UNIVERSIDAD NACIONAL DEL ALTIPLANO

ESCUELA DE POSGRADO

PROGRAMA DE MAESTRÍA

MAESTRÍA EN INFORMÁTICA

TESIS

IMPLEMENTACIÓN DEL ALGORITMO WAVELET PARA LA DETECCIÓN DE ATAQUES DE LAS REDES DE COMUNICACIONES ABANCAY 2016.

PRESENTADA POR:

KARINA GAMARRA PERALTA

PARA OPTAR EL GRADO ACADÉMICO DE:

MAGISTER SCIENTIAE EN INFORMÁTICA

MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

PUNO, PERÚ

2017

UNIVERSIDAD NACIONAL DEL ALTIPLANO

ESCUELA DE POSGRADO

PROGRAMA DE MAESTRÍA

MAESTRÍA EN INFORMÁTICA

TESIS

IMPLEMENTACIÓN DEL ALGORITMO WAVELET PARA LA DETECCIÓN DE ATAQUES DE LAS REDES DE COMUNICACIONES ABANCAY 2016.

PRESENTADA POR:

KARINA GAMARRA PERALTA

PARA OPTAR EL GRADO ACADÉMICO DE:

MAGISTER SCIENTIAE EN INFORMÁTICA

MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

APROBADA POR EL SIGUIENTE JURADO:

PRESIDENTE

M.C. CONFESOR MILÁN VARGAS VALVERDE

PRIMER MIEMBRO

M.Sc. SAMUEL DONATO PÉREZ QUISPE

SEGUNDO MIEMBRO

M.Sc. FREDY HERIC VILLASANTE SARAVIA

ASESOR DE TESIS

Dr.Sc. ALEJANDRO APAZA TARQUI

Puno, 14 de Setiembre de 2017

ÁREA: Redes y comunicación de datos.
TEMA: Innovacion en las medidas de protección en redes Wireless

DEDICATORIA

A dios, por darme la vida, fe y esperanza.

A mí amada familia Sánchez Gamarra.

A Darío, Dante Edu y Anhely Letizia, quienes son la razón de mí existir, fuente de inspiración por quienes cualquier reto es posible.

A mis adorados padres, María Isabel y Eloy Guillermo, a quienes dios puso en mi camino para guiarme y así mismo son el impulso que siempre he necesitado para salir adelante.

A mis hermanos, sobrinos, abuelos, mis amistades, en especial a mi querida amiga Diana Castillo y a todos los que compartieron conmigo este sueño y muchos momentos difíciles e inolvidables.

AGRADECIMIENTOS

- Agradezco a la Universidad Nacional del Altiplano, que inicio este reto de extender sus conocimientos en la ciudad Abancay y por haberme admitidito en este programa de maestría, brindándonos todas las facilidades para alcanzar niveles educativos.
- Agradezco a los docentes y sobre todo a los miembros del jurado de este tema de investigación por realizar la transferencia tecnológica de sus conocimientos y la dedicación al presente tema de investigación.
- Agradezco al asesor de tesis quien mostro dedicación y permitió enriquecer presente trabajo de investigación.

ÍNDICE GENERAL

ÍNDICE DE CUADROS

Pág.

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE ANEXOS

RESUMEN

El presente documento; propone mejorar la seguridad en la protección de información en una red de comunicaciones, garantizando a los usuarios la óptima detección de ataques de seguridad en redes de comunicaciones, por lo que se desarrolla un algoritmo wavelet, basada en características de aprendizaje. La mayoría de los problemas de seguridad son causados intencionalmente por personas maliciosas que intentan ganar algo o hacer daño a una determinada información, representando ataques hasta lograr transgredir nuestra seguridad, por lo que es necesario proteger nuestra red de comunicaciones, tomando en cuenta el algoritmo wavelet como medida de prevención, para detectar los ataques y recuperarse de cualquier perturbación o retardo, dicha solución se denomina “Implementación del algoritmo wavelet para la detección de ataques de las redes de comunicaciones Abancay 2016”. Por lo que se identifican los tipos de ataques en redes de comunicaciones, se diseña un mecanismo de detección de ataques seguridad, implementando un prototipo de algoritmo Wavelet, entrenado con tres neuronas, para el reconocimiento de patrones de ataques por determinados puertos. Finalmente se mide el nivel de cumplimiento de estándares de gestión de seguridad ISO 27002, del cual se desprende resultados, obteniendo una red de comunicaciones cumpliendo con la gestión de seguridad de nivel 4 es decir que es medible y estable en un 80%, por lo tanto, es una red de comunicaciones más confiable, integra y disponible.

Palabras clave: Algoritmo, Ataque, Red de computadoras, Seguridad, Wavelet neuronal.

ABSTRACT

This document; proposes to improve security in the protection of information in a communications network, guaranteeing users the optimal detection of security attacks in communications networks, for which a wavelet algorithm is developed, based on learning characteristics. Most security problems are caused intentionally by malicious people who try to gain something or harm certain information, representing attacks to breach our security, so it is necessary to protect our communications network, taking into account the wavelet algorithm as a preventive measure, to detect attacks and recover from any disturbance or delay, said solution is called "Implementation of the wavelet algorithm for the detection of attacks of the Abancay 2016 communication networks". As far as the types of attacks in communications networks are identified, a security attack detection mechanism is designed, implementing a Wavelet algorithm prototype, trained with three neurons, for the recognition of attack patterns by certain ports. Finally, the level of compliance with ISO 27002 safety management standards is measured, from which results are obtained, obtaining a communications network complying with level 4 safety management, that is to say that it is measurable and stable by 80%, so Therefore, it is a more reliable, integrated and available communications network.

Keywords: Algorithm, Attack, Computer Network, Neuronal Wavelet, Security.

INTRODUCCIÓN

Según Aldea & Ruiz (1997) Shakespeare, dice: “Ser lo que soy, no es nada sin seguridad”, que propone un concepto avanzado y visionario sobre seguridad en nuestros tiempos y más aún en seguridad de redes de comunicaciones debido al auge que ha tomado por la comunicación a través de redes e internet ya sea en redes públicas o privadas, por lo que están expuestas a sufrir distintos tipos de ataques pasivos o activos, que vulneran su infraestructura, aplicando e incorporando nuevos métodos y técnicas. Aun cuando los ataques con frecuencia son iniciados desde el exterior, el aislamiento físico del segmento de red no garantiza la protección contra incidentes originados en el interior, es entonces cuando se hace necesario incorporar distintos algoritmos de protección para detectar diversos ataques y preservar la confidencialidad e integridad de la información de los usuarios. La vía para alcanzar la seguridad de la información, son los sistemas para detección de intrusos, representados a través de un algoritmo de seguridad wavelet, cuyo objetivo principal es detectar actividades no autorizadas e identificar de manera positiva ataques a una red de comunicaciones. A lo largo del desarrollo de estos sistemas se ha experimentado con distintos enfoques en su implementación, para mejorar su efectividad en la detección de ataques y adaptabilidad de conductas intrusivas. La investigación encaminada en la seguridad de la información, nos brinda nuevos prototipos de aplicación es por ello que la Implementación del algoritmo wavelet para la detección de ataques de las redes de comunicaciones Abancay 2016, pone en razonamiento la seguridad por lo que identifica los tipos de ataques en redes de comunicaciones, diseña mecanismos de detección de ataques

de seguridad en redes de comunicaciones, para implementar un prototipo de algoritmo wavelet para la detección de ataques de seguridad en redes de comunicaciones en Abancay 2016. El uso de la función wavelet busca aprovechar sus características de análisis para detectar una intromisión y reconocimiento de patrones para su clasificación y al mismo tiempo la localización que poseen la función, es decir, la forma en la que produce la salida a partir de un estímulo o entrada dado, además de indicar las restricciones en sus parámetros. Otras de las características de la implementación de un algoritmo wavelet, implica una etapa de diseño donde se establezcan las características generales, así como la deducción del algoritmo de entrenamiento wavelet a usar, que se llevara a cabo en un escenario de simulación a través del simulador aleatorio, donde se podrá obtener resultados cuantitativos y por lo tanto el desempeño que permita concluir la viabilidad de la implementación. Teniendo diversos capítulos como son: Capítulo I, que presenta el planteamiento y formulación del problema de la investigación, justificación, objetivos de la investigación e Investigación; Capítulo II, los antecedentes de la investigación y el marco conceptual; Capítulo III, la metodología usada para esta investigación; Capítulo IV, los resultados y discusión, que contemplará la capacidad de detectar ataques de seguridad en un segmento de red donde se sitúa el algoritmo de detección de ataques, cumpliendo estándares de seguridad y consiguientemente se tiene la discusión de investigación, las conclusiones y referencias.

CAPÍTULO I

PROBLEMÁTICA DE INVESTIGACIÓN

1.1 PLANTEAMIENTO DE LA INVESTIGACIÓN

La seguridad informática es un reto cada vez mayor en este mundo en el que la tecnología se ha convertido en un quehacer del día a día, creándose e incrementándose nuevos delitos informáticos y desarrollando conductas enfocadas en la obtención de información no autorizada o peor aún dirigida a causar daño en diferentes sistemas informáticos e incluso físico, destrucción de datos, creación de datos falsos, etc.

La investigación sobre la seguridad informática durante las últimas décadas se ha centrado principalmente en el aseguramiento de información, confidencialidad de los datos y la integridad de los mismo a través de algoritmos de seguridad como: criptográficos, Wavelet, de firmas digitales, de códigos de autenticación. La aplicación de estos recursos hace que los procesos informáticos garanticen mínimamente la protección de datos según normas establecidas.

Muchos y diversos ataques a la infraestructura de una red de computadoras, afectan a grandes fragmentos de la Información, a la vez que crean grandes

cantidades de perturbación de los servicios, debido a las infracciones tales como la suplantación de IP, el envenenamiento de las tablas de enrutamiento o robos de sesiones. Las operaciones diarias en todo el mundo cada vez más dependen de la disponibilidad y fiabilidad de la obtención de información a través de Internet, lo que hace a la seguridad un factor muy importante en una infraestructura de red la misma que es un problema de máxima prioridad en el campo informático.

En la actualidad existen leyes que protegen la información en el Perú, como son Ley N°30096 delitos informáticos y su modificación de la Ley N°30171, basados en el convenio de la ciberdelincuencia, realizado en la Conferencia de Ministros de los Países Iberoamericanos, firmado en Budapest.

En un análisis Bestuzhev (2015) afirma que nadie está seguro en internet: que las cifras del cibercrimen en América Latina se ha incrementado. En 250 días de análisis, una empresa de seguridad detectó 398,628,611 de intentos de ataques de virus en la región de América Latina. Cifra que se traduce a más de 20 incidentes por segundo. En Perú un 20.5% de usuarios han sufrido amenazas en línea.

Al mismo tiempo existen organismos nacionales como el Instituto Nacional de Estadística e Informática (INEI), el cual no maneja mucha información del tema debido a que la legislación es débil y los usuarios no denuncian estos incidentes, el mismo que no cuenta con información a nivel regional y menos en la ciudad de Abancay. Existiendo instituciones internacionales encargados de difundir y prevenir sobre vulnerabilidades informáticas como son: CERT (ComputerEmergency Response Team)/ CSIRT (Computer Security Incident

Response Team). Todo ello con la finalidad de protegerse contra robo o corrupción de información y mejorar el índice de detección de ataques y conductas intrusivas sobre redes de comunicación, es necesario explorar nuevos modelos que nos aproximen a una mayor seguridad de datos, modelos, sistemas y/o algoritmos, en vista que una gran cantidad de información se encuentra vulnerable y expuesto a los llamados ciberdelincuentes, quienes aplican diversos tipos de ataques para dañar los activos de información de una organización, que conllevan a una pérdida económica, cometiendo un ilícito al vulnerar las barreras de protección, dicho ilícito en nuestra realidad regional no se tiene informes estadísticos, por lo que nos queda proteger nuestra red de comunicación de estos ataques que no son considerados por los administradores de red.

1.1.1 Problema General

¿En qué medida la implementación del algoritmo Wavelet mejorará la detección de ataques de las redes de comunicaciones en Abancay 2016?

1.1.2 Problema específicos

- ¿Cuáles son los tipos de taques en redes de comunicaciones en Abancay 2016?
- ¿Qué mecanismos de detección de ataques se aplica en la seguridad de redes de comunicaciones en Abancay 2016?
- ¿Qué prototipo se implementa para atenuar los ataques de seguridad en redes de comunicaciones en Abancay 2016?
- ¿En qué medida el algoritmo wavelet cumple con estándares de seguridad de redes de comunicaciones?

1.2 JUSTIFICACIÓN

El aporte de la investigación es brindar una herramienta alternativa y confiable que garanticen una seguridad y detecte ataques de ciberdelincuentes comunes y como se aprecia en el planteamiento del problema, es la protección de los datos y la información en general de una organización, por lo que se propone como herramienta de solución el implementar un algoritmo wavelet que detecte oportunamente los ataques en redes de comunicaciones y que permitan tener una reacción oportuna frente a los diversos ataques en una red de comunicaciones vulnerable, brindando así apoyo en la administración de una red de comunicaciones. Debido a que la infinidad de ataques son cada día nuevos y variantes se tomará en cuenta ataques más comunes por medio de un análisis de wavelet y de sus funciones de morlet y sombrero mexicano, con la finalidad de generar un prototipo que se aplicable en tiempo real y lo más importante que se entrene para poder predecir un determinado ataque de seguridad en redes de comunicaciones incrementando la seguridad, con el objetivo de sensibilizar a los administradores de redes de comunicaciones y a las empresas a tomar en cuenta la información como un activo, cumpliendo con la normativa vigente en materia de seguridad, ISO 27002.

Por otro lado, cabe resaltar que el algoritmo wavelet se aplica integrándose a otras herramientas como por ejemplo a los sistemas de detección de intrusos y con esta información el algoritmo wavelet a través de las redes neuronales incrementara la seguridad, recordando que la seguridad no es al 100%, procuramos alcanzar niveles deseados de seguridad.

1.3 OBJETIVOS

1.3.1 Objetivo General

Desarrollar el algoritmo Wavelet para la detección de ataques en las redes de comunicaciones Abancay 2016.

1.3.2 Objetivos Específicos

- Identificar los tipos de ataques en redes de comunicaciones.
- Diseñar mecanismos de detección de ataques seguridad de redes de comunicaciones.
- Implementar un prototipo de algoritmo Wavelet.
- Medir el nivel de gestión de seguridad del algoritmo wavelet para la detección de ataques de las redes de comunicaciones.

1.4 HIPÓTESIS

1.4.1 Hipótesis General

El desarrollo del algoritmo wavelet detectará eficientemente los ataques en las redes de comunicaciones disminuyendo la vulnerabilidad en una red de comunicaciones.

1.4.2 Hipótesis Específicas

- Se identifica los tipos de ataques en redes de comunicaciones de Abancay 2016.
- Se diseña mecanismos de detección de ataques seguridad de redes de comunicaciones.
- Se Implementa el prototipo de algoritmo Wavelet neuronal.

- La implementación del algoritmo wavelet de redes de comunicaciones, cumple con niveles altos de gestión de seguridad.

CAPÍTULO II

MARCO TEÓRICO

2.1 ANTECEDENTES DE LA INVESTIGACIÓN

A partir de los primeros trabajos en el área de detección de intrusos según Denning (1987) se describe un modelo de un sistema experto en detección de intrusos en tiempo real capaz de detectar invasiones, penetraciones y otras formas de abuso informático. El modelo se basa en la hipótesis de infracciones de seguridad detectadas mediante el control de registros de auditoría de una red para patrones anormales. El modelo incluye perfiles para representar el comportamiento de los sujetos con respecto a los objetos en términos de métricas y modelos estadísticos y reglas para adquirir conocimiento sobre este comportamiento a partir de registros de auditoría y para detectar comportamientos anómalos. El entorno de aplicación, vulnerabilidad del sistema o tipo de intrusión, proporcionando así un marco para un sistema experto de detección de intrusos de uso general. Concluyendo que cada uno de los IDS, están basados en mecanismos distintos.

Según Ptacek & Newsham (1998) los sistemas de detección de intrusos de red se basan en un mecanismo de análisis de protocolos pasivos. Aquí el sistema de detección de intrusiones observa discretamente todos los ataques en la red, analiza patrones de actividad sospechosa, analiza protocolos y encuentra tres clases de ataques que explotan estos problemas fundamentales de inserción, evasión y Ataques de denegación de servicio y describir cómo aplicar estos tres tipos de ataques al análisis de protocolos IP y TCP. Teniendo como resultados de pruebas de la eficacia de nuestros ataques contra cuatro de los sistemas de detección de intrusos de red más populares del mercado. Se encontró que todos los sistemas de ID probados eran vulnerables a cada uno de nuestros ataques, lo que indica que los sistemas de ID de red no pueden confiar plenamente hasta que se rediseñen.

Según Bai & Kobayashi (2003) la investigación en ésta área contempla distintos enfoques como el estadístico, la generación predictiva de patrones y el uso de redes neuronales. Concluyendo que los ataques a la infraestructura de red en la actualidad son las principales amenazas contra la red y la información. Con el rápido crecimiento de las actividades no autorizadas en redes, detección de intrusos como componente de defensa en profundidad es muy necesaria porque las técnicas de firewall tradicional no pueden ofrecer una protección completa contra la intrusión. La detección de intrusos, es un área de investigación activa e importante de la seguridad de la red.

Según Botello (2010) se implementa un sistema de detección de intrusos (IDS) portable que hace uso de la base de datos de firmas de Snort, que es un sistema de detección de intrusos creado por Martin Roesch, que monitorea el tráfico dentro de un segmento de red, ofrece características como análisis y filtrado de

paquetes en tiempo real, monitoreo de puertos y análisis de protocolos, detectando intrusiones.

Según Hernacki & Bennett (2009) se describe la evasión de la red y la detección de la desinformación. Se proporcionan técnicas para la seguridad de la red, incluida la determinación de la retransmisión de un determinado paquete, segmento, marco u otro encapsulado de datos. Mediante la detección y seguimiento de retransmisiones, el paquete puede compararse con el paquete original para determinar si existe un ataque. Mediante la evaluación del flujo de datos original y una copia del flujo de datos original modificado con el paquete retransmitido, se puede detectar un intento de evasión o desinformación, invocando la coincidencia de patrón o firma para determinar si se intenta un ataque contra un host de destino.

Según Kim et al. (2015) a medida que aumenta el número de ataques basados en la red, las operaciones de red y las tareas de administración se vuelven cada vez más complejas, es importante poder proporcionar medidas de seguridad que sean eficientes tanto en términos de velocidad de procesamiento como en la detección de ataques no conocidos. Los IDS, basados en anomalías permiten la detección de ataques desconocidos, nunca vistos y efectivos. Estos dispositivos son atractivos, ya que permite que una característica de seguridad adicional se despliegue rápidamente sin agregar a la complejidad de gestión de los sistemas existentes. Se resistente al tráfico contaminado y se entrena en tiempo real. Esta característica se presta naturalmente a un despliegue más rápido ya gestionar sistemas en entornos cambiantes. Se desarrolló un prototipo físico usando una plataforma incorporada, demostrando rapidez y ser un dispositivo autónomo de seguridad física.

Según Oussar & Reyfus (2000) la inicialización original para los parámetros de las redes de wavelets feed forward, antes del entrenamiento por técnicas basadas en gradiente. Se aprovecha de los marcos wavelet procedentes de la transformada wavelet discreta y utiliza un método de selección para determinar un conjunto de mejores wavelets cuyos centros y parámetros de dilatación se utilizan como valor inicial para el entrenamiento posterior. Los resultados obtenidos para el modelado de dos procesos simulados se comparan con los obtenidos con un procedimiento de inicialización heurística y demuestran la efectividad del método propuesto en detección de ataques de redes.

Según Engel et al. (2006) los ataques en esquema cifrado ligero para datos visuales que se basan en aplicación del filtro wavelet para proporcionar seguridad. Los ataques construyen una representación simbólica de la transformada wavelet inversa. Mostramos que esta representación puede ser utilizada en ataques de texto cifrado, ataques de texto claro conocidos y en ataques en los que se dispone de cierta información sobre el texto sin formato. Investigamos el éxito y la viabilidad de cada uno de estos ataques y concluimos que el tipo de ataque plantea un problema para el esquema de cifrado ligero basado en la medición de una transformada (lineal).

Según Kukielka & Kotuslki (2008) dentro de la incorporación de redes neuronales a los sistemas de detección de intrusos se ha experimentado con distintas arquitecturas y algoritmos de aprendizaje para solucionar los problemas señalados anteriormente se han propuesto métodos que incluyen el uso del algoritmo annealing, simulado junto con algoritmos genéticos para superar el mínimo local, la aceleración del proceso de entrenamiento mediante algoritmos como Levenberg – Marquardt y gradiente conjugado.

2.2 MARCO CONCEPTUAL

2.2.1 Seguridad

La seguridad se debe entender como un camino o un proceso continuo y de la misma manera que se puede observar a un potencial delincuente por la videocamara, para ver como perpetro el robo, debe disponer de un sistema que pudiera monitorizar el tráfico de la red en caso de anomalías (Ramos et al., 2015).

2.2.1.1 La Seguridad de las comunicaciones

La seguridad en los computadores implica tres exigencias que se extienden al sistema de comunicaciones cuando aquellos se integran en este (Enguita, 2004):

- Secreto: Acceso a la información y recursos solo a entes autorizados
- Integridad: Modificación de la información de recursos solo por entes autorizados
- Disponibilidad: La información y recursos deben estar disponibles para los entes autorizados.

2.2.1.2 Politicas de Seguridad

Las políticas de seguridad son los lineamientos y formas de comunicación con los usuarios, que establecen un canal de actuación en relación a los recursos y servicios de la red. Esto no significa que las políticas sean una descripción técnica de mecanismos y tecnologías de seguridad específicas y tampoco

términos legales que impliquen sanciones. Las políticas son una descripción de lo que se desea proteger y la razón por la cual debe hacerse. Estos lineamientos deben abordar aspectos como la evaluación de los riesgos, protección perimétrica, control de acceso, y normas de uso de Internet y correo electrónico, protección contra virus y copias de seguridad entre otros (Jaime & Vanegas, 2006).

Establecer políticas estrictas de seguridad de acceso a los recursos con información sensible o confidencial es totalmente imprescindible. Cuanto más estrictas sean, menor será el riesgo de fuga de información (Cto, 2017).

2.2.1.3 Organismos entendidos en temas de seguridad

CCN-CERT (2016). Es el Centro Criptológico Nacional (CNN), dependiente del Centro Nacional de Inteligencia (CNI). Este servicio se creó a finales del año 2006 como CERT gubernamental español, y sus funciones quedan recogidas en el Esquema Nacional de Seguridad. Este texto legal, en su artículo 37 señala los servicios que el CCN-CERT ya prestaba desde su constitución (en parte recogidos en el RD 421/2004 de regulación del CCN). Su principal objetivo es contribuir a la mejora del nivel de seguridad de los sistemas de información de las tres administraciones públicas existentes en España (general, autonómica y local).

INTECO-CERT (2016). Instituto Nacional de Tecnologías de la Comunicación (INTECO-CERT) tiene como finalidad servir de

apoyo preventivo y reactivo en materia de seguridad en tecnologías de la información y la comunicación tanto a entidades como a ciudadanos. Tiene vocación de servicio público sin ánimo de lucro y ofrece ayuda que, en todos los casos, es gratuita y de rápida gestión.

