UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

Tema: "LOS ATAQUES INFORMÁTICOS Y SU INCIDENCIA EN LA SEGURIDAD DE SERVIDORES CON SISTEMA OPERATIVO LINUX DE ENTIDADES DE GOBIERNO LOCAL"

Trabajo de Investigación, previo a la obtención del Grado Académico de Magister en Gerencia de Sistemas de Información

Autor: Ing. Francisco Javier Aguilar Feijóo

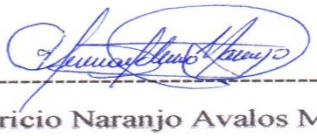
Ambato – Ecuador

2019

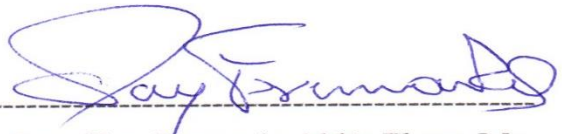
A la Unidad Académica de Titulación de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

El Tribunal receptor del Trabajo de Investigación presidido por la Ingeniera Elsa Pilar Urrutia Urrutia Magister, e integrado por Ingeniero Hernán Fabricio Naranjo Avalos Magister, Ingeniero Clay Fernando Aldás Flores Magister, designados por la Unidad Académica de Titulación de la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato, para receptar el Trabajo de Investigación con el tema: "Los ataques informáticos y su incidencia en la seguridad de servidores con sistema operativo Linux del Gobierno Autónomo Descentralizado de la Provincia de Orellana", elaborado y presentado por el señor Ingeniero Francisco Javier Aguilar Feijóo, para optar por el Grado Académico de Magister en Gerencia de Sistemas de Información; una vez escuchada la defensa oral del Trabajo de Investigación el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Elsa Pilar Urrutia Urrutia Mg.
Presidente del Tribunal



Ing. Hernán Fabricio Naranjo Avalos Mg.
Miembro del Tribunal



Ing. Clay Fernando Aldás Flores Mg.
Miembro del Tribunal

AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Investigación presentado con el tema: "Los ataques informáticos y su incidencia en la seguridad de servidores con sistema operativo Linux del GADPO", le corresponde exclusivamente a: Ingeniero Francisco Javier Aguilar Feijóo, Autor bajo la dirección de Ingeniero Luis Fabián Hurtado Vargas, Mgs., Director del Trabajo de Investigación; y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ing. Francisco Javier Aguilar Feijóo

c.c. 0705034155

AUTOR

Ing. Luis Fabián Hurtado Vargas, Mgs.

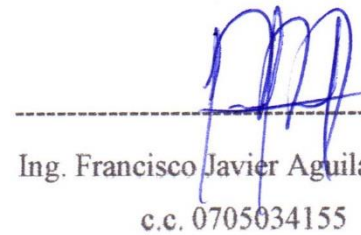
c.i. 0913563326

DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Investigación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.



Ing. Francisco Javier Aguilar Feijóo

c.c. 0705034155

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

AGRADECIMIENTO

A Dios, por darme una vida y salud para luchar por mis sueños.

A mis padres, por ser mi mayor inspiración y ejemplo de superación, de que con esfuerzo y perseverancia es posible hacer realidad nuestros sueños.

A mis hermanos por todo el cariño que siempre me brindan.

Al Gobierno Autónomo Descentralizado de la Provincia de Orellana, por el apoyo brindado para el desarrollo del presente proyecto de investigación.

A Fabián, director del presente proyecto de investigación, por todas las directrices brindadas para la culminación exitosa del presente estudio.

Javier Aguilar

DEDICATORIA

Con mucho amor dedico el presente proyecto de investigación a mis padres y hermanos por todo el apoyo que siempre me han brindado.

A mis sobrinos Santiago y Doménica, por ser unos niños maravillosos que siempre me sorprenden con sus ocurrencias.

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL
MAESTRÍAS EN GERENCIA DE SISTEMAS

TEMA

"Los ataques informáticos y su incidencia en la seguridad de servidores con sistema operativo Linux de entidades de gobierno local"

AUTOR: Ing. Francisco Javier Aguilar Feijóo
DIRECTOR: Ing. Luis Fabián Hurtado Vargas, Mgs.
FECHA: 29 de julio de 2019

RESUMEN EJECUTIVO

La presente investigación tuvo como finalidad determinar la incidencia de los ataques informáticos en los servidores con sistema operativo Linux del Gobierno Autónomo Descentralizado de la Provincia de Orellana (GADPO), para lo cual inicialmente se determinó los ataques informáticos más comunes que han afectado a las organizaciones los últimos años. Fue de gran utilidad el uso del cuadrante mágico de Gartner para conocer las empresas líderes del mercado en lo que respecta a seguridad informática, para a partir de sus reportes estadísticos publicados obtener los ataques informáticos a ser estudiados.

Se estableció, como ataques informáticos objeto de estudio, los ataques de pishing y Distributed Denial of Service (DDoS).

Para realizar los ataques de phishing se utilizó la herramienta Social Engineer Toolkit (SET), la misma que permitió cuantificar la cantidad de usuarios afectados por el ataque. Los ataques informáticos DDoS SYN Flood fueron realizados

utilizando la herramienta hping3 para inundar la red de datos, y Multi Router Traffic Grapher (MRTG) para cuantificar el uso de ancho de banda que originaba el ataque. Con los resultados obtenidos de los ataques de phishing y DDoS SYN Flood, mediante la aplicación de la metodología de gestión de riesgos de los sistemas de información (MAGERIT) se procedió a calcular la vulnerabilidad impacto y riesgo que los ataques informáticos provocaban en los servidores Linux del GADPO.

Para mitigar los efectos de los ataques informáticos estudiados, se propuso en el caso de phishing un plan de concientización y entrenamiento basado en la "NIST SP 800-50 Construcción de un Programa de Concientización y Entrenamiento de Seguridad de Tecnologías de Información" del Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio de los Estados Unidos, que fue aplicado a los funcionarios del GADPO. En lo que respecta al ataque DDoS de tipo SYN Flood, se utilizó reglas de iptables que fueron configuradas en el servidor firewall, equipo que fue objetivo de este tipo de ataques por ser considerado un servicio crítico que, en caso de verse comprometido, provocaría el colapso de la red de datos.

Descriptores: ataque informático, phishing, seguridad de servidores, ddos, riesgo, servidores Linux, Magerit, NIST SP 800-50, ciberseguridad, endurecimiento de servidores.

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL
MAESTRÍAS EN GERENCIA DE SISTEMAS

THEME

"Computer attacks and their impact on server security with Linux operating system of the local goverment"

AUTHOR: Ing. Francisco Javier Aguilar Feijóo
DIRECTED BY: Ing. Luis Fabián Hurtado Vargas, Mgs.
DATE:29/07/2019

EXECUTIVE SUMMARY

The purpose of this research was to determine the incidence of computer attacks on servers with Linux operating system of the Gobierno Autónomo Descentralizado de la Provincia de Orellana (GADPO), for which initially the most common computer attacks that have affected organizations were determined the last years. It was very useful to use Gartner's magic quadrant to know the leading companies in the market in terms of computer security, to obtain the computer attacks to be studied from their published statistical reports.

Pishing attacks and Distributed Denial of Service (DDoS) were established as computer attacks under study.

The Social Engineer Toolkit (SET) tool was used to carry out the phishing attacks, which allowed quantifying the number of users affected by the attack, and based on this result with the use of the systems risk management methodology information (MAGERIT), calculate the impact and risk vulnerability that this threat caused. Similarly, for DDoS computer attacks, unlike the tools used for the attack that in this case was hping3 for the SYN Flood and Multi Router Traffic Grapher (MRTG)

type attack to quantify the use of bandwidth that originated the attack, the effects on the target team were determined.

To mitigate the effects of the computerized attacks studied, an awareness and training plan based on the "NIST SP 800-50 Construction of an Information Technology Security Awareness and Training Program" of the National Institute was proposed in the case of phishing of Standards and Technology (NIST) of the US Department of Commerce, which was applied to GADPO officials. Regarding the DDoS attack of the SYN Flood type, iptables rules were used that were configured in the firewall server, equipment that was the target of this type of attacks because it was considered a critical service that, in case of being compromised, would cause data network collapse.

Keywords: computer attack, phishing, server security, ddos, risk, linux servers, Magerit, NIST SP 800-50, cybersecurity, server hardening.

INTRODUCCIÓN

El creciente y continuo uso de las tecnologías de la información ha significado a la vez para las organizaciones tener que luchar contra un sinnúmero de ataques informáticos, lo que pone en evidencia la necesidad de establecer mecanismos que permitan mantener a buen recaudo los activos informáticos y especialmente la información con la que cuentan (Aguilar, 2017).

El 23 de abril de 2008 se publicó el decreto ejecutivo 1014, el cual establece como política pública el uso de software libre en sistemas y equipos informáticos del sector público, por lo que, en Ecuador el software libre se convierte en una política tecnológica, en donde el uso de estándares abiertos y el trabajo comunitario, conllevan a la inclusión digital, la soberanía tecnológica y la innovación local (Subsecretaría de Gobierno Electrónico, 2018).

El GADPO como ente público y como caso de estudio de la presente investigación, mantiene una infraestructura de servidores en su mayoría con sistemas operativo Linux, donde se almacena la información que genera y además se brinda el acceso a la misma. Por esta razón surgió la necesidad de investigar la incidencia que provocarían los ataques informáticos de phishing y DDoS en este tipo de infraestructura, y en base a los resultados obtenidos determinar qué medidas se podrían tomar para mitigar los efectos de los mismos.

Como alternativa de solución, en el presente trabajo de investigación se propone una metodología de aseguramiento de servidores Linux, que pretende servir como guía a las organizaciones para implementar mecanismos de protección frente a los ataques informáticos que puedan poner en riesgo la confidencialidad, integridad y disponibilidad del activo más valioso que poseen hoy en día como es la información.

El proyecto de investigación se encuentra estructurado en seis capítulos:

EL CAPÍTULO I EL PROBLEMA contiene: el tema de investigación, el planteamiento del problema, su contexto, análisis crítico, prognosis, formulación del problema, interrogantes, delimitación, justificación y objetivos.

EL CAPÍTULO II MARCO TEÓRICO contiene: antecedentes de la investigación, fundamentación filosófica, fundamentación legal, categorías fundamentales, hipótesis y señalamiento de variables.

EL CAPÍTULO III METODOLOGÍA contiene: el enfoque de investigación, modalidad básica de la investigación, nivel o tipo de investigación, población y muestra, operacionalización de variables, plan de recolección de información y plan de procesamiento de la información.

EL CAPÍTULO IV ANÁLISIS E INTERPRETACIÓN DE RESULTADOS contiene: análisis e interpretación de resultados, identificación de riesgos de los servidores Linux y la verificación de hipótesis.

EL CAPÍTULO V contiene: CONCLUSIONES Y RECOMENDACIONES.

EL CAPÍTULO VI PROPUESTA contiene: datos informativos, antecedentes de la propuesta, justificación, objetivo general, objetivos específicos, factibilidad técnica, factibilidad operativa, factibilidad económica, fundamentación, metodología, modelo operativo, administración, previsión de la evaluación, conclusiones y recomendaciones.

CAPÍTULO 1. EL PROBLEMA

1.1. Tema

Los ataques informáticos y su incidencia en la seguridad de servidores con sistema operativo Linux de entidades de gobierno local.

1.2. Planteamiento del problema

1.2.1. Contextualización

A lo largo del tiempo, el avance de los medios tecnológicos y de comunicación han provocado el surgimiento de nuevos vectores de ataques y de nuevas modalidades delictivas que han transformado a Internet y las tecnologías informáticas en aspectos sumamente hostiles para cualquier tipo de organización y persona (Mieres, 2009).

Al hacer uso de las tecnologías para almacenar, mantener, transmitir y recobrar información, las amenazas existentes podrían afectar la confidencialidad, disponibilidad e integridad de la información vital para la organización, el negocio y los clientes, provocando de esta forma graves pérdidas económicas, y de tiempo para la organización (Aguinaga, 2013).

En la figura 1 se puede apreciar como los activos de información de una organización están rodeados de un ambiente complejo lleno de amenazas que pueden ir desde simples virus de computadora hasta robo de la propiedad intelectual de la empresa.

Figura 1. Amenazas a los activos de información

Elaborado por: Investigador

Fuente: (Aguinaga, 2013)

Miles de servidores Linux y Unix, y empresas entre las que destacan algunas de alto perfil como cPanel (la empresa tras el famoso panel de control de hosting de sitios web) y kernel.org de la Fundación Linux (repositorio principal de código fuente para el núcleo de Linux) fueron afectados por una operación de gran magnitud denominada Windigo, que buscaba enviar spam y robar credenciales por SSH para redirigir a quienes visitan los sitios web a contenido malicioso (Bilodeau et al., 2014).

Según el reporte de Eset Security del año 2017, las principales preocupaciones de las empresas latinoamericanas respecto a la seguridad de la información están relacionadas principalmente con el phishing, malware, ataques de denegación de servicio y las vulnerabilidades de software y sistemas (Eset Security, 2017).

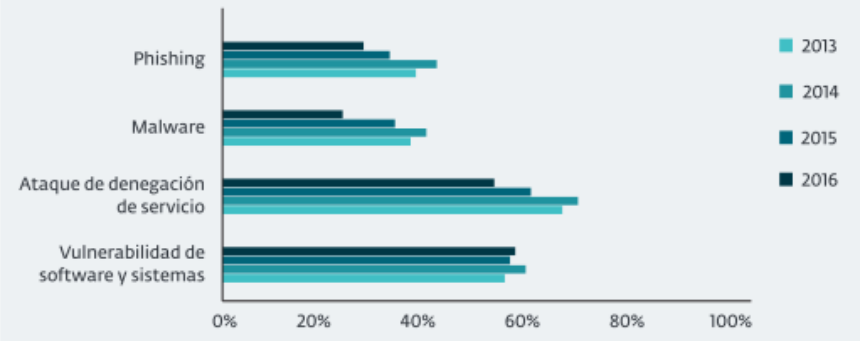


Figura 2. Principales preocupaciones de las empresas de Latinoamérica respecto a la seguridad de la información
Fuente: (Eset Security, 2017)

Según Digiware proveedor experto en la generación de estrategias integrales en seguridad de la información, en Latinoamérica el sector más vulnerable a ataques informáticos son el del gobierno con un 49.53% donde predominan los ataques de denegación de servicio, exploit, fuerza bruta y Cross Site Scripting (CSS), seguido por el sector financiero con 14.34%, comunicaciones con el 12.83%, industria con un 10.70% y energía con el 6.54% (Digiware, 2015).

En el año 2011 algunas instituciones del sector público ecuatoriano fueron víctimas de ataques informáticos por parte del grupo de hackers denominado Anonymous. Entre las instituciones afectadas se encontraban la Corporación Nacional de Telecomunicaciones (CNT) de la cual publicaron el diagrama físico de la red de

servidores, las municipalidades de Guayaquil y Francisco de Orellana cuyas páginas web fueron vulneradas (El Telégrafo, 2011).

En la ciudad de Francisco de Orellana, capital de la provincia de Orellana, país Ecuador, se encuentra ubicado el GADPO, gobierno local con autonomía política, administrativa y financiera, que entre sus competencias establecidas en el Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD) tiene (COOTAD, 2010):

- "Planificar junto con otras instituciones del sector público y actores de la sociedad, el desarrollo provincial y formular los correspondientes planes de ordenamiento territorial, en el ámbito de sus competencias, de manera articulada con la planificación nacional, regional, cantonal y parroquial, en el marco de la interculturalidad, plurinacionalidad y el respeto a la biodiversidad."
- "Planificar, construir y mantener el sistema vial de ámbito provincial, que no incluya las zonas urbanas."
- "Ejecutar, en coordinación con el gobierno regional y los demás gobiernos autónomos descentralizados, obras en cuencas y micro cuencas."
- "La gestión ambiental provincial."
- "Planificar, construir, operar y mantener sistemas de riego de acuerdo con la constitución y la ley."
- "Fomentar las actividades productivas provinciales, especialmente las agropecuarias."
- "Gestionar la cooperación internacional para el cumplimiento de sus competencias."

La Jefatura de Informática y Tecnología (JIT) administra la infraestructura tecnológica del GADPO, en la cual, en lo que respecta a servidores, priman los servidores basados en software libre ya que según el Decreto Ejecutivo 1014, se debe utilizar software libre en la administración pública, salvo ciertos casos donde la relación costo – beneficio no lo considere adecuado.

Las implementaciones de servidores realizadas no contemplan el uso de estándares de seguridad, no se conocen los riesgos a los que están expuestos los mismos, ni se cuenta con políticas y procedimientos de seguridad definidos que garanticen la protección del activo más importante para toda organización como lo es la

información. En virtud a lo anteriormente expuesto es de gran interés la realización de una investigación que permita determinar cómo se puede proteger adecuadamente la infraestructura de servidores, garantizando de esta forma la confidencialidad, integridad y disponibilidad de la información.

1.2.2. Análisis crítico

Es muy importante identificar las vulnerabilidades a las que están expuestas todos los días la infraestructura de red (LAN, WAN, VPN) de una organización y la plataforma de servidores de diferentes sistemas operativos (Microsoft Windows, Sistemas Linux y Unix, etc), que se tengan en cuenta los diferentes riesgos que se pueden presentar en la infraestructura tecnológica si estas vulnerabilidades no son contrarrestadas (Montoya, 2013).

En la JIT del GADPO, se desconocen los riesgos a los que están expuestos la infraestructura de servidores Linux, lo que dificulta notablemente que se puedan implementar políticas para evitar, transferir, mitigar o aceptar el riesgo.

La implementación y puesta en marcha de servidores no está basada en el uso de políticas y procedimientos establecidos que permitan contar con configuraciones estandarizadas y basadas en buenas prácticas, provocando de esta forma que la infraestructura tecnológica sea vulnerable a distintos tipos de ataques informáticos como accesos no autorizados, ataques de denegación de servicio, inyección SQL, ya sea por contar con software desactualizado o servicios innecesarios activos.

1.2.3. Prognosis

Actualmente la JIT del GADPO, no cuenta con un proceso establecido, en donde se identifiquen los riesgos, se definan políticas y procedimientos a seguir basados en herramientas y buenas prácticas para el aseguramiento de los servidores con sistema operativo Linux.

De mantenerse esta situación y no aplicar la metodología propuesta, se continuará implementando servidores, de los cuales se desconoce su nivel de vulnerabilidad y las amenazas a los cuales están expuestos, comprometiendo de esta forma la disponibilidad, seguridad e integridad de la información almacenada en los mismos.

1.2.4. Formulación del problema

¿Cómo inciden los ataques informáticos en la seguridad de servidores con sistema operativo Linux del GADPO?

1.2.5. Interrogantes (Subproblemas)

¿Cuáles son los mecanismos utilizados actualmente en el GADPO, para realizar el aseguramiento de servidores Linux?

¿Cuáles son las mejores prácticas y herramientas existentes para el aseguramiento de servidores con sistema operativo Linux del GADPO?

¿Cómo se puede determinar los riesgos a los que están expuestos los servidores con sistema operativo Linux del GADPO?

¿Se puede elaborar una metodología de hardening que permita asegurar los servidores con sistema operativo Linux del GADPO y protegerlos frente a ataques informáticos más comunes?

¿Cómo se puede determinar el nivel de vulnerabilidad de los servidores con sistema operativo Linux del GADPO, luego de haber aplicado la metodología de hardening?

1.2.6. Delimitación del objeto de investigación

Campo: Gobierno Local

Área: Seguridad Informática

Aspecto: Aseguramiento de servidores con sistema operativo Linux del GADPO.

1.2.6.1. Delimitación espacial

Gobierno Autónomo Descentralizado de la Provincia de Orellana.

1.2.6.2. Delimitación temporal

El tiempo de desarrollo será de 7 meses a partir de la fecha de aprobación del tema de investigación.

1.2.6.3. Unidades de observación

Gobierno Autónomo Descentralizado de la Provincia de Orellana.

1.3. Justificación

La información y los procesos que la apoyan, los sistemas y las redes, son bienes importantes de las entidades, por lo que requieren ser protegidos convenientemente frente a amenazas que pongan en peligro la disponibilidad, la integridad, la confidencialidad de la información, la estabilidad de los procesos, los niveles de competitividad, la imagen corporativa, la rentabilidad y la legalidad, aspectos necesarios para alcanzar los objetivos de la organización (Dirección Nacional de Seguridad y Protección de Cuba, 2013).

Es de interés del GADPO conocer los riesgos a los cuales están expuestos la infraestructura de servidores Linux, así como también establecer un proceso de aseguramiento mediante la adopción de estándares y buenas prácticas de seguridad que salvaguarden la información, y que permitan disminuir el nivel de vulnerabilidad de los servidores frente a un ataque informático.

Por todo lo expuesto, es notorio el interés por parte del GADPO, en especial de la JIT en el presente proyecto de investigación, lo cual influye directamente en que será posible llevar a cabo el mismo, ya que se brindará todo el apoyo necesario para contar con los recursos que se requieran para el cumplimiento de los objetivos propuestos.

- **Factibilidad técnica:**

Fue factible técnicamente de realizar el presente proyecto de investigación ya que se contó con los recursos y herramientas tecnológicas necesarias, así como también se tuvo acceso a los datos e información requerida.

- **Factibilidad operativa:**

El presente proyecto fue factible operativamente de realizar ya que se contó con la autorización de la máxima autoridad del GADPO, así como también se tuvo el apoyo de la JIT, lo que garantizó poder tener acceso a la información requerida, asegurar que los resultados obtenidos sean de utilidad y además puedan ser aplicados en beneficio de la institución.

- **Factibilidad económica:**

Fue factible económicamente de realizar ya que los costos que implican el análisis, estudio, tiempo empleado en el desarrollo del proyecto fueron asumidos por el investigador. Los tiempos del personal de la institución involucrado en la investigación los asumió el GADPO.

1.4. Objetivos

1.4.1. General

Determinar la incidencia de los ataques informáticos en la seguridad de servidores con sistema operativo Linux del GADPO.

1.4.2. Específicos

- Determinar los mecanismos de aseguramiento de servidores con sistema operativo Linux utilizados actualmente en el GADPO.
- Investigar cuales son las mejores prácticas y herramientas existentes para el aseguramiento de servidores.
- Identificar los riesgos a los que están expuestos los servidores con sistema operativo Linux del GADPO.
- Elaborar una metodología de hardening para el aseguramiento de servidores con sistema operativo Linux del GADPO frente a los ataques informáticos más comunes.
- Determinar el nivel de vulnerabilidad de los servidores con sistema operativo Linux del GADPO luego de haber aplicado la metodología de hardening.

CAPÍTULO 2. MARCO TEÓRICO

2.1. Antecedentes investigativos (Investigaciones Previas, Estado del Arte)

En materia de seguridad de la información y aseguramiento de servidores, se han realizado diversos estudios, entre los que destacan:

- Un estudio realizado por la Universidad Piloto de Colombia, denominado "DEFENSA EN PROFUNDIDAD BASADA EN SERVIDORES", concluye que con el aseguramiento bajo la seguridad en profundidad se encuentran estrategias para fortalecer nuestra infraestructura, cada capa con un objetivo diferente pero que se deben complementar cada una con la otra iniciando desde la parte física, infraestructura, corriente eléctrica, aires acondicionados y finalizando con los datos. Además, se indica también que asegurar los servidores no implica comprar dispositivos robustos ni software fuera de lo común, el aseguramiento conlleva un estudio y conocimiento previo para lograr buenas políticas y herramientas que nos permitan actuar ante una falla de seguridad (Rico Ávila, 2013).
- Entre otro de los trabajos de investigación que destacan, denominado "ASEGURAMIENTO DE INFRAESTRUCTURAS DE RED Y SERVIDORES", elaborado por la Universidad Piloto de Colombia, indican que actualmente existen muchos riesgos y que se pueden presentar una gran cantidad de amenazas para atacar las vulnerabilidades de seguridad en una infraestructura de tecnología, para lo cual es vital en primera instancia conocer cómo se efectúan estos ataques, para luego poder establecer los mecanismos de seguridad necesarios a nivel de guías, procedimientos, y buenas prácticas de seguridad, basados en estándares y normativas internacionales como ISO 27001:2005, ISO 27002, Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Health Insurance Portability and Accountability (HIPA) (Montoya, 2013).
- En el proyecto de investigación "ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2005 PARA UNA EMPRESA DE PRODUCCIÓN Y COMERCIALIZACIÓN DE PRODUCTOS DE CONSUMO MASIVO", realizado por la Pontificia Universidad Católica del Perú, se concluye que la

adecuada gestión de la seguridad de la información es algo que debe estar ya incluido en la cultura organizacional de las empresas; y en todas ellas esta adecuada gestión no se lograría sin el apoyo de la alta gerencia como promotor activo de la seguridad de la empresa (Aguinaga, 2013).

