para aprovechar sus grandes capacidades de conmutación y mejorar la velocidad de transmisión de datos de una Red Área Local (LAN, Local Area Network) a una Red de Área Amplia (WAN, Wide Area Network). Esta evolución del switch lo hace ascender a la capa de red del modelo OSI, en la cual se lo conoce como switch de capa 3 o switch multicapa y cuyas nuevas funcionalidades es la del enrutamiento entre redes [5]. En este artículo sólo se hace referencia al switch de capa 2.

Seguridad en la capa 2

Según el FBI, el 80% de los ataques informáticos provienen del interior de la organización. 99% de los puertos de las redes LAN corporativas están desprotegidos. Es decir, cualquiera puede conectarse a ellos [8].

El modelo OSI fue diseñado para que cada capa trabaje de manera independiente de las otras, su relación existe cuando una capa brinda servicios a la siguiente en jerarquía; sin embargo la capa superior no puede validar si la capa inferior fue comprometida o no. Por consiguiente, si la capa de enlace de datos es atacada, las comunicaciones se verán comprometidas sin que las otras capas se enteren del problema.

En la capa 2 los equipos son visibles unos a otros mediante una dirección física MAC. El tráfico entre equipos es administrado por un switch, el cual permite el uso de los recursos de la red de manera eficiente. El uso de switches ha creado algunos mitos, como son:

- La dirección MAC de un equipo es física por lo tanto no puede ser cambiada o falsificada.
- El switch no es vulnerable a Sniffing de tráfico.
- Las LAN Virtuales (VLAN, Virtual LAN)

están completamente aisladas unas de otras.

Ataques a la capa 2

Los ataques de capa 2 suelen requerir acceso desde el interior, ya sea un empleado o un visitante. A continuación se analizan algunos ataques a la capa de enlace de datos.

3.1.1 CAM TABLE OVERFLOW

Un switch guarda la asociación entre MAC y el puerto donde está conectado un equipo en la una tabla llamada Memoria de Contenido Direccionable (CAM, Content Addressable Memory), la cual tiene un tamaño fijo. Cuando este espacio ha sido usado en su totalidad, el switch envía a todos los puertos las tramas que tengan una dirección MAC destino no almacenada en la tabla CAM; por lo tanto, un switch se convierte en un hub para todo equipo que no esté en su tabla CAM. Si un atacante enviará hacia cualquier puerto de un switch un gran número de tramas con direcciones MAC generadas aleatoriamente hasta que se llene la tabla CAM entonces se generan problemas.

Si la tabla CAM está ll ena, no se aceptan nuevas entradas y cuando la tabla CAM no puede almacenar más asociaciones MAC-Puerto el switch empieza a enviar por todos los puertos de que dispone (Broadcast) las tramas que tengan una dirección MAC destino no almacenada en la tabla CAM. Esto es, el switch empieza a comportarse como un hub para cualquier MAC que no haya aprendido porque su tabla CAM está llena.

Esto ocasiona dos efectos adversos graves:

Un dispositivo intruso puede conectarse a cualquier puerto del switch y capturar un tráfico que normalmente no vería por ese puerto en circunstancias normales.

El tráfico saliente del switch es claramente ineficiente e innecesariamente voluminoso, lo que puede llegar a causar que se produzca un caso de Denegación de Servicios (DoS, Denial of Service).

Este ataque puede ser mitigado configurando seguridad de puertos en el switch.

Con la seguridad de puertos, el administrador puede especificar en forma estática las direcciones MAC en un puerto particular del switch o bien puede permitir que el switch aprenda en forma dinámica un número determinado de direcciones MAC por cada puerto. En general, especificar en forma estática las direcciones MAC no es una solución administrable en un ambiente de producción. Permitir que el switch aprenda en forma dinámica un número fijo de direcciones MAC es una solución administrativamente escalable.

ARP spoofing

Para que la capa 2 pueda dar servicios a capa 3 existen dos protocolos llamados Protocolo de Resolución de Direcciones (ARP, Address Resolution Protocol) y el Protocolo de Resolución de Direcciones Inverso (RARP, Reverse Address Resolution Protocol), en los cuales cada dirección MAC está asociada a una dirección de Protocolo de Internet (IP, Internet Protocol). Estas asociaciones son almacenadas en una tabla de direcciones MAC contra direcciones IP, tanto en los switches como en los dispositivos que estén conectados en una red. ARP no proporciona seguridad o algún mecanismo para reservar direcciones IP o MAC. En algunos Sistemas Operativos (SO, Operating System) inclusive las entradas ARP estáticas son sobre escritas por las solicitudes ARP.