IRIS-CERT (2016). Es el servicio de seguridad de Red IRIS (IRIS-CERT), que tiene como finalidad la detección de problemas que afecten a la seguridad de las redes de centros de RedI RIS, así como la actuación coordinada con dichos centros para poner solución a estos problemas. También realiza una labor preventiva, avisando con tiempo sobre problemas potenciales, ofreciendo asesoramiento, organizando actividades de acuerdo con los mismos y ofreciendo servicios complementarios. IRIS-CERT actúa como último punto de contacto para los incidentes graves que puedan afectar al dominio, aceptando cualquier incidente como evidencia para dar soporte a nuestra comunidad. Es la red académica y de investigación española y proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional y a nivel internacional y tiene su campo de acción en su propia página web (RedIRIS, 2016).

CVE-MITRE (2016). Dedicada a detectar Vulnerabilidades y Exposiciones Comunes, es patrocinado por US-CERT en la oficina de la seguridad cibernética y las Comunicaciones en el Departamento de Seguridad Nacional de Estados Unidos.

2.2.2 Ataques de seguridad en redes de comunicaciones

Un ataque es una acción llevada a cabo por un cibernauta delinquiendo a una víctima potencial y puede tener diferentes perspectivas. Desde la perspectiva del administrador responsable de la seguridad, un ataque es un conjunto de uno o más sucesos que tienen una o más consecuencias de seguridad; desde la perspectiva de un observador neutral, el ataque puede tener éxito o no en un intento de intrusión y desde la perspectiva de un intruso, un ataque es un mecanismo para cumplir un objetivo. Una intrusión supone una entrada forzada, mientras que un ataque exige la aplicación de la fuerza; la búsqueda de información y las exploraciones realizadas por un intruso se pueden consideran, los ataques pasivos y ataques activos como en la Figura1. De tipos de ataque.

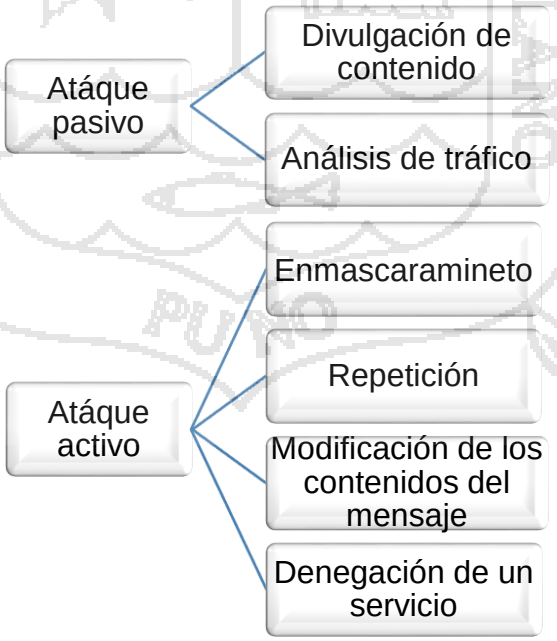


Figura 1**.** Tipos de ataque
Fuente: (Lozano et al, 2000).

2.2.2.1 Las etapas del ataque

- Reconocimiento
- Incursión
- Descubrimiento
- Captura y
- Filtración

2.2.2.2 Motivaciones de los Atacantes

La mayoría de motivaciones son consideraciones económicas, diversión, ideología, autorrealización, búsqueda de reconocimiento social y de un cierto estatus dentro de una comunidad de usuarios. Todo intruso debe disponer de medios técnicos, conocimientos, herramientas adecuadas, con motivación o finalidad aprovechando la oportunidad y sobre todo la vulnerabilidad. Estos tres factores crean el triángulo de la seguridad.

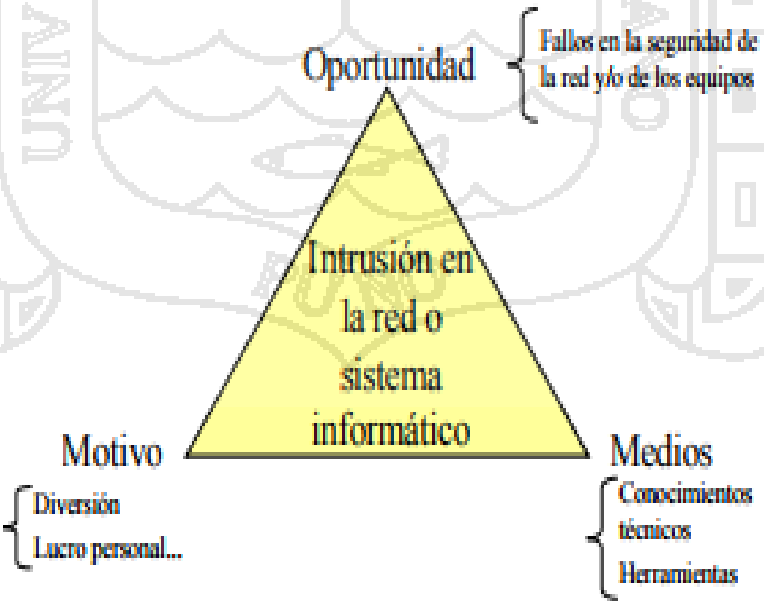


Figura 2. Triángulo de intrusión
Fuente: (Gómez, 2014).

2.2.3 Servicios de seguridad de redes de comunicaciones

2.2.3.1 Confidencialidad

Esta almacenada, procesada, puede ser confidencial, puede ser mal utilizada o divulgada, puede estar siguiendo a robos, sabotajes, accidentes o fraudes, ISO/IEC 13335-2004. (ISO/IEC, 2016).

2.2.3.2 Integridad

Propiedad de estar en salbaguardar, la exactutud y totalidad de los activos, ISO/IEC, 13335-2004. (ISO/IEC, 2016).

2.2.3.3 Disponbilidad

Propiedad de estar accecible y utilizable bajo la demanda de una entidad autorizada, ISO/IEC,13335-2004. (ISO/IEC, 2016).

2.2.4 ISO 27002

El organismo acreditador, a nivel mundial en ISO 27002, es el único acreditador, a nivel mundial en ISO/IEC según sus lineamientos, es considerado como el documento a utilizar para acreditación de organismos, operando sistemas de gestión de seguridad información. Las empresas acreditadoras tienen la finalidad de seleccionar y evaluar a las empresas certificadoras. Conteniendo tabien el ultimo estandar liberado que es el ISO 27035. El cual trata sobre gestión de incidencias respecto a seguridad de redes de comunicaciones. ISO/IEC 27001 es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la

comisión International Electrotechnical Commission, Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información según Ciclo de Deming (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002 (Alexander, 2007).

2.2.5 Entorno legal

Ley Nº30096. Ley respecto a delitos informáticos y la modificación de la Ley Nº30171. En esta ley se da mayor énfasis a la seguridad de la información vulnerada mediante:

- Acceso Ilícito,
- Atentado a la integridad de datos informáticos,
- Atentado a la integridad de sistemas informáticos,
- Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos,
- Interceptación de datos informáticos,
- Fraude informático, Abuso de mecanismos y dispositivos informáticos.

En tanto el Gobierno peruano a formalizo el convenio de la ciberdelincuencia, realizado en la Conferencia de Ministros de los Países Iberoamericanos, firmado en Budapest.

Por lo que designa la coordinación para el cumplimiento con organización (Pe-CERT) a través de la oficina de ONGEI y el Ministerio Público, con la finalidad de cumplir con las penas estipuladas en la Ley, no teniendo ninguna aplicación de estas leyes en Apurímac-Abancay.

2.2.6 Amenazas

Cualquier circunstancia o evento que pueda explotar, intencionalmente o no, una vulnerabilidad especifica de un sistema de información y comunicaciones resultado en una pérdida de confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información de manejada o de la integridad o disponibilidad del propio sistema (Merino & Cañizares 2011).

2.2.7 Vulnerabilidad

Es la posibilidad de que un código malicioso penetre nuestra red de comunicaciones, por lo que tenemos que tomar medidas preventivas mediante la detección y respuesta. La vulnerabilidad en la detección de intrusos, con el tiempo, ha quedado claro que los días de la "Identificación de una vulnerabilidad para gobernarlos a todos" estaban llegando a su fin y tenemos que empezar a planificar para que el cambio, una de las principales observaciones que hemos hecho ha sido la creciente necesidad de múltiples identificadora de vulnerabilidad y bases de datos que sirven para diferentes audiencias, apoyan diversas prácticas comerciales, y

operan a velocidades diferentes características (Householder, 2016).

Vulnerabilidad es la susceptibilidad de un sistema o componente a sufrir daños por un ataque específico, o equivalentemente una debilidad del sistema de protección de un recurso que puede ser explotado por un ataque (Pastrana et al., 2000).

2.2.8 Evaluación de riesgo

El riesgo constituye la sumatoria de vulnerabilidad más amenaza, el cual normalmente nace de es el análisis y evaluación de riesgo. Por lo tanto, el cálculo de riesgo es factible realizarlo en función a los activos.

Existen diferentes maneras de relacionar los valores asignados a los activos y aquellos asignados a las vulnerabilidades y amenazas para así obtener mediciones del riesgo. (Sheffi, 2005).

2.3 INFRAESTRUCTURA TECNOLÓGICA DE SEGURIDAD DE REDES

Describe las funciones del servidor de seguridad: controla el acceso a las redes internas de la organización actuando como el encargado que examina las credenciales de cada usuario antes de que pueda examinar la red. El servidor de seguridad identifica nombres, direcciones de Protocolo Internet (IP), aplicaciones y otras características del tráfico entrante, y compara esta información contra las reglas de acceso que el administrador de la red ha programado en el sistema. El servidor de seguridad impide la comunicación no autorizada dentro y fuera de la red, permitiendo que la organización aplique una

política de seguridad en el tráfico que fluye entre su red e Internet. (Oppliger, 1997).

La infraestructura de red, requiere de un servidor de seguridad que gestione los sistemas de seguridad Segev *et al.* (1998) dice que para crear un buen servidor de seguridad, alguien debe describir de manera bastante detallada y conservar las reglas internas que identifican a las personas, aplicaciones o direcciones que se permiten o rechazan. Los servidores de seguridad pueden desalentar, pero no impedir del todo, la penetración de la red por intrusos y deben verse como un elemento más en un plan de seguridad global. Para tratar con eficacia la seguridad de Internet, es posible que se requieran políticas corporativas y procedimientos más amplios, responsabilidades del usuario y capacitación en el conocimiento de seguridad.

2.4 SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

Según RedIRIS (2016), Una de las aplicaciones muy importantes son los sistemas de detección de intrusos, define a los IDS como medios que intentan detectar actividades inapropiadas y proveen un sistema de alarma activado en caso de intrusiones o ataques.

Este sistema de alarma puede realizar acciones reactivas como la reconfiguración del firewall, ejecución de rutinas para manejar el evento, guardar información en la bitácora del sistema, terminar la sesión de comunicación y guardar información sobre el atacante. que dentro de la técnica de análisis basada en anomalías, se trata de detectar ataques o intrusiones a partir de desviaciones significativas del perfil de comportamiento normal, es decir, se

trabaja en el principio de comparar las acciones de los usuarios contra un perfil de conducta normal o aceptable (Watkins & Wallace 2008).

Transmite su preocupación por la seguridad de red de redes y dice que las redes neuronales artificiales permiten a las computadoras el aprendizaje y la adaptación de distintas tareas que se les presentan, se inspiran en la forma en la que funciona el cerebro humano que dependiendo del impulso de entrada, manifiestan una respuesta. El impulso que las neuronas reciben de entrada se traduce en una decisión como salida en la red neuronal. Para llevar a cabo decisiones, la red neuronal necesita una fase de entrenamiento iterativo, en la cual se aplican muestras de datos y se ajustan pesos hasta que el factor resultante se encuentre cerca del resultado deseado. Las redes neuronales poseen características predictivas y de reconocimiento de patrones que las hacen una herramienta atractiva para los sistemas de detección de intrusos (Hagan et al.,1996).

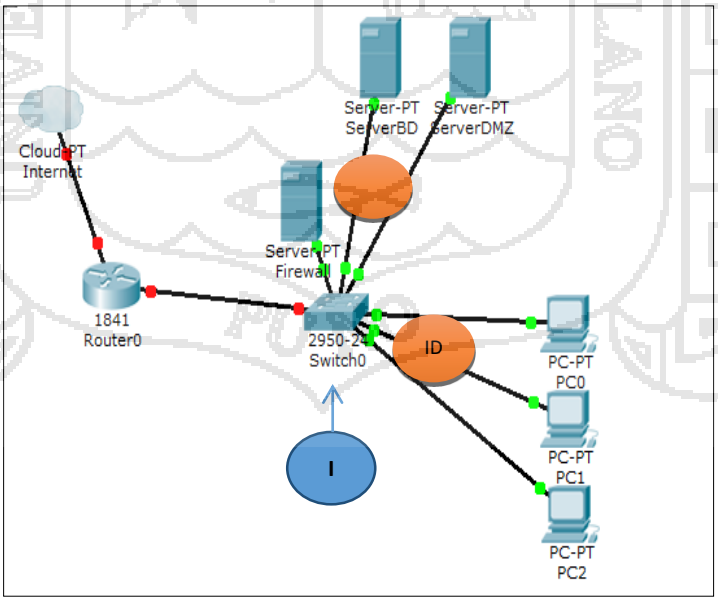


Figura 3. Sistemas de prevención de detección de intrusos
Fuente: (Hagan et al., 2000)

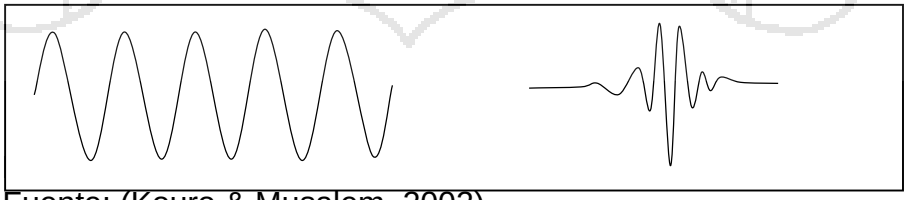
La mayoría de investigaciones de los sistemas de detección de intrusos tiene como objetivo el ser más reactivos contando con una topología de red como el de la Figura 3. El cual nos muestra la priorización de seguridad de redes, ayudándonos a dar prioridades al momento de configurar la seguridad.

2.5 TRANSFORMADA WAVELET

Según Thulliard (2002) la transformada de wavelet remonta y encumbra el inicio de las redes neuronales basadas en wavelets en la investigación de (Daugman, 1988), en el cual se utilizaron wavelets Gabor para la clasificación de imágenes. También se señala que las redes wavelet se volvieron más conocidas después de varios trabajos realizados por: Pati (1992) presenta en su investigación una red wavelet con alimentación hacia adelante, Zhang (1992) ocupa un modelo neuronal con wavelets para el control de un robot y centra su investigación en clasificación de fonemas y reconocimiento de voz.

Las redes wavelet o wavenets son redes neuronales que combinan la teoría wavelet con el campo de las redes neuronales. Las redes wavelet han sido empleadas en problemas de clasificación e identificación de información de manera exitosa que van desde monitoreo de procesos de manufactura, procesamiento de voz, problemas de control y procesamiento de imágenes. La arquitectura típica de las redes neuronales basadas en wavelet utiliza un conjunto de funciones wavelet que reemplazan a las funciones sigmoides, la combinación de teoría wavelet con redes neuronales tiene las siguientes ventajas (Yu et al., 2007):

- Las unidades están basadas en el análisis teórico wavelet, lo que permite una mayor flexibilidad en las funciones de transferencia aplicadas a los vectores de entrada.
- Las redes neuronales basadas en wavelets tienen menos parámetros que tienen que ser ajustados durante el proceso de entrenamiento.
- Cada unidad que utiliza funciones wavelet tienen poca influencia sobre las otras unidades demás de ésta manera se incrementa la velocidad de entrenamiento.
- El proceso de aprendizaje en las redes neuronales basadas en wavelet es un proceso de aproximación para obtener una solución global óptima en contraste con los puntos locales mínimos.
- La función wavelet, analiza señales que se descomponen ortogonalmente de las ondas, es usualmente asociada a la teoría de análisis multirresolución. Donde los frames de onda son construidos por simples operaciones de traslación y dilatación de una única función fija denominada wavelet madre, que debe satisfacer condiciones de ortogonalidad. Como se observa en la Figura 5, la transformada de wavelet, es una señal o (forma de onda) de duración limitada cuyo valor medio es cero. Al mismo tiempo en la Figura 4, tenemos el ejemplo de una señal sinusoidal y señal wavelet.



Fuente: (Kouro & Musalem, 2002)

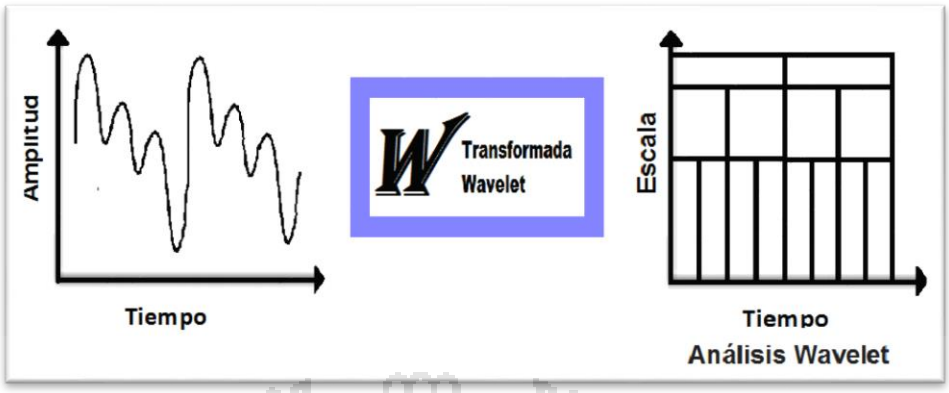


Figura 5. Esquema Transformada de wavelet
Fuente: (Kouro & Musalem, 2002)

El análisis de señales a través de transformada de la transformada wavelet descompone la señal en versiones trasladadas en el tiempo y escalas de wavelet original, conocidas como wavelet madre. Que serán medidas y segmentadas, por lo que la función wavelet nos ayuda en la tarea de análisis de señales grandes. Esta señal nos servirá como modelo para simular la detección de ataques en una red de datos.

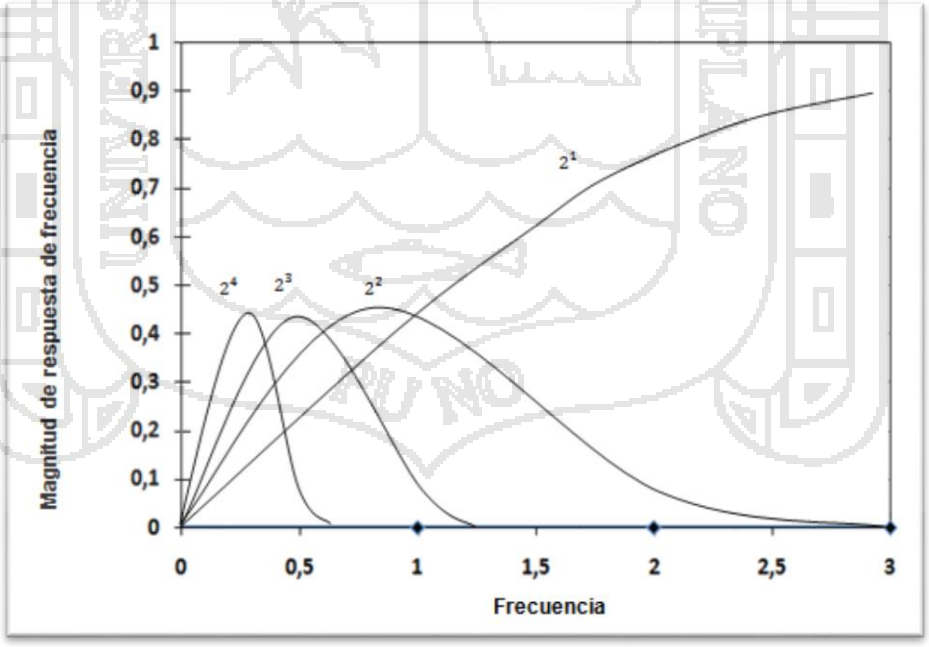


Figura 6. Señal madre wavelet - Segmentos de red y coeficientes de una función wavelet. Escalas de señal madre de las $\mathbf{2^{1,}}$ **al** $\mathbf{2^4}$
Fuente: (Alarcón & Barria, 2001)

2.5.1 Descomposición de una señal wavelet en ondas

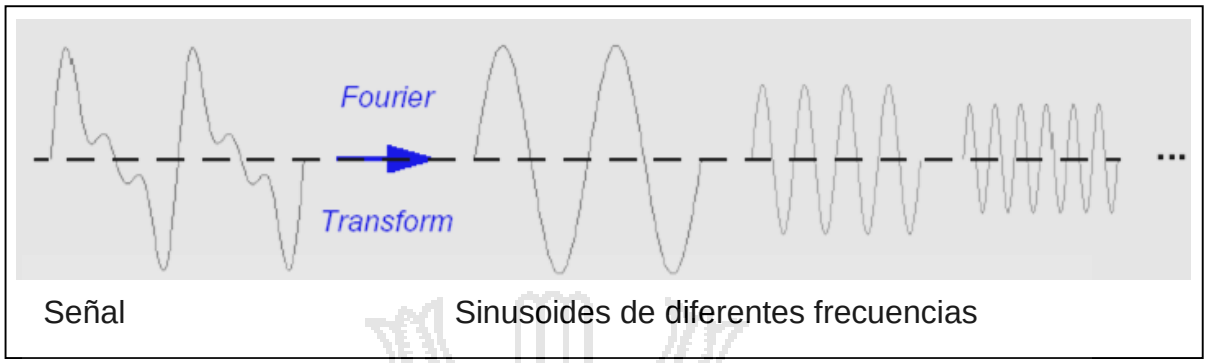


Figura 7. Señales fourier de diferentes frecuencias
Fuente: (López, 2004)

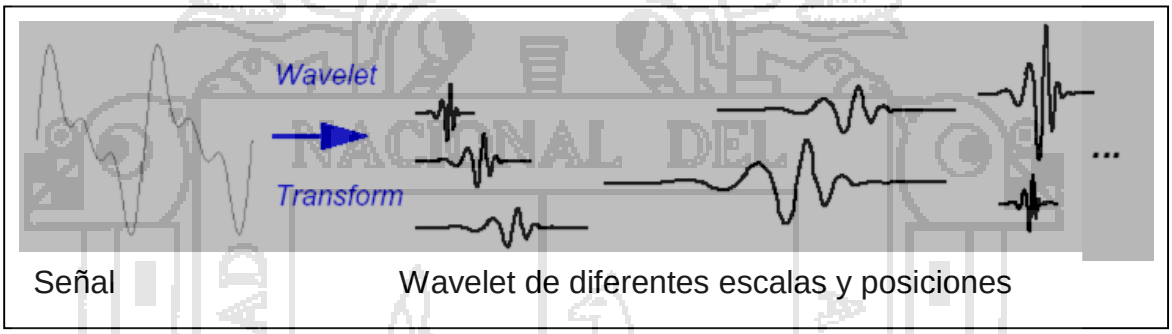


Figura 8. Señales Wavelet de diferentes frecuencias
Fuente: (López, 2004)