- En el artículo denominado "METODOLOGÍA DE ANÁLISIS DE VULNERABILIDADES PARA EMPRESAS DE MEDIA Y PEQUEÑA ESCALA", desarrollado por la Pontificia Universidad Javeriana de Colombia, donde se abordó principalmente el aseguramiento de los recursos de la empresa, tomando como base cinco pilares fundamentales de la seguridad informática como son la Integridad, Confidencialidad, Disponibilidad, Auditabilidad y no Repudio. Se concluye que una adecuada configuración de los dispositivos, servicios y aplicaciones le permite a la empresa solucionar en gran proporción las brechas de seguridad que estos presentan, disminuyendo así la probabilidad de un posible ataque por parte de terceros que aprovechen tal vulnerabilidad (Garzón, Ratkovich, & Vergara, 2013).
- Otro de los trabajos de investigación consultados relacionado con el aseguramiento de servidores Linux fue el proyecto "ASEGURAMIENTO DE SISTEMA OPERATIVO DE RED HAT 6.6 ENTERPRISE PARA CUMPLIMIENTO DE NORMATIVA PCI Data Security Standard (DSS) 3.0", realizado por la Escuela Superior Politécnica del Litoral, el mismo que tuvo como objetivo el aseguramiento del sistema operativo Linux en su distribución Red Hat versión 6.6 para un servidor que cumple con la función de switch transaccional, en una empresa que presta servicios de interconexión de instituciones financieras, con la finalidad de cumplir con la normativa establecida por el estándar de seguridad en los datos de la industria de pagos por tarjetas de crédito y débito (PCI DSS) (Robles Tomalá, 2015) (Security Standard Council).

2.2. Fundamentación filosófica

La presente investigación se enmarca en el paradigma crítico propositivo, es crítico por que realiza un análisis crítico del problema, y es propositivo porque busca proponer una solución factible al problema.

2.3. Fundamentación legal

El presente proyecto de investigación se sustenta en las siguientes leyes:

LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS

Capítulo II PRINCIPIOS GENERALES DEL REGISTRO DE DATOS PÚBLICOS

Art. 4.- Responsabilidad de la información. – "Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información."

"Las personas afectadas por información falsa o imprecisa, difundida o certificada por registradoras o registradores, tendrán derecho a las indemnizaciones correspondientes, previo el ejercicio de la respectiva acción legal."

"La Dirección Nacional de Registro de Datos Públicos establecerá los casos en los que deba rendirse caución."

CÓDIGO ORGÁNICO INTEGRAL PENAL

Art 178.- "La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años."

Art 229.- "La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años."

NORMAS DE CONTROL INTERNO DE LA CONTRALORÍA GENERAL DEL ESTADO

410 -10 Seguridad de tecnología de información

"La Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:"

"Ubicación adecuada y control de acceso físico a la Unidad de Tecnología de Información y en especial a las áreas de: servidores, desarrollo y bibliotecas."

1. "Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado."
2. "En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación."
3. "Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización."
4. "Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados."
5. "Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire."
6. "Consideración y disposición de sitios de procesamiento alternativos."
7. "Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana."

410-11 Plan de contingencias

"Corresponde a la Unidad Tecnología de Información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado."

Los aspectos a considerar son:

1. “Plan de respuesta a los riesgos que incluirá la definición y asignación de roles críticos para administrar los riesgos de tecnología de información, escenarios de contingencias, la responsabilidad específica de la seguridad de la información, la seguridad física y su cumplimiento.”

2. “Definición y ejecución de procedimientos de control de cambios, para asegurar que el plan de continuidad de tecnología de información se mantenga actualizado y refleje de manera permanente los requerimientos actuales de la organización.”

3. “Plan de continuidad de las operaciones que contemplará la puesta en marcha de un centro de cómputo alterno propio o de uso compartido en un Data Center Estatal, mientras dure la contingencia con el restablecimiento de las comunicaciones y recuperación de la información de respaldos.”

4. “Plan de recuperación de desastres que comprenderá:”

- Actividades previas al desastre (bitácora de operaciones).
- Actividades durante el desastre (plan de emergencias, entrenamiento).
- Actividades despúes del desastre.

5. “Es indispensable designar un comité con roles específicos y nombre de los encargados de ejecutar las funciones de contingencia en casos de suscitarse una emergencia.”

6. “El plan de contingencias será un documento de carácter confidencial que describa los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación del plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.”

7. “El plan de contingencias aprobado, será difundido entre el personal responsable de su ejecución y deberá ser sometido a pruebas, entrenamientos y evaluaciones periódicas o cuando se haya efectuado algún cambio en la configuración de los equipos o el esquema de procesamiento.”

410-12 Administración de soporte de tecnología de información

“La Unidad de Tecnología de Información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte

tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen."

Los aspectos a considerar son:

1. "Revisiones periódicas para determinar si la capacidad y desempeño actual y futuro de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios."
2. "Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad."
3. "Estandarización de la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas"
4. "Revisiones regulares de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de información."
5. "Medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos."
6. "Definición y manejo de niveles de servicio y de operación para todos los procesos críticos de tecnología de información sobre la base de los requerimientos de los usuarios o clientes internos y externos de la entidad y a las capacidades tecnológicas"
7. "Alineación de los servicios claves de tecnología de información con los requerimientos y las prioridades de la organización sustentados en la revisión, monitoreo y notificación de la efectividad y cumplimiento de dichos acuerdos"
8. "Administración de los incidentes reportados, requerimientos de servicio y solicitudes de información y de cambios que demandan los usuarios, a través de mecanismos efectivos y oportunos como mesas de ayuda o de servicios, entre otros."
9. "Mantenimiento de un repositorio de diagramas y configuraciones de hardware y software actualizado que garantice su integridad, disponibilidad y faciliten una rápida resolución de los problemas de producción."

10. “Administración adecuada de la información, librerías de software, respaldos y recuperación de datos.”

11. “Incorporación de mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos, así como la protección y conservación de información utilizada para encriptación y autenticación”.

2.4. Categorías fundamentales

2.4.1. Supra-ordinación de variables

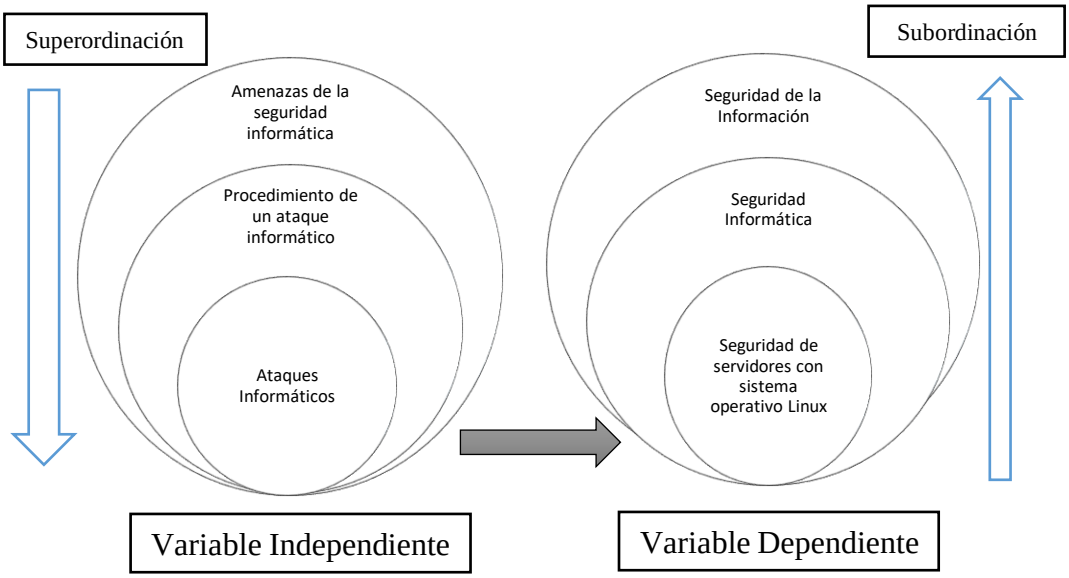


Figura 3. Inclusiones conceptuales

Elaborado por: Investigador

2.4.2. Sub-ordinación de variables

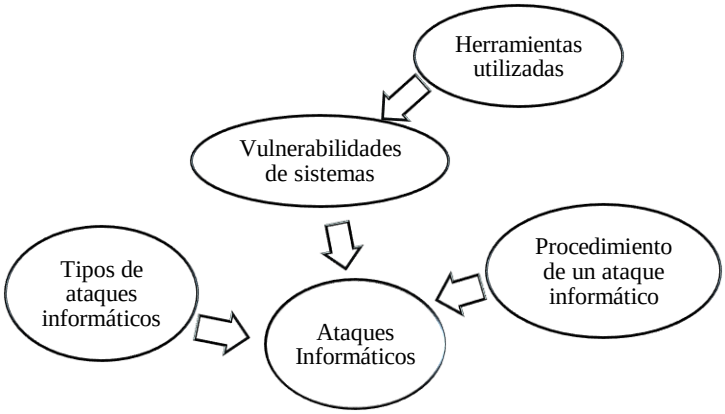


Figura 4. Constelación de ideas variable independiente

Elaborado por: Investigador

2.4.3. Sub-ordinación de variables

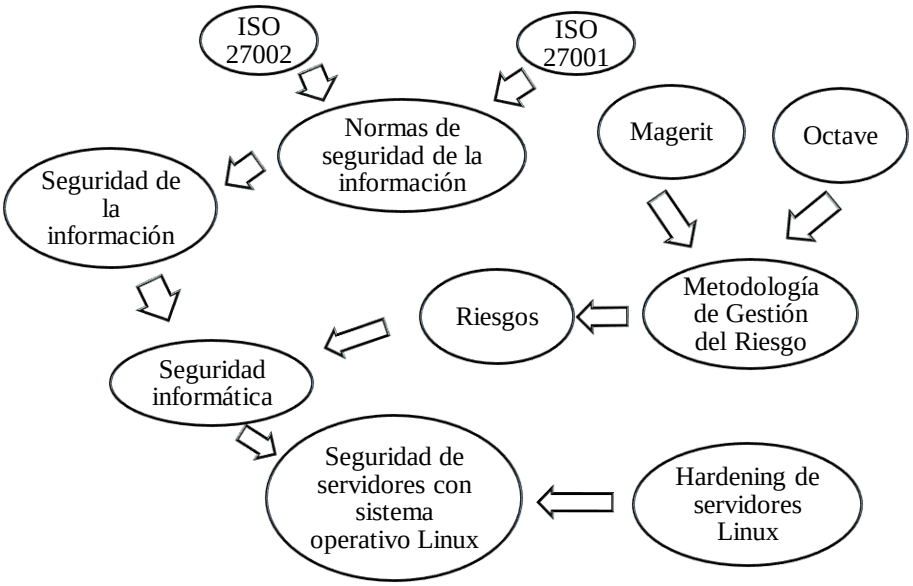


Figura 5. Constelación de ideas variable dependiente

Elaborado por: Investigador

2.4.4. Categorías de la variable independiente

Amenazas de la seguridad informática

La amenaza es alguien o algo que aprovecha una vulnerabilidad existente y la utiliza para provocar un daño a un sistema informático, donde puede causar pérdida de información, destrucción de información o problemas funcionales de un sistema o red informática (Robayo & Rodríguez, 2015) (Portantier, 2012).

Se pueden clasificar en amenazas físicas y lógicas, las mismas que pueden ser intencionales y no intencionales:

Tabla 1. Amenazas a la seguridad informática

Amenaza	Intencionales	No intencionales
Lógicas	• Hackers • Malware • Empleados descontentos	• Fallas de sistema • Empleados(errores de uso)
Físicas	• Ataques terroristas • Empleados descontentos	• Inundaciones • Terremotos • Fallas de hardware

Elaborado por: Investigador

Fuente: (Portantier, 2012)

Procedimiento de un ataque informático

Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad (Mieres, 2009).

Las etapas por las que suele pasar un ataque informático son las siguientes:

1. **Reconocimiento:** También llamada footpriting, es la primera fase en donde el hacker investiga toda la información que puede obtener con el uso de herramientas o métodos de la persona, institución o empresa a la cual va a atacar (Guamán, 2014).
2. **Escaneo:** El fin es encontrar a los activos objetivo que puedan poseer vulnerabilidades (Salgado, 2014).
3. **Obtener Acceso:** Esta fase también es conocida como explotación o hacking donde se ejecutan exploits, que buscan aprovechar la vulnerabilidad de un sistema para conseguir un comportamiento o lograr acceder a más información. Es en esta fase donde se utilizan los frameworks de explotación (Yánez, 2015). Algunas de las técnicas que el atacante puede utilizar son ataques de Buffer Overflow, Denial of Service (DoS), DDoS, Password Filtering y Sessionhijacking (Pita, 2014).
4. **Mantener Acceso:** Es dar la continuidad al ataque con la finalidad de hacer más daño a la víctima, controlando el sistema que ya se logró acceder. Se puede decir que es la fase más peligrosa para un atacante mal intencionado, porque puede lograr robar información personal como números de tarjetas de crédito u otra información clave (Guamán, 2014).
5. **Borrar Huellas:** Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todos los archivos de registro (logs) o alarmas del Sistema de Detección de Intrusos (IDS), para evitar ser detectado por el profesional de seguridad o los administradores de red (Pita, 2014).

Ataques informáticos

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, hardware, e incluso en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de

índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización (Pita, 2014).

Entre los tipos de ataques informáticos, podríamos diferenciar en primer lugar entre los ataques activos, que producen cambios en la información y en la situación de los recursos del sistema, y los ataques pasivos, que se limitan a registrar el uso de los recursos y/o acceder a la información guardada o transmitida por el sistema (Álvaro, 2014).

1. **Ataques Pasivos:** Entre los ataques pasivos tenemos (Soriano, 2014):

- **Espionaje:** En general, la mayoría de información que se transmite por la red se envía de forma no segura (sin cifrar), permitiendo a un atacante escuchar o interpretar los datos intercambiados.
- **Análisis de tráfico:** Se refiere al proceso de interceptar y examinar los mensajes con el fin de deducir información de patrones en la comunicación. En general, cuanto mayor es el número de mensajes observados, interceptados y almacenados, más se puede inferir del tráfico.

La siguiente figura muestra un modelo de ataque pasivo:

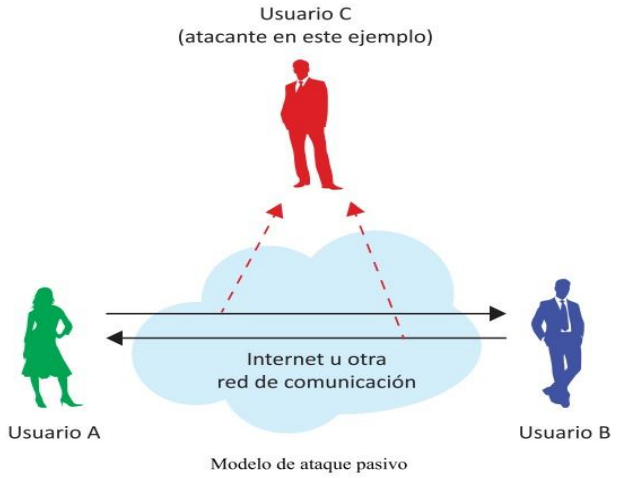


Figura 6. Modelo de ataque informático pasivo

Fuente: (Soriano, 2014)

2. **Ataques activos:** Los ataques activos engloban alguna modificación del flujo de datos o la creación de datos falsos. Pueden dividirse en seis categorías (Soriano, 2014):

- **Suplantación de identidad:** Es un tipo de ataque en el que el atacante suplanta la identidad de otro usuario
- **Repetición:** Una transmisión de datos válida es repetida o retardada de forma maliciosa. Este ataque lo puede provocar el mismo emisor de datos originales o bien un atacante que los intercepta y posteriormente los retransmite, posiblemente como parte de un ataque de suplantación de identidad.
- **Modificación de mensajes:** El atacante elimina un mensaje que atraviesa la red, lo altera y lo reinserta.
- **Hombre en el medio (Man in the Middle, MitM):** En este tipo de ataques, un atacante intercepta las comunicaciones entre dos entidades, por ejemplo, entre un usuario y un sitio web.
- **DoS y DDoS:** Un DoS es una situación en la que un usuario u organización se ve privado de los servicios o recursos que normalmente debería tener. En DDoS, un gran número de sistemas comprometidos (a veces llamado botnet) atacan a un solo objetivo.
- **Amenazas Avanzadas Persistentes (Advanced Persistent Threat, APT):** Es un ataque a la red en el que un atacante consigue un acceso no autorizado a la red y permanece allí sin ser detectado durante un largo período de tiempo. La principal intención de un ataque APT es robar datos más que causar daños a la red u organización.

La siguiente figura muestra un modelo de ataque activo:

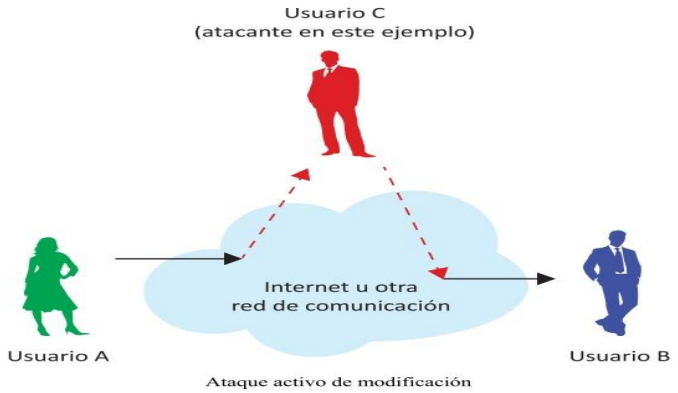


Figura 7. Modelo de ataque informático activo

Fuente: (Soriano, 2014)

2.4.5. Categorías de la variable dependiente

Seguridad de la información

La seguridad de la información es la protección de la información de un amplio rango de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales (Jiménez, 2010).

El estándar para gestionar la seguridad de la información en una empresa es la norma internacional ISO 27001. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. Además, también permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001 (Nieves, 2017).

Como complemento a la norma ISO 27001 se tiene a la norma ISO/IEC 27002, la cual proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información. La norma ISO 27000 en la versión 2013 cuenta con 19 secciones, 35 objetivos de control y 114 objetivos específicos. Es necesario recalcar que las 5 secciones iniciales son generales para la familia de las normas 27000.

Las 14 secciones de la norma ISO/IEC 27002:2013 comprende las políticas de seguridad ,aspectos organizativos de la seguridad de la información, seguridad ligada a los recursos humanos, gestión de activos, control de acceso, cifrado, la seguridad física y ambiental, seguridad en las operaciones, seguridad en las telecomunicaciones, adquisición, desarrollo y mantenimiento de los sistemas de información, relaciones con los proveedores, gestión de los incidentes en la seguridad de la información y mejoras, aspectos de seguridad de la información en

la gestión de la continuidad del negocio y cumplimiento (de la Torre, de la Torre, de la Torre, & de la Torre, 2017) (E. Torres, 2015).

Seguridad informática

La seguridad informática es un área de la informática que se enfoca en proteger a los activos concernientes a las tecnologías de la información ante cualquier amenaza, garantizando la triada de la seguridad como se menciona a continuación (Salgado, 2014):

a) Confidencialidad: Garantiza que solo aquellas personas o procesos autorizados puedan acceder a la información.
b) Integridad: Se encarga de conservar la exactitud y totalidad de la información, esto es, que la información no sea modificada de alguna forma por usuarios o procesos no autorizados.
c) Disponibilidad: Garantiza que usuarios y procesos autorizados tengan acceso a la información cuando lo necesiten y cuantas veces se requiera.

- **Riesgos:** Es la posibilidad de que una amenaza se origine, dando lugar a un ataque a la empresa (Gaona, 2013).

Según la Organización Internacional para la Normalización (ISO), define riesgo tecnológico como:

"La probabilidad que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o grupo de activos, generando pérdida o daños"

El riesgo siempre involucra:

- Incertidumbre: Es una situación en la cual no se tiene certeza de que ocurra determinado evento.
- Pérdida potencial: Son las fallas o deficiencias en los sistemas de información, en los controles internos o por errores en el procesamiento de las operaciones.
- **Metodologías para el análisis de riesgos**

Existen varias metodologías para realizar el análisis de riesgos que se pueden presentar en una organización, entre ellas tenemos:

- **Metodología OCTAVE:** La metodología OCTAVE (Operationally Critical Threats Assets and Vulnerability Evaluation), desarrollada por el equipo de respuesta ante emergencias informáticas (CERT, por sus siglas en inglés), evalúa

los riesgos de seguridad de la información y propone un plan de mitigación de los mismos dentro de una empresa. OCTAVE equilibra aspectos de riesgos operativos, prácticas de seguridad y tecnología para que, a partir de estos, los entes empresariales puedan tomar decisiones de protección de información basados en los principios de seguridad de la información (Calderón, 2015).

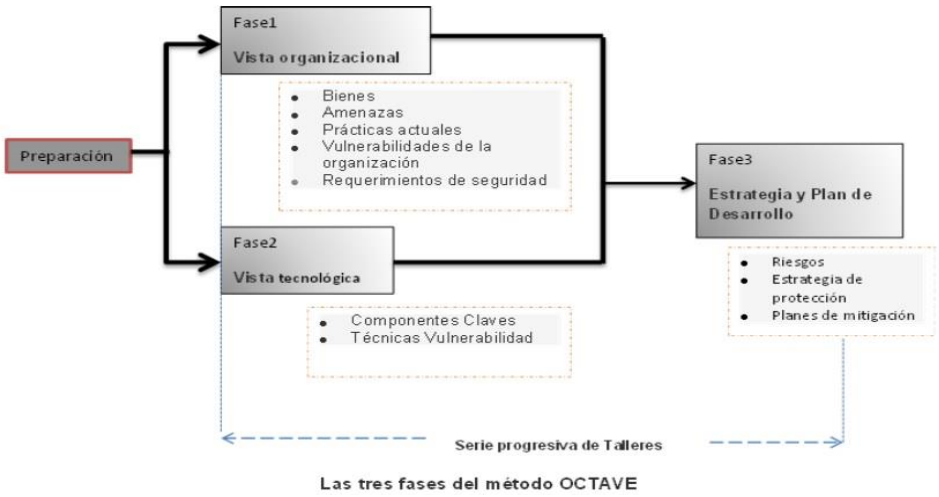


Figura 8. Fases de la metodología OCTAVE

Fuente: (Moncayo, 2014)

- **Metodología MAGERIT:** La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información **(**MAGERIT): Es de carácter público, perteneciente al Ministerio de Administraciones Públicas y fue elaborado por el Consejo Superior de Administración Electrónica de España. Ofrece una clasificación amplia de activos y describe métodos prácticos para la realización de análisis de riesgos (Moncayo, 2014).

Los activos que propone MAGERIT para su implementación son: servicios, datos, hardware, software, soportes de información, redes de comunicaciones, equipos auxiliares, instalaciones y personas.

Seguridad de servidores con sistema operativo Linux

El sistema operativo Linux ha evolucionado notablemente desde que Linux Torvalds produjera la primera versión del kernel de Linux, o núcleo del sistema operativo en 1991. Las reglas de código abierto bajo las que se publican todos los kernel de Linux han hecho que su desarrollo sea constante y entusiasta, y el

resultado es una gran cantidad de aplicaciones útiles para todos los consumidores (Sophos, 2006).

Cuando se utiliza un servidor en una red pública, se convierte en objetivo para los agresores. Por lo tanto, es de suma importancia para el administrador de sistemas fortalecer el sistema y bloquear los servicios. La seguridad del servidor es tan importante, porque los servidores suelen contener una gran cantidad de información vital de una organización. Si un servidor está comprometido, todos sus contenidos pueden estar disponibles para que el cracker robe o manipule a su antojo.

Para, mejorar la seguridad de un servidor, de forma general se deberían tomar en cuenta los siguientes aspectos (RedHat, 2017):

- Mantener todos los servicios actualizados, para protegerse contra las últimas amenazas.
- Usar protocolos seguros cada vez que sea posible.
- Servir un tipo de servicio por máquina cuando sea posible.
- Monitorizar todos los servicios para actividades sospechosas.

2.5. Hipótesis

Los ataques informáticos inciden en la seguridad de servidores con sistema operativo Linux del GADPO.