Mediante peticiones falsas de ARP es posible falsificar cualquier dirección MAC en una red de

cómputo; por lo tanto, cualquier tráfico puede ser redireccionado a un equipo falso y esto permite realizar varios ataques:

Tipos de ataque ARP Spoofing

a) Switch Port Stealing (Sniffing):

Utilizando ARP Spoofing el atacante consigue que todas las tramas dirigidas hacia otro puerto del switch lleguen al puerto del atacante para luego enviarlos hacia su destinatario y de esta manera poder ver el tráfico que viaja desde el remitente hacia el destinatario.

b) Man in the Middle (Sniffing):

Utilizando ARP Spoofing el atacante logra que todas las tramas que intercambian las víctimas pasen primero por su equipo (Inclusive en ambientes switcheados).

c) Denial of service (DoS):

Utilizando ARP Spoofing el atacante puede hacer que un equipo crítico de la red tenga una dirección MAC inexistente. Con esto se logra que las tramas dirigidas a la IP de este dispositivo se pierdan.

d) Secuestro (Hijacking):

Utilizando ARP Spoofing el atacante puede lograr redirigir el flujo de tramas entre dos dispositivos hacia su equipo. Así puede lograr colocarse en cualquiera de los dos extremos de la comunicación y secuestrar la sesión.

Vlan hopping attack

Para que un switch administre VLANs requiere de la creación de un puerto truck que tiene acceso a todas las VLANs, este puerto se usa para transmitir tráfico de múltiples VLAN. Para la administración se usa el Protocolo de enlace Troncal Dinámico (DTP, Dynamic Trunking Protocol), el cual por defecto se encuentra configurado de manera “Automática”. El atacante puede configurar un dispositivo para que simule ser un switch y se haga pasar como tal ante otro switch permitiéndole al atacante convertirse en miembro de todas las VLAN, y por lo tanto tener acceso a servicios y/o información de toda la red.

La mejor forma de prevenir los ataques básicos de salto de VLAN consiste en deshabilitar el trunking en todos los puertos, a excepción de aquellos que lo requieran.

En los puertos donde el trunking deba estar disponible, se deben deshabilitar las negociaciones DTP y habilitar el trunking en forma manual.

Ataques A STP

El Protocolo de Árbol de Extensión (STP, Spanning Tree Protocol) permite crear topologías de red libres de bucles (forma de árbol), es decir, asegura que el tráfico broadcast no se vuelva una tormenta. Cuando un atacante logra estar conectado en dos switches, puede inundar la red con paquetes de configuración del tipo BPDU (Bridge Protocol Data Units), con lo que puede redireccionar todo el tráfico a su equipo de cómputo.

Este ataque puede ser utilizado para usurpar los tres objetivos de la seguridad: confidencialidad, integridad y disponibilidad.

Las técnicas de mitigación para la manipulación de STP incluyen la habilitación de PortFast y la utilización de root guard y BPDU guard.

Ataques de tormenta en lan

Una tormenta de LAN ocurre cuando los

paquetes inundan la LAN, creando saturación y degradando el desempeño de la red. Estas tormentas pueden ser causadas por errores en la configuración de la red, o por usuarios realizando ataques DoS. También pueden ocurrir tormentas de broadcast como se observa en la figura 8 [9].

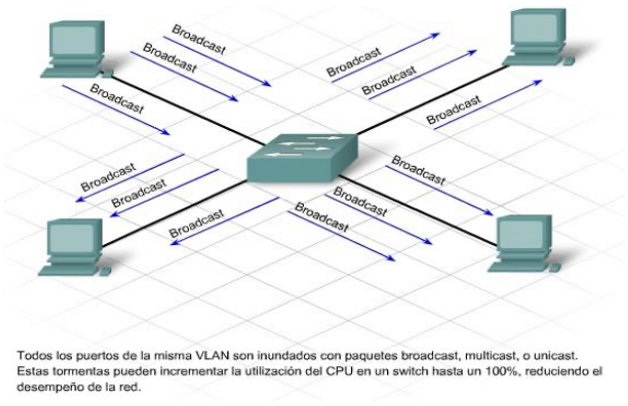


Figura 3. Tormenta LAN – broadcast.