2.5.2 Tipos de wavelet

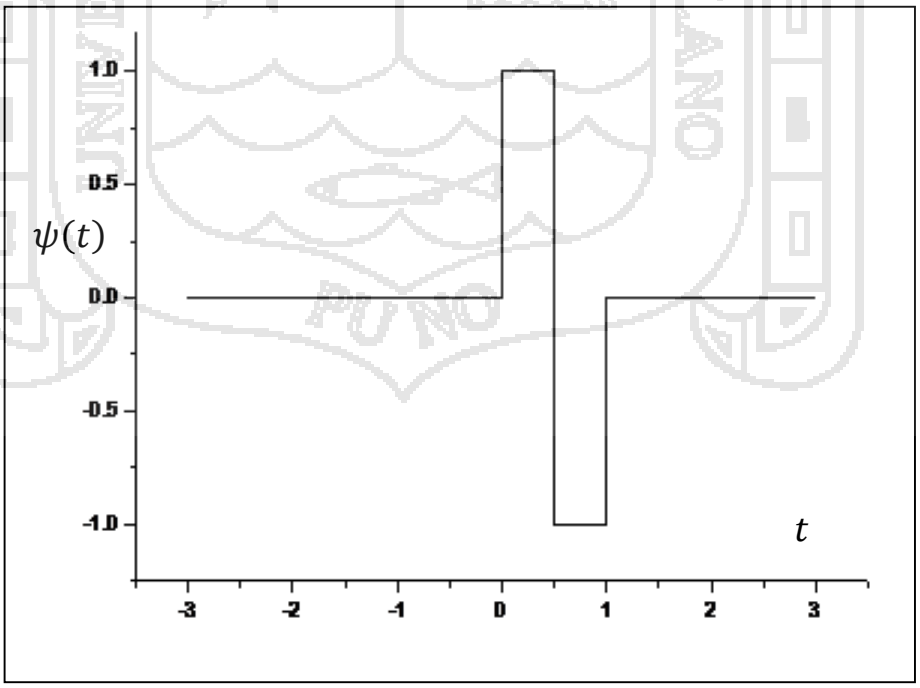


Figura 9. Wavelet de haar [wavelet madre ψ(t)]
Fuente: (López, 2004)

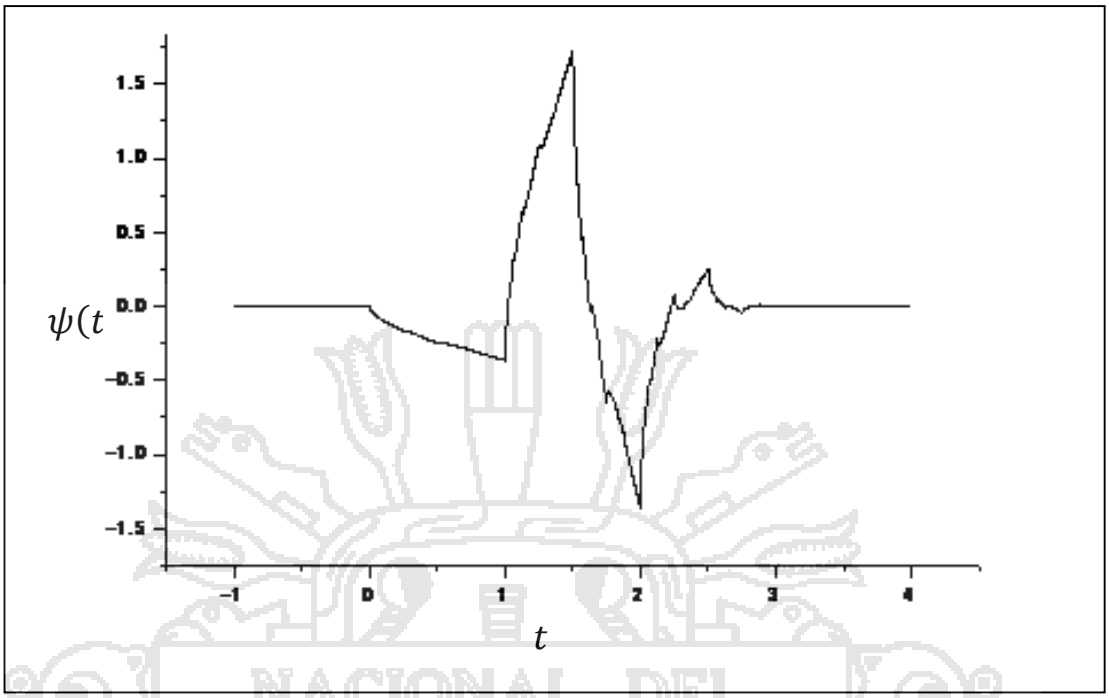


Figura 10. Wavelet daubechie (orden 4) Wavelet madre n=4 [ψ(t)]
Fuente: (López, 2004)

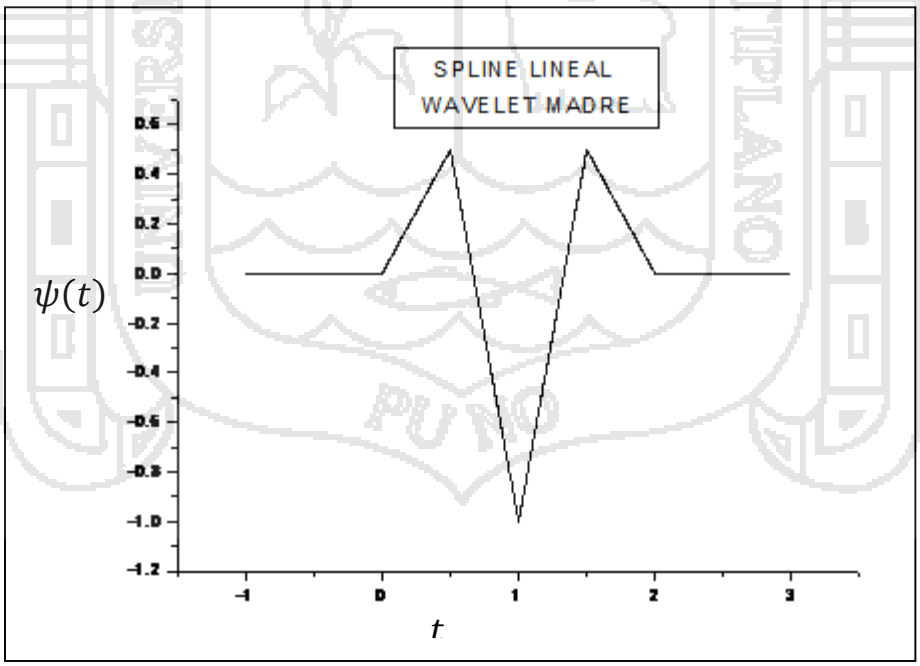


Figura 11. Wavelet con spline lineal
Fuente: (López, 2004)

El número de wavelets existentes son muchos. Generalmente es conveniente hacer uso de aquel cuya forma se adecúe mejor al tipo de señal con la que se va a trabajar. Algunos wavelets tienen enunciados analíticos. Por ejemplo las siguientes:

Cuadro 1. Fórmulas Wavelet

WAVELET DE MORLET	WAVELETSOMBRERO MEXICANO
$\Psi_0(t) = \sqrt{\beta} \cdot \pi^{-1/4} \cdot e^{i\omega_0 t} \cdot e^{-\beta^2 t^2/2}$	$\Psi_0(t) = (1 - t^2) \cdot e^{-t^2/2}$

Fuente: (Roman, 2004)

La segunda derivada de una gaussiana y otros en cambio se obtienen mediante fórmulas de recurrencia.

2.5.3 Representación gráfica de los coeficientes de la transformada discreta de wavelets

El análisis de wavelets, nos da información sobre el espectro de frecuencias en función del tiempo.

- La resolución espectral de una frecuencia f es: Df $\propto$ f
- La resolución temporal de esta frecuencia es: Dt $\propto$ 1/f ($\Rightarrow$Dt.Df = cte).

Realizando una Transformada discreta de Wavelets, obtenemos una serie de coeficientes que podemos interpretar gráficamente.

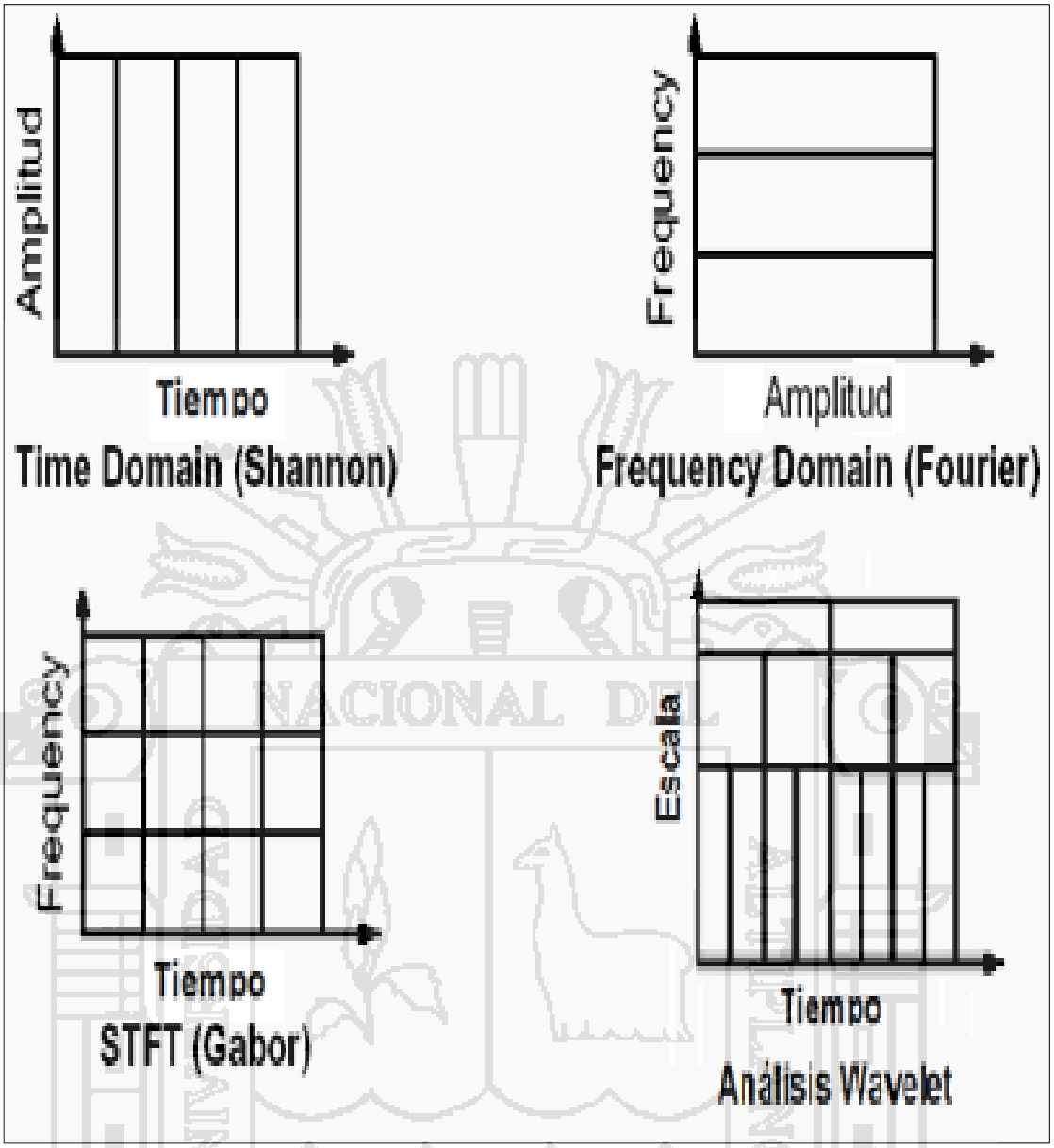


Figura 12. Representación de diversas frecuencias
Fuente: (López, 2004)

2.5.3.1 Traslaciones y Dilataciones

Tal como se ha visto, una transformada de wavelets de una función $S(t)$viene dada por:

$$S(a,t) = \int_{-\infty}^{\infty} \psi^*{}_a(t-\tau).S(t).dt$$

El término "t" nos brindalas traslaciones y el término "a" las dilataciones del wavelet.

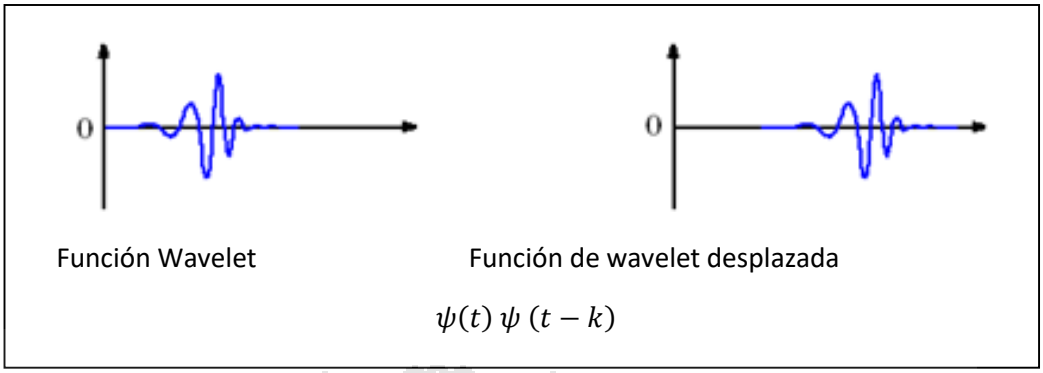


Figura 13. Traslaciones
Fuente: (López, 2004)

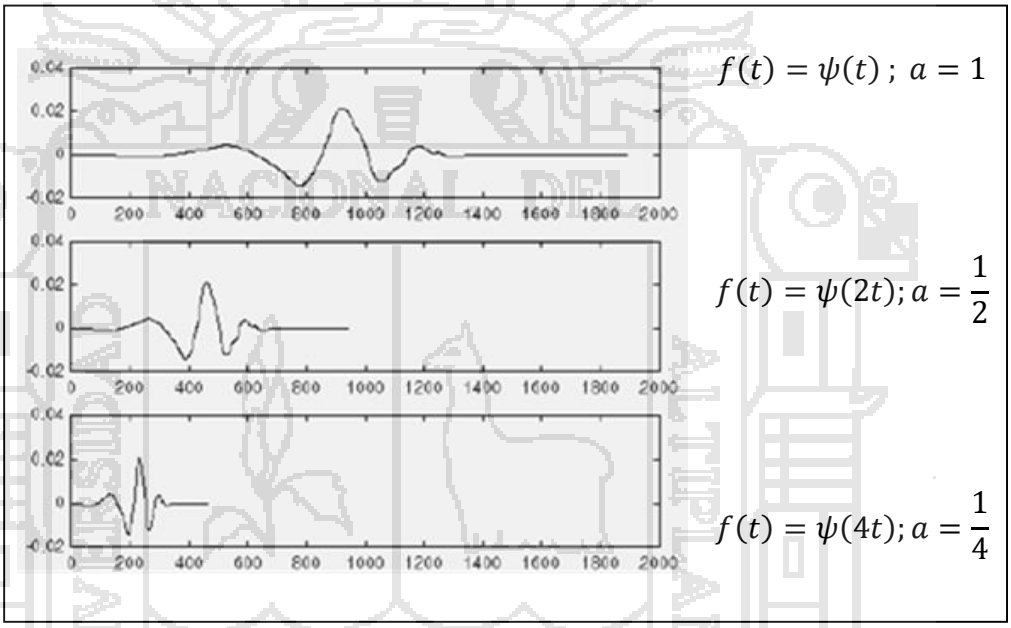


Figura 14. Dilataciones
Fuente: (López, 2004)

La señal $S(t)$,muestra versiones del wavelet madre (dilatados y trasladados), estudiando punto a punto para qué las dilataciones y traslaciones de la señal $S(t)$y el wavelet son mucho más similares.

Como es lógico, la frecuencia de la señal $S(t)$estudiada está relacionada íntimamente con la escala del wavelet. Por otro lado, que el análisis sea local, es lo que da a la transformada de wavelets propiedades propias e interesantes.

2.5.4 Coeficiente de transformada wavelet

Esta forma de descomponer una señal es bastante natural: los eventos de baja frecuencia suelen durar en el tiempo, mientras que los eventos de frecuencia alta suelen ser breves**.**

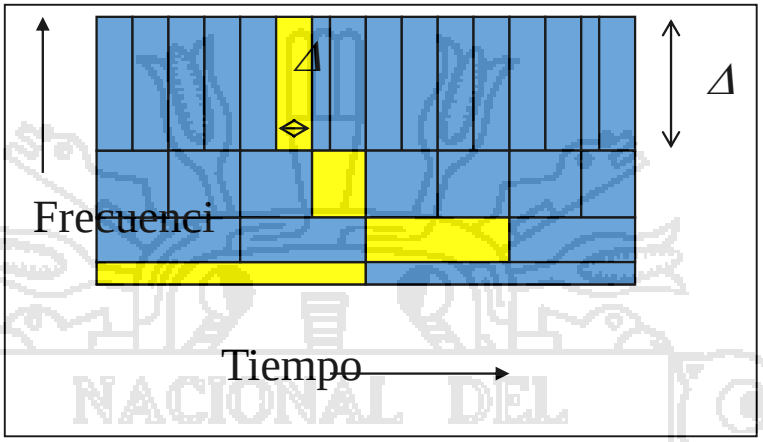


Figura 15. Coeficiente de transformada wavelet
Fuente: (López, 2004)

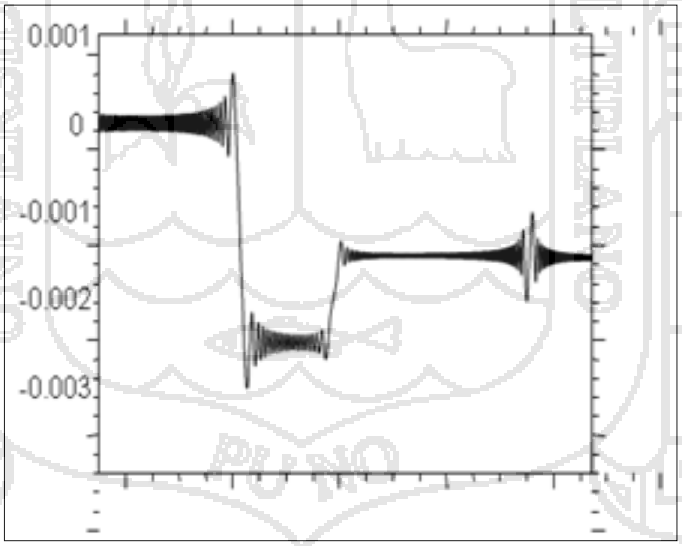


Figura 16. Señal con altas y bajas frecuencias
Fuente: (López, 2004)

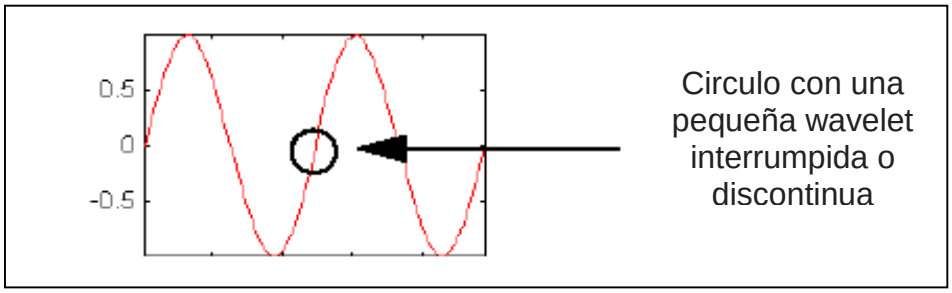


Figura 17. Discontinuidades en una señal pequeña
Fuente: (López, 2004)

Figura 18. Coeficiente de wavelet
Fuente: (López, 2004)

2.5.4 Algoritmo de seguridad con funciones de transformada de wavelet

La Transformada Wavelet, es generada a partir de una función Wavelet básica, mediante traslaciones y dilataciones. Estas funciones permiten reconstruir la señal original a través de la Transformada Wavelet inversa. La Transformada Wavelet no es solamente local en tiempo, sino también en frecuencia. Dentro de los usos de esta poderosa herramienta podemos nombrar, además del análisis local de señales no estacionarias, el análisis de señales electrocardiográficas, sísmicas, de sonido, de radar, así como también es utilizada para la compresión y procesamiento de imágenes y reconocimiento de patrones, análisis de redes. Función a analizar es en función del tiempo t.

Dado que la transformación lineal y continua de una función $S(t)$, es (López, 2004):

$$S(a,t) = \int_{-\infty}^{\infty} \psi^*{}_a(t-\tau).S(t).dt$$

2.6 REDES NEURONALES

Las Redes Neuronales son sistemas de software que modelan el proceso de los humanos de aprendizaje y recuerdos. Una red neuronal puede ser usada en seguridad informática para detectar una transacción fraudulenta o una intrusión a un sistema computacional. Mediante las Redes Neuronales se ha intentado simular dos de las características más importantes con que cuenta el cerebro humano: la capacidad de aprendizaje y el poder procesar información incompleta o que no es precisa. Esto se ha solicitado para la solución de problemas tanto científicos como el de la vida diaria.

Las Redes Neuronales intentan imitar el proceso de aprendizaje del cerebro humano, que está formado por millones de neuronas conectadas entre sí. Utilizan información que es percibida y transmitida hasta las neuronas, y al ser procesadas por ellas, dan una respuesta a cada uno de los diferentes estímulos. Cada neurona biológica tiene tres partes: un cuerpo celular, una estructura de entrada (Dendrita) y una de salida (Axón. La mayoría de las terminales de los axones se conectan con las dendritas de otras neuronas, generando así la Sinapsis. Matemáticamente el comportamiento de la neurona puede representarse por una lista de sus señales de entrada que son multiplicadas por sus pesos respectivos y posteriormente sumados, el resultado es llamado nivel de activación de la neurona del cual depende de la señal de salida que es enviada a cada una de las neuronas a las que está conectada a ella

dependiendo de la estructura de la red neuronal existen varias tipologías, algunas de estas son: Perceptrón lineal, Perceptrón multicapa, Backpropagation, Elman, Hopfield, Kohonen, etc. Las redes neuronales artificiales pueden ser vistas como grafos dirigidos con peso, en las cuales las neuronas artificiales son nodos y las conexiones dirigidas (con pesos) están entre las salidas y entradas de las neuronas. Basándose en las arquitecturas de conexión, las redes neuronales pueden ser agrupadas en dos categorías:

- Redes Neuronales hacia adelante (feed-forward), en las cuales los grafos no tienen ciclos.
- Redes Neuronales Recurrentes (feedback), en las cuales los ciclos ocurrren por las conexiones hacia atrás.