2.6. Señalamiento de variables

2.6.1. Variable independiente: Ataques Informáticos

2.6.2. Variable dependiente: Seguridad de servidores con sistema operativo Linux del GADPO.

CAPÍTULO 3. METODOLOGÍA

3.1. Enfoque

El presente trabajo de investigación tiene un enfoque cuali-cuantitativo, es cuantitativa porque se buscará determinar la incidencia de los ataques informáticos en la seguridad de servidores Linux en base a la medición numérica y el análisis estadístico; también es cualitativa ya que se va emitir juicios de valor respecto de la seguridad de servidores Linux en la institución.

3.2. Modalidad básica de la investigación

Investigación Bibliográfica

La investigación será bibliográfica, ya que haremos uso de libros, tesis del área de seguridad informática y tecnologías de la información, artículos científicos y leyes existentes para la elaboración del marco teórico sobre las variables objeto del presente estudio.

Investigación de Campo

La investigación será de campo, porque se buscará obtener información sobre los ataques informáticos a la seguridad de servidores Linux.

3.3. Nivel o tipo de investigación

Investigación Experimental

La investigación experimental, permitirá provocar voluntariamente situaciones que afecten la seguridad de los servidores Linux, y evaluar los resultados obtenidos, de tal forma que se pueda determinar el proceso de aseguramiento más adecuado.

Investigación Descriptiva

La investigación es descriptiva por que se realiza un análisis para llegar a determinar la incidencia que tienen los ataques informáticos en la seguridad de servidores con sistema operativo Linux.

Investigación Explicativa

La investigación es explicativa, porque se va poder sustentar la importancia que tiene conocer cómo se efectúan los ataques informáticos para poder establecer un adecuado proceso de aseguramiento de los servidores.

Investigación Correlacional

La investigación será correlacional, ya que busca medir el grado de relación entre los ataques informáticos y la seguridad de servidores con sistema operativo Linux.

3.4. Población y muestra

La población a estudiar para la realización de la presente investigación serán los ataques informáticos.

Dado la existencia de una gran cantidad de ataques informáticos se hace necesario establecer una muestra que permita realizar un adecuado estudio. Para ello en primer lugar se procede a seleccionar las empresas líderes en lo que respecta al estudio de los ataques informáticos y seguridad informática, mediante la utilización del cuadrante mágico de Gartner de los años 2016, 2017 y 2018.

Gartner es una organización de investigación global para la industria tecnológica, y el cuadrante mágico de Gartner es una gráfica que indica la situación del mercado de un producto tecnológico en un determinado momento (Samaniego, 2012).

El cuadrante mágico tiene dos ejes, en el eje X corresponde a la integridad de visión, y refleja cuantas características puede tener un producto y la innovación que obliga a otros proveedores a reaccionar para mantener el ritmo.

El eje vertical Y representa la capacidad de ejecución y está determinado por los ingresos, el número y calidad de los revendedores y distribuidores, el número de empleados y su distribución entre las áreas de ingeniería, ventas, soporte.

Por lo tanto, en el cuadrante superior derecho están ubicados los líderes, la parte inferior derecha los visionarios, la inferior izquierda es el nicho, y la parte superior izquierda representa los desafíos (CIO PERÚ, 2012).

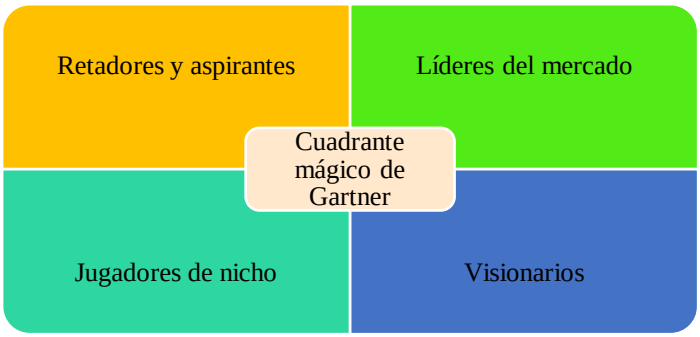


Figura 9. Cuadrante mágico de Gartner

Elaborado por: Investigador

Entre las tres empresas líderes en plataformas de protección de endpoints que destacan en el año 2016 tenemos a Trend Micro, Intel Security y Kaspersky Lab.

Figura 10. Cuadrante mágico de Gartner para plataformas de protección de endpoints del año 2016.

Fuente: (Tecnozero, 2016)

Las empresas que destacan en el año 2017 son Trend Micro, Kaspersky Lab y Sophos.

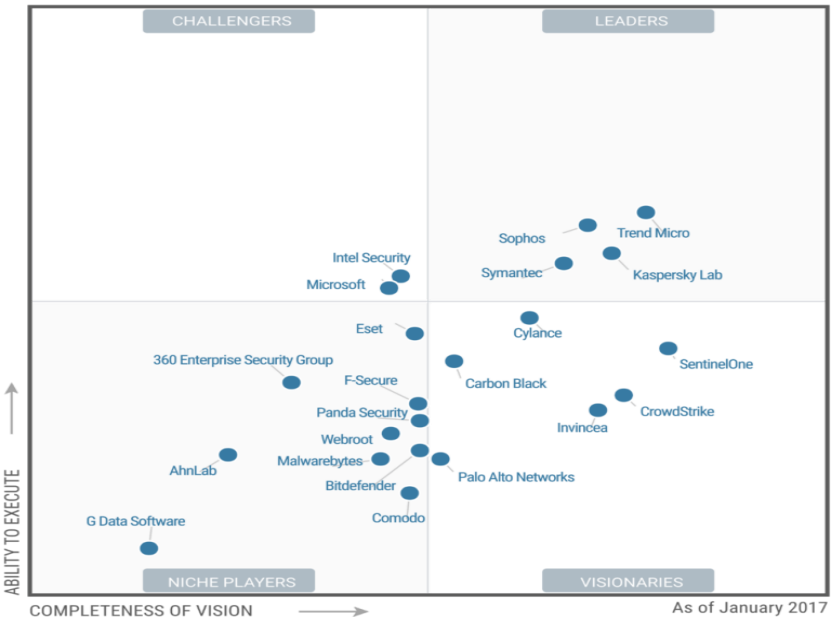


Figura 11. Cuadrante mágico de Gartner para plataformas de protección de endpoints del año 2017.

Fuente: (Trend Micro, 2017)

En el año 2018 destacan como líderes las empresas Symantec, Sophos y Trend Micro.

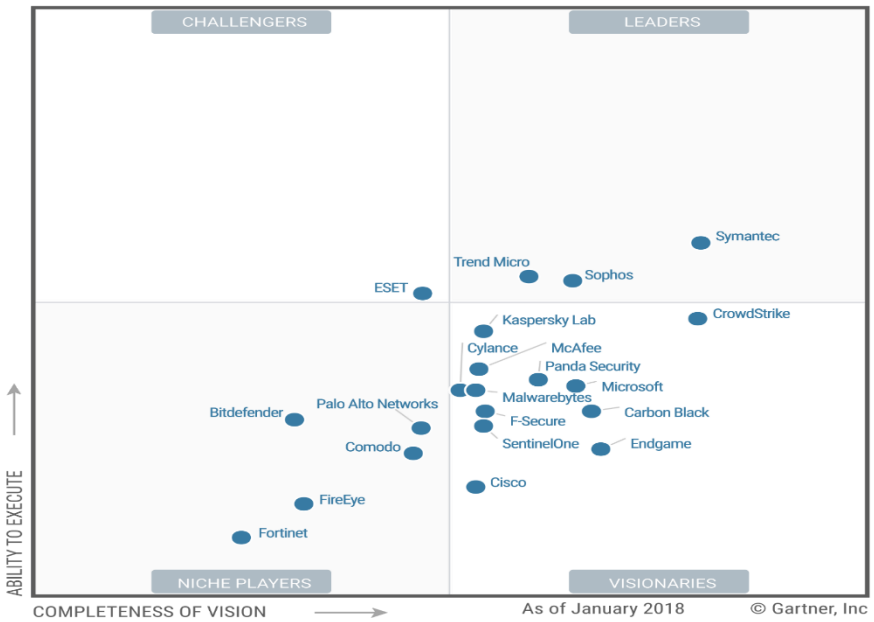


Figura 12. Cuadrante mágico de Gartner para plataformas de protección de endpoints del año 2018.

Fuente: (Sophos, 2018)

Las empresas líderes en cuanto a plataformas de protección de endpoints en los últimos tres años se pueden observar en la siguiente tabla:

Tabla 2. Plataformas destacadas de protección de endpoints.

Año	Puesto	Plataformas de protección de Endpoints
2016	1	Trend Micro
	2	Intel Security
	3	Kaspersky Lab
2017	1	Trend Micro
	2	Kaspersky Lab
	3	Sophos
2018	1	Symantec
	2	Sophos
	3	Trend Micro

Elaborado por: Investigador

Finalmente, la selección de los ataques informáticos a estudiar en la presente investigación se la realizará a partir de estudios y reportes de las siguientes empresas que se han mantenido más tiempo como líderes.

Tabla 3. Plataformas de protección de endpoints

Plataforma de protección de endpoints
Trend Micro
Kaspersky Lab
Sophos

Elaborado por: Investigador

Según el reporte de seguridad cibernética e infraestructura crítica de las Américas elaborado por Trend Micro en el año 2015, los principales métodos utilizados para atacar a las organizaciones son el phishing, las vulnerabilidades sin parches, ataques DDoS, inyección SQL, CSS, ataques originados por hacktivistas y los APTs (amenaza persistente avanzada) (Trend Micro, 2015).

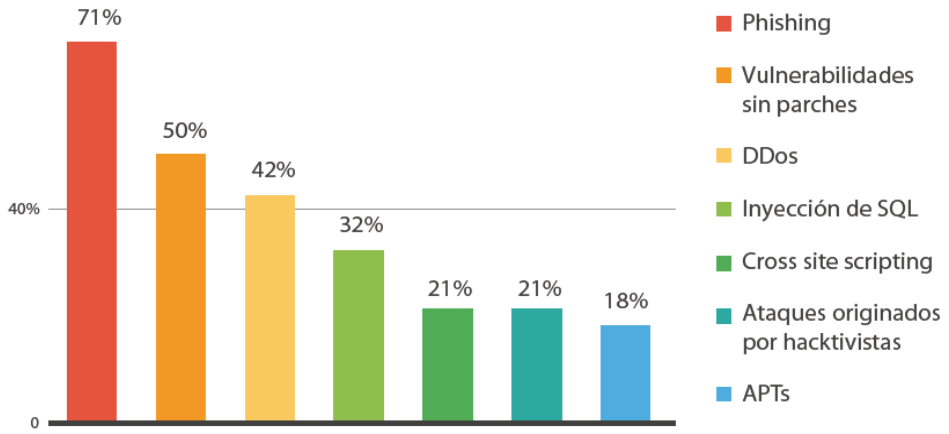


Figura 13. Tipos de ataques informáticos contra organizaciones según Trend Micro.
Fuente: (Trend Micro, 2015)

El reporte global de riesgos de tecnologías de la información elaborado por Kaspersky Lab en el año 2018, indica que las empresas han experimentado ataques, siendo los más comunes el malware, seguidos por el spam y los ataques de phishing (Kaspersky Lab, 2018).

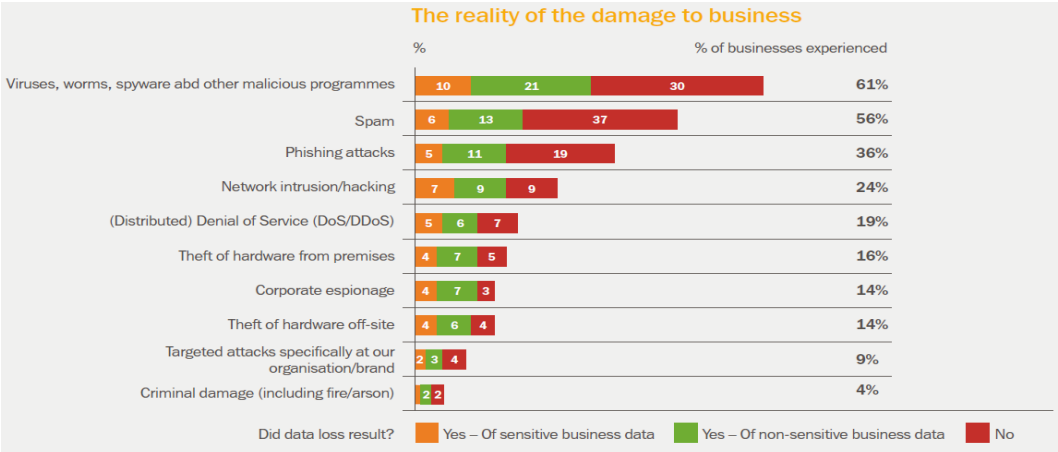


Figura 14. Realidad de los daños al negocio

Fuente: (Kaspersky Lab, 2018)

Con base al estudio denominado "Estado actual de la seguridad de endpoints", realizado por Sophos a finales del año 2017 a 2700 medianas empresas en cinco continentes, el 54% de las empresas se vieron afectadas por ransomware en el último año, con una media del impacto por empresa afectada de 133.000 USD. Los sectores afectados fueron principalmente el sanitario, seguido por el energético, los servicios profesionales y la venta al por menor. Los países más afectados fueron la India, seguida de México, EE. UU. y Canadá (Sophos, 2017).

En la siguiente figura se puede observar el porcentaje de empresas afectadas por ataques de ransomware.

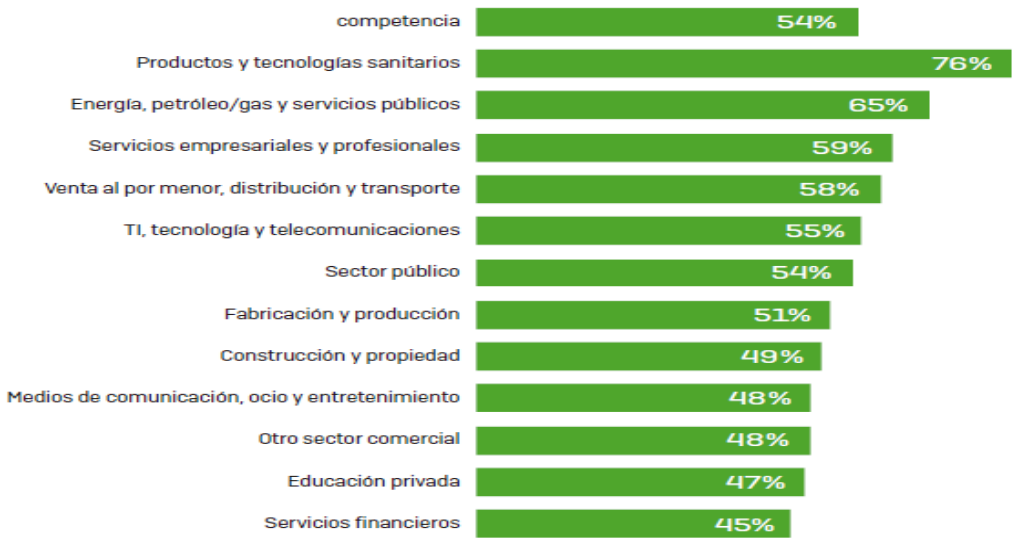


Figura 15. Empresas afectadas por ransomware en el año 2017

Fuente: (Sophos, 2017)

En la siguiente tabla se listan los ataques informáticos más comunes según las investigaciones realizadas por Trend Micro, Kaspersky Lab y Sophos, las tres empresas líderes en seguridad de plataformas endpoints.

Tabla 4. Ataques informáticos más comunes

Plataforma Endpoint	Ataque Informático
Trend Micro	Pishing
	Vulnerabilidades sin parches
	DDoS
	Inyección de SQL
	Cross site scripting
Kaspersky Lab	Virus, gusanos y spyware
	Spam
	Phising
	Intrusiones a la red
	DDoS
Sophos	Ransomware

Elaborado por: Investigador

Tomando en cuenta que los ataques de phishing y los de DDoS, son considerados tanto por Trend Micro como por Kaspersky Lab como los ataques informáticos que han afectado a las organizaciones en el año 2018, se obtiene la muestra para la presente investigación, la cual se puede observar en la siguiente tabla:

Tabla 5. Muestra

Ataque Informático
Phishing
DDoS (Denegación de servicio distribuido)

Elaborado por: Investigador

3.5. Operacionalización de variables

3.5.1. Variable independiente:

Tabla 6. Operacionalización de la variable independiente: Ataques informáticos

Conceptualización o descripción	Dimensiones	Indicadores	Ítems Básicos	Técnicas e instrumentos
Un ataque informático consiste en explotar alguna debilidad o falla que pueda existir en un sistema o en las personas que forman parte de un ambiente informático, todo esto con la finalidad de obtener algún beneficio, por lo general beneficios económicos, provocando daños en la seguridad del sistema que luego afectan directamente a los activos de la organización.	• Debilidades en los sistemas	• Vulnerabilidad	¿Los servidores Linux del GADPO son vulnerables a los ataques DDoS y Phising?	Metodología para efectuar un ataque informático
	• Daños en la seguridad del sistema	• Impacto	¿Cuál es el impacto de los ataques de pishing y DDoS en los servidores Linux del GADPO?	Herramientas para efectuar ataques informáticos Social Engineer Toolkit (SET), Hping3
	• Amenaza	• Nivel de riesgo	¿Qué nivel de riesgo generan los ataques pishing y DDoS en la seguridad de los servidores Linux del GADPO?	Metodología MAGERIT

Elaborado por: Investigador

3.5.2. Variable dependiente:

Tabla 7. Operacionalización de la variable dependiente: Seguridad de servidores con sistema operativo Linux

Conceptualización o descripción	Dimensiones	Indicadores	Ítems Básicos	Técnicas e instrumentos
Consiste en asegurar el servidor, de tal forma que se garantice la integridad, accesibilidad y disponibilidad del activo más importante de una organización como lo es la información, tomando en cuenta principalmente aspectos como uso de protocolos seguros, servicios siempre actualizados y monitoreo de todos los servicios frente a actividades sospechosas.	• Confidencialidad • Integridad • Disponibilidad	• Usuarios atacados • Ataques satisfactorios • Uso de ancho de banda	¿Qué porcentaje de usuarios atacados mordieron el anzuelo y entregaron información confidencial? ¿Los ataques informáticos afectan la disponibilidad de los servicios?	Análisis de la información recolectada Herramientas de monitoreo de servicios, MRTG

Elaborado por: Investigador

3.6. Plan de recolección de información

Tabla 8. Plan de recolección de información

Preguntas básicas	Explicación
¿Para qué?	Para alcanzar los objetivos de la investigación y sustentar la hipótesis planteada.
¿De qué personas u objetos?	Servidores con sistema operativo Linux del GADPO
¿Sobre qué aspectos?	Ataques informáticos a servidores con sistema operativo Linux
¿Quién, Quiénes?	Investigador: Ing. Francisco Javier Aguilar Feijóo
¿Cuándo?	Febrero a Junio de 2019
¿Dónde?	Gobierno Autónomo Descentralizado de la Provincia de Orellana
¿Cuántas veces?	Una
¿Qué técnicas de recolección?	Observación Pruebas
¿Con qué?	Herramientas de Software Inspecciones
¿En qué situación?	En los horarios laborales con profesionalismo investigativo y con absoluta reserva

Elaborado por: Investigador

3.7. Plan de procesamiento de información

Para el procesamiento de la información recolectada, se realizó lo siguiente:

- Revisión minuciosa de la información, depuración de la información defectuosa o irrelevante.
- Repetición de la recolección, en ciertos casos individuales para corregir errores.
- Tabulación de la información.
- Manejo de información (reajuste de cuadros con casillas vacías o con datos reducidos cuantitativamente que no influyen en el análisis).
- Estudio estadístico de datos para presentación de resultados.
- Interpretación de los resultados.

CAPÍTULO 4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. Análisis e interpretación de los resultados

4.1.1. Mecanismos de aseguramiento de servidores con sistema operativo Linux utilizados actualmente en el GADPO

La arquitectura cliente – servidor del sistema de información del GADPO, actualmente se encuentra estructurado en tres niveles, siendo estos las aplicaciones, servidores de aplicaciones y el sistema operativo.

Los principales servicios web con los que cuenta el GADPO son la página web institucional, un aplicativo para la visualización de datos capturados por las estaciones meteorológicas, el geoportal para la visualización de información geográfica, un servidor de proyectos, el servicio de correo electrónico institucional, el servidor de mensajería instantánea Spark y el servicio de seguimiento de trámites Consedoc.

Las distribuciones Linux utilizadas para la implementación de servidores son principalmente Debian y Centos. Todas las implementaciones de servidores se realizan de forma virtual sobre la plataforma de virtualización VMware.

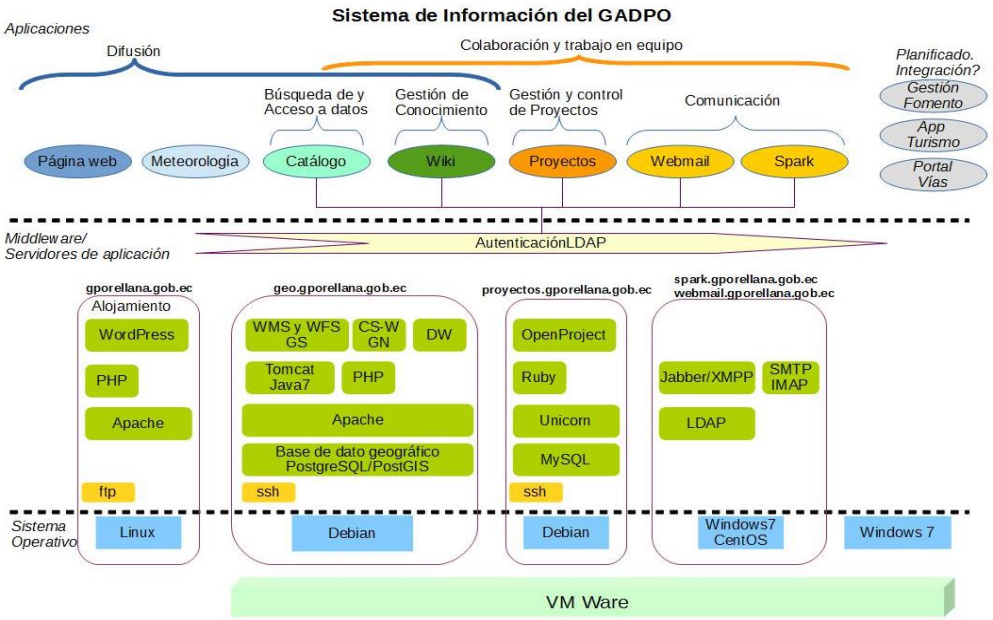


Figura 16. Arquitectura cliente - servidor sistema de información del GADPO

Fuente: Geoportal GADPO

Los servidores Linux con los que cuenta el GADPO se detallan a continuación:

Tabla 9. Servidores Linux del GADPO

Servidor	Función
Consedoc	Sistema para seguimiento de trámites
Zimbra	Servidor de correos institucional
Zentyal	Firewall de la red de datos del GADPO
Openproject	Servidor de Gestión de proyectos
Geoportal	Portal de publicación de información geográfica
Financiero	Base de datos del sistema financiero

Elaborado por Investigador

Como guía para determinar los mecanismos de seguridad de servidores implementados actualmente, se toma la norma internacional ISO 27002:2013, la cual es un manual de buenas prácticas y que como principal objetivo tiene proteger la información de accesos no autorizados, daños físicos, ambientales (M. Torres, 2015).

Entre los mecanismos de seguridad implementados actualmente en el GADPO se tiene:

1. **Control de accesos**

- **Control de acceso a sistemas y aplicaciones**

- **Procedimientos seguros de inicio de sesión**

Para la administración de los servidores Linux del GADPO, se ha implementado el mecanismo de autentificación Secure Shell (ssh) mediante llave pública/privada. Las llaves privadas se han configurado en los equipos del Jefe de Informática y Tecnología, Profesional Informático 3 y en el equipo del Profesional Informático 2, siendo los profesionales antes mencionados los únicos que pueden acceder remotamente a los servidores Linux para realizar labores de administración.