Si bien este ataque no es posible prevenirlo en su totalidad, sí es posible mitigarlo implementando un control de tormentas. El control de tormentas previene las alteraciones en el tráfico de una LAN causadas por tormentas de broadcast, multicast o unicast provenientes de una interfaz física. El control de tormentas (o supresión de tráfico) monitorea los paquetes que pasan desde una interfaz hacia el bus de conmutación y determina si el paquete es unicast, multicast o broadcast.

El switch cuenta el número de paquetes de cada tipo específico recibidos en un cierto período de tiempo y compara estas medidas con un umbral de supresión predefinido. El control de tormentas bloquea el tráfico cuando el límite definido es alcanzado [10].

CONCLUSIONES

Los riesgos de seguridad en una red corporativa no se pueden eliminar o prevenir completamente, pero sí se pueden mitigar con una buenas políticas de seguridad de la información y haciendo uso del aseguramiento (hardening) de los dispositivos de red y servidores.

Se debe tener en cuenta que las vulnerabilidades de una red pueden ser aprovechadas por agentes externos o internos de la organización.

La seguridad de los dispositivos no es solo a nivel de red y aplicación, también hay que tener en cuenta la seguridad a nivel físico, contemplando un buen respaldo de contingencia de energía y unas buenas políticas de control de acceso hacia los lugares donde se encuentran todos los dispositivos.

El análisis de tráfico en un dispositivo consiste en “desarmar” cada trama, paquete, segmento, bloque de información y analizarlos “bit” a “bit”, aquí se esconde la razón de ser de la seguridad.

Cuando un dispositivo de red comienza a recibir información cada uno de los niveles de la pila TCP/IP comienza su tarea identificando “bit” a “bit” a qué módulo le corresponde trabajar. Un módulo no es más que un código, script o programa que tiene todas las órdenes que debe realizar en ese nivel y con esa secuencia de bits. Una vez que reúne suficiente información para identificar unívocamente a qué módulo llamar, automáticamente le pasa el control a éste y a partir de allí comienza su tarea.

Tener contingencia de los dispositivos de red y servidores, con sus respectivos respaldos de configuraciones y de información, es de vital importancia para que haya continuidad del negocio en caso de que haya un ataque de denegación de servicios.

REFERENCIAS

1]Claros Iver. Modelo OSI. Universidad Privada Cumbre. [En línea]. Disponible en: http://belarmino.galeon.com/

[2] J. Hernández. El modelo OSI y los protocols de red. (2010). [En línea]. Disponible en: http://blyx.com/public/docs/pila_OSI.pdf

[3] R. Cárdenas Gómez. Seguridad en Redes y Telecomunicaciones. (2013). [En línea]. Disponible en: http://cryptomex.org/SlidesSeguridad/SegRedesTelecom.pdf

[4]Museo de la Informática y Computación Aplicada. El modelo OSI. [En línea]. Disponible en: http://www.tecnotopia.com.mx/redes/redosi.htm

[5]Bustamante Rubén. Seguridad en Redes. Universidad Autónoma del Estado de Hidalgo. [En línea]. Disponible en: http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20 redes.pdf

[6] G. Vasquez. Redes de Comunicaciones. Universidad Autónoma de Baja California Sur. [En línea]. Disponible en: http://growitsol.com/support/UABCS/RedesI/Unidad-II-LIC.pdf

[7] IEEE. Formato de trama Ethernet. IBM. (2014). [En línea]. Disponible en: http://publib.boulder.ibm.com/html/as400/v4r5/ic2931/info/RZAJYETHERNETFRAMEFORMAT.HTM

[8] G. Arellano. Seguridad en capa 2. (2014) [en línea]. Disponible en: https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CC4QFjAA&url=http%3A%2F%2Fwww gabriel-arellano.com.

[9] A. Alex, O. Federico, O. Christian. Seguridad en Infraestructura de Red. Universidad Pontificia Bolivariana. (2014).

[10] J. Vicente. Network Time Protocol. (2013). [en línea].Disponible en: https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDAQFjAA&url=http%3A%2F%2Fwww.uv.es%2F~montanan%2Fredes%2Ftrabajos%2Fntp.doc&ei=YoxMUo6EB4-K9QS40YGwDw&usg=AFQjCNHfNtdIdW2FGd5lKia5IgFPSaCTnQ&sig2=anfq5t9aqDM5nczO3Ia2GA&bvm=bv.53371865,d. eWU&cad=rja