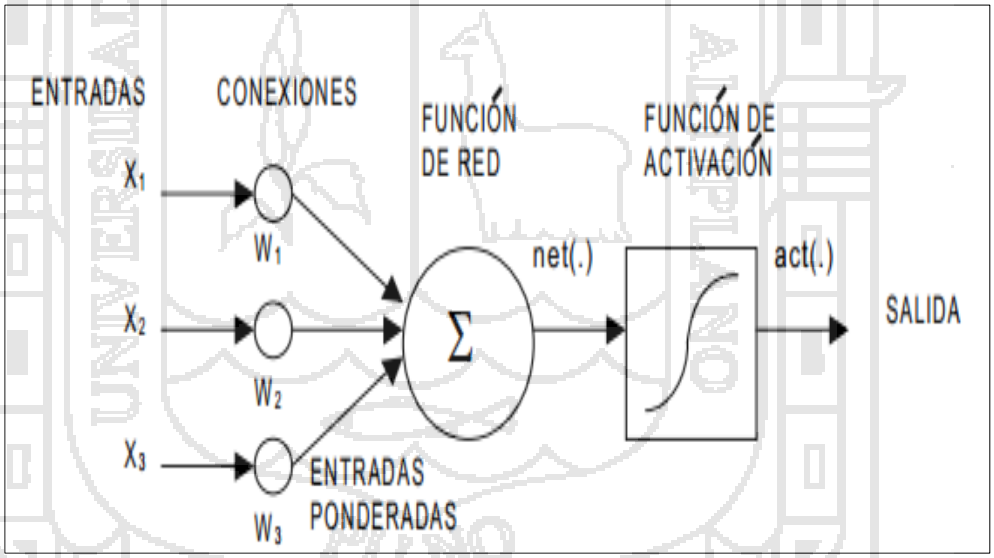


Figura 19. Neurón de tres capas
Fuente: (Aguilar, 2008)

2.6.1 Red Neuronal Recurrente (RNN)

Son sistemas dinámicos no lineales capaces de detectar regularidades temporales en las secuencias que pueden ser procesadas, pudiendo ser aplicadas, por lo tanto, a una multitud de tareas de procesamiento de dichas secuencias. La red neuronal con

conexiones recurrentes, como su nombre lo indica, describe la periodicidad de la información. Aquí la señal viaja desde la capa de entrada hasta la capa de salida, mientras al mismo tiempo, algunos o todos los datos de salida regresan desde la capa de salida ya sea a la capa de entrada o a una capa intermedia, formando un ciclo, pudiendo la salida regresar al mismo nodo de salida un instante después.

La red neuronal empleada consiste de dos capas: capa de entrada y capa de salida. La estructura de esta red difiere de la red perceptrón simple incluyendo una recurrencia en la capa de salida porque se trata de un clasificador de tipo supervisado con el objetivo de separar las diferentes clases conociendo su pertenencia. Las neuronas de la capa de salida de la red están completamente conectadas con las neuronas de las capas de entrada y las neuronas de la capa de salida están conectadas a ellas mismas. Cada conexión de pesos cuyo valor es modificado durante el proceso de entrenamiento. Por lo tanto, la salida "Y" de la red en el tiempo "t", es obtenida de la siguiente manera:

$$\mathrm{Y_k(t)} = f\left(\sum_{j=1}^{m} V_{jk}\, Y_k(t-1) + \sum_{i=1}^{q} W_{ij}\, X_i(t)\right)$$

Dónde:

- X_i , es el i-ésimo elemento de entrada de la capa de entrada de tiempo t.

- $W_{ij}(t)$, es el peso de conexión entre i-ésimo elemento de entrada de la capa de entrada y el j-ésimo elemento de salida de la capa de salida.
- V_{jk}, es el elemento recurrente de la capa de salida en el tiempo $t-1$.
- q, es el número de elementos de entrada y m es el número de elementos de salida. La función de activación es no lineal.
- m, es el número de neuronas.

La aplicación de los pesos de conexión se realiza usando los datos de entrada y de salida, no se requiere de un dato de referencia. La Red Neuronal Recurrente funciona de la siguiente manera:

Los pesos de la conexión W_{ij} y V_{jk}, se inicializan con valores aleatorios en el instante $t=0$, y con los valores existentes desde q neuronas de entrada hasta m neuronas de salida para los tiempos $t>0$, los valores de los pesos V_{jk}, se inicializan con valores existentes desde m neuronas de salidas hasta k neuronas de salida, ya que se trata de la recurrencia de la misma capa que es de salida. Los valores con los cuales se inicializan los pesos en $t=0$, son valores aleatorios muy pequeños:

- $Y_k(t)-1$, inicializa con valores de ceros.
- Calcula la salida deseada de la red aplicando la función de activación que es no lineal.
- Se repite el proceso en tiempo t hasta que el error de aprendizaje sea cero.

2.6.2 Algoritmo de aprendizaje

Se utiliza la regla delta para el entrenamiento de cualquier tipo de red neuronal, en la que se aplica el concepto de gradiente descendente, que consiste principalmente en una técnica de disminución del error. El objetivo consiste en minimizar la función de error cuadrático medio entre la salida real y la salida deseada de la red. El error de k-ásimo elemento de la capa de salida en el tiempo t es definido por la siguiente formula:

$$E = \sum_{k=1}^{N} e_k^2$$

Dónde: $e_k = (d_k - Y_k)$, Error de salida

d_k= Salida deseada

Y_k= Salida real de la red

En la salida real de la red tiene dos posibles resultados, 0 si se trata de un flujo normal y 1 si es un flujo con algún ataque.

2.6.3 Redes Neuronales Wavelet

En el trabajo Thulliard (2002), habla del origen de las redes neuronales basadas en wavelets y en el trabajo de Daugman (1988), en el cual se utilizó wavelets de Gabor para la clasificación de imágenes. También se señala que las redes wavelet se volvieron más conocidas después de varios trabajos realizados: Pati (1992) que presenta en su investigación una red wavelet con alimentación hacia delante, (Zhang,1992) ocupa un modelo neuronal con wavelets para el control de un robot y centra su investigación en clasificación de fonemas y reconocimiento de voz.

Las redes wavelet o wavenets son redes neuronales que combinan la teoría wavelet con el campo de las redes neuronales. Las redes wavelet han sido aplicadas a problemas de clasificación e identificación de manera exitosa. La arquitectura típica de las redes neuronales basadas en wavelet utiliza un conjunto de funciones wavelet que reemplazan a las funciones sigmoides, la combinación de teoría wavelet con redes neuronales tiene las siguientes ventajas (Yu et al.,2007):

1. Las unidades están basadas en el análisis teórico wavelet, lo que permite una mayor flexibilidad en las funciones de transferencia aplicadas a los vectores de entrada.
2. El proceso de aprendizaje en las redes neuronales basadas en wavelet es un proceso de aproximación para obtener una solución global óptima en contraste con los puntos locales mínimos
3. Las redes neuronales basadas en wavelets tienen menos parámetros que tienen que ser ajustados durante el proceso de entrenamiento.
4. Cada unidad que utiliza funciones wavelet tienen poca influencia sobre las otras unidades demás de ésta manera se incrementa la velocidad de entrenamiento.

2.6.2 Redes neuronales aplicadas a los sistemas de detección de intrusos

Los IDS intentan detectar actividades inapropiadas y proveen un sistema de alarma activado en caso de intrusiones o ataques. Este

sistema de alarma puede realizar acciones reactivas como la reconfiguración del firewall, ejecución de rutinas para manejar el evento, guardar información en la bitácora del sistema, terminar la sesión de comunicación y guardar información sobre el atacante.

Watkins & wallace (2008) aplica dentro de la técnica de análisis basada en anomalías y trata de detectar ataques o intrusiones a partir de desviaciones significativas del perfil de comportamiento normal, es decir, se trabaja en el principio de comparar las acciones de los usuarios contra un perfil de conducta normal o aceptable.

Las redes neuronales artificiales permiten a las computadoras el aprendizaje y la adaptación de distintas tareas que se les presentan, se inspiran en la forma en la que funciona el cerebro humano. Existen neuronas interconectadas las cuales, dependiendo del impulso de entrada, manifiestan una respuesta. El impulso que las neuronas reciben de entrada se traduce en una decisión como salida en la red neuronal. Para llevar a cabo decisiones, la red neuronal necesita una fase de entrenamiento iterativo, en la cual se aplican muestras de datos y se ajustan pesos hasta que el factor resultante se encuentre cerca del resultado deseado (Hagan et al., 1996).

Las redes neuronales poseen características predictivas y de reconocimiento de patrones que las hacen una herramienta atractiva para los sistemas de detección de intrusos. La investigación en esta área se enfoca en explorar diversas topologías y algoritmos de entrenamiento que permitan establecer mejores resultados de desempeño, tanto en la etapa de entrenamiento como en la de

prueba. Debido a su propiedad de generalización una red neuronal puede reconocer patrones no presentados durante la etapa de entrenamiento, de esta forma se detectan variantes de ataques entrenados que hayan traspasado otros niveles de protección como firewalls (Kukielka & Kotuslki, 2008).

Dentro de la incorporación de redes neuronales a los IDS se ha experimentado con distintas arquitecturas y algoritmos de aprendizaje para solucionar los problemas señalados anteriormente se han propuesto métodos que incluyen el uso del algoritmo annealing simulado junto con algoritmos genéticos para superar el mínimo local, la aceleración del proceso de entrenamiento mediante algoritmos como Levenberg – Marquardt y gradiente conjugado.

CAPÍTULO III

METODOLOGÍA

3.1 ÁMBITO Y LUGAR DE ESTUDIO

El estudio es un trabajo con diseño no experimental; dicho estudio de investigación se realizará en la provincia de Apurímac, departamento de Abancay en el año 2016. En un entorno de sistema virtualizado y simulado.

3.2 POBLACIÓN Y MUESTRA

3.2.1 Población

La población esta conformada por los 25 puertos vulnerables detectados en las 10 Instituciones encuentadas en las Redes de comunicaciones de Abancay 2016, que tienen un minimo de seguridad en el área de tecnologías de información.

3.2.2 Muestra

La muestra es no probabilística debido a que se determinó que tres de los veinticinco puertos detectados en las redes de Abancay 2016, son los más vulnerables y el algoritmo requiere de 3 datos para su

funcionamiento.

M=3 puertos.

Cuadro 2. Puertos de muestra

Puerto	Protocolo	Servicios
80	TCP	HTTP
22	TCP	SSH
23	TCP	TELNET

Cuadro 3. Puertos vulnerables en redes comunicaciones de Abancay

N°	Puerto	Protocolo	Servicios
1	21	TCP	SMUX
2	22	TCP	SSH
3	23	TCP	TELNET
4	25	TCP	SMTP
5	42	TCP	NAME SERVER
6	53	TCP	TCPWRAPPED - DOMAIN
7	80	TCP	HTTP
8	110	TCP	POP3
9	111	TCP	RPCBIND
10	135	TCP	MSRPC
11	139	TCP	NETBIOS-SSN
12	143	TCP	IMAP
13	199	TCP	HTTPS
14	427	TCP	SVRLOC
15	443	TCP	HTTPS
16	445	TCP	MICROSOFT-DS
17	515	TCP	PRINTER
18	554	TCP	RTSP
19	555	TCP	DSF
20	631	TCP	IPP
21	1022	TCP	SSH
22	2601	TCP	ZEBRA
23	5200	TCP	TARGUS-GETDATA
26	8080	TCP	HTTPD-HTTP-PROXY
25	9100	TCP	JETDIRECT

3.3 DESCRIPCIÓN DE MÉTODOS POR OBJETIVOS ESPECÍFICOS

3.3.1 Metodología para identificar los tipos de ataques en redes de comunicaciones.

a) Frecuencia requerida para la toma de datos: Búsqueda de información aproximadamente una semana de encuesta y búsqueda de datos de instituciones como CERT.
b) Materiales y equipos a ser utilizados: Recolección, encuesta, Observación, Verificación de Datos, Presentación de datos y equipo de computo.
c) Variables a ser analizadas: Ataques
d) Prueba(s) para probar las hipótesis. Conteo de Cantidad de diversos tipos de ataques recolectados.

3.3.2 Metodología para diseño de mecanismos de detección de ataques seguridad de redes de comunicaciones.

a) Frecuencia requerida para la toma de datos: Búsqueda de información aproximadamente una semana de encuesta y búsqueda de datos de instituciones de Abancay.
b) Materiales y equipos a ser utilizados: Recolección, Observación, Verificación de Datos, Presentación de datos y equipo de cómputo.
c) Variables a ser analizadas: Sistemas de Detección de Ataques.
d) Prueba(s) para probar las hipótesis. Identificación del conocimiento de seguridad de comunicaciones e identificación del método de seguridad más utilizado.

3.3.3 Metodología para implementar un prototipo de algoritmo wavelet.

a) Frecuencia requerida para la toma de datos: 8 Semanas.

b) Materiales y equipos a ser utilizados: Análisis algoritmo. Equipos: Equipo de cómputo, redes de comunicaciones equipo virtualizado.

c) Variables a ser analizadas: porcentaje de eficiencia Detección de Ataques del Algoritmo wavelet y el identificado.

d) Prueba(s) para probar las hipótesis: pruebas de funcionamiento del Algoritmo wavelet en funcionamiento con fórmulas de redes neuronales que determinan tiempo, detecciones, funciones, entradas y salidas de datos.

3.3.4 Metodología para Medir el nivel de gestión de seguridad del algoritmo wavelet para la detección de ataques de las redes de comunicaciones.

a) Frecuencia requerida para la toma de datos: 1 Semana.

b) Materiales y equipos a ser utilizados: Formatos de Normas ISO 27002 y equipo de cómputo.

c) Variables a ser analizadas: Niveles de seguridad del Algoritmo wavelet, y porcentaje de cumplimiento según norma ISO.

d) Prueba(s) hipótesis: Gestión de seguridad, Norma- ISO/EIEC 27002.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1 IDENTIFICACIÓN DE TIPOS DE ATAQUES EN REDES DE COMUNICACIONES.

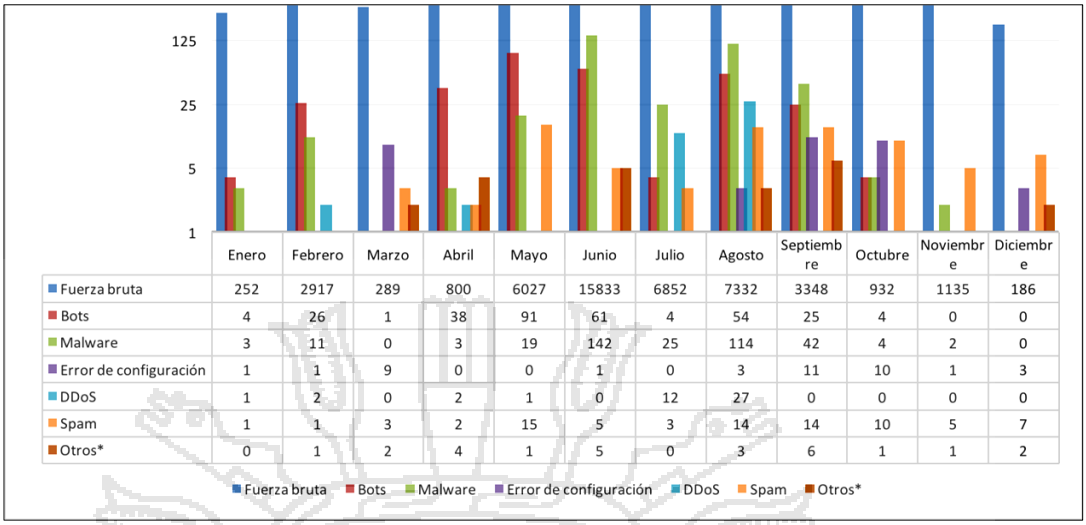
Para la precisión de tipos de ataques primeramente de realizo la búsqueda de información para realizar el respectivo análisis y evaluación de la misma, luego se simulo ser un atacante para entender mejor lo perpetrado y finalmente se realizó una encuesta.

4.1.1 Análisis de la información

Del análisis de la información se obtiene lo siguiente:

No existe información mínima de los tipos de ataques en la ciudad de Abancay, debido a que no se tiene una real conciencia de la seguridad de redes, aplicando seguridad básica, pero sin embargo a nivel de internacional existe una gran cantidad de ataques detectados, los cuales se mencionan en el Cuadro 4. y Cuadro 5. Para mejor información se tiene ataques generales en diferentes años. Así mismo se clasifican de tal manera que tenemos la información mensualizada.

Cuadro 4. Comparación de Ataques sufridos el año 2016



	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Fuerza bruta	252	2917	289	800	6027	15833	6852	7332	3348	932	1135	186
Bots	4	26	1	38	91	61	4	54	25	4	0	0
Malware	3	11	0	3	19	142	25	114	42	4	2	0
Error de configuración	1	1	9	0	0	1	0	3	11	10	1	3
DDoS	1	2	0	2	1	0	12	27	0	0	0	0
Spam	1	1	3	2	15	5	3	14	14	10	5	7
Otros*	0	1	2	4	1	5	0	3	6	1	1	2

Fuente: Cert (2016).

Cuadro 5. Ataques mensuales más sufridos el año 2016

Nº	ATAQUES	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SETIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE	TOTAL
1.	FUERZA BRUTA	252	2917	289	800	6027	15833	6852	7332	3348	932	1135	186	45903
2.	BOOTS	4	26	1	38	91	61	4	54	25	4	0	0	308
3.	MALWARE	3	11	0	3	19	142	25	114	42	4	2	0	365
4.	ERROR DE CONFIGURACION	1	1	9	0	0	1	0	3	11	10	1	3	40
5.	DDoS	1	2	0	2	1	0	12	17	0	0	0	0	35
6.	SPAN	1	1	3	2	15	5	3	14	14	10	5	7	80
7.	OTROS*	0	1	2	4	1	5	0	3	6	1	1	2	26

Fuente: Cert (2016)

Cuadro 6. Ataques mensuales más sufridos el año 2015

Nº	ATAQUES	ENERO	FECBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SETIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE	TOTAL
1.	FUERZA BRUTA	2214	219	116	15	74	4	39	4	2433	5	42	485	5650
2.	BOOTS	158	112	101	348	43	4	1	0	69	22	1	0	859
3.	MALWARE	3	7	3	0	1	4	1	0	151	0	1	7	178
4.	WORMS	2	0	0	7	0	12	63	0	0	0	0	0	84
5.	DDOS	10	1	4	0	0	1	0	3	1	0	0	0	20
6.	SPAN	1	2	2	1	3	0	0	1	1	2	0	0	13
7.	DEFACEMENT	1	1	3	2	1	0	0	1	0	0	1	1	11
8.	XSS	0	0	0	0	3	1	1	0	0	0	0	0	5
9.	REDIRECCIONAMIENTO	4	0	0	3	1	0	0	0	0	0	0	0	4
10.	PHISHING	1	0	0	0	0	0	1	0	0	0	0	0	1

Fuente: Cert (2015)

4.1.2 Simulación de ataque

Reconocimiento: Para la precisión de ataques se simulo un ambiente de virtualización Vmware7, con el Sistema Operativo Kali-linux, para luego escanear puertos vulnerables como se observa en la Figura Nº20, mediante técnicas de rastreo como, por ejemplo: NMAP, con la finalidad de observar y extraer información detallada de las vulnerabilidades de red de comunicaciones. Como se observa en la Figura 21. De la aplicación del comando NMAP y el comando VULSCAN, podemos encontrar vulnerabilidades.

Figura 20. Aplicación de Nmap

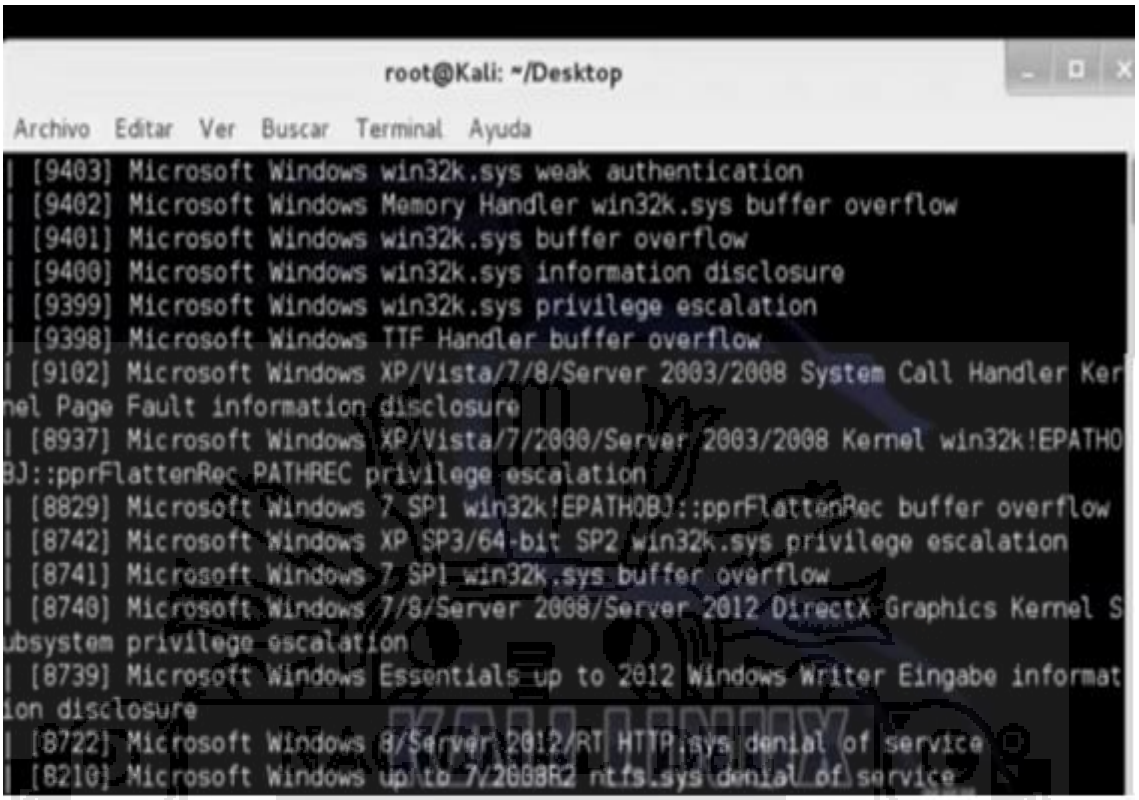


Figura 21. Aplicación de Vulcscan

Cuadro 7. Puertos vulnerables según NMAP

Estado	Protocolo	Nro. De puerto
Abierto/Open	TCP	80
Abierto/Open	TCP	139
Abierto/Open	TCP	445
Abierto/Open	TCP	Del 49152 al 49156

El cuadro 7, muestra el número de puertos vulnerables en vista que se encuentran abiertos es decir expuestos en el protocolo TCP como son el número de puerto 80 que es web y muchos otros, esto a los diversos ataques mencionados en el cuadro 3.

Incursión: Informados de las vulnerabilidades, se decide incursionar por cualquiera de los puertos.

Descubrimiento: Buscamos la información que nos interesa.

Captura: La cual será encapsulada en un archivo cifrado de preferencia.

Filtración: El archivo de será extraído mediante uno de los puertos expuestos, generalmente es el puerto indicado en el cuadro 5 y para que nadie se dé cuenta de procederá a filtrar por el puerto 80, que es el más utilizado.

Mediante este mismo método se realizó las infiltraciones en 10 diversas redes de comunicaciones es decir en instituciones que aparentemente tienen una zona desmilitarizada, obteniendo más listados de puertos Vulnerables.