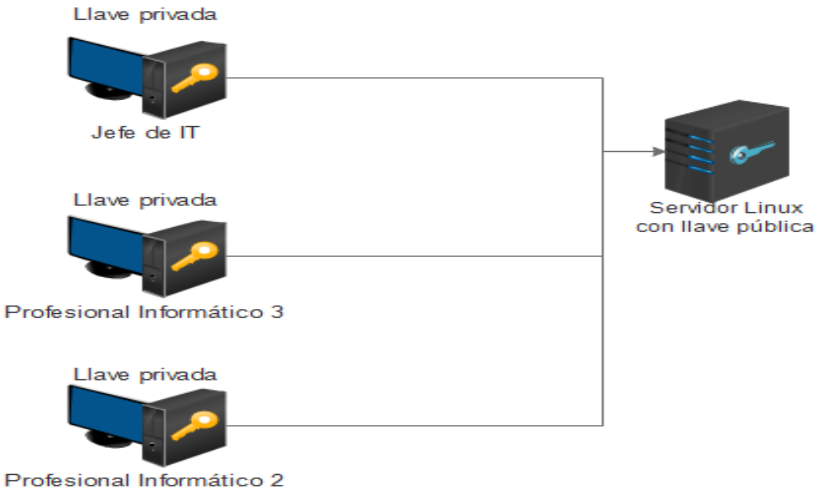


Figura 17. Autenticación mediante llave pública/privada

Elaborado por: Investigador

2. Seguridad operativa

- **Copias de seguridad**

Como mecanismo de protección frente a los desastres que se puedan presentar ya sea de tipo natural, o por algún fallo humano que puedan ocasionar pérdidas de información, el GADPO cuenta con una licencia de la librería de respaldos de IBM, llamada Tivoli Storage Manager (TSM), la misma que realiza los respaldos de información de los servidores existentes en el centro de datos a un sistema de cintas. En la siguiente figura se puede observar el esquema del sistema de respaldos existente.

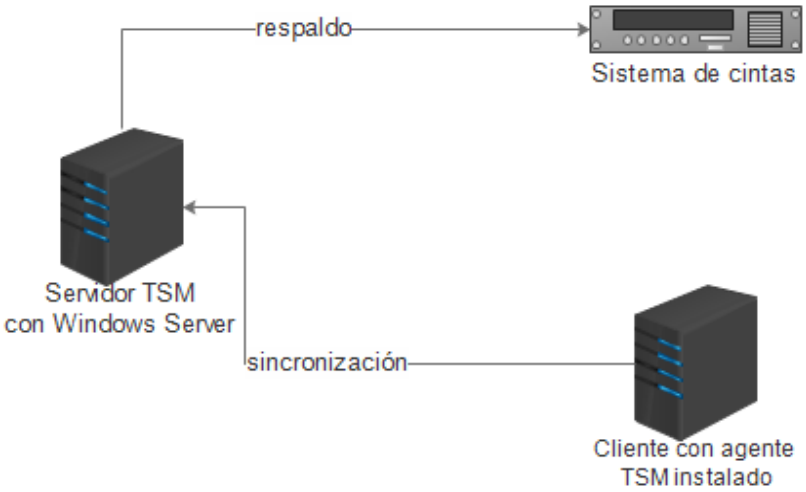


Figura 18. Esquema del sistema de respaldos del GADPO

Elaborado por: Investigador

El calendario establecido para los respaldos de información es el siguiente:

Nodo	Sistema operativo	Directorio	Backup Incremental	Backup full	Backup mensual	Backup anual	Tipo de servidor
Financiero	Centos	/opt/databases/* /opt/postgresql/* /home/*	L– V (23h00)	Sábado (18h00)	Tercer domingo del mes a las 10h00	Primer domingo de enero a las 10h00	Máquina virtual
Correo Electrónico	Centos	/opt/zimbra/* /root/*		Sábado (17h00)	Tercer domingo del mes a las 04h00	Primer domingo de enero a las 04h00	Máquina virtual
Consedoc	Centos	/var/www/* /var/lib/pgsql/*	L – V (20h00)	Sábado (14h00)	Tercer domingo del mes a las 08h00	Primer domingo de enero a las 08h00	Máquina virtual
Proyectos	Debian	/var/www/* /var/lib/pgsql/*	L – V (18h00)	Sábado (13h00)	Tercer domingo del mes a las 09h00	Primer domingo de enero a las 09h00	Máquina virtual
Geoportal	Debian	/var/www/* /var/lib/pgsql/*	L – V (19h00)	Sábado (12h00)	Tercer domingo del mes a las 07h00	Primer domingo de enero a las 07h00	Máquina virtual

Elaborado por: Investigador

Fuente: Jefatura de Informática y Tecnología del GADPO

3. Seguridad física y ambiental

- **Áreas seguras**

- **Acceso al centro de datos**

El acceso al centro de datos está autorizado únicamente para el personal que labora en la JIT mediante el uso de una tarjeta magnética.

Figura 19. Puerta de acceso al centro de datos del GADPO
Elaborado por: Investigador

- **Seguridad de los equipos**

- **Detectores de Humo**

Para minimizar el riesgo de que los equipos informáticos puedan verse comprometidos por un incendio, se tiene instalado un detector de humo, el cual emite una alarma en caso de detectar humo en el aire. En la siguiente figura se puede observar el equipo instalado:

Figura 20. Detector de humo del centro de datos

Elaborado por: Investigador

- **Sistema de alimentación ininterrumpida**

Para proteger los equipos informáticos existentes en el centro de datos del GADPO de las variaciones de voltaje y los cortes del suministro de energía eléctrica se ha implementado un sistema de alimentación ininterrumpida (SAI). El equipo instalado tiene una potencia de 15 KVA y brinda una autonomía de 45 minutos en caso de cortes de energía eléctrica. La siguiente figura muestra el equipo instalado.

Elaborado por: Investigador

Figura 21. SAI del centro de datos del GADPO

4. Seguridad en las telecomunicaciones

- **Controles de red**

- **Firewall de red**

Para proteger la infraestructura de servidores de accesos no autorizados desde internet se cuenta con un cortafuego (Firewall) implementado con la distribución Linux Zentyal. Además de proteger la red de datos, este equipo brinda los servicios de configuración dinámica de host (DHCP), resolución de nombres (DNS), servidor intermediario (PROXY) y permite establecer la comunicación entre las distintas Vlans existentes como también el acceso a internet de los usuarios internos.

En la siguiente figura se muestra un esquema general de la red de datos del GADPO.

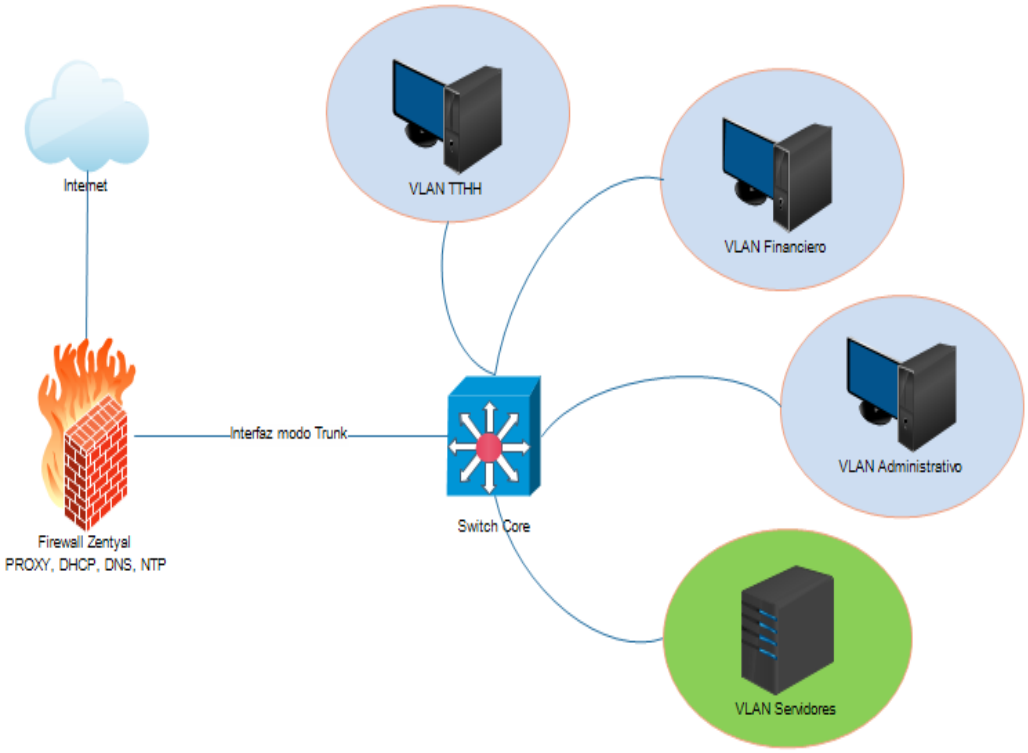


Figura 22. Esquema general de la red de datos del GADPO

Elaborado por: Investigador

- **Mecanismos de seguridad asociados a servicios en red**

- **Certificado de seguridad SSL**

Como medida de prevención frente al espionaje electrónico y el uso mal intencionado de la información, se cuenta con un certificado de seguridad para el cifrado de la información que se transmite por la red. Dicho certificado ha sido

instalado en los servidores Linux que ofrecen servicios que requieren autenticación web.

Las características del certificado adquirido son las siguientes:

Tabla 10. Certificado SSL adquirido por el GADPO

Tipo de certificado	Encriptación	Precio anual	Número de subdominios
Wildcard SSL	256 – bit	439 USD	Ilimitado

Elaborado por: Investigador

4.1.2. Mejores prácticas y herramientas existentes para el aseguramiento de servidores

Con la finalidad de poder minimizar el impacto que puedan provocar los ataques informáticos de phishing y DDoS en la seguridad de los servidores Linux del GADPO, es necesario determinar las mejores prácticas y herramientas existentes para contrarrestar los efectos de este tipo de ataques.

4.1.2.1. Alternativas para combatir el phishing

Para el caso de los ataques informáticos de phishing, se pueden mitigar haciendo uso de respuestas organizativas y respuestas técnicas:

4.1.2.1.1. Respuestas organizativas

Esta estrategia adoptada por algunas empresas para combatir el phishing, consiste en entrenar a sus empleados, de tal forma que puedan reconocer posibles ataques(González & Peña, 2013) (Alvarado, 2017).

El Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio de los Estados Unidos, propone una iniciativa en materia de implantar en las organizaciones una cultura de seguridad de la información denominada "NIST SP 800-50 Construcción de un Programa de Concientización y Entrenamiento de Seguridad de Tecnologías de Información" (Vega, 2015).

La NIST SP 800-50 establece cuatro pasos en lo que respecta a un programa de concientización y entrenamiento de seguridad de la información, los mismos que se pueden observar en la siguiente figura (Álvarez, 2017):

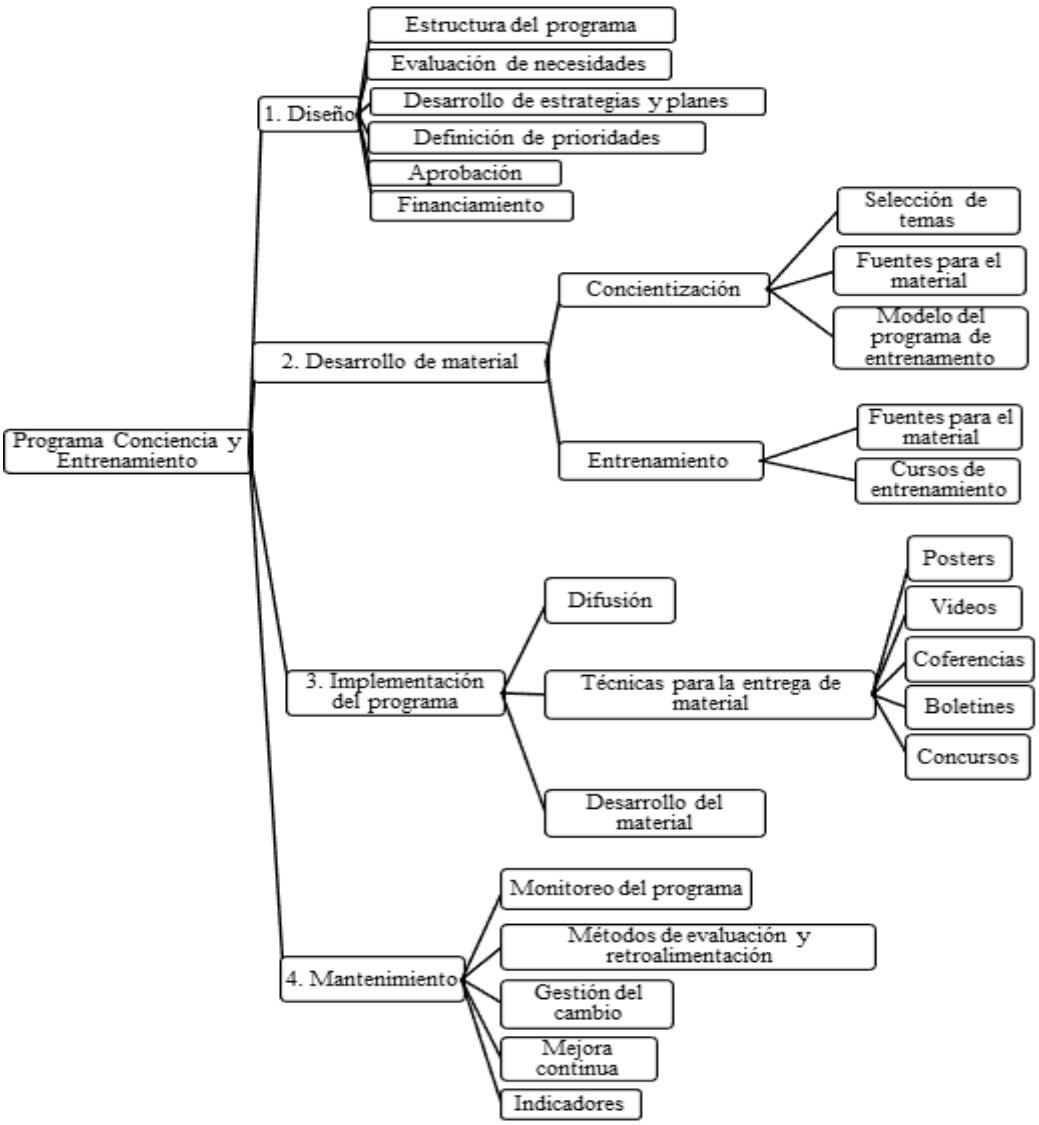


Figura 23. Estructura de un plan de capacitación según NIST SP 800-50

Elaborado por: Investigador

- **Diseño**

En este punto es importante que el área de TI realice una evaluación sobre la estrategia de entrenamiento que será desarrollada y aprobada. Es importante que el programa de capacitación sea relevante a la cultura organizacional.

El diseño del plan de concientización comprende:

- **Estructura del programa de concientización y entrenamiento**

El modelo del programa puede ser centralizado o descentralizado, en el primer caso la responsabilidad y presupuesto para el área de TI en materia de capacitación se asignan a una autoridad central. En lo que respecta al modelo descentralizado existe

una autoridad coordinadora central, pero la ejecución se delega a la línea de gestión de los funcionarios de la organización.

- **Evaluación de necesidades**

Es un proceso que puede ser empleado para determinar las necesidades de concientización y entrenamiento en la organización. Los resultados de la evaluación pueden proporcionar la justificación para que la alta gerencia asigne los recursos necesarios para las necesidades detectadas.

- **Desarrollo de estrategias y planes**

Una vez identificadas las falencias existentes dentro de la organización, se debe proceder con la elaboración del plan, que de incluir entre sus principales elementos el alcance del plan, objetivos del plan, roles y responsabilidades, a quién va dirigido, temas a tratar, frecuencia de las capacitaciones y la evaluación y renovación del material creado.

- **Definición de prioridades**

Si existen limitaciones presupuestarias, se debe priorizar sobre aquellas áreas que la organización considere más sensibles.

- **Aprobación**

Establece quien o quienes serán los responsables de la revisión y aprobación del plan de capacitación.

- **Financiamiento**

Se debe planificar e indicar los recursos a ser utilizados en el programa de capacitación.

- **Desarrollo del material de concientización**

Según los requerimientos de la NIST SP 800-16 “Requerimientos para entrenamiento en Seguridad de Tecnologías de la Información” el material para el desarrollo del plan se puede obtener de diferentes fuentes como Organizaciones profesionales de seguridad de la información, periódicos, conferencias de seguridad, seminarios online, boletines sobre seguridad en sitios web.

5. Implementación del programa

Para iniciar la implementación del programa, en primer lugar, se debe socializar el programa con la alta gerencia de la organización para conseguir los recursos necesarios, y de esta forma dar inicio a la implementación del mismo.

Las técnicas para difundir la información deben de estar acorde a la tecnología con que disponga la organización, entre las que se podrían utilizar tenemos (Álvarez, 2017):

- Posters sobre lo que debería hacerse y lo que no.
- Videos interactivos institucionales.
- Fondos de pantalla con mensajes de sensibilización.
- Cuadernos, relojes o elementos de oficina con mensajes alusivos.
- Boletines vía email.
- Sesiones con instructores.

6. Mantenimiento

Un plan de concientización y entrenamiento, no podrá renovarse sin antes haber evaluado su desempeño dentro de la organización, para ello pueden utilizarse algunos métodos como los siguientes (Álvarez, 2017):

- Evaluaciones o cuestionarios
- Foros abiertos con usuarios que participaron en la capacitación.
- Entrevistas
- "Benchmarking", es decir comparar el método que se ha implementado con el de otras instituciones similares.
- Realizar ataques de ingeniería social, una vez realizadas las capacitaciones.

4.1.2.1.2. Respuestas Técnicas

Para protegerse del phishing con respuestas técnicas las empresas hacen uso de programas informáticos anti-phishing. La mayoría de estos programas trabajan identificando phishing en sitios web y correos electrónicos; algunos software anti – phishing pueden por ejemplo, integrarse con los navegadores web y clientes de correo electrónico (Alvarado, 2017).

El Instituto Nacional de Ciberseguridad de España (INCIBE), en su catálogo de empresas y soluciones de ciberseguridad del año 2016 presenta algunas de las más destacadas soluciones antiphishing existentes.

- **Cisco ProtectLink Gateway**

Es una potente solución que brinda protección completa del correo electrónico y la web. Integra un potente antispam, antiphishing, filtrado de contenido de URL, y

evalúa la reputación de los sitios web al fin de bloquear los ataques online y por correo electrónico.

- **Spam & Virus Firewall**

Es una solución integral de hardware y software diseñada para proteger a los servidores de correo electrónico de ataques de correos no deseados, phishing y software espías.

- **Cyber Security**

Una solución de seguridad de propiedad de la empresa Codine, protege a los empleados de su empresa contra los intentos de phishing y de suplantación de identidad gracias a un filtro permanente activo que analiza todo lo que pasa por su red.

- **Netcraft Toolbar**

Desarrollado por la empresa Netcraft, es una extensión de navegador que permite comprobar la veracidad de las páginas web y el riesgo de ataque de phishing.

- **Optenet Mailsecure**

Ofrece en una misma solución la capacidad de filtrado de contenidos, antispam, antiphishing, antivirus y antispyware, garantizando la seguridad de las redes empresariales.

Una vez analizadas las alternativas existentes para mitigar los ataques informáticos de phishing, es importante mencionar que una organización puede contar con la mejor tecnología, el mejor software de seguridad; pero esto no es suficiente para mitigar este tipo de ataques, lo que es verdaderamente fundamental es crear una conciencia real en los empleados, considerados como el eslabón más débil en la cadena de seguridad de la información. Para ello es de vital importancia la capacitación en el ámbito de la seguridad informática para que tomen conciencia sobre los riesgos a los que están expuestos tanto ellos como las organizaciones. (Alvarado, 2017) (Álvarez, 2013) (Ministerio de Tecnologías de la Información y Comunicaciones de Colombia, 2016).

4.1.2.2. Alternativas para mitigar los ataques DDoS

Los ataques DDoS se dividen en tres tipos, los ataques basados en volumen entre los que se encuentran los ataques User Datagram Protocol (UDP) Flood, Internet Control Message Protocol (ICMP) Flood que tienen como objetivo saturar el ancho de banda del sitio atacado y la magnitud es medida en bits por segundo (Bps). Se tiene también los ataques de protocolo que incluyen los ataques SYN floods, ataques de fragmentación de paquetes, ping de la muerte, Smurf DDoS entre otros, este tipo de ataque consume recursos reales del servidor o de los equipos de comunicación intermedios como firewalls y balanceadores de carga, la magnitud se mide en paquetes por segundo (Pps) (Rosety, 2016).

Por último, se tiene los ataques a la capa de aplicación que incluye inundaciones GET/POST, ataques dirigidos a vulnerabilidades de Apache, Windows, etc. El objetivo de estos ataques es bloquear el servidor web y la magnitud se mide en solicitudes por segundo (Rps) (Rosety, 2016).

En la siguiente figura se puede observar la taxonomía de un ataque DDoS:

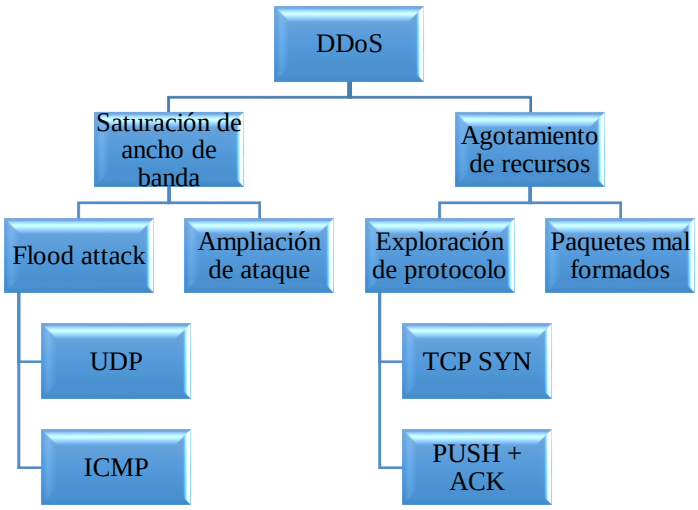


Figura 24. Taxonomía de un ataque DDoS

Fuente: Rocha & Moreira, 2015)

Elaborado por: Investigador

Según el reporte de ataques DDoS elaborado por Kaspersky Lab, en el segundo trimestre del año 2018 el 80.2% de los ataques fueron de tipo SYN Flood, un 10.6% de tipo UDP, mientras que los ataques TCP, HTTP e ICMP constituyen un mínimo porcentaje.

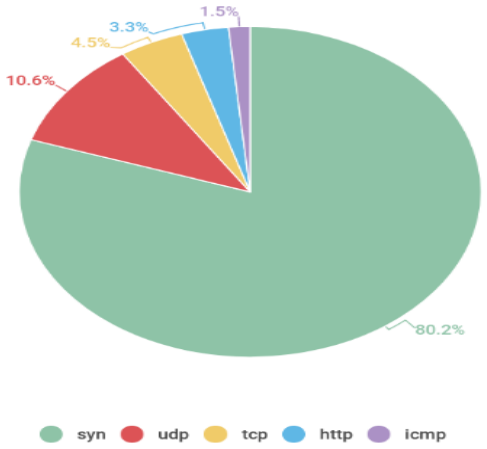


Figura 25. Ataques DDoS realizados en el segundo trimestre de 2018

Fuente: Kaspersky Lab

En el tercer y cuarto trimestre del año 2018, Karsperky Lab afirma que los ataques DDoS de tipo SYN Flood siguen siendo los más populares ubicándose en un primer lugar con un 58,20%.

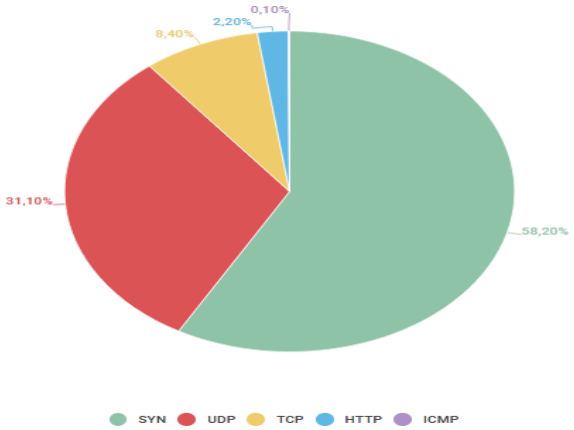


Figura 26. Ataques DDoS realizados en el tercer y cuarto trimestre de 2018

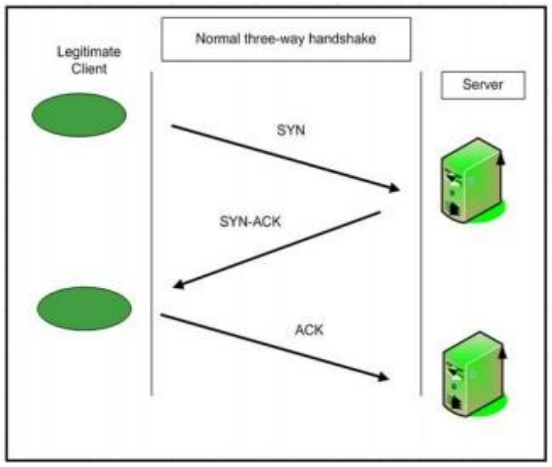
Fuente: Kaspersky Lab

La figura 49, muestra que el ataque de tipo SYN Flood ocupa el 80.2% de los ataques DDoS ocurridos en el segundo trimestre del año 2018. La figura 50 muestra de igual forma que este tipo de ataque sigue estando en los primeros lugares en el tercer y cuarto trimestre de 2018 con un 58.20%, por lo cual en la presente investigación serán objeto de estudio los ataques DDoS de este tipo.