4.1.3. Encuestas

Mediante la técnica de encuesta a 10 administradores de red de comunicaciones, en la ciudad de Abancay se determinó los ataques sufridos según CERT, los cuales se realizan por diversos puertos vulnerables. Al momento de realizar las encuestas se obtuvo diversos resultados de ataques sufridos, aquí presentamos 2 preguntas de importancia para determinar los tipos de ataques sufridos, como son:

Según la Encuesta N°001, realizada en Abancay el 2016,

Pregunta 1: ¿Considera usted que alguna vez la red de comunicaciones que administra ha sufrido algún ataque de seguridad?, se obtuvo que un 100% de las instituciones, sufren ataques de seguridad en la red de comunicaciones que administran, deduciendo que existe un tiempo de recuperación de fallas siendo un riesgo la perdida de información e incluso de equipos y según mencionan con daños irreparables debido a ello se implementó algún mecanismo de seguridad improvisado, considerando las políticas de seguridad poco usuales, aplicación de criterios de gestión

de seguridad inexistentes. En algunos casos se presenció páginas web atacadas en Abancay como son la Universidad Nacional Micaela Bastidas hasta en 2 ocasiones, el diario el chasqui en una ocasión. Y muchos otros incidentes nunca denunciados ni socializados.

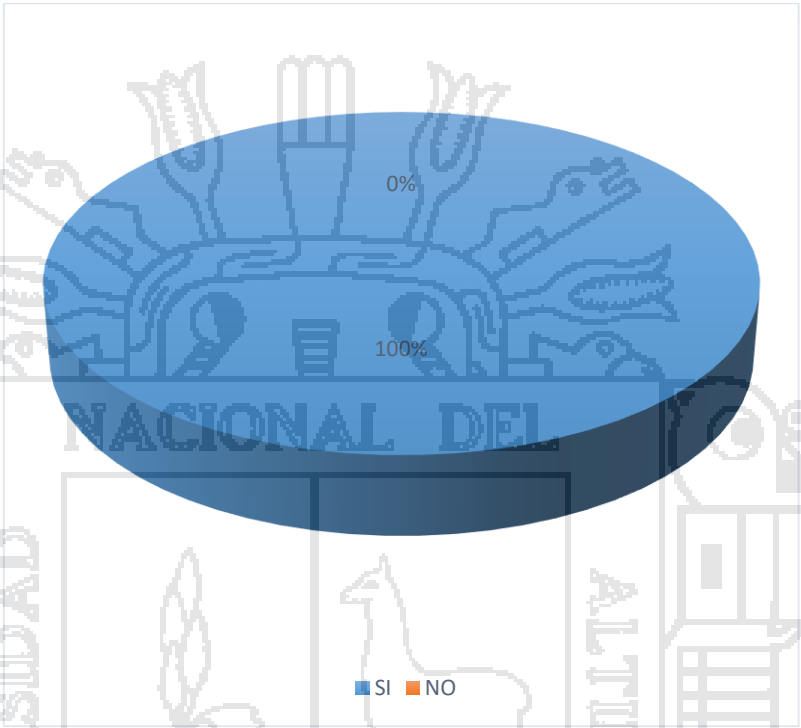


Figura 22. ¿Considera usted que alguna vez la red de comunicaciones que administra ha sufrido algún ataque de seguridad?

Pregunta 16. ¿Qué tipos de ataques de seguridad en redes de comunicaciones ha sufrido el año 2016? Marque todas las que considere, de los 10 encuestados:

En la figura 22. Se observa a un 80% que considera el malware como principal ataque de seguridad; ocupando un segundo lugar y empate al 30%, la negación de servicios y algún error de configuración de equipos de seguridad; en tercer lugar, con empate al 20% de incidencia tenemos la fuerza bruta, el direccionamiento y envenenamiento por IP como

causantes de ataques de seguridad; en cuarto lugar y ultimo, tenemos también con empate al 10% los siguientes problemas de seguridad como son: Phishing, boots y otros como el virus, exploit, clonación de IP o MAC, e incluso ingeniería social.

De los cuales el virus ocupa el primer lugar y la ingeniería un segundo lugar. Así tenemos los ataques de seguridad identificados según el criterio de los encuestados en la ciudad de Abancay el 2016.

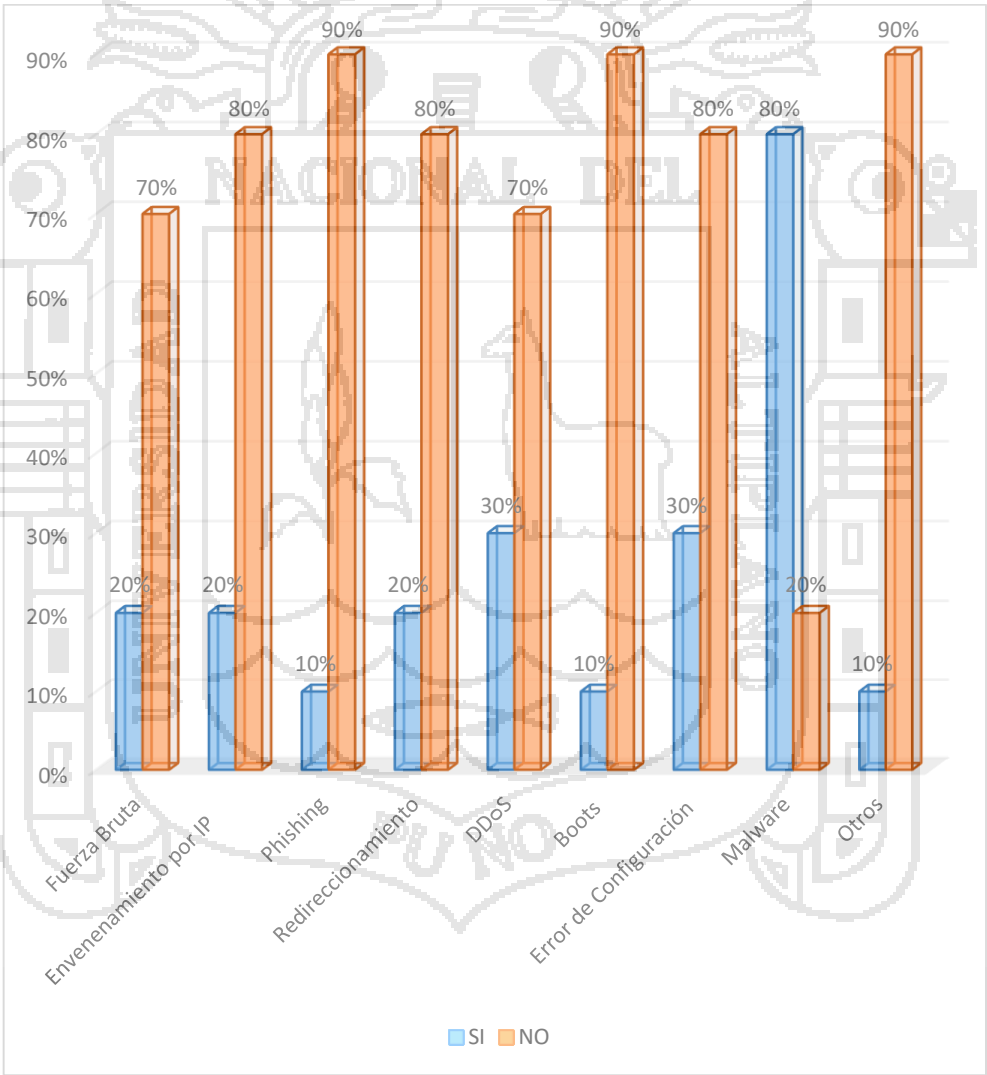


Figura 23. ¿Qué tipos de ataques de seguridad en redes de comunicaciones ha sufrido el año 2016?

4.2 DISEÑAR MECANISMOS DE DETECCIÓN DE ATAQUES DE SEGURIDAD EN REDES DE COMUNICACIONES

4.1.1 Encuetas

Mediante la técnica de encuentra se realizó diversas preguntas a 10 administradores de red de comunicaciones de diversas instituciones públicas con el objetivo identificar algún sistema de detección intrusos en una red de comunicaciones y al mismo tiempo de concientizar sobre la aplicación de un sistema de seguridad que incluya algoritmo wavelet neuronal en sus zonas desmilitarizadas, en vista de que no se tiene la suficiente garantía a la hora de elegir seguridad en la red de comunicaciones debido a que en el peor de los casos la medida será poco rentable, dándonos una falta certeza de seguridad. por ello para una organización, debemos tener en cuenta que existe un riesgo dado que no hay medida perfecta. Poniendo muchas pruebas periódicamente y confiar medianamente en ello. Por todo ello se realizaron diversas preguntas, como son:

Interpretación: Según la Encuesta N°001, realizada en Abancay el 2016.

Pregunta 2: ¿Conoce algún sistema de seguridad?, de los encuestados solo 60% conocía algún sistema de seguridad y un 40% desconocía sistemas de seguridad.

Pregunta 3: ¿Aplica algún sistema de seguridad?, de los encuestados 60% aplica algún sistema de seguridad y un 40% no aplica sistemas de seguridad.

Por lo que se deduce que los administradores que conocen algún sistema de seguridad lo aplican en su mayoría, y el resto de los encuestados que no conocen un sistema de seguridad o no están capacitados para la aplicación no lo ponen en práctica.

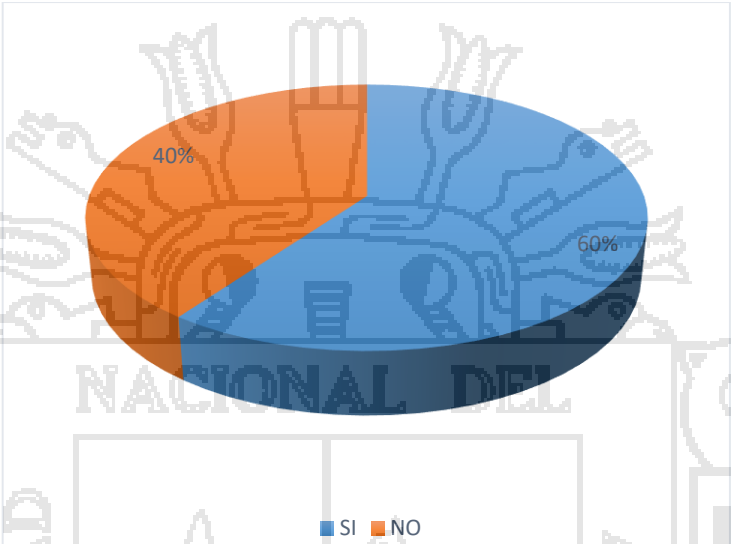


Figura 244. ¿Conoce algún sistema de seguridad?

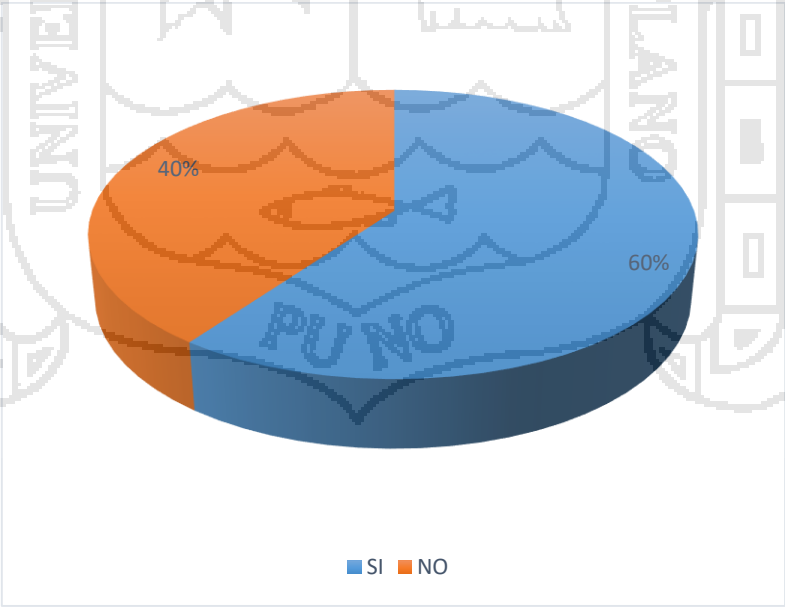


Figura 25. ¿Aplica algún sistema de seguridad?

Pregunta 4: ¿Conoce algún sistema de seguridad de detección de intrusos?, de los encuestados solo 25% conocía algún sistema de seguridad y un 75% desconocía sistemas de seguridad de detección de intrusos.

Pregunta 5: ¿Aplica IDS?, de los encuestados 0% aplica algún sistema de seguridad de detección de intrusos y un 100% no aplica sistemas detección de intrusos.

La mayoría de administradores de red de comunicaciones no considera la seguridad de detección de intrusos en sus sistemas de zona desmilitarizada, suponiendo que el sistema de seguridad ya es suficiente y creyendo que, al aplicar cualquier sistema, ya es suficiente. Debido a ello todas las instituciones evaluadas presentaron muchos puertos vulnerables.

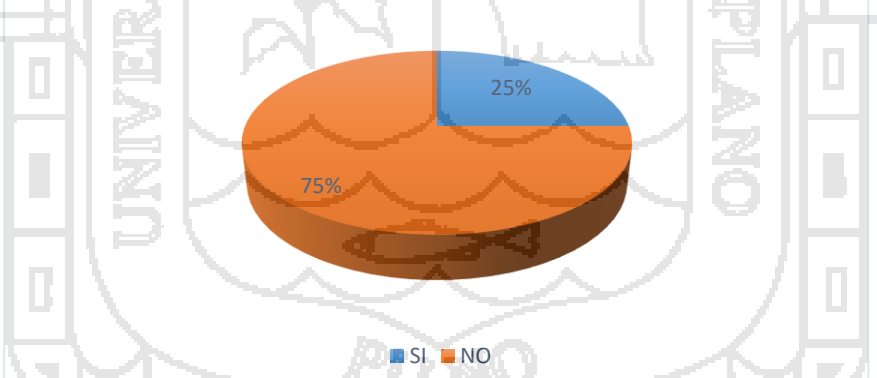


Figura 26. ¿Conoce los Sistemas de detección de intrusos IDS?

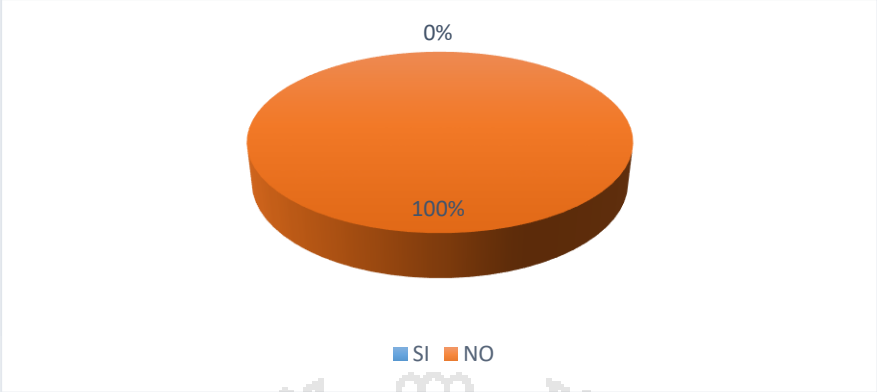


Figura 27. ¿Aplica IDS?

Pregunta 6: ¿Conoce el algoritmo de seguridad wavelet?, de los encuestados 0% conocía algún algoritmo de seguridad y un 100% desconocía algún algoritmo se seguridad.

Pregunta 7: ¿Aplica algún algoritmo de seguridad wavelet en la seguridad?, de los encuestados 0% aplica algún algoritmo se seguridad wavelet, y un 100% no aplica algún algoritmo se seguridad.

En vista de la respuesta, del total desconocimiento se les explicó respecto a las bondades de dicho algoritmo wavelet y mostraron cierto interés en lo dicho debido a que se les realizo una concientización de la seguridad de la red de comunicaciones que administran realizando una evaluación de rentabilidad de seguridad según sus incidentes.

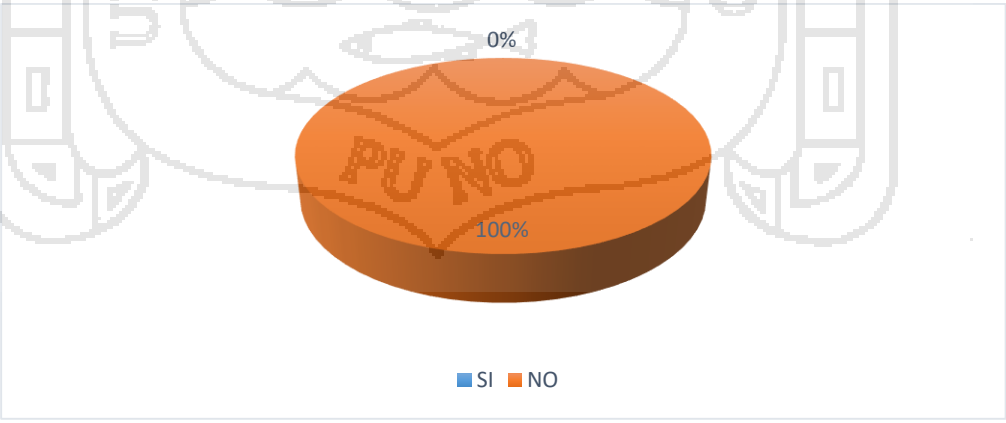


Figura 28. ¿Conoce el algoritmo de seguridad wavelet?

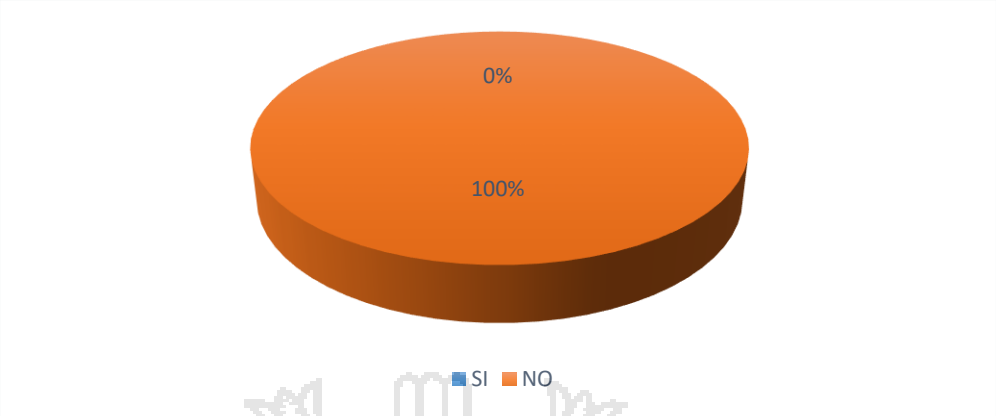


Figura 29. ¿Aplica algún algoritmo de seguridad wavelet en la seguridad?

Pregunta 8: Ahora que conoce el algoritmo wavelet neuronal; ¿Lo aplicaría? de los encuestados 100% aplicaría el algoritmo de seguridad wavelet y 0% no lo haría. Deduciendo que, en Abancay, el 100% de los administradores encuestados han adquirido conciencia de la seguridad en las redes de comunicaciones, y nosotros esperamos la disminución de los incidentes y desconocimiento de la pérdida sufrida ya sea tangible o intangible, al mismo tiempo mejoren sus políticas de seguridad aplicando con vital significancia un método eficiente en la seguridad de las redes de comunicaciones.

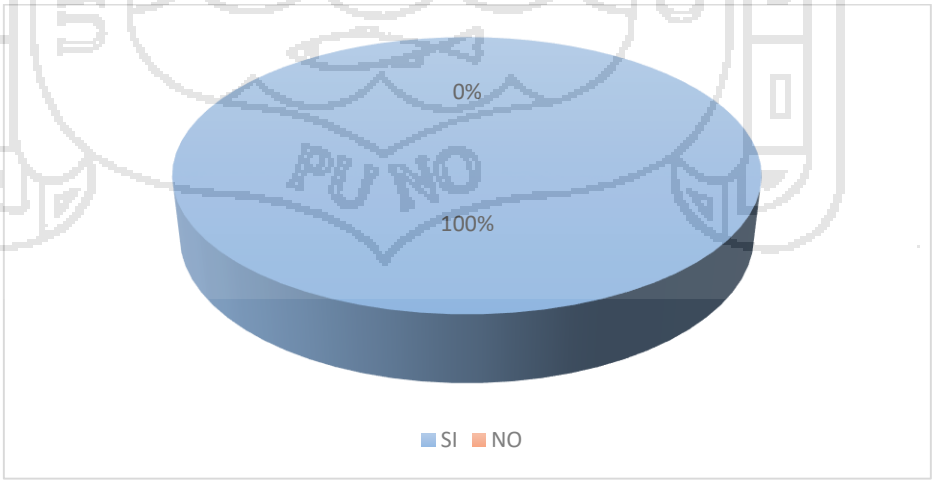


Figura 30. Ahora que conoce el algoritmo wavelet neuronal; ¿Lo aplicaría?

Pregunta 9: ¿Su tiempo de administración lo dedica a detener ataques de seguridad de redes de comunicaciones?, de los 10 encuestados el 100%, considerada que más tiempo lo dedican a detener ataques de seguridad a pesar de algunas medidas de seguridad tomadas por los administradores red, no están seguros de que son sus ataques de red de comunicaciones por lo que requiere de más tiempo restablecerse de un infiltración o ataque.

Figura 31. ¿Su tiempo de administración lo dedica a detener ataques de seguridad de redes de comunicaciones?

Pregunta 10: ¿Se autoriza los accesos a la administración de equipos de seguridad?, de los encuestados el 80%, nunca mantiene un control de accesos a la administración de sus equipos de seguridad de redes de comunicaciones por lo que incrementa la vulnerabilidad incumpliendo con la disponibilidad de acceso y confidencialidad en las redes de comunicaciones y un 20 % que cumple A veces con este requisito por lo requiere mejorar estos mecanismos seguridad pues no es suficiente cualquier seguridad, así mismo se debe tener un data center adecuado con restricciones de acceso a servidores de seguridad y otros.

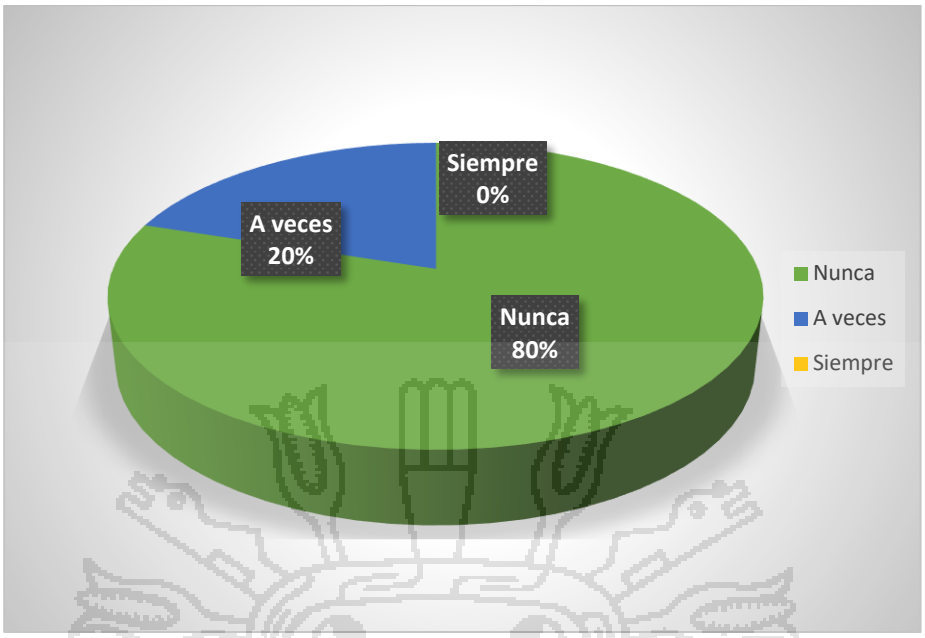


Figura 32. ¿Se autoriza los accesos a la administración de equipos de seguridad?

Pregunta 10.1: ¿Tiene perfiles de acceso a la seguridad de la información?, 100% de encuestados nunca crearon perfiles de acceso a la seguridad de la información, incrementando así el nivel de vulnerabilidad interna y se sigue cometiendo errores de seguridad manteniendo la disponibilidad en peligro.

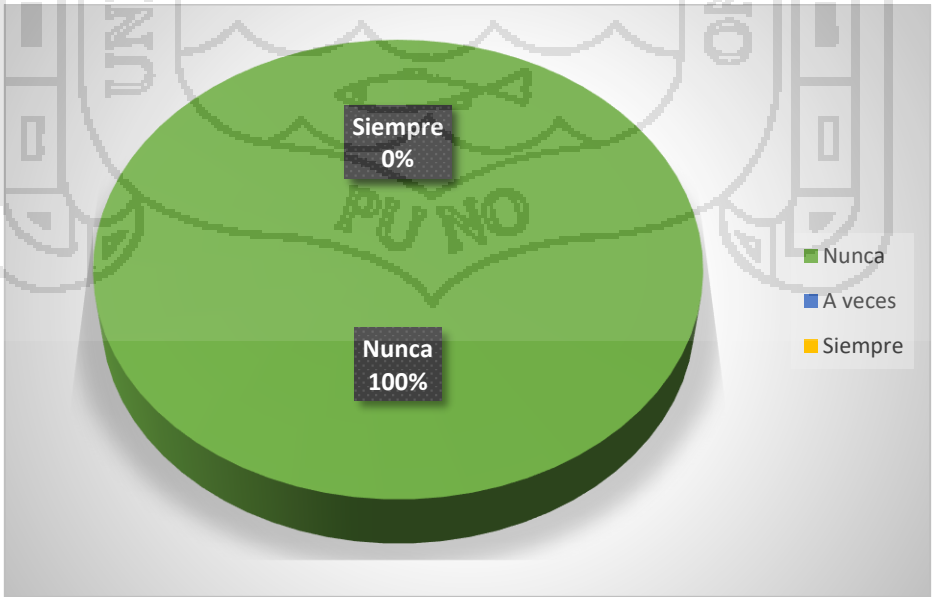


Figura 33. ¿Se autoriza los accesos a la administración de equipos de seguridad?

Pregunta 11: ¿La información ha sido borrada, copiada o alterada?, de los 10 encuestados 60%, considera que A veces la información ha sido borrada, copiada o alterada, ya que no utiliza aplicativos de control e se seguridad, por lo que no tiene datos claros de que su información ha sido dañada en su integridad, por ataques o intromisiones en las redes de comunicaciones, es decir si aplican un mínimo de seguridad, pero esta no es medible. Por lo que un 40%, dice que Siempre encuentra su información dañada, y un 0% Nunca encontró dañada su información.

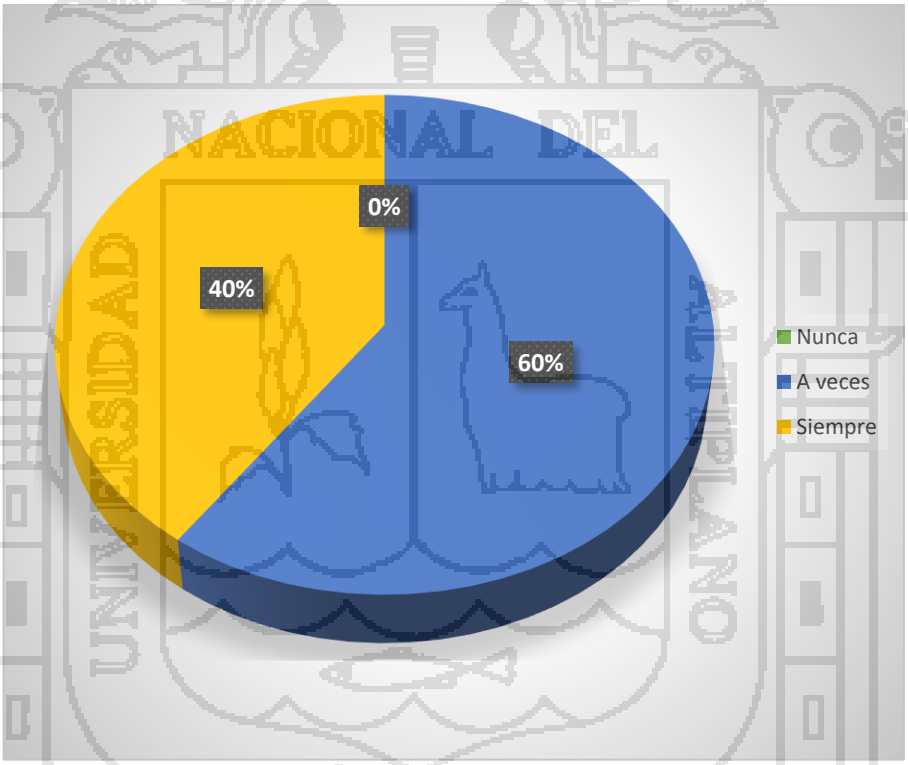


Figura 34. ¿La información ha sido borrada, copiada o alterada**?**

Pregunta 12: ¿La información ha sido accedida por personas no autorizadas para hacerlo?, de los 10 encuestados 70%, mencionan que A veces personas no autorizadas acceden a la información, debido a que no tienen información de accesos, ataques o intromisiones en las redes de comunicaciones, y un 30% que siempre aceden a su información

poniendo en riesgo la confidencialidad de la información. Frente a un 0% que nunca ha expuesto su información.

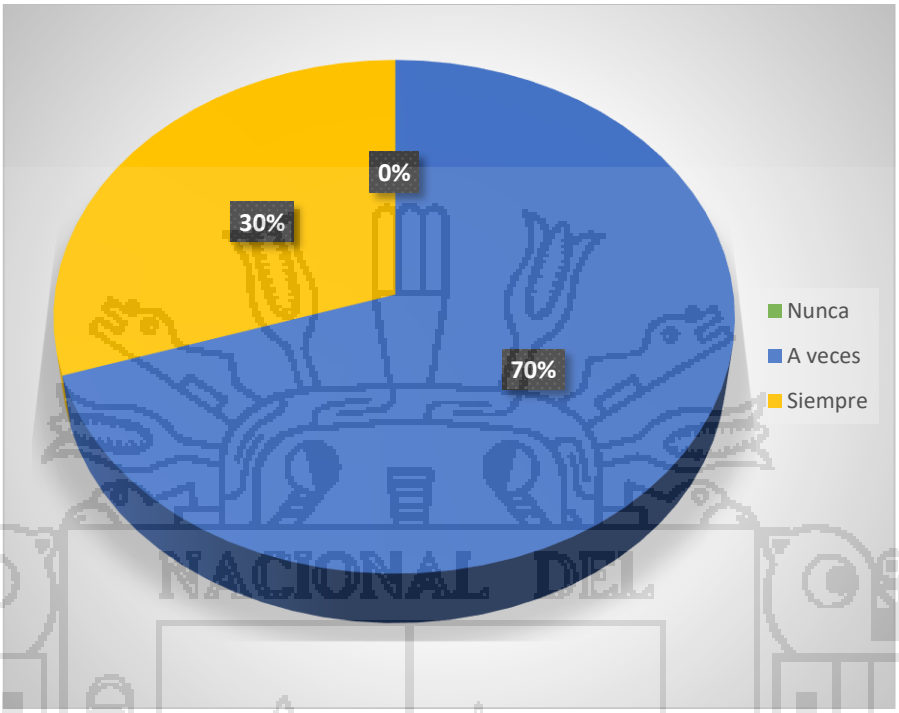


Figura 35. ¿La información ha sido accedida por personas no autorizadas para hacerlo?

Pregunta 13: ¿Verifica la autenticidad de la información?, de los 10 encuestados 100%, nunca verifica a autenticidad de la información, deduciendo que no existe la garantía de autenticidad de los documentos existentes ni de cualquier información. Frente a un 0% que siempre revisa la autenticidad de sus archivos o documentación, incumpliendo con una de los requisitos de calidad de seguridad de la información. Así mismo un 0% que Siempre realiza la evaluación de autenticidad de sus archivos y documentos.

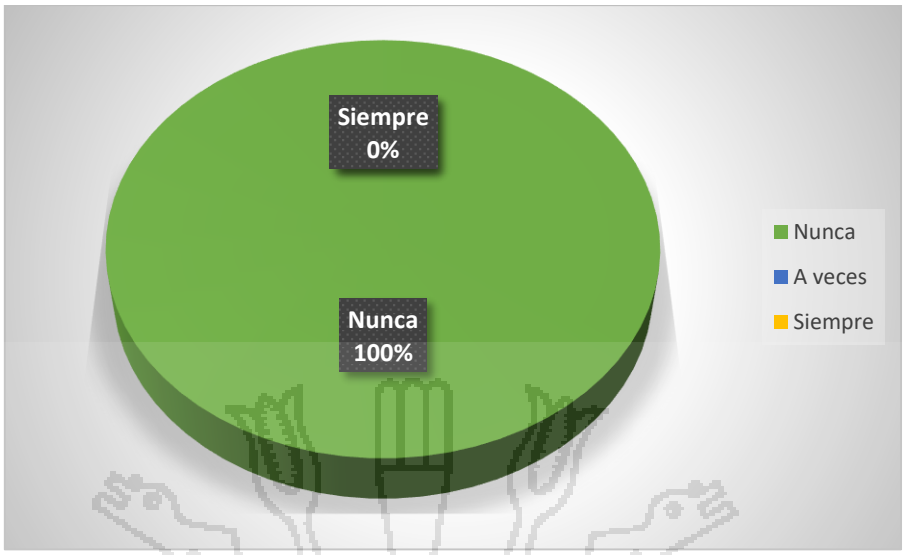


Figura 36. ¿Verifica la autenticidad de la información?

Pregunta 14: Marque el presupuesto anual en soles S/. que considere pertinente, De los 10 encuestados el 80% de las instituciones consideran en su presupuesto de 0 a 5000 S/. como monto de mantenimiento de los servicios de seguridad, de los cuales son considerados de muy baja importancia es decir no previenen la seguridad casi todo el año.

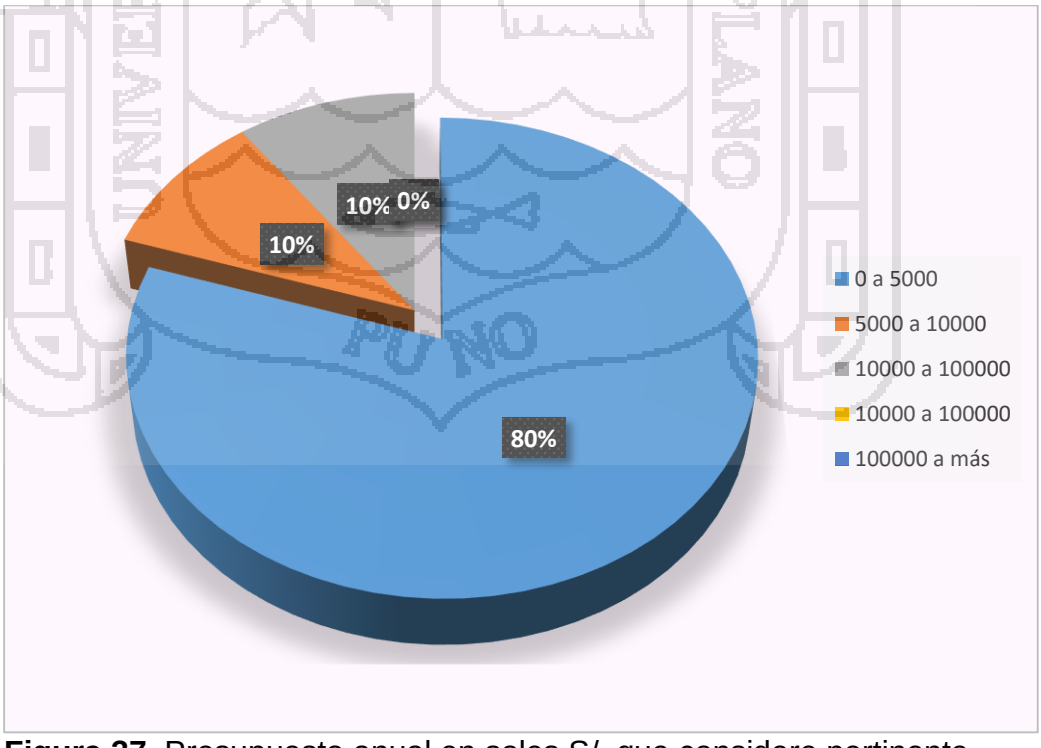


Figura 37. Presupuesto anual en soles S/. que considere pertinente

Pregunta 15: ¿Qué herramientas de seguridad aplican en la red de comunicaciones que administra?, Marque todas las que considere., de los 10 encuestados el 90%, considera al Antivirus como una de las herramientas infaltables en la seguridad, el 50% de las instituciones consideran la solución de seguridad en la aplicación del firewall, el 40% aplica como alternativo o juntamente con el proxy, los IDS es decir los sistemas de detección de intrusos, con 0%, al igual que el monitoreo de red en un 0% por desconocimiento, y otros en un 100%, de ello tenemos alternativos como son herramientas de seguridad como por ejemplo detector de malware, spam y ninguno menciona el algoritmo de wavelet ni redes neuronales.

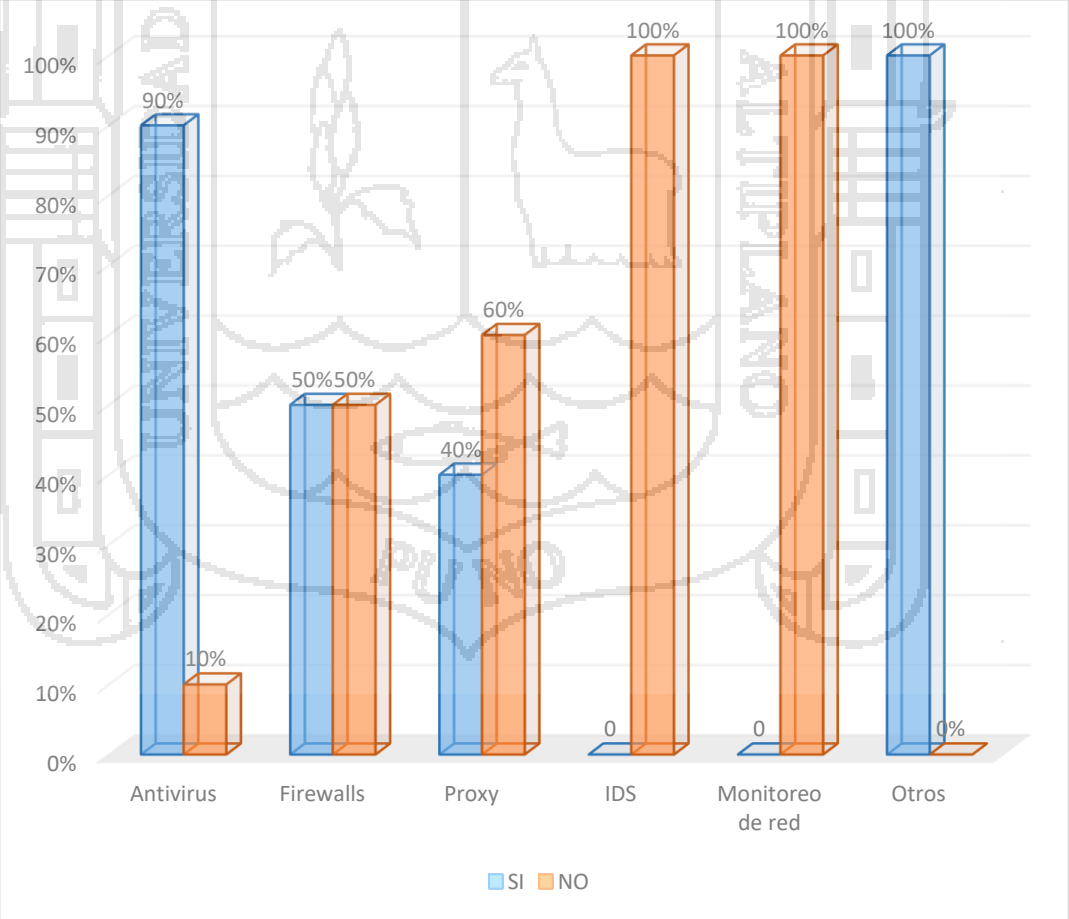


Figura 38. ¿Qué herramientas de seguridad aplican en la red de comunicaciones que administra?

4.3 IMPLEMENTAR UN PROTOTIPO DE ALGORITMO WAVELET

El proceso de implementación se prolongó debido a la implementación del módulo virtualizado, herramienta fundamental para el proceso de implementación y pruebas de detección de intrusos con su herramienta transformada de wavelet y tres neuronas.

4.3.1 Evaluación de la transformada de wavelet

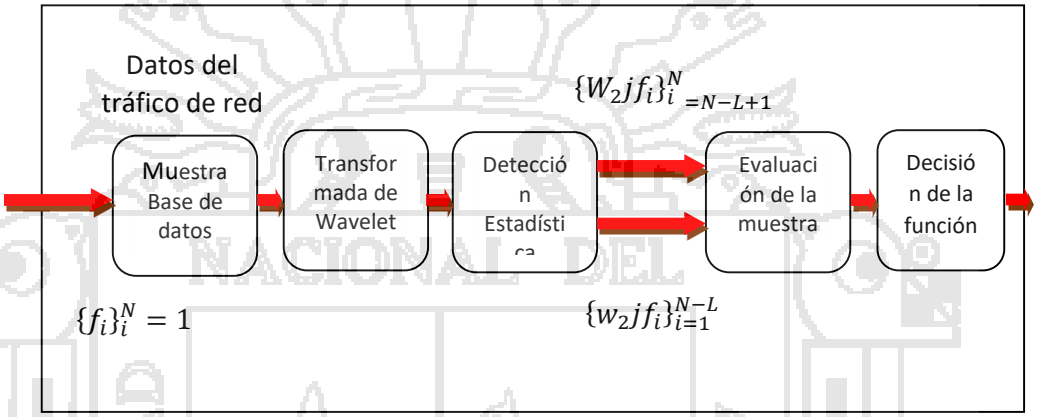


Figura 39. Arquitectura de proceso de transformada de wavelet
Fuente: (Alarcón & Barria, 2001)

En el trabajo de investigación se utilizó la muestra o base de datos de vulnerabilidades, recogidos al momento de simular de los ataques de red de comunicaciones, obteniendo información de tráfico de red de comunicaciones, utilizado como muestra de análisis para el algoritmo wavelet neuronal, que al ser analizada se transformará en datos de entrada multinivel.

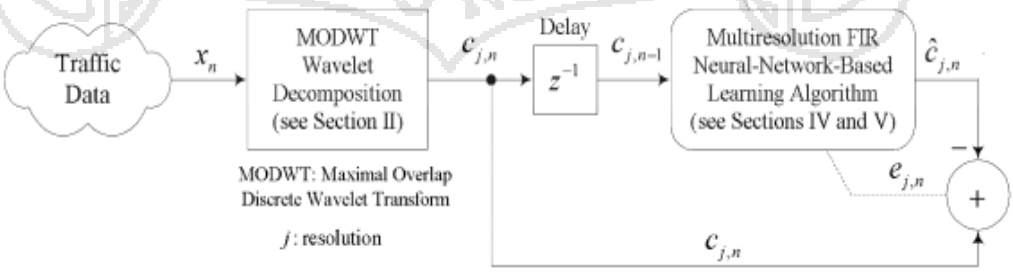


Figura 40. Esquema de detección de ataques por red neuronal wavelet multirresolución
Fuente: (Alarcón & Barria, 2006)

La detección de ataques se inicia con la detección de información del tráfico de red, todo ello se descompone en secciones y como se puede observar en el Figura 40, está la información cuando tiene algún retraso y se analiza en el Delay, para ser resuelta por la transformada de wavelet multiresolución traducida en un algoritmo wavelet de aprendizaje, con la lógica de una red neuronal para detección de ataques de redes de comunicaciones.

4.3.2 Topología de red neuronal wavelet de tres capas

Como se observa la red neuronal está compuesta de tres capas:

- Una capa de entrada, que tiene M nodos.
- Una capa oculta, que compone de un número finito de wavelet representando la Señal.
- Una capa de salida que sólo tiene una neurona cuya salida es la señal representada por la suma ponderada de varias wavelets que emite una respuesta en función.

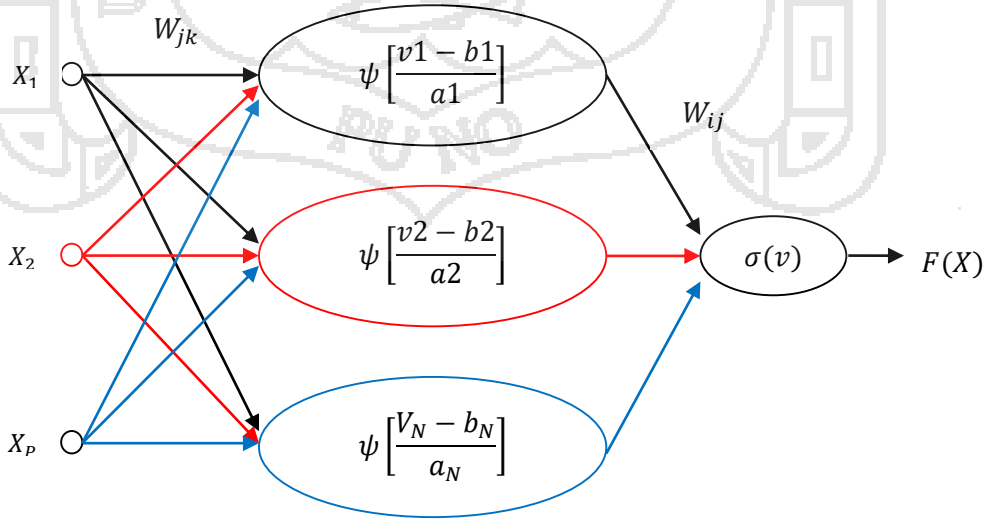


Figura 41. Red neuronal wavelet de tres capas

4.3.2 Cálculos de desarrollo de la red neuronal wavelet

Considerando los siguientes datos:

- $x\,(n)$, Denota la M-1 por -1 vector de entrada externa aplicada a la red.
- $y\,(n)$, Que denota la salida de la red.
- $w_{ji}(n)$, que presenta el peso entre la unidad escondida j y k de la unidad de entrada.
- $W_{ij}(n)$, Denota el peso de conexión entre la unidad de salida i y j , a la unidad escondida.
- (n) y $b(n)$, Representa los coeficientes de dilatación y traslación en las capas ocultas en tiempo discreto n, respectivamente.