El ataque de inundación SYN Flood, se basa en el enlace normal de tres vías (three way handshake) que se realiza en una conexión TCP.

En un enlace normal de tres vías sucede lo siguiente (Salunkhe, 2017):

1. El cliente envía un paquete inicial SYN.
2. El servidor responde al cliente con un paquete SYN – ACK (SA), mediante el cual le indica que el puerto está activo y se están aceptando conexiones.
3. Finalmente, el cliente responde con un paquete ACK, quedando de esta forma establecida la conexión.



(Salunkhe, 2017) Figura 27. Enlace normal de tres vías en una conexión TCP

Fuente: (Salunkhe, 2017)

En un ataque SYN Flood, el atacante envía conexiones TCP SYN a alta velocidad a la máquina víctima, más de lo que esta puede procesar. Este tipo de ataque provoca una denegación de servicio que agota los recursos del servidor.

El atacante puede hacer efectivo el ataque SYN Flood usando dos métodos (Salunkhe, 2017):

1. El cliente malicioso enviará paquetes SYN que suelen ser de 64 bytes, la víctima en un intento de reconocimiento responderá con un paquete SYN-ACK al atacante y este simplemente ignorará los SYN-ACK enviados por el servidor y continuará enviando nuevos paquetes SYN.
2. En otro método el atacante falsifica la dirección ip de origen (IP Spoofing) y envía paquetes SYN al servidor. El servidor víctima comenzará a enviar paquetes SYN-ACK a las direcciones ip falsificadas quedando a la espera de la respuesta ACK. Dado que las direcciones ip falsificadas no responden, el servidor quedará con conexiones abiertas, lo que provocará una denegación de servicios a clientes legítimos por agotamiento de recursos.

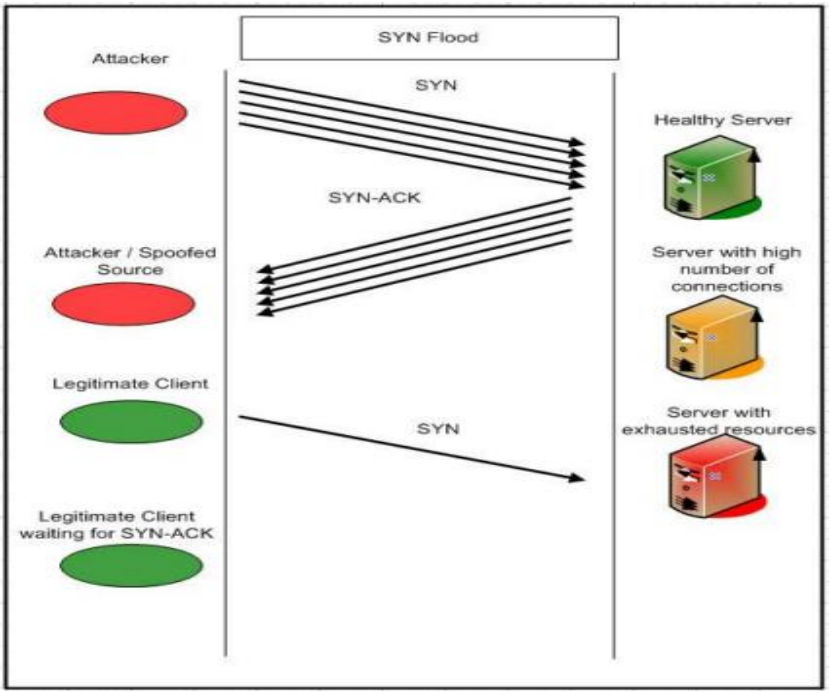


Figura 28. Ataque SYN Flood

Fuente: Salunkhe, 2017

Entre las alternativas para mitigar los efectos de los ataques DDoS SYN Flood tenemos:

4.1.2.2.1. Uso de Iptables

Para mitigar los efectos de los ataques DDoS de tipo SYN Flood se puede utilizar Iptables, conjuntamente con SYN-Cookies, SYN-Cache y SYN-Proxy (INCIBE, 2018) (RedHat, 2014).

Iptables es parte del proyecto NetFilter un framework que permite manipular paquetes de red (Qasim & Musawi, 2012).

TCP SYN Cookies fue implementada para mitigar los ataques DDoS SYN Flood. Asegura que el servidor no tenga que almacenar cualquier información para conexiones medio abiertas. SYN Cookies contiene toda la información requerida por el servidor para que la solicitud sea válida, y cuando están activadas el servidor no sabe que el paquete ACK de retorno se pierde y por lo tanto la retransmisión no sería posible (Shah & Kumar, 2018).

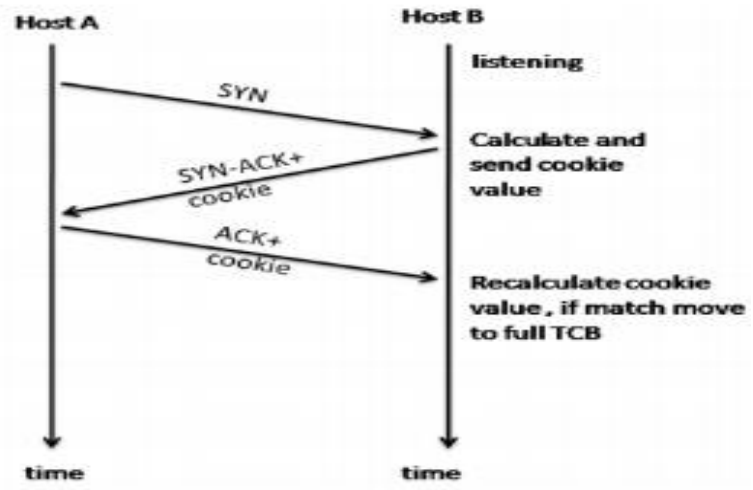


Figura 29. Esquema de funcionamiento de Syn Cookies

Fuente: (Bani-hani & Al-ali, 2013)

TCP SYN Cache almacena cada nueva conexión en un Thread Control Block (TCB), que a su vez es almacenado en una tabla hash con un depósito limitado. El depósito en el que se almacena el TCB se selecciona mediante hashing las direcciones IP, puertos y bits secretos que el servidor eligió de antemano. Los paquetes que usen direcciones ip falsificadas no serán recibidos ya que el cliente es ahora autenticado. Con el uso de SYN Cache el servidor no asigna recursos para conexiones incompletas; como dispositivo de mitigación asegura que la conexión sea legítima (Julian, 2019) (Bani-hani & Al-ali, 2013).

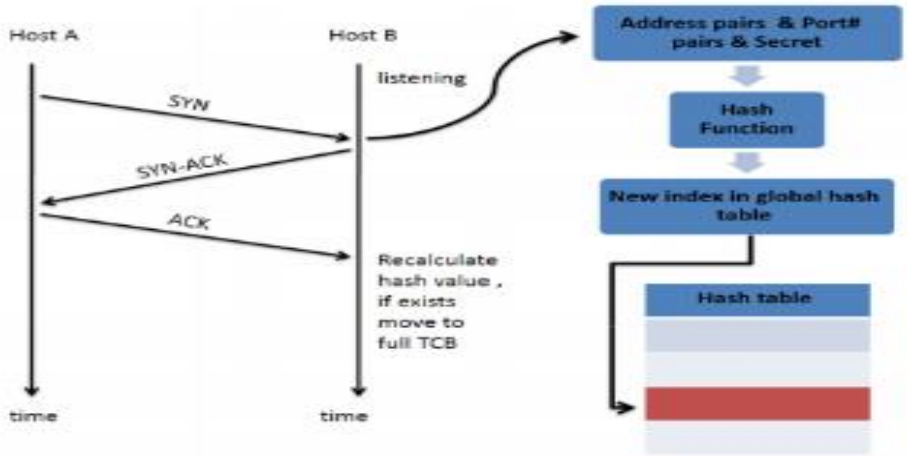


Figura 30. Esquema de funcionamiento de SYN Cache

Fuente: (Bani-hani & Al-ali, 2013)

SYN Proxy trabaja conjuntamente con SYN Cookies para mitigar el problema de inundación que se genera por la gran cantidad de conexiones falsas que crea este tipo de ataque. Para ello se envía una SYN Cookie y evita crear cualquier estado hasta que se vea el paquete SYN – ACK (RedHat, 2014).

4.1.2.2.2. Protección basada en Appliances

Este tipo de protección hace uso de dispositivos especiales de protección DDoS que se pueden conectar a la red o centros de datos para proteger los servicios contra los diversos tipos de ataques DDoS (Malina, Dzurenda, & Hajny, 2015).

Entre las soluciones que destacan se tiene:

- **Radware DefensePro.-** Diseñado para brindar protección DDoS a datacenters de empresas que generan grandes volúmenes de tráfico en especial empresas que se dedican al comercio electrónico o son proveedores de servicios en la nube.
- **Check Point DDoS Protector.-** Brinda protección frente a los ataques DDoS de tipo TCP, UDP, ICMP, IGMP. Es una solución ideal para extensos data centers que generan un tráfico de red sobre los 40 Gbps.
- **Juniper DDoS Secure.-** Protege la infraestructura contra los ataques DDoS SYN Flood y los ataques DDoS a la capa de aplicación. Es ideal para redes que generan un tráfico de 10 Gbps.

Las soluciones antes mencionadas son desarrolladas por empresas que se dedican a la seguridad de redes y son utilizados por lo general en data centers de empresas que se dedican al comercio electrónico y que manejan altos presupuestos para la implementación de este tipo de tecnologías (Malina et al., 2015).

4.1.2.2.3. Protección basada en una solución en la nube

Este tipo de soluciones están diseñadas para pequeñas y medianas empresas que no pueden adquirir appliances anti – DDoS.

Destaca entre las soluciones en la nube para la protección de ataques DDoS CloudFlare Enterprise.

En la siguiente tabla se muestra el costo aproximado de implementación según la información proporcionada por la empresa CloudFlare.

Tabla 11. Costo implementación solución anti DDoS en la nube CloudFlare

Número de empleados	Dominios	Subdominios	Ancho de banda	Valor Mensual	Valor Anual
600	5	Ilimitado	40 Mbps	1500 USD	18000 USD

Elaborado por Investigador

Fuente: (CloudFlare, 2019)

De las tres alternativas analizadas para la mitigación de los ataques DDoS, en la presente investigación se implementó la mitigación de ataques DDoS con iptables conjuntamente con TCP SYN Cookies, TCP SYN Cache y SYN Proxy, dado que estas herramientas están recomendadas por la importante empresa Red Hat líder a nivel mundial en soluciones de código abierto, y además al ser herramientas basadas en software libre no se requiere la adquisición de licencias para su implementación.

4.1.3. Ejecución de ataques informáticos

La selección de las herramientas para efectuar los ataques informáticos de pishing y DDoS a los servidores Linux del GADPO fue realizada en base a la revisión de estudios como tesis y artículos, con la finalidad de que los resultados obtenidos sean confiables.

El sistema operativo utilizado fue Kali Linux, el cual es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad (Avilés & Silva, 2017).

El ataque de pishing fue elaborado con la ayuda de la herramienta SET, la misma que constituye una de las mejores soluciones para crear ataques de este tipo (Esquerra, 2014).

Para realizar el ataque DDoS se utilizó la herramienta de código abierto HPING3, su fin es generar paquetes de conexión para explotar vulnerabilidades del protocolo de control de transmisión/protocolo de internet (TCP/IP). Por su capacidad para generar paquetes TCP, es considerada una de las herramientas más completa para simular ataques de inundación TCP SYN (Mosquera, 2018).

La siguiente tabla muestra un resumen de las herramientas utilizadas:

Tabla 12. Herramientas utilizadas para efectuar ataques informáticos

Herramienta	Finalidad
Kali Linux	Sistema operativo a utilizar para realizar las pruebas de penetración
Social Engineer Toolkit	Efectuar ataques de pishing
Hping3	Efectuar ataques de denegación de servicio distribuido

Elaborado por Investigador

Al momento de realizar un pen testing, existen tres tipos de pruebas que se pueden realizar, las pruebas de caja blanca (white boxtesting) en donde el atacante tiene conocimiento total del objetivo, las pruebas de caja negra (black boxtesting) en las cuales no se tiene conocimiento de la red ni de los sistemas que van a ser atacados y las pruebas de caja gris (gray boxtesting) en las que el pentester tiene conocimiento sobre algunos aspectos del sistema (Esquerra, 2014).

Las pruebas de seguridad a realizar en la presente investigación, adoptarán la modalidad de las pruebas de caja gris, ya que se tiene cierto conocimiento sobre la arquitectura de la red de datos e infraestructura de servidores del GADPO.

Los ambientes para realizar los ataques tanto de pishing como de DDoS se detallan a continuación:

4.1.4. Ataque de phishing a servidores Linux del GADPO

Para llevar a cabo el ataque de pishing se estableció el siguiente esquema de red:

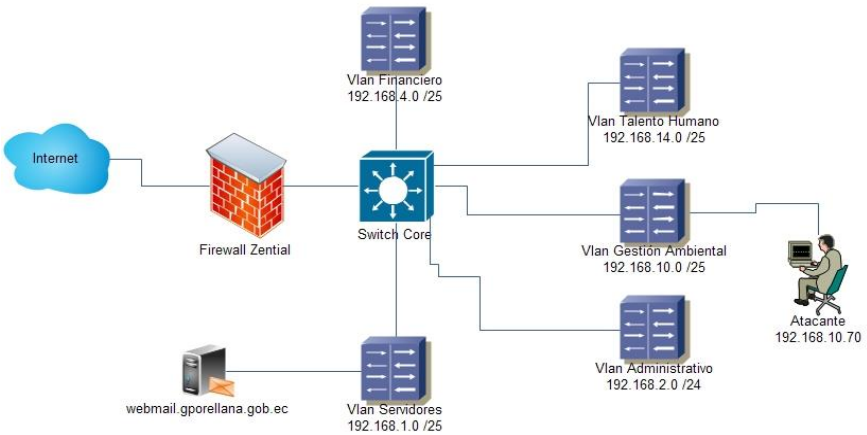


Figura 31. Esquema de red para realizar ataque de pishing

Elaborado por: Investigador

Se realizaron varios ataques de pishing a los servidores Linux del GADPO, se seleccionó aquellos que requerían autenticación vía web, y cuyos sitios se podían clonar para realizar este tipo de intrusión.

Intento 1: Ataque de pishing al servidor de correo electrónico institucional

Para efectuar el ataque de pishing, se configuró una máquina virtual con Kali Linux, se utilizó la herramienta SET para clonar en primer lugar el sitio web del servidor de correos, y como medio de difusión para realizar el engaño de pishing a los usuarios se utilizó el sistema de mensajería interna Spark.

En la consola de Kali Linux se inicia la herramienta SET

```
root@kali:~/Descargas# setoolkit
```

Se muestran las distintas opciones que posee la herramienta, se escoge la opción Social – Engineering Attacks

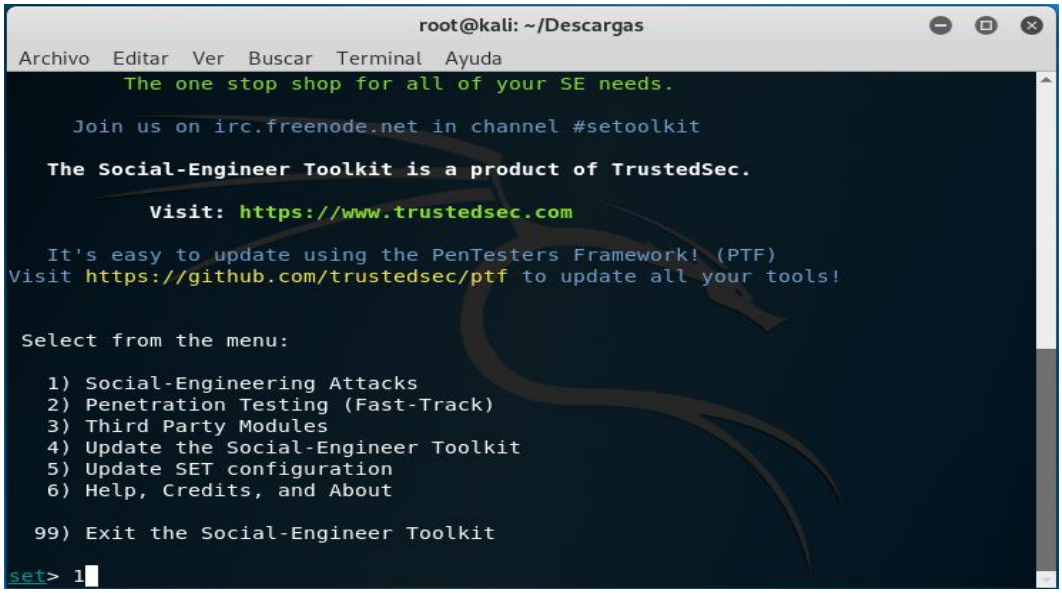


Figura 32. Opciones herramienta Social Engineering Toolkit

Elaborado por: Investigador

A continuación, aparece el siguiente menú de opciones en el que se escoge Website Attack Vectors

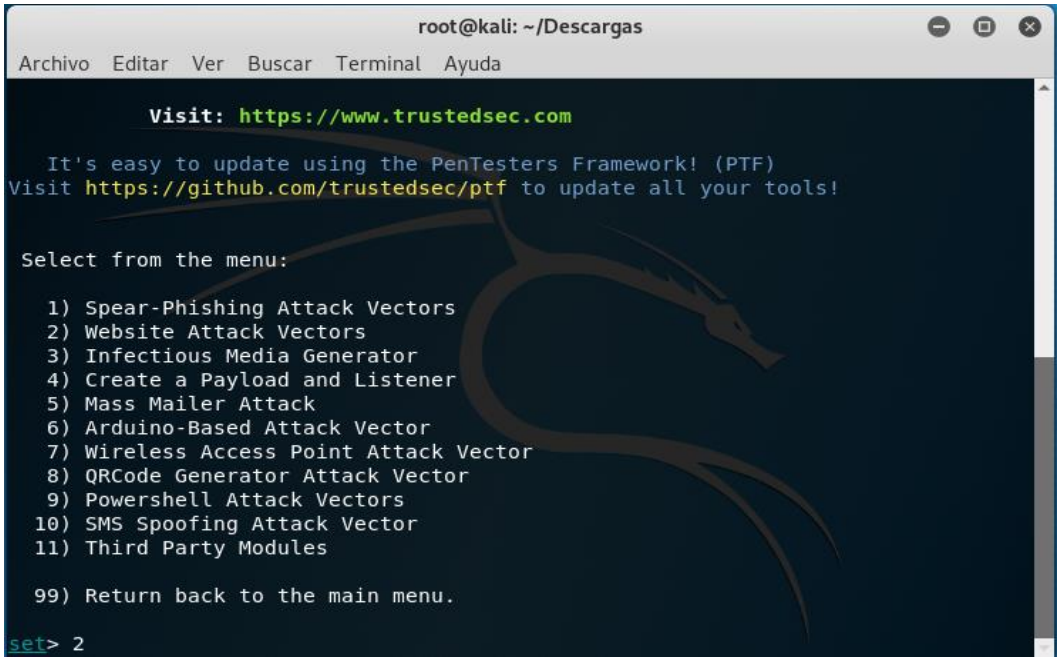


Figura 33. Herramientas para Ingeniería Social

Elaborado por: Investigador

Se selecciona la opción Credential Harvester Attack Method

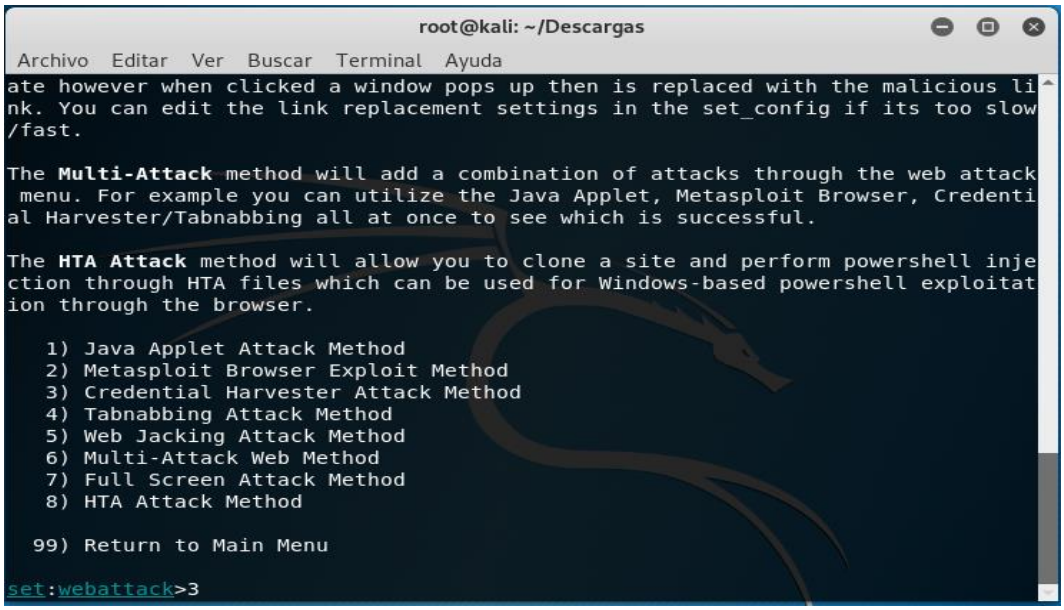


Figura 34. Tipo de ataque de pishing

Elaborado por: Investigador

Se escoge la opción Site Cloner

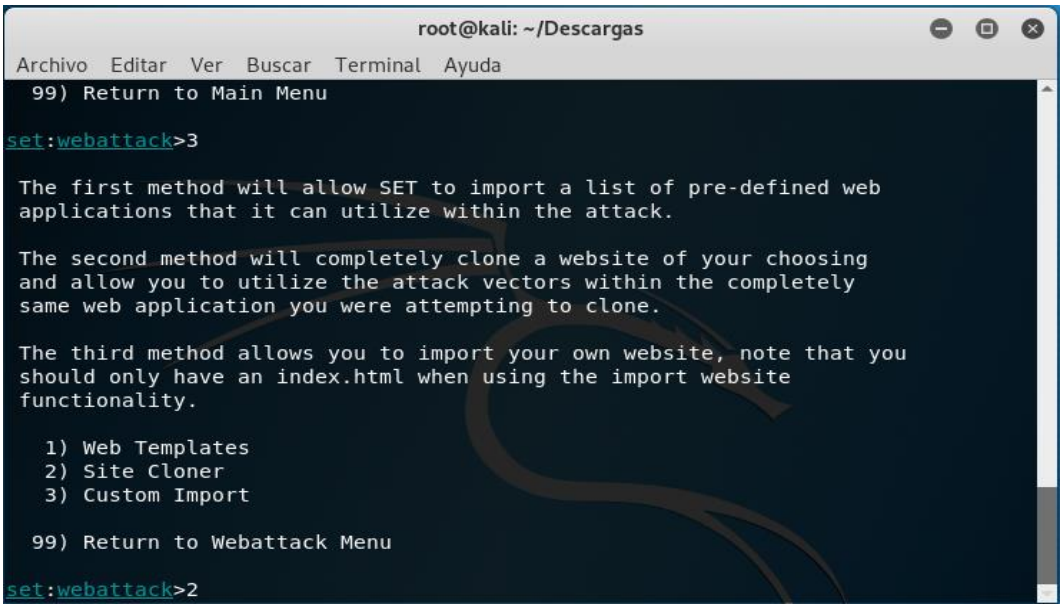


Figura 35. Opciones de clonado de un sitio web

Elaborado por: Investigador

Finalmente se especifica la dirección ip del equipo desde donde se va escuchar para realizar el ataque y la url del sitio que se desea clonar. En este caso la url será el nombre del servidor de correos webmail.gporellana.gob.ec.