La actividad interna neta de la neurona *j* al tiempo *n*, está dada por la siguiente fórmula:

$$v_j(n) = \sum_{k=0}^{k=m} w_{jk}\,(n) * x_k(n)$$

Dónde:

- $v_j(n)$, es la suma de las iteraciones de j y k neuronas ocultas.
- $x_k(n)$, k, es el momento de entrada n.

La salida de la neurona j se calcula pasando $v_j(n)$ a través del wavelet: $\boldsymbol{\psi_{a,b}}(.)$;

Dónde:

$$\psi_{a,b}\big[v_j(n)\big] = \psi[(v_j(n) - bj(n))/(aj(n))]$$

La suma de los resultados a la salida de la neurona es obtenida por:

$$v_j(n) = \sum_{j=0}^{j=N} w_{ij}\,(n) * \psi_{a,b}[v_j(n)]$$

La salida de red es calculada por pasar mediante la función lineal $v(n)$, obteniendo:

$$y(n) = \sigma[v(n)]$$

4.3.4 Algoritmo de aprendizaje de una red neuronal wavelet

La suma breve de error al cuadrado en el tiempo n , siendo:

$$E(n) = \frac{1}{2}e^2(n) = \frac{1}{2}[y(n) - d(n)]^2$$

Dónde:

$D(n)$, Se denomina la respuesta deseada de salida n; el método de salida que utiliza normalmente para minimizar el tiempo por encima de la función.

El peso entre la unidad escondida j y k de la unidad de entrada puede ser ajustado según:

$$\Delta w_{jk}(n+1) = -\eta * \frac{\partial \mathrm{E}(n)}{\partial w_{jk}(n)} + \mu * \Delta w_{jk}(n)$$

$$= -\eta * e(n) * \sigma[v(n)] * w_{ij}\,(n) * \psi_{a,b}\left[v_j(n)\right] * \frac{x_k(n)}{a_{i(n)}} + \mu * \Delta w_{jk}(n)$$

Dónde:

$\eta =$ Es una tasa de aprendizaje y I es el peso de la conexión entre la unidad de salida y la unidad oculta i y j, que se actualizan como sigue:

$$\Delta w_{ij}(n+1) = -\eta * \frac{\partial \mathrm{E}(n)}{\partial w_{ij}(n)} + \mu * \Delta w_{ij}(n)$$

$$= \eta * e(n) * \sigma[v(n)] * \psi_{a,b}\left[v_j(n)\right] + \mu * \Delta w_{ij}(n)$$

El coeficiente de traslación de la capa oculta puede ajustarse según:

$$\Delta b_j(n+1) = -\eta * \frac{\partial E(n)}{\partial b_j(n)} + \mu * \Delta b_j(n)$$

$$= -\eta * e(n) * \sigma[v(n)] * w_{ij}(n) * [v_{j(n)}] * \frac{1}{a_{j(n)}} + \mu . \Delta b_j(n)$$

El coeficiente de dilatación de la capa oculta se actualiza como sigue:

$$\Delta a_j(n+1) = -\eta * \frac{\partial \mathrm{E}(n)}{\partial a_j(n)} + \mu * \Delta a_j(n)$$

$$= -\eta * e(n) * \sigma[v(n)] * w_{ij}(n) * \psi_{\mathrm{a},b} \quad [v_{j(n)}] * \frac{v_j(n) - b_j(n)}{a_j(n)^2} + \mu . \Delta \mathrm{a}_j(n)$$

Las funciones de wavelets que pueden usarse son:

- Función morlet: $\Psi(x) = \cos(1.75) * exp^{(-x2/2)}$
- Función wavelet sombrero mexicano: $\Psi(x) = (1 - \mathrm{x\text{^}2}) * \exp(-\mathrm{x\text{^}2/2})$

4.3.3 Implementación del algoritmo wavelet

Paso 1.-

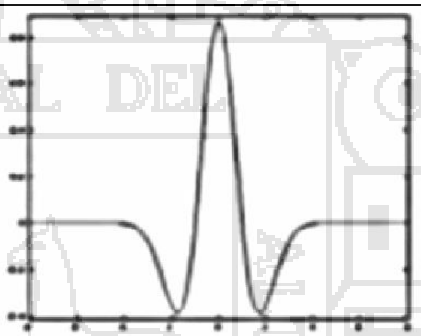
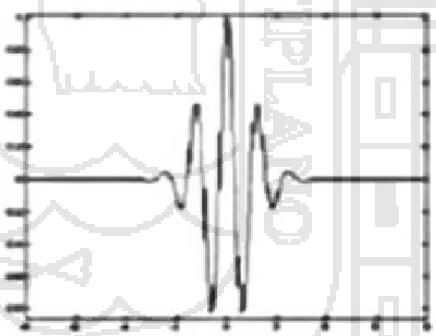
Análisis: Para la elaboración del algoritmo se elige 2 funciones wavelet por lo que mostraremos el siguiente cuadro las propiedades de cada wavelet elegida:

Cuadro 8. Funciones Wavelet.

Familia	Ortogonalidad	Simetría	Momentos de Desvanecimiento	Datos extras
Sombrero mexicano	Si	Si	1	Segunda derivada de la función de Probabilidad Gaussiana
Morlet	Si	Si	1	Primera Wavelets madre

Fuente: (Abarca et al, 2015)

Cuadro 9. Gráfica de las funciones wavelet

Familia	Abreviatura	Función Característica
Sombrero mexicano	Mexh	
Morlet	Morl	

Fuente: (Abarca et al, 2015)

Se elige:

- El wavelet Sombrero mexicano por ser una función de probabilidad y
- La función Morlet por ser una de las primeras Wavelets madres neuronales, así mismo cumplen con criterios de ortogonalidad, Simetría, con momentos de desvanecimientos en menor cantidades como es una única vez.

Paso 2.- Desarrollo

Se realizó el algoritmo con las funciones morlet y sombrero mexicano con la siguiente sintaxis para las dos funciones a ser entrenadas:

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%cálculo de wavelet morlet y salida de wavelet con sombrero mexicano
  for p=1:P
for j=1:n
u=net(p,j);
                  u=(u-b(j))/a(j);
phi(p,j)=cos(1.75*u)*exp(-u*u/2); % wavelet morlet
                  %phi(p,j)=(1-u^2)*exp(-u*u/2); %wavelet sombrero mexicano
end
end
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

Figura 42. Sintaxis del algoritmo para dos funciones wavelet

Paso 3.- Pruebas

Cuadro 10. Datos de entrada

m =1	n =10	N =1
x = 4	5	6
d = 1.3000	3.6000	6.7000

Cuadro 11. Resultados del análisis wavelet en general

W = Columnas 1 Filas 8							
0.4070	0.7487	0.8256	0.7900	0.3165	0.5341	0.0900	0.1117
Columnas 9	Filas 10						
0.1363	0.6786						

Cuadro 12. Resultados de wavelet de morlet y sombrero mexicano

WWW =	0.4952	0.8154
	0.1897	0.8790
	0.4950	0.9889
	0.1476	0.0005
	0.0550	0.8654
	0.8507	0.6126
	0.5606	0.9900
	0.9296	0.5277
	0.6967	0.4795
	0.5828	0.8013

Cuadro 13. Resultados de las detenciones de ataques

a=									
1	1	1	1	1	1	1	1	1	1

Name	Value
a	[1 1 1 1 1 1 1 1 1 1]
b	[0.3000 0.6000 0.9000 ...
d	[1.3000;3.6000;6.7000]
delta	1
epo	100
epoch	1
err	0.0100
error	0.0500
j	1
k	2
lin	0.7000
m	2
n	10
N	1
p	1
P	3
u	1.9807
W	[0.4070 0.7487 0.8256 ...
WW	*10x2 double*
x	[4;5;6]

Figura 43. Datos de simulador

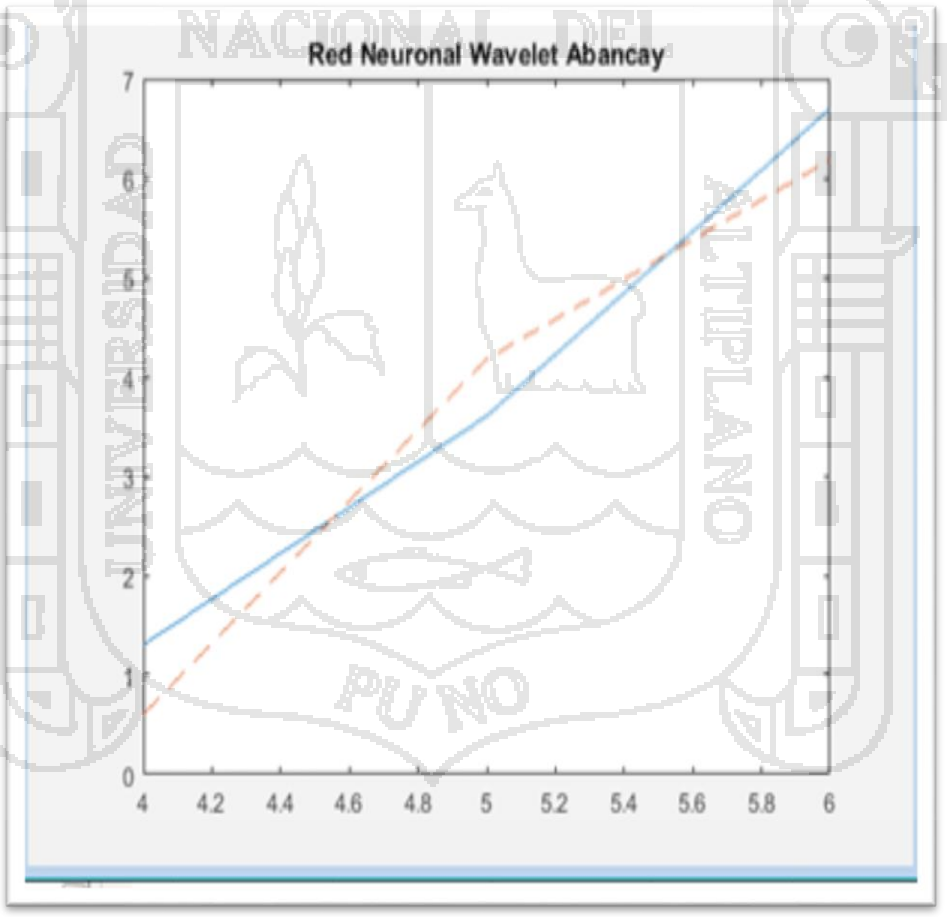


Figura 44. Frecuencia de ataques de red detectados mediante el algoritmo wavelet con funciones de morlet y sombreo mexicano en diversos tiempos.

De la figura 44. Se deduce que la línea de la frecuencia de ataques es más consistente, a mayor tiempo de entrenamiento de las funciones de wavelet, de ello se desprende la línea de color azul siendo una función ortogonal.

Paso 4.- Resultados: Se realizó las diferentes pruebas en los cuales mostro los siguientes resultados.

Cuadro 14. Resultado de las pruebas del algoritmo wavelet en la detección de ataques.

Test	Cantidad de Detecciones	% Detectados
Test1	1	19.52%
Test2	2	80.98%
Test3	3	96.19%
Test4	4	100.00%
Test5	4	100.00%
Test6	1	80.00%
Test7	1	87.14%
Test8	2	97.62%
Test9	2	99.52%
Test10	3	100.00%

4.4 GESTIÓN DE SEGURIDAD CON EL ALGORITMO WAVELET PARA LA DETECCIÓN DE ATAQUES DE LAS REDES DE COMUNICACIONES.

La gestión de seguridad cumple parámetros de medida como son requisitos de declaración de aplicabilidad, según el cuadro adjunto:

Cuadro 15. Declaración de aplicabilidad del algoritmo wavelet

Tipo de declaración de aplicabilidad	Etapas	Acciones
Gestión de Vulnerabilidades	Control de Vulnerabilidades	Aplica información oportuna a cerca de las vulnerabilidades técnicas, en el algoritmo.
	Mecanismo	Test de Algoritmo Wavelet de detección de ataques de seguridad.
	Informe de Análisis de Gestión	El algoritmo wavelet permite determinar la cantidad de detecciones de ataques de seguridad y porcentajes de las mismas.
Gestión de riesgo	Evaluación de Riesgos	Mitigar las detenciones de ataques mediante el algoritmo wavelet

Fuente: (Alexander, 2007).

La evaluación de la gestión requiere del cumplimiento de requerimientos de aplicabilidad del algoritmo wavelet en vista del cumplimiento del mismo mediante la gestión de vulnerabilidades. Se realizó la evaluación de gestión de seguridad.

Cuadro 16. Evaluación de gestión de seguridad

Nivel	Gestión de seguridad	% de Eficacia
Nivel 0	Nulo	0
Nivel 1	Inicial	20
Nivel 2	Repetible	40
Nivel 3	Definido/Establecido	60
Nivel 4	Gestionado/Medible	80
Nivel 5	Optimizado	100

Fuente: (ISO/IEC, 2016)

Cuadro 17. Asignación de Nivel de Gestión de seguridad de redes de comunicaciones de algoritmo wavelet

Tipo de Seguridad	Nivel de gestión	Calidad
Algoritmo Wavelet	Gestionado o medible	80%

Del presente cuadro ubicaríamos la implementación del algoritmo wavelet neuronal como un mecanismo de seguridad Gestionado y Medible, en vista que es factible determinar las detecciones de ataques en seguridad en las redes de comunicaciones y al mismo tiempo reducir la incidencia de los ataques del cual tendríamos mayor información al ser cuantificado. Por lo que se estaría alcanzando el Nivel 4, obteniendo un 80% del cumplimento en la gestión de seguridad en redes de comunicaciones, frente a un 0%, del Nivel 1 hasta el nivel 3, con un 60% de eficiencia.

4.5 DISCUCIÓN

Según Según Botello (2010) se implementa un sistema de detección de intrusos (IDS) portable que hace uso de la base de datos de firmas de

Snort, que es un sistema de detección de intrusos creado por Martin Roesch, que monitorea el tráfico dentro de un segmento de red, ofrece características como análisis y filtrado de paquetes en tiempo real, monitoreo de puertos y análisis de protocolos, detectando intrusiones, el cual si bien es cierto detecta intrusiones en puertos establecidos no terminaríamos de configurar este sistema que es muy bueno para brindar seguridad incluso en dos modalidades como es IDS internos y IDS externos, pero si implantamos el algoritmo wavelet que con la función Morlet y fución sombreo mexicano a la vez brinda una poderosa detección de manera que podamos entrenarla mediante redes neuronales en la tarea de detección de ataques diversos, que se presenten en cualquier puerto; Así mismo el trabajo de Botello (2010), de Bai & Kobayashi (2003), engel et al., (2006), de no realiza una evaluación del nivel de gestión de seguridad que garantice la Confidencialidad, Integridad y Disponibilidad al 80%, según el cuadro de gestión de seguridad.

CONCLUSIONES

- Se logró identificarlos tipos de ataques más comunes en redes de comunicaciones en Abancay 2016 y sus modos de infiltración simulando alguno con la finalidad determinar puertos vulnerables.
- Se diseñó mecanismos de detección de ataques seguridad de redes de comunicaciones, observando que para un detector de escaneos de puertos es imposible desligar la cantidad y la temporalidad, ya que son elementos complementarios y que ignorar cualquier puerto o malinterpretarlo generaría una gran cantidad de falsos negativos o positivos en la detección propuesta y permite obtener una tasa del 60% al 80% de anomalías en los paquetes.
- Al Implementar el prototipo de algoritmo Wavelet, se aplicó dos funciones wavelet sombrero mexicano y wavelet de morlet, en una función principal de red neuronal de 3 capas, lo que permite entrenar las detecciones de ataques de seguridad.
- El algoritmo de wavelet, en detección de ataques de las redes de comunicaciones, nos permite aumentar la seguridad en casi un 80%, debido la aplicabilidad en gestión de seguridad siendo medible, así mismo

uso esta técnica ahorra tiempo de reacción según la frecuencia de ocurrencia para detectar y predecir posibles, ataques en una red y no estar expuestos a prueba de fallos cumpliendo el estándar de gestión de seguridad de comunicaciones.

- Se tomó en cuenta la gestión de seguridad de redes de comunicaciones y tener un horizonte definido en cuestiones de seguridad aplicar estándares de seguridad de redes de comunicaciones, como ISO 27002 que conlleven a una seguridad máxima, la garantizar la operatividad, y seguridad de la información.
- Los administradores de red de comunicaciones de la ciudad de Abancay tomaron conciencia en un 100% de lo implica tener un alto nivel de gestión de seguridad.

RECOMENDACIONES

- Realizar nuevos algoritmos wavelets con funciones de Haar, Daubechies u otros como también con funciones como Gabor para incrementar la seguridad en redes de comunicaciones.
- Diseñar sistemas de gestión seguridad capaces de reaccionar a prueba de fallos y alcanzar buenos niveles de seguridad cumpliendo estándares que incluyan buenas prácticas de políticas de seguridad, incidiendo en mayor inversión en la misma.
- Aplicar funciones wavelet en diversos campos de la tecnología de señales o frecuencias e imágenes, debido a la potencia que esta implica, detecta determinadas señales anómalas en diversos espacios, por ejemplo, en área de salud, detectando paros cardiacos atreves de señales, detección de enfermedades según imágenes o frecuencias, y si incluimos alguna neurona de aprendizaje podría entrenar para detectar con mayor precisión.

BIBLIOGRAFÍA

Abarca, Y., Calle, D., Castillo, M., Guayllas, J., Narváez, E., Narváez, I., y otros. (2015). Transformada Wavelet aplicada en imágenes. *Señales y Sistemas G 3, Universidad Politecnica Saleciana* .

Aguilar, D. R. (2008). Redes Neuronales Redes Neuronales. *Revista de Información, Tenologica y Sociedad*.

Alarcón, V, & Barria, J. (2001). Anomaly detection in communication networks using wavelets. *Dept. of Electr. & Electron. Eng*.

Alarcón, V., & Barria, J. (2006). Multiresolution FIR neural-network-based learning algorithm applied to network traffic prediction. . *Mexico: Dept. of Electr. & Electron. Eng., Univ. de las Américas-Puebla* .

Aldea , Q., & Ruiz, F. (1997). *El Cardenal Infante Don Fernando o la Fomación de un Principe de España.* España: Real Académia de la Historia.

Alexander, A. (2007). *Diseño de un sistema de gestión de seguridad de información.* Bogotá: Alfaomega.

Bai, Y., & Kobayashi, H. (2003). Intrusion Detection Systems: Technology and development. *Proceedings of the 17th International Conference on Advanced Information Networking and Applications (* (pág. 710). Washington: IEEE Computer: IEEE Computer.

Bestuzhev, D. (2015). Nadie está seguro en Internet: Las cifras del cibercrimen en América Latina. *Perú21*.

Botello, P. (2010). Modelado de un sistema detección de intrusos. México: Universidad las Américas de puebla: Departamento de computación electrónica y mecatrónica.

Cano, J. (2009). *Computación forense.* Bogotá: Alfaomega.

Cert. (2017). *Carnegie Mellon University's Computer Emergency Response Team. CERT Statistics.* Obtenido de www.cert.org/stats

Cto, J. (2017). Software de Seguridad Cibernética, B2B / Enterprise. *Simarkssoftware*.

Daugman, J. G. (1988). *Complete Discrete 2-D Gabor Transforms by Neural* (Vol. 36). Cambridge, Harvard: IEEE TRANSACTIONS ON ACOUSTICS, SPEECH, AND SIGNAL PROCESSING.

Denning, D. (1987). An Intrusion-Detection Model. *IEEE Transaction Software Engineering*.

Engel, E., Kutil, R., & Uhl, A. (2006). Un ataque de transformación simbólica en el cifrado simple basado en la parametrización del analisis Wavelet. Austria.

Enguita, J. M. (2004). *Redes.* España: Universidad de Oviedo, Ingeniería de Sistemas y Automática.

Gómez Vieites, Á. (2014). Tipos de Ataques e Intrusos en las Redes Informáticas. *Edisa*, 10-11.

Hagan, T., Demuth, H., & Beale, M. (1996). Neural Network Desig. China: CITIC Publishing House.

Hernacki, B., & Bennett, J. (2009). Detecting network evasion and misinformation. *Symatec Corporation*, 1-2.

Householder, A. (2016). A Wavelet Perspective on the Allan Variance. *USA: Software Engineering Institute. IEEE Trans Ultrason FerroelectrFreq Control*.

Iana. (2017). *Registro de Nombres de Servicio y Protocolo de transporte. Número de puerto*. Obtenido de https://www.iana.org

ISO/IEC. (2016). *Organización International de Estandardizaión*. Obtenido de ISO27000: https://www.iso.org/ Y http://www.iso27000.es/

Jaime, G., & Vanegas, C. (2006). La seguridad en las redes de comunicaciones. *Udistrital. Centro de investigaciones y desarrollo científico*.

Kim, I., Karuppanchetty, C., Edmonds, W., & Nwanz, N. (2015). Artificially Augmented Training for Anomaly-based Network Intrusion Detection Systems.

Kouro, S., & Musalem, R. (2002). Tutorial introductorio a la Teoría de Wavelet. *Técnicas modernas en Automatica*, (págs. 2-3).

Kukielka, P., & Kotuslki, Z. (2008). Analysis of different architectures of neural networks for application in Intrusion Detection Systems. *International Multiconference on Computer Science and Information Technology*, (págs. 807-811).

López, J. (Octubre de 2004). *Wavelets.* Madrid: Departamento de Física Atómica, Molecular y Nuclear, Universidad Complutense.

Lozano, I., Ballesteros, B., Lozano, K., & Salas, I. (2000). Seguridad en la Red.

Merino, C., & Cañizares, R. (2011). Implantación de un sistema de gestión de seguridad de la información según ISO 27002. Madrid: Fundación CONFEMETAL.

Oppliger, R. (1997). Firewall and beyond. Communications of they ACM. *Internet security*.

Oussar, Y., & Reyfus, G. (2000). Initialization by Selection for Wavelet Network Training. *France Paris: Laboratoired Électronique.*

Pastrana, S., Orfila, A., & Ribagorda, A. (2000). Modeling NIDS evasion with Genetic programming. Madrid: IT security group.

Pati. (1992). Orthogonal Matching Pursuit: Recursive Function Approximation with Applications to Wavelet Decomposition.

Ptacek, T., & Newsham, T. (1998). *Insertion, evasion and denial of service: eluding network intrusion detection.* Belvoir: IATAC Information Assurance Technology Analysis Center.

Ramos, A., Barbero, C., Gonsalez, J., Picouto, F., & Serrano, E. (2015). *Seguridad perimetra, monitorizacion y ataques en redes* (Vol. 1). Colombia, Bogota: Ra-ma.

RedIRIS. (2016). *Red académica y de investigación que conecta la I+D+i*. Obtenido de http://www.rediris.es

Román, E. (2004). Wavelets. Centro de Geociencia, UNAM.

Segev, A, Gebauer, J., & Beam, C. (1998). Impact Of The Internet On Procuredmend.

Sheffi, Y. (2005). The resilient Enterprise. Cambridge: M.I.T Pres.

Thuillard, M. (2002). A review of wavelet networks, wavenets, fuzzy wavenets and their applications. Proceeding Advances in Computational Intelligence and Learning: Methods and Applications., (págs. 43-60). Deventer.