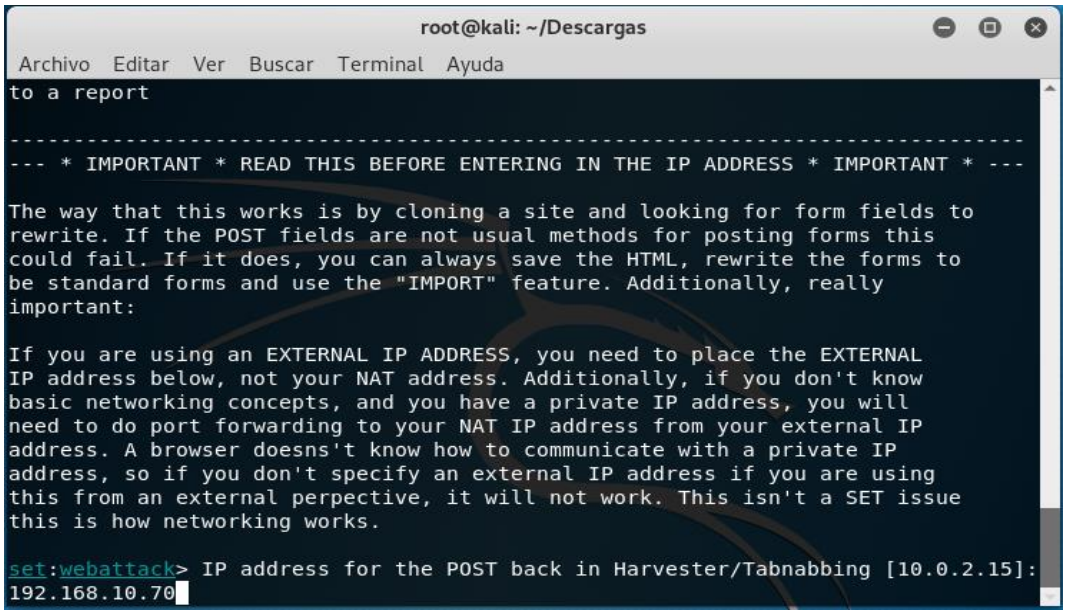


Figura 36. Especificación de dirección IP

Elaborado por: Investigador

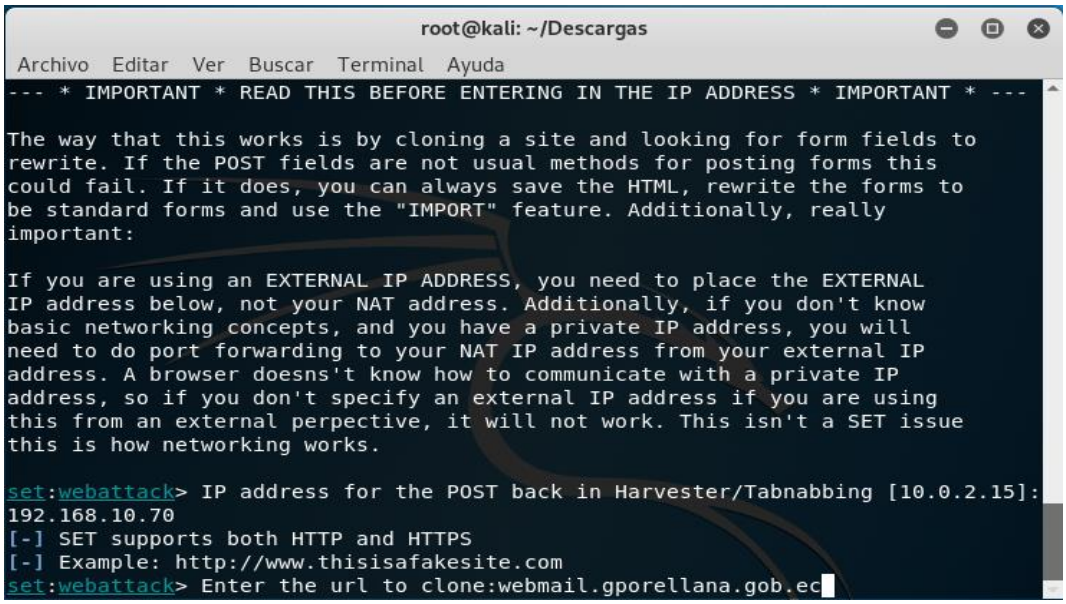


Figura 37. Ingreso de la url del sitio a clonar

Elaborado por Investigador

Con esto ya se tiene clonado el sitio web del servidor de correo electrónico institucional. Se puede verificar accediendo mediante un navegador a la dirección ip del servidor donde está instalado Kali Linux.

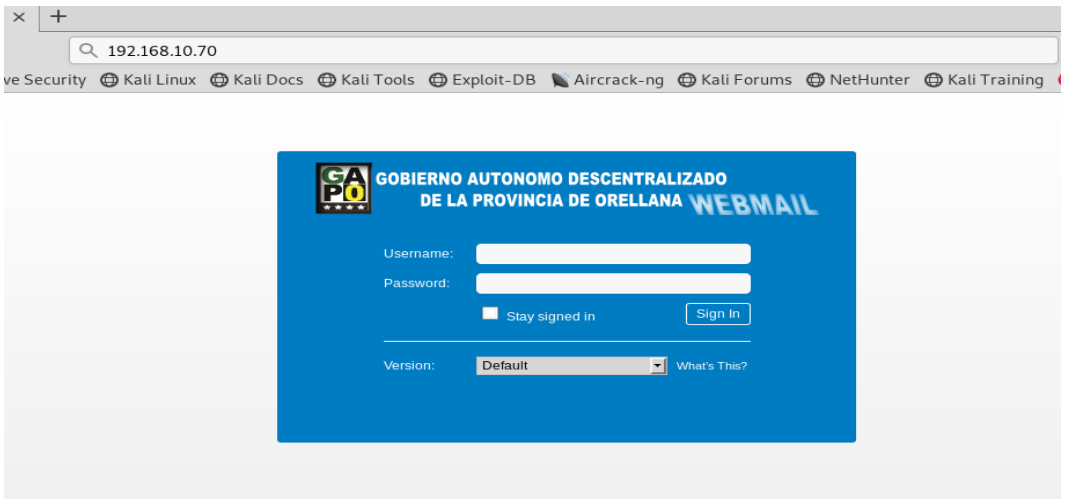


Figura 38. Sitio web falso para ataque de pishing

Elaborado por: Investigador

Una vez listos para realizar el ataque, se procede a redactar un mensaje, el mismo que debe ser lo suficientemente convincente, de tal forma que el usuario muerda el anzuelo y proporcione las credenciales de acceso al correo electrónico institucional. El mensaje que se difundió a los usuarios del GADPO, a través del sistema de mensajería fue el siguiente:

"*Buen día compañeros estamos verificando las cuentas de correo electrónico institucional activas. Favor ingresar en el siguiente enlace http://192.168.10.70 para verificar el estado de su cuenta. Gracias por su colaboración*."

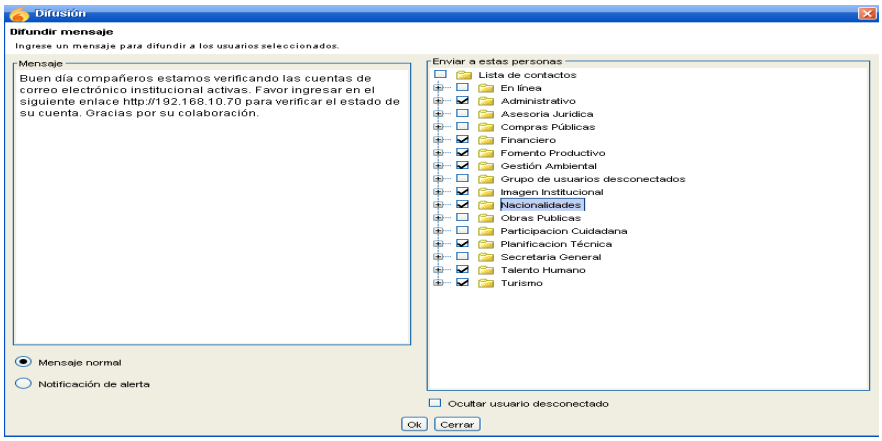


Figura 39. Difusión de mensaje para ataque de pishing

Elaborado por: Investigador

Los resultados obtenidos fueron los siguientes:

Tabla 13. Resultados ataque pishing intento 1

Coordinación	Usuarios atacados	Ataques satisfactorios
Administrativo	9	8
Financiero	13	7
Talento Humano	10	5
Planificación Técnica	10	9
Turismo	6	6
Fomento Productivo	7	4
Gestión Ambiental	10	6
Imagen Institucional	3	2
Nacionalidades	5	5
TOTAL	73	52

Elaborado por: Investigador

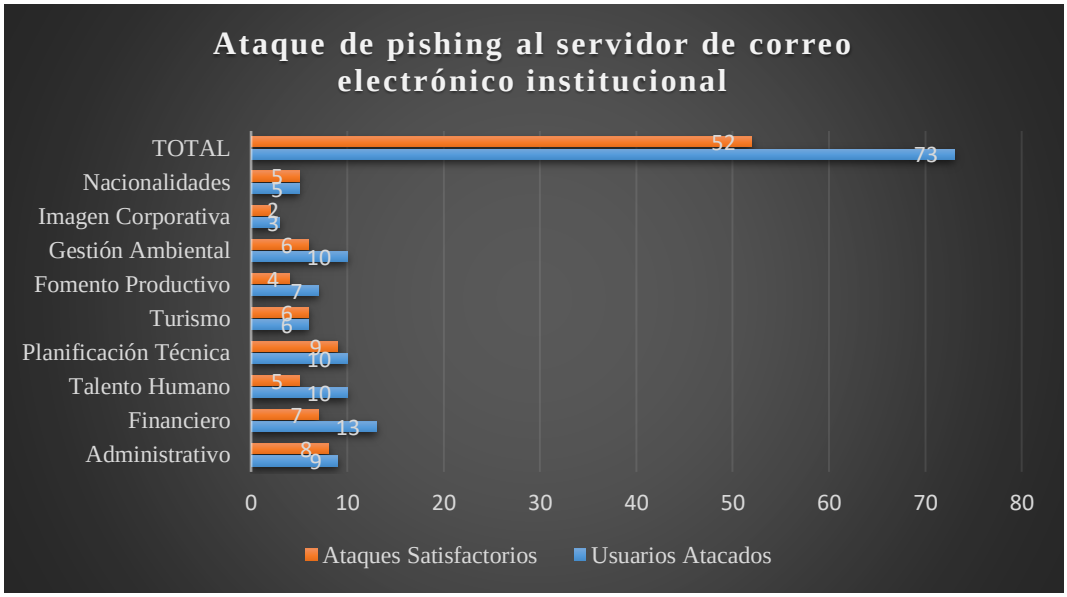


Figura 40. Ataque de pishing intento 1
Elaborado por Investigador

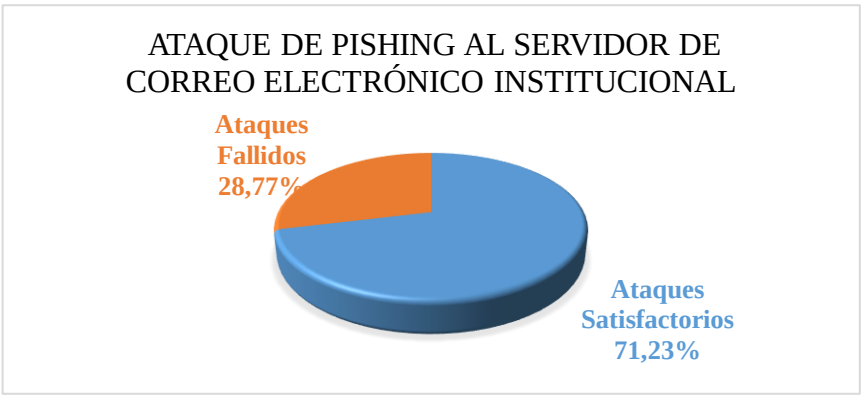


Figura 41. Resultado final ataque de pishing intento 1

Elaborado por: Investigador

Como resultado final del primer intento de ataque de pishing efectuado mediante la clonación del acceso web del servicio de correo electrónico institucional, de los 73 usuarios a los cuales se les envió el mensaje de engaño, 52 correspondiente a un 71.23% cayeron en la trampa y otorgaron sus credenciales de acceso al correo electrónico, mientras que 21 usuarios correspondiente a un 28.77% del total de usuarios atacados ignoraron el mensaje.

Se muestra el reporte generado por la herramienta SET, en donde constan algunas de las credenciales de acceso al correo electrónico institucional capturadas.

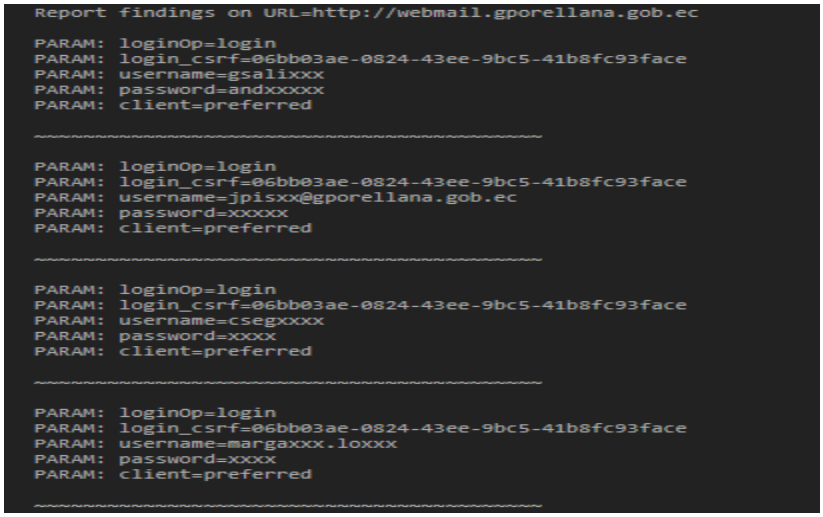


Figura 42. Reporte de credenciales capturadas por el ataque de pishing
Elaborado por: Investigador

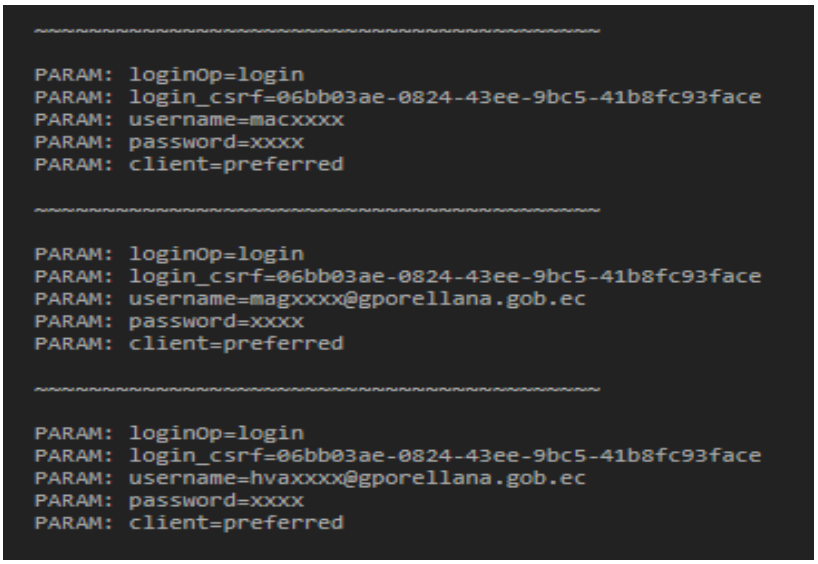


Figura 43. Reporte de credenciales capturadas por el ataque de pishing
Elaborado por: Investigador

Intento 2: Ataque de pishing al servidor de correo electrónico institucional

Siguiendo el mismo procedimiento descrito en el intento 1, se realizó un nuevo ataque de pishing, esta vez a aquellos usuarios que no se encontraban disponibles cuando se realizó el primer intento de intrusión.

Se obtuvieron los siguientes resultados:

Tabla 14. Resultados ataque de pishing intento 2

Coordinación	Usuarios atacados	Ataques satisfactorios
Compras Públicas	4	4
Participación Ciudadana	3	1
Financiero	6	3
Fomento Productivo	6	3
Obras Públicas	2	1
TOTAL	21	12

Elaborado por: Investigador

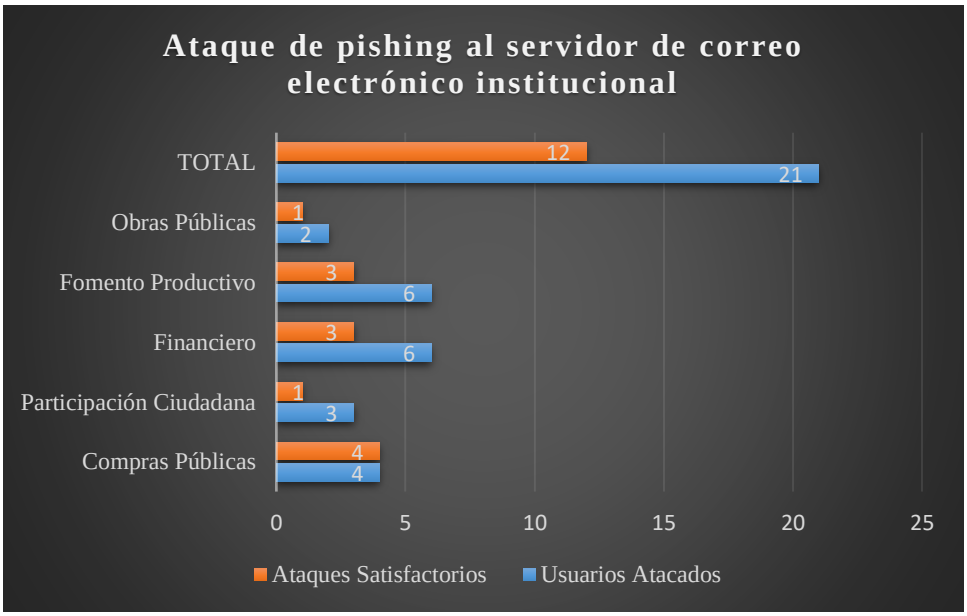


Figura 44. Ataque de pishing intento 2

Elaborado por: Investigador

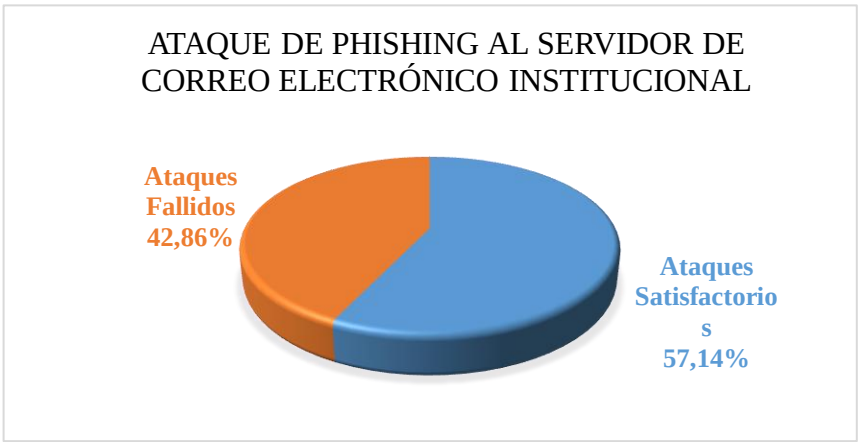


Figura 45. Resultado final ataque de pishing intento 2

Elaborado por: Investigador

En el segundo intento, de los 21 usuarios atacados, 12 correspondiente al 57.14% entregaron sus credenciales de acceso al correo electrónico institucional, mientras que los 9 restantes correspondiente a un 42.86% hicieron caso omiso del mensaje.

Intento 3: Ataque de pishing al servidor de trámites en línea Consedoc.

La función del servidor Consedoc, es permitir realizar el seguimiento en línea de los trámites. Cada uno de los asistentes administrativos de las distintas coordinaciones poseen una cuenta en este sistema, y son los responsables de establecer el estado y ubicación de un determinado trámite. Los usuarios objetivos de este nuevo intento de ataque fueron los asistentes administrativos.

El procedimiento para clonar el sitio web de este servicio fue el descrito en el intento 1.

La Figura 32 muestra un clon del sitio web del sistema Consedoc.

Figura 46. Sitio web falso sistema Consedoc

Elaborado por: Investigador

El mensaje enviado fue el siguiente:

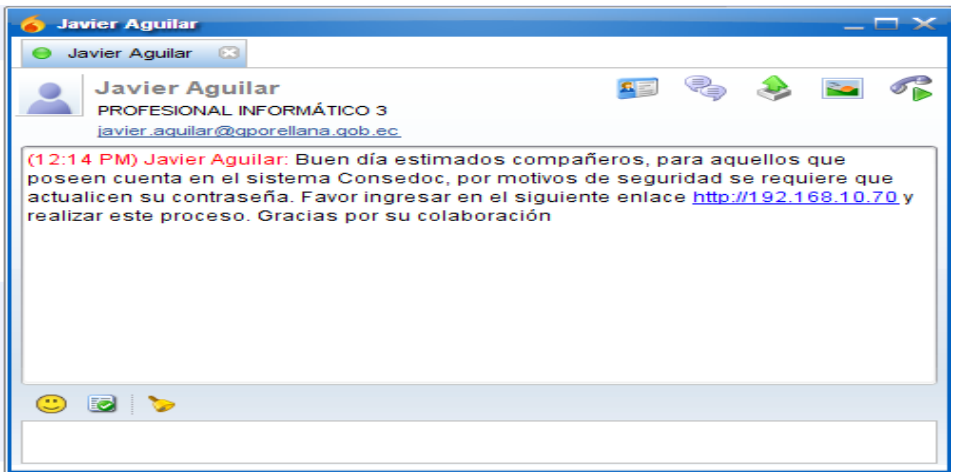


Figura 47. Mensaje enviado a usuarios del sistema Consedoc

Elaborado por: Investigador

A continuación, se detallan los resultados obtenidos.

Tabla 15. Resultado ataque pishing intento 3

Coordinación	Usuarios atacados	Ataques satisfactorios
Gestión Ambiental	6	5
Fomento Productivo	5	3
Participación Ciudadana	5	2
Financiero	5	5
TOTAL	21	15

Elaborado por: Investigador

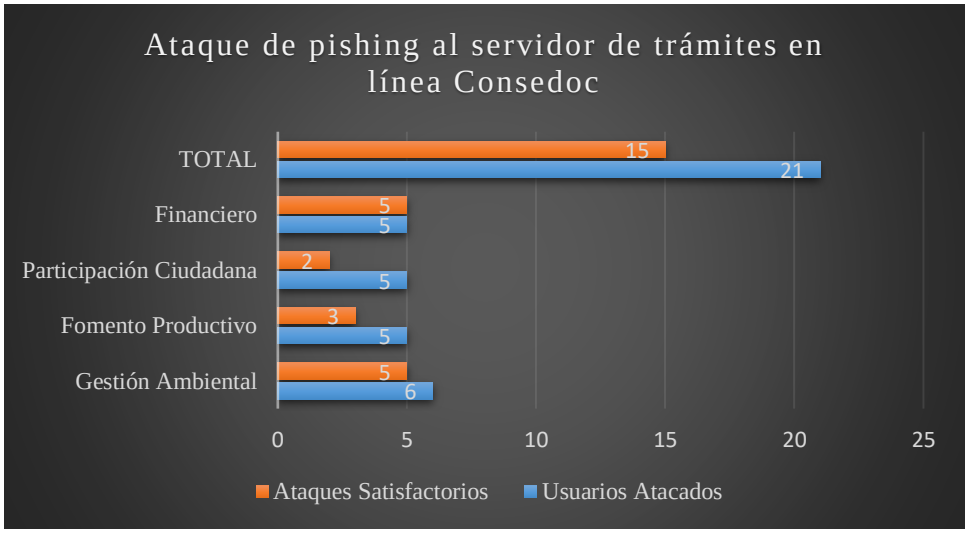


Figura 48. Ataque de pishing intento 3

Elaborado por: Investigador

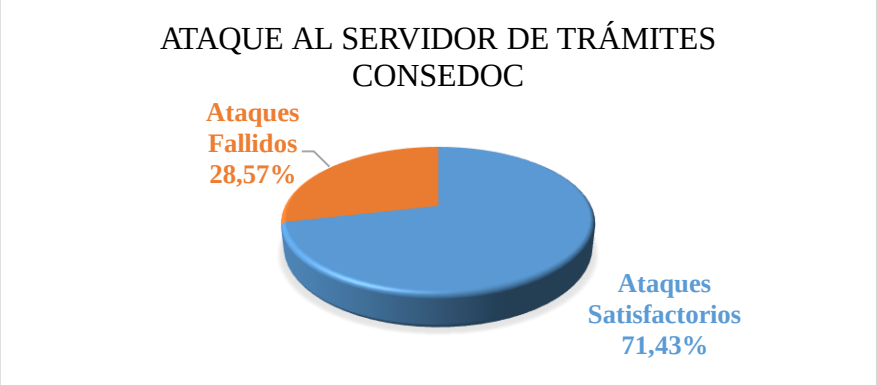


Figura 49. Resultado final ataque pishing intento 3

Elaborado por: Investigador

De 21 usuarios atacados, se obtuvo las credenciales de acceso de 15 usuarios correspondiente a un 71.43%, mientras tanto que los 6 restante correspondiente a un 28.57% no entregaron sus claves de acceso.

Intento 4: Ataque de pishing al servidor de trámites en línea Consedoc.

Los resultados obtenidos fueron los siguientes:

Tabla 16. Resultados ataque pishing intento 4

Coordinación	Usuarios Atacados	Ataques Satisfactorios
Turismo	3	2
Nacionalidades	2	1
Planificación	3	1
Obras Públicas	3	1
Administrativo	5	5
TOTAL	16	10

Elaborado por: Investigador

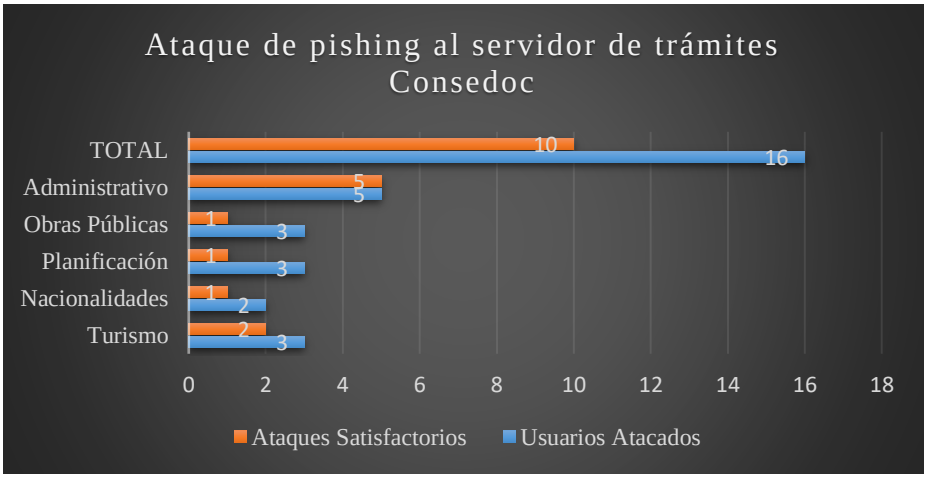


Figura 50. Resultados ataque pishing intento 4

Elaborado por: Investigador

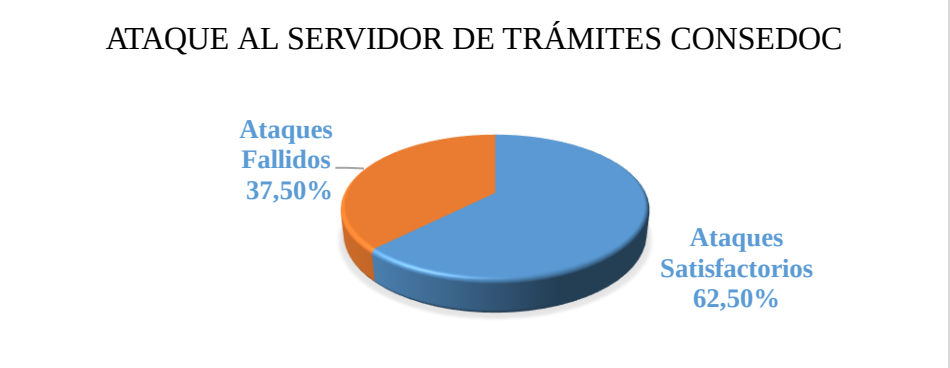


Figura 51. Resultado final ataque pishing intento 4

Elaborado por: Investigador

De los 16 usuarios atacados, 10 usuarios correspondiente a un 62.50% cayeron en la trampa, mientras que los 6 restantes correspondiente a un 37.50% no accedieron al engaño.

A continuación, se presenta un resumen de los resultados obtenidos en los distintos ataques de pishing:

Tabla 17. Resultados de los ataques de pishing

Semana	Numero de ataque	Usuarios atacados	Ataques satisfactorios	Ataques fallidos	Servidor
1	1	73	52	21	Correo Electrónico
2	2	21	12	9	Correo Electrónico
2	3	21	15	6	Consedoc
3	4	16	10	6	Consedoc
TOTAL		131	89	42	

Elaborado por: Investigador

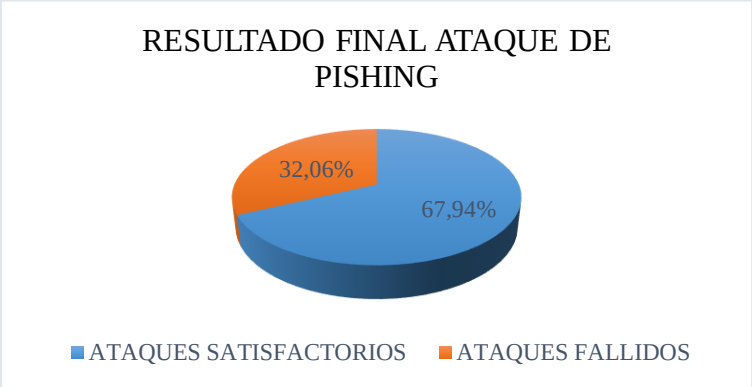


Figura 52. Resultado final ataque de pishing

Elaborado por: Investigador

Como resultado final de los distintos ataques de pishing realizados se tiene que 89 ataques correspondientes a un 67.94% fueron satisfactorios, mientras que 42 correspondientes a un 32.06% fueron ataques fallidos.

4.1.5. Ataque DDoS al servidor Firewall del GADPO

El servidor Firewall brinda protección a toda la red de datos del GADPO, así como también permite establecer la comunicación entre las distintas subredes que existen en la red local como con la red externa. Un fallo en este servidor provocaría que no se puedan establecer las comunicaciones tanto con los servicios internos como con Internet.

El esquema propuesto para realizar los ataques DDoS de tipo SYN Flood, se puede observar en la siguiente figura.

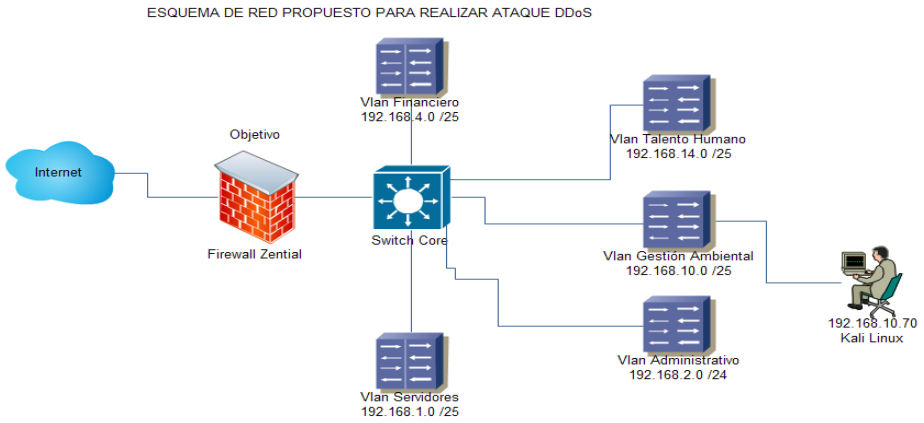


Figura 53. Esquema de red para realizar ataque DDoS

Elaborado por: Investigador

Para no afectar los servicios y el normal funcionamiento de la red de datos del GADPO, se generó un backup de las configuraciones del servidor firewall y se realizó una nueva instalación sobre la cual se efectuaron los ataques de denegación de servicio. La dirección ip de la interfaz de red local configurada fue la 192.168.10.55. Se verificó el acceso a la interfaz web del servidor mediante el siguiente enlace https://192.168.10.55:8443

Figura 54. Acceso web a servidor Zentyal

Elaborado por: Investigador

Desde Kali Linux, con la herramienta hping3 se puede verificar si un determinado servicio está activo. En este caso se constató que el puerto 8443 está aceptando conexiones, ya que devuelve un flag SA que se corresponde con SYN/ACK.

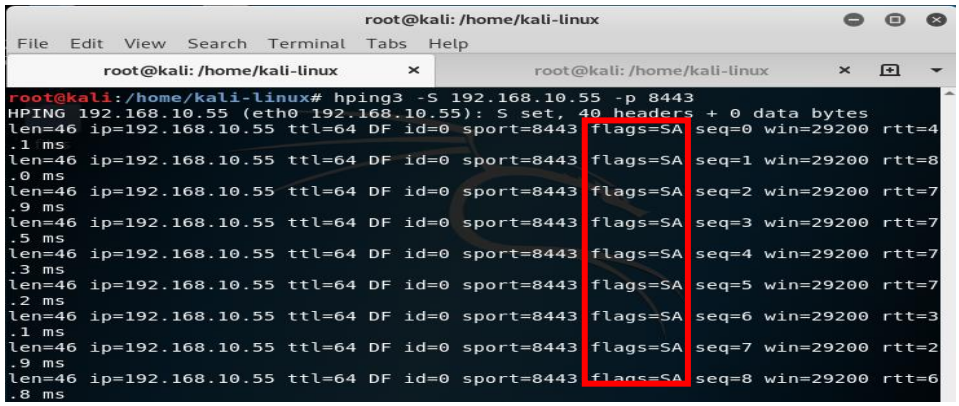


Figura 55. Escaneo de puertos usando el flag SYN
Elaborado por: Investigador

Para analizar el tráfico de red en el servidor objetivo del ataque se utilizó Multi Router Traffic Grapher (MRTG), el cual es una herramienta escrita en lenguaje C y Perl por Tobias Oetiker y Dave Rand y permite recolectar información sobre la carga actual de los recursos hardware de dispositivos como routers y servidores (G. Torres, 2010).

El procedimiento para instalar MRTG bajo el sistema operativo Linux (Zentyal) fue el siguiente:

- Instalación de apache:

apt-get install apache2

- Instalación y configuraciòn de Simple Network Management Protocol (SNMP):

Se instalarón los paquetes snmp con el siguiente comando:

apt-get install snmpd snmp

Luego se habilitó el acceso para localhost editando el archivo snmpd.conf

nano /etc/snmp/snmpd.conf y añadiendo la siguiente línea:

rocommunity public localhost

Por último, se reinicia el servicio snmpd para que los cambios realizados surtan efecto

systemctl restart snmpd

- Instalación y configuración de MRTG

Se instaló MRTG con el siguiente comando:

apt-get install mrtg

Se configuró el directorio de trabajo de MRTG

mkdir /var/www/html/mrtg

Se estableció como propietario del directorio de trabajo a apache

chown –R www-data:www-data /var/www/html

Se editó el archivo /etc/mrtg.cfg para establecer el directorio de trabajo

nano /etc/mrtg.cfg

WorkDir: /var/www/html/mrtg

Una vez realizados los cambios se reconstruyó la configuración de MRTG desde el archivo modificado:

cfgmaker public@localhost > /etc/mrtg.cfg

Finalmente se generó el archive index para el web server

indexmaker /etc/mrtg.cfg > /var/www/html/index.html

Se verificó el acceso al servicio MRTG mediante un navegador web:

Figura 56. Acceso web a MRTG

Elaborado por: Investigador

Las configuraciones realizadas para monitorear el uso de la tarjeta de red se detallan en el Anexo 1.

Antes de efectuar el ataque DDoS se monitoreó el uso de ancho de banda en el equipo víctima por un tiempo aproximado de dos horas, obteniendo los siguientes resultados:

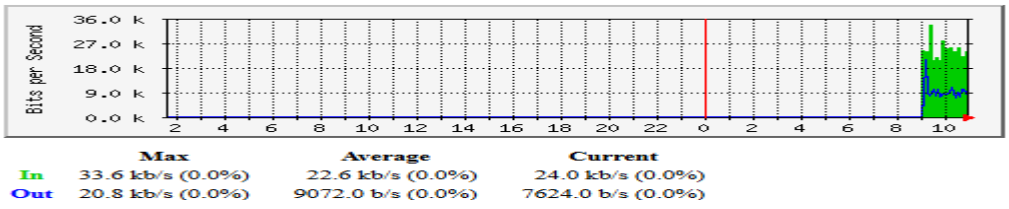


Figura 57. Uso de ancho de banda antes del ataque DDoS

Elaborado por: Investigador

El ancho de banda máximo alcanzado antes de efectuar el ataque fue de 36.6 kb/s

El ataque DDoS SYN Flood se realizó ejecutando el siguiente comando:

hping3 -V -c 1000 -d 100 -S -p 8443 –flood --rand-source 192.168.10.55

La siguiente tabla describe cada uno de los parámetros utilizados del comando hping3.

Tabla 18. Descripción de parámetros comando hping3

Parámetro	Descripción
-c 2500	Cantidad de paquetes a enviar
-d 100	Tamaño en bytes de cada uno de los paquetes
-S	Especifica que el indicador SYN debe estar habilitado
-p 8443	Especificación de puerto al que será dirigido el ataque
--flood	Enviar paquetes lo más rápido posible
--rand-source	Genera direcciones ip falsificadas para disfrazar la fuente real, y al mismo tiempo detener los paquetes de respuesta SYN-ACK de la víctima al atacante.

Elaborado por: Investigador

Los ataques DDoS realizados fueron los siguientes:

Ataque 1: Ataque realizado con una cantidad de 1000 paquetes, un tamaño de 100 bytes. El comando utilizado fue el siguiente:

hping3 -V -c 1000 -d 100 -S -p 8443 –flood --rand-source 192.168.10.55

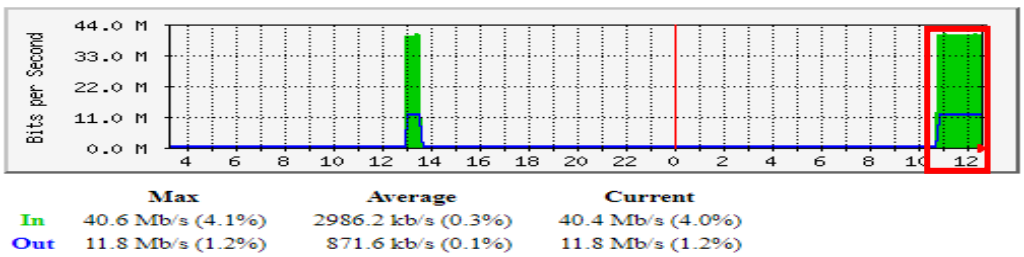


Figura 58. Uso de ancho de banda ataque 1 DDoS

Elaborado por: Investigador

El uso de ancho de banda alcanzado fue de 40.4 Mb/s (4.0%).

Ataque 2: La cantidad de paquetes utilizados fue 1500, con un tamaño de cada paquete de 200 bytes. El comando utilizado fue el siguiente:

hping3 -V -c 1500 -d 200 -S -p 8443 –flood --rand-source 192.168.10.55

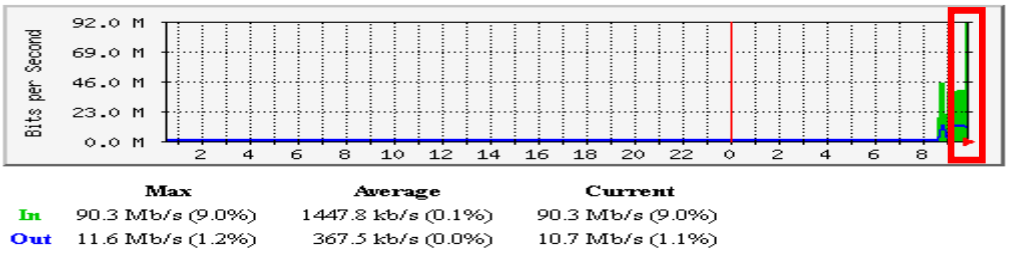


Figura 59. Uso de ancho de banda ataque 2 DDoS

Elaborado por: Investigador

Se logró generar un tráfico de 90 Mb/s lo que representa un 9% de los 1 Gb/s que corresponde a la velocidad máxima soportada por la tarjeta de red.

Ataque 3: La cantidad de paquetes utilizados fue 2000, con un tamaño de cada paquete de 300 bytes. El comando utilizado fue el siguiente:

hping3 -V -c 2000 -d 300 -S -p 8443 –flood --rand-source 192.168.10.55

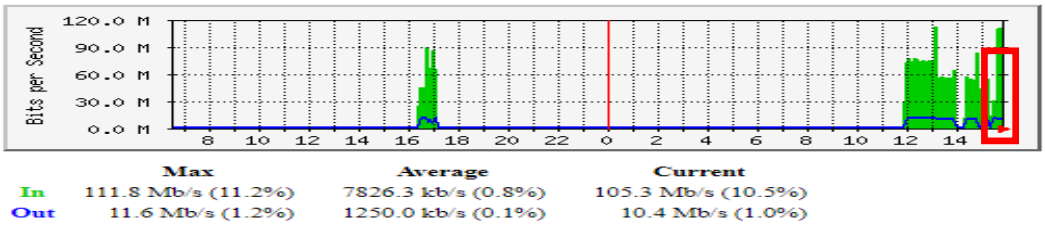


Figura 60. Uso de ancho de banda ataque 3 DDOS

Elaborado por: Investigador

Se logró generar un tráfico de 105.3 Mb/s lo que representa un 10.53% de los 1 Gb/s que corresponde a la velocidad máxima soportada por la tarjeta de red.

Ataque 4: La cantidad de paquetes utilizados fue de 2500, y un tamaño de cada paquete de 400 bytes. El comando utilizado fue el siguiente:

hping3 -V -c 2500 -d 400 -S -p 8443 –flood --rand-source 192.168.10.55

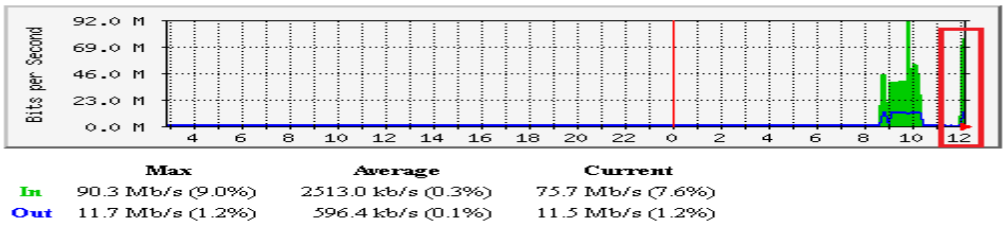


Figura 61. Uso ancho de banda ataque 4 DDoS

Elaborado por: Investigador

El tráfico generado fue de 75.7 Mb/s correspondiente a un 7.60%.

Ataque 5: La cantidad de paquetes utilizados fue de 3000, y un tamaño de cada paquete de 500 bytes. El comando utilizado fue el siguiente:

hping3 -V -c 3000 –d 500 -S -p 8443 –flood --rand-source 192.168.10.55

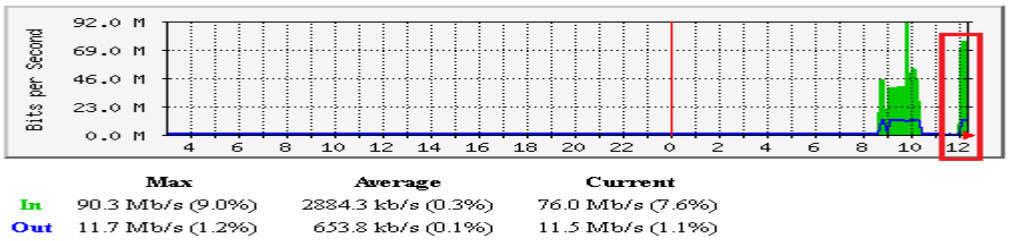


Figura 62. Uso de ancho de banda ataque 5 DDoS

Elaborado por: Investigador

El tráfico generado fue de 76 Mb/s correspondiente a un 7.6%.

Ataque 6: La cantidad de paquetes utilizados fue de 3500, y un tamaño de cada paquete de 600 bytes. El comando utilizado fue el siguiente:

hping3 -V -c 3500 -d 600 -S -p 8443 –flood --rand-source 192.168.10.55

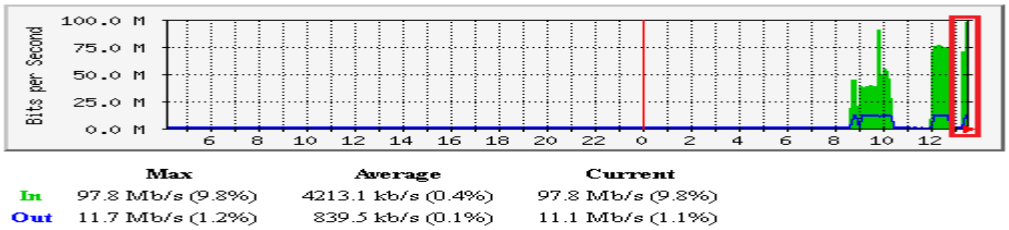


Figura 63. Uso de ancho de banda ataque 6 DDoS

Elaborado por: Investigador

El tráfico generado fue de 97.80 Mb/s correspondiente a un 9.80%.

Ataque 7: La cantidad de paquetes utilizados fue de 4000, y un tamaño de cada paquete de 700 bytes. El comando utilizado fue el siguiente:

hping3 -V -c 4000 -d 700 -S -p 8443 –flood --rand-source 192.168.10.55

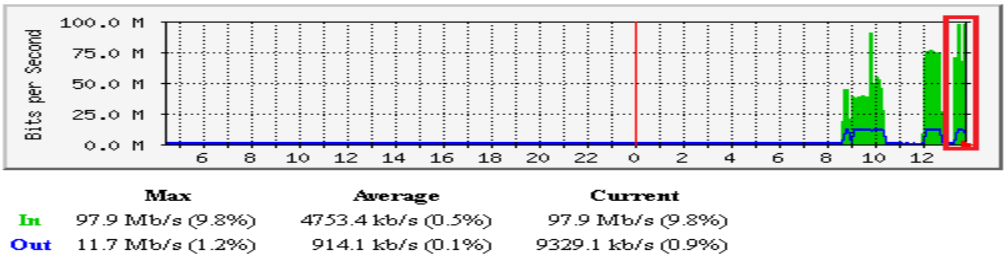


Figura 64. Uso de ancho de banda ataque 7 DDoS

Elaborado por: Investigador

El tráfico generado fue de 97.90 Mb/s correspondiente a un 9.80%.

Ataque 8: La cantidad de paquetes utilizados fue de 4500, y un tamaño de cada paquete de 800 bytes. El comando utilizado fue el siguiente:

hping3 -V -c 4500 -d 800 -S -p 8443 –flood --rand-source 192.168.10.55

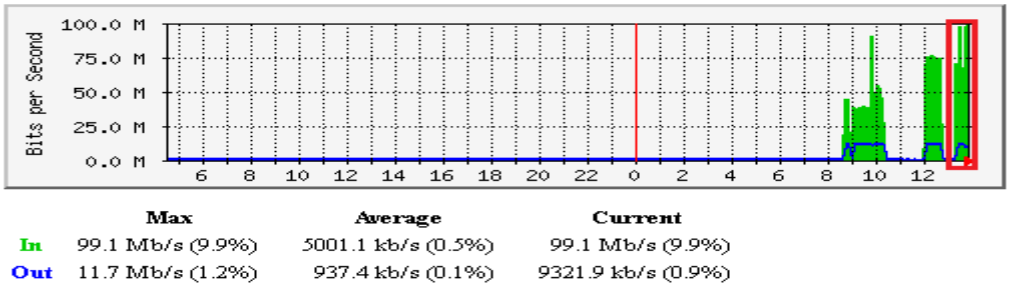


Figura 65. Uso de ancho de banda ataque 8 DDoS

Elaborado por: Investigador

El tráfico generado fue de 99.10 Mb/s correspondiente a un 9.90%.