Watkins, M., & Wallace, K. (2008). CCNA Security official exam certification guide. Indianapolis, indiana, united states of America: Cisco Press.

Yu, L., Chen, B., & Xiao, J. (2007). An Integrated System of Intrusion Detection Based on Rough Set and Wavelet Neural Network. Third International Conference on Natural Computation.

Zhang, Q. (1992). *Wavelet networks.* IEEE transactions on neuronal networks.

ANEXOS

Anexo 1. Algoritmo Wavelet Neuronal

```
%%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%

clear all

%iniciar de datos

P=3 %Número de muestra

m=4 %Número de nodo de entrada

n=10%Número de nodo oculto

N=1 %Número de formato de nodo

%

% a(n) b(n) Escala y cambio de la matriz de parámetros

%x(P,m) Matriz de entrada muestra P

%net(P,n) Salida del nodo oculto

%y(P,N) Salida de red

%d(P,N) de la red de salida ideal

% phi(P,n) de salida función wavelet nodo oculto

% W(N,n)El valor del peso entre la salida y oculto

% WW(n,m) peso valor entre oculto y nodo de entrada

x=[4;5;6]

d=[1.3;3.6;6.7]

W=rand(N,n)

WW=rand(n,m)

a=ones(1,n)

for j=1:n

b(j)=j*P/n;
```

```
end

%%%%%%%%%%%%%%%%%%

%EW(N,n) gradiente de W

%EWW(n,m) gradiente de WW

%Ea(n) gradiente de a

%Eb(n) gradiente de b

%%%%%%%%%%%%%%

epoch=1;

epo=100;

error=0.05;

err=0.01;

delta =1;

lin=0.7;

while (error>=err&epoch<=epo)

   u=0; %u es la variante intermedia

   %cálculo de entrada neta (sin ataques)

   for p=1:P

for j=1:n

u=0;

for k=1:m

u=u+WW(j,k)*x(p,k);

end

net(p,j)=u;

end
```

```
end

    %cálculo de wavelet morlet y salida de wavelet con sombrero mexicano

        for p=1:P

for j=1:n

u=net(p,j);

                u=(u-b(j))/a(j);

phi(p,j)=cos(1.75*u)*exp(-u*u/2); % wavelet morlet

                %phi(p,j)=(1-u^2)*exp(-u*u/2); %wavelet sombrero mexicano

end

end

    %cálculo de la obtención de red

       for p=1:P

for i=1:N

u=0;

for j=1:n

                u=u+W(i,j)*phi(p,j);

end

y(p,i)=delta*abs(u);

end

end

      %cálculo de error en la salida

u=0;

for p=1:P

for i=1:N
```

```
%u=u+abs(d(p,i)*log(y(p,i))+(1-d(p,i)*log(1-y(p,i))));

u=u+(d(p,i)-y(p,i))^2;

end

end

%u=u/2

error=u;

    % cálculo de la gradiente de red

for i=1:N

for j=1:n

        u=0;

for p=1:P

u=u+(d(p,i)-y(p,i))*phi(p,j);

end

EW(i,j)=u;

        %EW(i,j)=-u;%el resultado sería erróneo

end

end

for j=1:n

for k=1:m

        u=0;

for p=1:P

for i=1:N

            u=u+(d(p,i)-y(p,i))*W(i,j)*phi(p,j)*x(p,k)/a(j) ;

end
```

```
end

EWW(j,k)=u;

%EWW(j,k)=u el resultado sería erróneo

end

end

for j=1:n

        u=0;

for p=1:P

for i=1:N

        u=u+(d(p,i)-y(p,i))*W(i,j)*phi(p,j)/a(j) ;

end

end

Eb(j)=u;

end

for j=1:n

        u=0;

for p=1:P

for i=1:N

        u=u+(d(p,i)-y(p,i))*W(i,j)*phi(p,j)*((net(p,j)-b(j))/b(j))/a(j);

end

end

Ea(j)=u;

end

   %ajustes del valor de peso
```

```
        WW=WW-lin*EWW;
            W=W-lin*EW;
            a=a-lin*Ea;
        b=b-lin*Eb;
        %número de epoch aumentaría en 1
        epoch=epoch+1;
        end
        plot(x,d,x,y,'--');
title ('Red Neuronal Wavelet Abancay')
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

Anexo 2. Puertos y protocolos autorizados y registrados

Cuadro 18. Puertos y protocolos utilizados por los servidores y clientes

Puerto	Protocolo	Nota
5060/5061	TCP MTLS	Los usan los servidores Standard Edition y los grupos de servidores Enterprise para todas las comunicaciones SIP internas entre los servidores y entre los servidores y Office Communicator.
443	HTTPS	Se utiliza para la comunicación entre los servidores front-end y los FQDN de la granja de servidores web (direcciones URL utilizadas por los componentes web).
444	HTTPS	Se utiliza para la comunicación entre el foco (componente de Office Communications Server que administra el estado de la conferencia) y los servidores de conferencia.
80	TCP	Se utiliza para la comunicación entre los servidores front-end y los FQDN de la granja de servidores web (direcciones URL utilizadas por los componentes web) cuando no se utiliza HTTPS.
135	DCOM y llamada a procedimiento remoto (RPC)	Se utiliza cuando se implementa un equilibrador de carga front-end. Los servidores front-end usan el puerto 135 para las operaciones de Instrumental de administración de Windows (WMI) y para trasladar a los usuarios (operaciones remotas de bases de datos basadas en DCOM).
5062	TCP	Se utiliza para las solicitudes de escucha SIP entrantes de las conferencias de mensajería instantánea.
5063	TCP	Se utiliza para las solicitudes de escucha SIP entrantes de las conferencias de audio y vídeo (A/V).
5064	TCP	Se utiliza para las solicitudes de escucha SIP entrantes de las conferencias telefónicas.
5065	TCP	Se utiliza para las solicitudes de escucha SIP entrantes para compartir las aplicaciones.
5069	TCP y MTLS	El agente QoE los usa en el servidor front-end.
5071	TCP	Se utiliza para las solicitudes de escucha SIP entrantes del servicio de grupo de respuesta.
5072	TCP	Se utiliza para las solicitudes de escucha SIP entrantes del operador de conferencia.
5073	TCP	Se utiliza para las solicitudes de escucha SIP entrantes del servicio de anuncio de conferencia.
5074	TLS	Se utiliza para las solicitudes de escucha SIP entrantes del control de voz externa.
8057	TLS	Se utiliza para escuchar las conexiones del Modelo de objetos compartidos persistentes (PSOM) directas desde un cliente de Microsoft Office Live Meeting 2007.
8404	TLS	Se utiliza para las comunicaciones de servidor internas (comunicación remota sobre MTLS) del servicio de grupo de respuesta.
49152-65335	Protocolo de datagramas de usuario (UDP)	Se utilizan para el intervalo de puertos de medios.
5060/5061	TCP MTLS	Los usan los servidores Standard Edition y los grupos de servidores Enterprise para todas las comunicaciones SIP internas entre los servidores y entre los servidores y Office Communicator.

443	HTTPS	Comunicación desde los servidores front-end a los FQDN de la granja de servidores web (direcciones URL utilizadas por los componentes web).
444	HTTPS	Comunicación entre el foco (componente de Office Communications Server que administra el estado de la conferencia) y los servidores de conferencia.
135	DCOM y RPC	Se utiliza cuando se implementa un equilibrador de carga front-end. El puerto 135 lo utilizan los servidores front-end para las operaciones WMI y para trasladar a los usuarios (operaciones remotas de bases de datos basadas en DCOM).
5065	TCP	Se utiliza para las solicitudes de escucha SIP entrantes para compartir las aplicaciones.
5069	TCP	El agente QoE los usa en los servidores front-end.
5071	TCP	Se utiliza para las solicitudes de escucha SIP entrantes del servicio de grupo de respuesta.
5072	TCP	Se utiliza para las solicitudes de escucha SIP entrantes del operador de conferencia.
5073	TCP	Se utiliza para las solicitudes de escucha SIP entrantes del servicio de anuncio de conferencia.
5074	TLS	Se utiliza para las solicitudes de escucha SIP entrantes del control de voz externa.
80	HTTP	Se utiliza si no se ha configurado HTTPS.
88	Kerberos	Se utiliza para la autenticación Kerberos.
389	LDAP	Se utiliza para el Protocolo ligero de acceso a directorios en el controlador de dominio.
443	HTTPS	HTTP sobre TLS o SSL.
3268	MSFT-GC	Se utiliza para LDAP en el catálogo global.
5061	SIP	Se utiliza para el tráfico SIP.
49152 - 65535		Se utiliza para uso compartido de escritorio.
49152-65335	TLS	Se utilizan para que el tráfico de SIP se comunique con servidores Office Communications Server 2007 R2.
443	HTTPS	Se utiliza para la transferencia de archivos segura con el servicio web de conversaciones en grupo.
8010	TLS	Se utiliza para los puertos WCF y de sincronización de los servidores del mismo nivel del servicio de búsqueda.
8011	TLS	Se utiliza para los puertos Windows CommunicationFoundation (WCF) y los puertos de sincronización de los servidores del mismo nivel del servicio de canal.
5041	MTLS	Se utiliza para el puerto de escucha del servicio de canal.
135	MessageQueue Server y RPC	Se utiliza para las operaciones RCP de la cola de mensajes.
135	MessageQueue Server y RPC	Se utiliza para las operaciones RCP de la cola de mensajes.
5060/5061	TCP	Se utilizan para las comunicaciones internas entre los servidores.
5060/5061	TCP	Se utilizan para las comunicaciones internas entre los servidores.
60000-64000	UDP	Se utilizan para el intervalo de puertos de medios.
5061	TCP	Se utiliza para realizar las escuchas.

5060	TCP	Se utiliza para el próximo salto y el puerto de escucha en la puerta de enlace.
443	TCP	Se utiliza en las comunicaciones SIP/TLS procedentes de usuarios externos en el firewall interno y externo para el acceso de usuarios externos.
5061	TCP	Se utiliza en las comunicaciones SIP/MTLS para el acceso de usuarios remotos o la federación.
5062	TCP	Se utiliza para la autenticación SIP/MTLS de los usuarios de audio y vídeo. Las comunicaciones salientes pasan por el firewall interno.
443	TCP	Se utiliza en las comunicaciones SIP/TLS para el acceso de usuarios remotos y el acceso a conferencias web internas, así como en las comunicaciones de medios STUN/TCP entrantes y salientes para el acceso a sesiones A/V y de medios internas.
8057	TCP	Se utiliza para realizar escuchas de las comunicaciones PSOM/MTLS del servidor de conferencia web en la interfaz interna del servidor perimetral de conferencia web.
3478	UDP	Se utiliza para las comunicaciones de medios STUN/UDP entrantes y salientes.
50,000-59,999	RTP/TCP	Se utilizan para las transferencias de medios entrantes y salientes a través del firewall externo.
443	TCP	Se utiliza para los puertos internos en las comunicaciones SIP/TLS para el acceso de usuarios remotos y el acceso a conferencias web internas, así como en las comunicaciones de medios STUN/TCP entrantes y salientes para el acceso a sesiones A/V y de medios internas.
5061	TCP	Se utiliza para los puertos internos en las comunicaciones SIP/MTLS para el acceso de usuarios remotos o la federación.
5062	TCP	Se utiliza para los puertos internos en la autenticación SIP/MTLS del flujo saliente de comunicaciones de mensajería instantánea a través del firewall interno.
3478	UDP	Se utiliza para los puertos internos en las comunicaciones de medios STUN/UDP entrantes y salientes.
443	TCP	Se utiliza para los puertos externos en las comunicaciones SIP/TLS para el acceso de usuarios remotos y el acceso a conferencias web internas, así como en las comunicaciones de medios STUN/TCP entrantes y salientes para el acceso a sesiones A/V y de medios internas.
5061	TCP	Se utiliza para los puertos externos en las comunicaciones SIP/MTLS para el acceso de usuarios remotos o la federación.
3478	TCP	Se utiliza para los puertos externos en las comunicaciones de medios STUN/UDP entrantes y salientes.
5060	TCP (SIP)	Lo usa Office Communicator para las comunicaciones SIP internas.
5061	TCP (SIP)	Lo usa Office Communicator para las comunicaciones SIP internas y para la autenticación SIP/MTLS de los usuarios de audio y vídeo. Las comunicaciones salientes pasan por el firewall interno.
443	TCP (HTTP)	Lo usan los clientes de Communicator que se conectan desde fuera de la intranet para comunicaciones SIP.
1024-65535	UDP/TCP	Intervalo de puertos utilizado para las transferencias de medios entrantes y salientes a través del firewall externo.

6891-6901	TCP	Intervalo de puertos utilizado por Office Communicator para las transferencias de archivos.
443	TCP	Lo usan los clientes de Live Meeting 2007 que se conectan desde fuera de la intranet para: • El tráfico SIP enviado al servidor perimetral de acceso • El tráfico PSOM enviado al servidor perimetral de conferencia web
8057	TCP	Se utiliza para el tráfico PSOM saliente enviado al servidor de conferencia web.
5061	TCP	Se utiliza para las comunicaciones SIP/TLS entre Live Meeting y los servidores front-end o el servidor perimetral de acceso y para la autenticación SIP/MTLS de los usuarios de audio y vídeo. Las comunicaciones salientes pasan por el firewall interno.
1024-65535	UDP/TCP	Intervalo de puertos utilizado para las transferencias de medios entrantes y salientes a través del firewall externo.
6891-6901	TCP	Intervalo de puertos utilizado por Live Meeting para las transferencias de archivos.
5060	TCP (SIP)	Lo usa Communicator Mobile para las comunicaciones SIP internas.
5061	TCP (SIP)	Lo usa Communicator Mobile para las comunicaciones SIP sobre TLS internas.
443	TCP (HTTP)	Lo usa Communicator Mobile para la conexión desde fuera de la intranet en las comunicaciones SIP.

Fuente: Iana, (2016).

Cuadro 19. Puertos usados en los Juegos

Puerto	Denominación
7777	Unreal, KlingonHonorGuard
7778	Unreal
22450	Sin
26000	Quake
26900	Hexen
26950	Hexenworld.
27015	Half-Life,FortressClassic.
27500	QuakeWorld
27910	Quake
28000/08	Starsiege
26900	Hexen
47624	Operation Point
1030	NeedSpeed3
2346	Rainbow
16638/39	Swat
2300	AgesEmpiresII
2350	AgesEmpiresconqueror
2611	Blackwhite.
28910/15	Soldierfortune.
6112	Startcraft658
2400	Everquest,ofEmpires
26214	Dark2

6112	Diablo
666	Doom
23077	Tzar
531	Counter
47624	Battlecom
28910	Herectic
3658	Delta2
6112	Warcraft

Fuente: (Iana, 2016).

Cuadro 20. Puertos usados por Troyanos

Puerto	Denominación
21	BladeRunner, DolyTrojan, Fore, WinCrash.
23	TinyTelnetServer.
25	Antigen, EmailPasswordSender, Haebu
80	Executor.
456	HackersParadise.
555	ni-Kiler, PhaseZero, StealthSpy.
666	SatansBackdoor.
1001	Silencer, WebEx.
1011	DolyTroyan.
1170	PsyberStreamServer, Voice.
1234	UltorsTrojan.
1245	VooDooDoll.
1492	FTP99CMP.
1600	Shivka-Burka.
1807	SpySender.
1981	Shockrave.
1999	BackDoor.
2001	TrojanCow.
2023	Ripper.
2115	Bugs.
2140	DeepThroat, TheInvasor.
2801	PhineasPhucker.
3024	WinCrash.
3129	MastersParadise.
3150	DeepThorat, TheInvasor.
3700	PortalofDoom.
4092	WinCrash.
4590	ICQTrojan.
5321	Firehotcker.
5400	BladeRunner.

5569	Robo-Hack.
5742	WinCrash.
6670	DeepThroat.
6969	GateCrasher, Priority.
7000	RemoteGrab.
7300,7301,7306-7308	NetMonitor.
7789	ICKiller.
9872-9875	PortalofDoom.
9989	iNI-Killer.

Fuente: (Iana, 2016).

Cuadro 21. Puertos más conocidos

Puerto	Denominación
1	TCP Port Service Multiplexer (TCPMUX)
5	Remote Job Entry (RJE)
7	Protocolo Echo (Responde con eco a llamadas remotas)
9	Protocolo Discard (Elimina cualquier dato que recibe)
13	Daytime (Fecha y hora actuales)
17	Quote of the Day (Cita del Día)
18	MessageSendProtocol (MSP)
19	Protocolo Chargen, Generador de caracteres
20	FTP — Datos
21	FTP — Control
22	SSH, scp, SFTP – Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
29	MSG ICP
37	Time
42	Host Name Server (Nameserv)
43	WhoIs
49	Login Host Protocol (Login)
53	DomainNameSystem (DNS)
66	Oracle SQLNet
67	BOOTP (BootStrapProtocol) (Server), también usado por DHCP
68	BOOTP (BootStrapProtocol) (Client), también usado por DHCP

Fuente: (Iana, 2016).

69	Trivial File Transfer Protocol (TFTP)
70	Gopher Services
79	Finger
80	HTTP
88	Agente de autenticación Kerberos
103	X.400 Standard
107	Remote Telnet Service
108	SNA Gateway Access Server
109	POP2
110	POP3
115	Simple File Transfer Protocol (SFTP)
118	SQL Services
119	Newsgroup (NNTP)
123	NTP
137	NetBIOS NameService
138	NetBIOS DatagramService
139	NetBIOS SessionService
143	Internet Message Access Protocol (IMAP)
156	SQL Server
161	SNMP
162	SNMP-trap
177	XDMCP (Protocolo de gestión de displays en X11)
179	Border Gateway Protocol (BGP)
190	Gateway Access Control Protocol (GACP)
194	Internet Relay Chat (IRC)
197	DirectoryLocationService (DLS)
209	Quick Mail Protocol
217	dBASE Unix
389	Lightweight Directory Access Protocol (LDAP)
396	Novell Netwareover IP
443	HTTPS
444	Simple Network Paging Protocol (SNPP)
445	Microsoft-DS (Active Directory, compartición en Windows, gusano Sasser, Agobot)
458	Apple QuickTime
500	IPSec ISAKMP, Autoridad de Seguridad Local
512	Exec
513	Login

514	syslog usado para logs del sistema
515	Printer
520	RIP
522	Netmeeting
531	Conference
546	DHCP Client
547	DHCP Server
563	SNEWS
569	MSN
631	CUPS: sistema de impresión de Unix
666	identificación de Doom para jugar sobre TCP
992	Telnet SSL
993	IMAP4 SSL
995	POP3 SSL
1080	Socks Proxy
1352	IBM Lotus Notes/Domino RCP
1433	Microsoft-SQL-Server
1434	Microsoft-SQL-Monitor
1494	Citrix MetaFrame Cliente ICA
1512	WINS
1521	Oracle listener
1701	Enrutamiento y Acceso Remoto para VPN con L2TP
1723	Enrutamiento y Acceso Remoto para VPN con PPTP
1761	Novell Zenworks Remote Control utility
1863	MSN Messenger
2049	NFS
2082	CPanel
2086	WHM (Web Host Manager)
2427	Cisco MGCP
3000	Calista IP phone (saliente)
3030	NetPanzer
3128	Squid Proxy
3306	MySQL
3389	Microsoft Terminal Server
3396	Novell agente de impresión NDPS
3690	SubVersion
4099	AIM Talk
4662	eMule
4672	eMule
4899	RAdmin
5000	UPNP (Universal plug-and-play)
5060	SIP (SessionInitiationProtocol)

Anexo 3.

5190	Calista IP phone (entrante)
5222	XMPP/Jabber: conexión de cliente
5223	XMPP/Jabber: puerto por defecto para conexiones de cliente SSL
5269	XMPP/Jabber: conexión de servidor
5432	PostgreSQL
5500	VNC (Virtual Network Computing)
5517	Setiqueue proyecto SETI@Home
5631	pcAnyWhere (host)
5632	pcAnyWhere (host)
5400,5500,5600,5700, 5800,5900	VNC (Virtual Network Computing)
6000	X11 usado para X-windows
6112	BlizzardEntertainment
6129	Dameware: Software conexión remota
6346-6355	Gnutella
6667	IRC
6881	BitTorrent: puerto por defecto
6891-6900	MSN Messenger (archivos)
6901	MSN Messenger (voz)
6969	BitTorrent: puerto de tracker
7100	Servidor de Fuentes X11
8000	Shoutcast
8080	HTTP alternativo al puerto 80. También Tomcat default
8118	Privoxy
8291	routersMicrotik
9009	Pichat peer-to-peer chat server
9898	Dabber (troyano)
10000	Webmin (Administración remota web)
12345	Netbus (troyano)
19226	Puerto de comunicaciones de Panda Agent
20000-20019	ICQ
28800-29000	MSN GameZone
31337	Back Orifice (troyanos)

Encuesta de seguridad de redes de comunicaciones

UNIVERSIDAD NACIONAL DEL ALTIPLANO
ESCUELA DE POSTGRADO- PROGRAMA DE MAESTRÍA
MAESTRIA EN INFORMATICA

ENCUESTA

Encuesta para analizar la seguridad de redes de comunicaciones:

I. OBJETIVOS DE LA ENCUESTA

Esta encuesta está dirigida a las instituciones públicas y/o empresas privadas que tiene un área de informática.

II. INSTRUCCIONES: Marque según su percepción el valor correspondiente en cada pregunta

Preguntas	Si	No
1.-¿La red de comunicaciones que administra ha sufrido algún ataque de seguridad?		
2.-¿Conoce algún sistema de seguridad?		
3.-¿Aplica algún sistema de seguridad?		
4.-¿Conoce algún sistema de seguridad de detección de intrusos?		
5.-¿Aplica sistemas de detección de intrusos?		
6.-¿Conoce algún algoritmo de seguridad wavelet en la seguridad?		
7.-¿Aplica algún algoritmo de seguridad wavelet en la seguridad?		
8.- Ahora que conoce el algoritmo wavelet ¿Lo Aplicaría?		
9.-¿Su tiempo de administración lo dedica a detener ataques de seguridad de redes de comunicaciones?		

10.-¿Se autoriza los accesos a la administración de equipos de seguridad?
a) Nunca b) A Veces c) Siempre
10.1.-¿Tiene perfiles de acceso a la seguridad de la información?
a) Nunca b) A Veces c) Siempre
11.-¿ La información ha sido borrada, copiada o alterada?.
a) Nunca b) A Veces c) Siempre
12.-¿La información ha sido accedida por personas no autorizadas para hacerlo?
a) Nunca b) A Veces c) Siempre
13.-¿Prestas garantía de seguridad brinda certificando la autenticidad de información?
a) Nunca b) A Veces c) Siempre
14.-Marque el presupuesto anual en soles S/. que considere pertinente, de inversión en seguridad de redes de computadoras en su organización:
a) 0 a 5000 b)5000 a 10000 c) 10000 a 100000 d) 100000 a más
15.-¿Qué herramientas de seguridad se encuentra en la red de comunicaciones que administra? Marque todas las que considere:
( )Antivirus ( )Firewalls ( )Proxy
( )IDS ( )Monitoreo de red ( )Otros_____
16.- ¿Qué tipos de ataques a sufrido? Marque todas las que considere:
( )Fuerza Bruta ( )Envenenamiento por IP ( )Boots
( )Phishing ( )Redireccionamiento ( )DDoS
( )Error de Configuración ( )Malware ( )Otros:_____