Ataque 9: La cantidad de paquetes utilizados fue de 5000, y un tamaño de cada paquete de 900 bytes. El comando utilizado fue el siguiente:

hping3 -V -c 5000 -d 900 -S -p 8443 –flood --rand-source 192.168.10.55

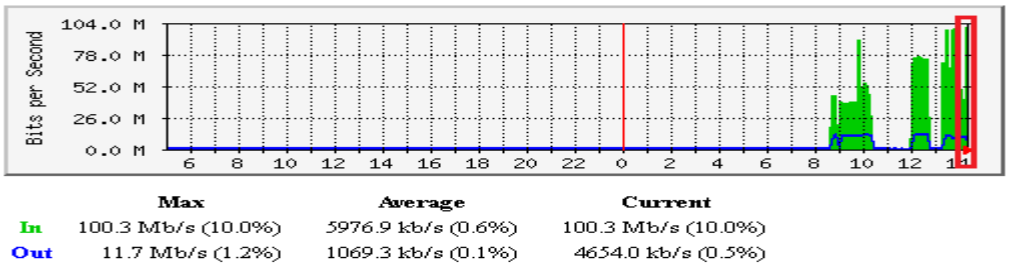


Figura 66. Uso de ancho de banda ataque 9 DDoS

Elaborado por: Investigador

El tráfico generado fue de 100.3 Mb/s correspondiente a un 10.00%.

Ataque 10: La cantidad de paquetes utilizados fue de 5500, y un tamaño de cada paquete de 1000 bytes. El comando utilizado fue el siguiente:

hping3 -V -c 5500 -d 1000 -S -p 8443 –flood --rand-source 192.168.10.55

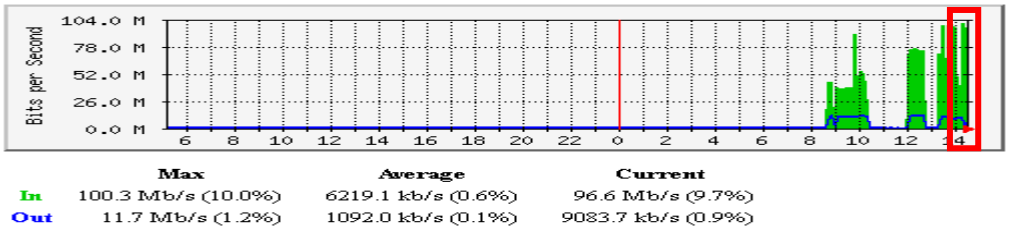


Figura 67. Uso de ancho de banda ataque 10 DDoS

Elaborado por: Investigador

El tráfico generado fue de 96.6 Mb/s correspondiente a un 9.70%.

Ataque 11: La cantidad de paquetes utilizados fue de 6000, y un tamaño de cada paquete de 1500 bytes. El comando utilizado fue el siguiente:

hping3 -V -c 6000 -d 1500 -S -p 8443 –flood --rand-source 192.168.10.55

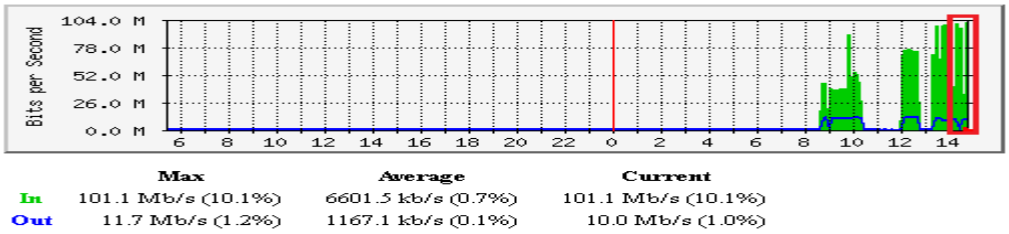


Figura 68. Uso ancho de banda ataque 11 DDoS

Elaborado por: Investigador

El tráfico generado fue de 101.1 Mb/s correspondiente a un 10.10%.

Ataque 12: La cantidad de paquetes utilizados fue de 7000, y un tamaño de cada paquete de 2000 bytes. El comando utilizado fue el siguiente:

hping3 -V -c 7000 -d 2000 -S -p 8443 –flood --rand-source 192.168.10.55

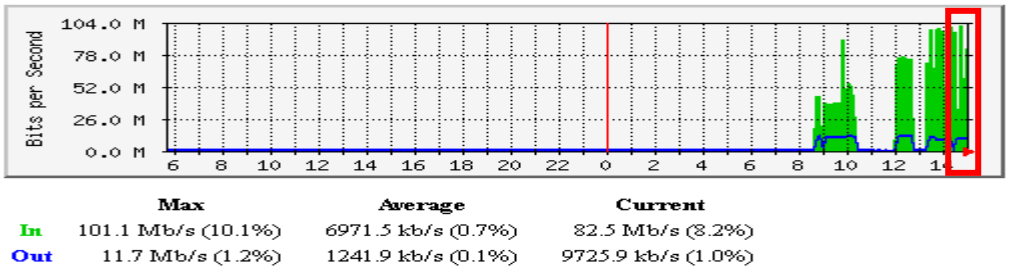


Figura 69. Uso de ancho de banda ataque 12 DDoS

Elaborado por: Investigador

El tráfico generado fue de 82.5 Mb/s correspondiente a un 8.20%.

Ataque 13: La cantidad de paquetes utilizados fue de 7500, y un tamaño de cada paquete de 2500 bytes. El comando utilizado fue el siguiente:

hping3 -V -c 7000 -d 2000 -S -p 8443 –flood --rand-source 192.168.10.55

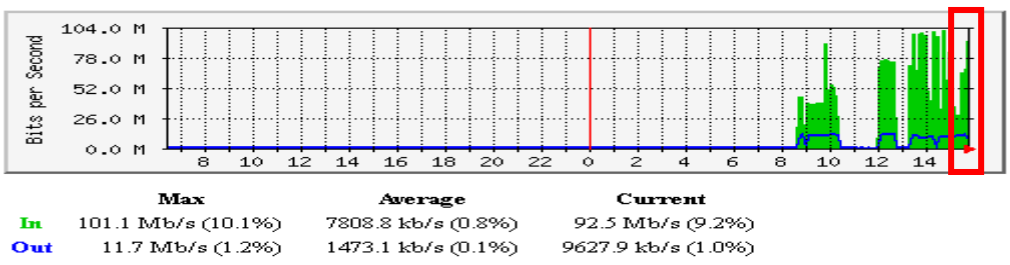


Figura 70. Uso de ancho de banda ataque 13 DDoS

Elaborado por: Investigador

El tráfico generado fue de 92.5 Mb/s correspondiente a un 9.20%.

Los resultados obtenidos en los distintos ataques DDoS efectuados se resumen en la siguiente tabla:

Tabla 19. Resultado final de ataques DDoS con un PC.

Número de PCs	Número de ataque	Cantidad de paquetes	Longitud de paquete (bytes)	% Uso de ancho de banda.
1	01	1000	100	4.00
1	02	1500	200	9.00
1	03	2000	300	10.50
1	04	2500	400	7.60
1	05	3000	500	7.60
1	06	3500	600	9.80
1	07	4000	700	9.80
1	08	4500	800	9.90
1	09	5000	900	10.00
1	10	5500	1000	9.70
1	11	6000	1500	10.10
1	12	6500	2000	8.20
1	13	7000	2500	9.20

Elaborado por: Investigador

Tomando en cuenta los resultados mostrados en la Tabla 19, en donde se indica los porcentajes de uso de ancho de banda alcanzados al realizar el ataque DDoS con un computador, se estima el porcentaje de uso de ancho de banda que se alcanzaría al realizar el mismo ataque con tres computadores.

Tabla 20. Resultados ataques DDoS con 3 PCs

Número de PCs	Número de ataque	Cantidad de paquetes	Longitud de paquete (bytes)	% Uso de ancho de banda.
3	01	1500	100	12.00
3	02	2000	200	27.00

3	03	2500	300	31.50
3	04	3000	400	22.80
3	05	3500	500	22.80
3	06	4000	600	29.40
3	07	4500	700	29.40
3	08	5000	800	29.70
3	09	5500	900	30.00
3	10	6000	1000	29.10
3	11	6500	1500	30.30
3	12	7000	2000	24.60
3	13	7500	2500	27.60
PROMEDIO USO ANCHO DE BANDA				26.63

Elaborado por: Investigador

4.1.6. Identificación de riesgos a los que están expuestos los servidores Linux del GADPO

Una vez realizados los ataques informáticos, se procedió a realizar la identificación y determinación del impacto de los riesgos a los que están expuestos los servidores. En este punto fue vital la utilización de la metodología de análisis y gestión de riesgos de tecnologías de la información (MAGERIT), ya que está metodología permite a cualquier organización que trabaja con información digital saber el valor de la misma y además conocer cómo protegerla (Joya & Sacristán, 2017).

Para medir el impacto que puede producir una determinada amenaza a un activo de información, MAGERIT presenta una escala la cual se detalla a continuación:

Tabla 21. Escala de impacto MAGERIT

Nivel de Impacto	Porcentaje
Bajo	0% - 25%
Intermedio	26% - 50%
Alto	51% - 75%
Muy Alto	>76%

Elaborado por: Investigador

Fuente: (Hurtado, 2017)

Las vulnerabilidades son las debilidades que presentan los activos y que facilitan que una determinada amenaza se llegue a materializar (INCIBE, 2015).

Tomando en cuenta que la presente investigación se enfocó en evaluar el impacto de los ataques de pishing y DDoS (SYN Flood), la vulnerabilidad se pudo expresar en base al porcentaje de ataques satisfactorios de pishing y el porcentaje de uso de ancho de banda que provocó el ataque DDoS.

Vulnerabilidad = Porcentaje de usuarios afectados

Vulnerabilidad = Porcentaje de uso de ancho de banda

Con los porcentajes de afectación obtenidos de 67.94% del ataque de pishing y 26.63% del ataque DDoS se calculó la vulnerabilidad.

Tabla 22. Cálculo de vulnerabilidad ataque de pishing

Ataque	% usuarios afectados	Vulnerabilidad
Pishing	67.94%	67.94%

Elaborado por: Investigador

Tabla 23. Cálculo de vulnerabilidad ataque DDoS

Ataque	% uso de ancho de banda	Vulnerabilidad
DDoS (SYN Flood)	26.63%	26.63%

Elaborado por: Investigador

Una vez determinada la vulnerabilidad se procedió a calcular el riesgo, haciendo uso de igual forma de la escala sugerida por MAGERIT v3.0

Tabla 24. Escalas de amenazas informáticas MAGERIT v3.0

Amenaza	Porcentaje
View Information	0.33
Information Gathering	0.66
Disable Services	0.99

Elaborado por: Investigador

Fuente: (Hurtado, 2017)

Además, MAGERIT v3.0 establece también las dimensiones de la seguridad de la información que se ven afectadas según el tipo de ataque informático.

Las dimensiones afectadas para el caso de los ataques de pishing y DDoS son:

Tabla 25. Afectación a dimensiones de seguridad de la información

Ataque	Dimensión		
	Integridad	Confidencialidad	Disponibilidad
Pishing	X	X	X
DDoS			X

Elaborado por: Investigador

Fuente: (**Ministerio de Hacienda y Administraciones Públicas, 2012)**

Se procedió a calcular el riesgo utilizando la siguiente fórmula:

Riesgo = Amenazas x Vulnerabilidad

Tabla 26. Cálculo del riesgo

Amenaza	Escala amenaza	Vulnerabilidad	Impacto	Riesgo
Pishing	View Information (0.33)	67.94%	Alto	22.42%
Pishing	Information Gathering(0.66)	67.94%	Alto	44.84%
Pishing	Disable Services (0.99)	67.94%	Alto	67.26%
DDoS	Disable Services (0.99)	26.63%	Intermedio	26.36%

Elaborado por: Investigador

4.1.7. Verificación de hipótesis

Para determinar el nivel de afectación de cada uno de los ataques informáticos realizados a los servidores Linux del GADPO, se utilizó la siguiente escala de Likert propuesta por Karina Arellano en la tesis denominada "Modelo de seguridad contra ataques de denegación de servicio (DoS) de tráfico SIP en servicios VOIP para redes LAN corporativas":

Tabla 27. Escala de Likert

Afectación	Valor	Porcentaje
No aplica	0	----
Muy Bajo	1	0 – 20
Bajo	2	21- 40
Medio	3	41 – 60
Alto	4	61 – 80
Muy Alto	5	81- 100

Elaborado por: Investigador

Fuente: (Arellano, 2017)

Variable independiente: Ataque Informático

Variable dependiente: Seguridad de Servidores con Sistema Operativo Linux.

Para realizar el análisis estadístico de la presente investigación, se plantearon las siguientes hipótesis:

Hipótesis nula (Ho): Los ataques informáticos no inciden en la seguridad de servidores con sistema operativo Linux del GADPO.

Hipótesis alternativa (Ha): Los ataques informáticos inciden en la seguridad de servidores con sistema operativo Linux del GADPO.

Utilizando las escalas de Likert de la Tabla 26, se estableció la siguiente tabla donde se especifica la afectación de cada ataque informático realizado a la seguridad de los servidores Linux del GADPO.

Tabla 28. Resultados ataques informáticos

RESULTADOS ATAQUES INFORMÁTICOS					TOTAL
Prueba	**Ataque**	**Indicadores**			
		Confidencialidad	**Integridad**	**Disponibilidad**	
Prueba 1	Phishing	4	4	4	12
Prueba 2	Phishing	3	3	3	9
Prueba 3	Phishing	4	4	4	12
Prueba 4	Phishing	4	4	4	12
Prueba 5	DDoS	0	0	1	1
Prueba 6	DDoS	0	0	2	2
Prueba 7	DDoS	0	0	2	2
Prueba 8	DDoS	0	0	2	2
Prueba 9	DDoS	0	0	2	2
Prueba 10	DDoS	0	0	2	2
Prueba 11	DDoS	0	0	2	2
Prueba 12	DDoS	0	0	2	2
Prueba 13	DDoS	0	0	2	2
Prueba 14	DDoS	0	0	2	2
Prueba 15	DDoS	0	0	2	2
Prueba 16	DDoS	0	0	2	2
Prueba 17	DDoS	0	0	2	2
Total		**15**	**15**	**40**	**70**
Likert		**3.75**	**3.75**	**3.08**	

Elaborado por: Investigador

Se utilizó la prueba de X^2 (Chi Cuadrado), la misma que nos permite obtener como resultado si dos variables están relacionadas (Luna, 2018).

A partir de la Tabla 28 contando las ocurrencias de cada valor de la escala de Likert establecida, se obtuvo la tabla de contingencia necesaria para proceder con la realización de la prueba de Chi Cuadrado.

Tabla 29. Tabla de contingencias

Afectación	Confidencialidad	Integridad	Disponibilidad	TOTAL
Bajo	0	0	1	**1**
Medio	0	0	12	**12**
Alto	1	1	1	**3**
Muy Alto	3	3	3	**9**
Total	**4**	**4**	**17**	**25**

Elaborado por: Investigador

La fórmula utilizada fue la siguiente:

$$X^2 = \sum \frac{(fo - ft)^2}{ft}$$

En donde:

fo = Frecuencias obtenidas, es decir el total de ocurrencias por cada nivel de afectación establecido en la tabla de contingencias.

ft = Frecuencia teórica, que se obtiene al multiplicar el total de cada columna de la tabla de contingencia por el total de la fila de cada nivel establecido, y este resultado se divide por el total de la intercepción de las filas y columnas.

Es necesario establecer además los grados de libertad y el nivel de significancia.

Los grados de libertad se obtienen a partir del número de filas y columnas de la tabla de contingencia. Para ello se utilizó la siguiente fórmula:

Grados de libertad (v)

v= (num_filas – 1) * (num_col – 1)

v = (4 – 1) * (3 – 1) = 6

v= 6

El nivel de significancia utilizado para la presente investigación fue de 0.05.

Con los grados de libertad y el nivel de confianza establecido se puede obtener el valor de referencia utilizando la tabla de Chi Cuadrado.

Tabla 30. Chi Cuadrado

v/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872

Elaborado por: Investigador

Valor de referencia X^2 = 12.596

En la siguiente tabla se muestran los cálculos realizados para obtener el resultado de la prueba Chi Cuadrado:

Tabla 31. Cálculo de Chi Cuadrado

Fo	Ft	fo-ft	(fo-ft)^2	x2
0	0.160	-0.16	0.026	0.160
0	1.920	-1.92	3.686	1.920
1	0.480	0.52	0.270	0.563
3	1.440	1.56	2.434	1.690
0	0.160	-0.16	0.026	0.160
0	1.920	-1.92	3.686	1.920
1	0.480	0.52	0.270	0.563
3	1.440	1.56	2.434	1.690
1	0.680	0.32	0.102	0.151
3	8.160	-5.16	26.626	3.263
1	2.040	-1.04	1.082	0.53
3	6.120	-3.12	9.734	1.591
		TOTAL		**14.201**

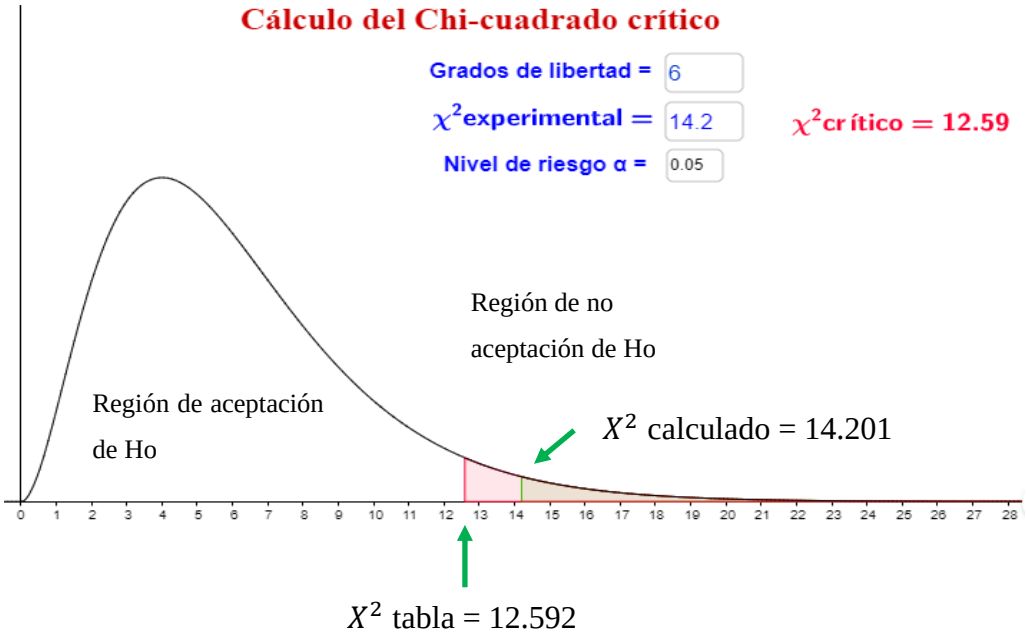
Elaborado por: Investigador

Valor de X^2 calculado = 14.201

El valor encontrado de la prueba Chi Cuadrado fue de 14.201 y es mayor al valor de referencia 12.596, por lo que se rechaza la hipótesis nula (Ho) y se acepta la

hipótesis alternativa (Ha), verificando de esta forma que los ataques informáticos si inciden en la seguridad de los servidores con sistema operativo Linux del GADPO.

Figura 71. Representación gráfica prueba Chi Cuadrado



Elaborado por: Investigador

CAPÍTULO 5. CONCLUSIONES Y RECOMENDACIONES

Luego de los resultados que se obtuvieron a partir de los ataques de pishing y DDoS efectuados a los servidores Linux del GADPO se concluye:

- Con los resultados obtenidos a partir de los ataques de pishing y DDoS; y con la ayuda de la metodología MAGERIT v3.0 se pudo determinar la vulnerabilidad, el nivel de impacto, y el riesgo de la seguridad de la información.
- Los ataques de pishing efectuados permitieron determinar un porcentaje de vulnerabilidad de 67.94%, lo que implica un impacto alto a la seguridad de la información; el riesgo de afectación a la confidencialidad fue de 22.42%, el riesgo de la disponibilidad de 67.26% y el riesgo de la integridad de la información de 44.84%.
- Los ataques DDoS alcanzaron una vulnerabilidad de 26.63%, un impacto a la seguridad de la información intermedio y un riesgo de la disponibilidad de la información de 26.36%.
- Con el uso de la prueba chi cuadrado se logró verificar la hipótesis de investigación obteniendo un valor de 14.201 mayor al valor de referencia 12.592, con lo cual se acepta la hipótesis alternativa y se rechaza la hipótesis nula.

Como recomendaciones se plantea lo siguiente:

- Elaborar un plan de capacitación y concientización sobre seguridad de la información para los usuarios del GADPO.
- Establecer mecanismos de protección para el servidor firewall frente a los ataques DDoS de tipo SYN Flood.

CAPÍTULO 6. PROPUESTA

6.1. Datos informativos

Tema: Los ataques informáticos y su incidencia en la seguridad de servidores Linux del GADPO

Institución: Gobierno Autónomo Descentralizado de la Provincia de Orellana.

Provincia: Orellana

Cantón: El Coca

Dirección: 9 de octubre entre Dayuma y César Andy

Beneficiarios: Funcionarios del GADPO, ciudadanía

Ejecución: febrero 2019 a septiembre 2019

Responsable: Ing. Francisco Javier Aguilar Feijóo

Director: Ing. Luis Fabián Hurtado Vargas Mgs.

6.2. Antecedentes de la propuesta

Uno de los activos de mayor valor dentro de una organización es la información, por lo que debemos protegerla de posibles ataques informáticos y evitar que pueda verse afectada la integridad, confidencialidad o disponibilidad de la misma (Álvarez, 2017).

(Álvarez, 2017) menciona además en su estudio denominado "Guía para la elaboración de un plan de entrenamiento, sobre seguridad de la información", que sensibilizar a los usuarios acerca de las amenazas y vulnerabilidades a las que están expuestos es de vital importancia para evitar que se produzcan problemas de seguridad de la información que puedan afectar gravemente a la organización.

6.3. Justificación

El uso de los sistemas de información (SI), comprende un factor esencial para el desarrollo económico y social de un país. Garantizar la seguridad de la información es de vital importancia para cualquier empresa, ya sea esta pública o privada (Gil & Gil, 2017).

Por lo antes expuesto se justifica la elaboración de una propuesta que permita reducir la vulnerabilidad, impacto y riesgo de la seguridad de los servidores Linux del GADPO frente a un ataque informático de tipo pishing y DDoS.

6.4. Objetivos

6.4.1. Objetivo general

- Elaborar una propuesta que permita mitigar los riesgos de los ataques de pishing y DDoS a los servidores Linux del GADPO.

6.4.2. Objetivos específicos

- Elaborar un plan de concientización y capacitación sobre seguridad de la información para los funcionarios del GADPO
- Determinar los mecanismos de aseguramiento para el servidor firewall contra ataques DDoS de tipo SYN Flood.
- Evaluar la efectividad de la propuesta desarrollada.

6.5. Análisis de factibilidad

6.5.1. Factibilidad técnica

Desde el punto de vista técnico fue factible llevar a cabo la implementación de la presente propuesta, debido a que se contó con el apoyo del GADPO, en especial de la JIT para el acceso a la información relacionada con la red de datos y servidores Linux.

6.5.2. Factibilidad operativa

El GADPO facilitó el acceso a la información requerida para el desarrollo de la presente investigación, por lo que fue operativamente factible realizar la implementación de la solución propuesta.

6.5.3. Factibilidad económica

La presente investigación fue factible económicamente, ya que los costos relacionados con el análisis, diseño e implementación de la propuesta fueron asumidos por el investigador.

6.6. Fundamentación

La metodología utilizada empezó con la determinación de aquellos ataques informáticos que comúnmente afectan a las organizaciones en base a los reportes

estadísticos de importantes empresas dedicadas a la seguridad informática. Posteriormente se realizaron simulaciones de los ataques informáticos y con la ayuda de la metodología MAGERIT v3.0 se pudo determinar la vulnerabilidad, impacto y riesgo que estos provocaban en la seguridad de los servidores Linux del GADPO. Finalmente se estableció una propuesta que contempla los mecanismos para el aseguramiento de los servidores contra los ataques de pishing y DDoS.

6.7. Metodología, modelo operativo

La presente propuesta se enfoca en establecer una metodología de endurecimiento de los servidores Linux del GADPO para los ataques informáticos de pishing y DDoS de tipo SYN Flood.

6.7.1. Protección contra ataques de pishing

Para contrarrestar los efectos de los ataques de pishing, se propone un plan de concientización y capacitación para los funcionarios del GADPO sobre seguridad de la información.

6.7.1.1. Plan de capacitación y concientización sobre seguridad de la información del GADPO

La mayoría de las organizaciones por lo general para proteger su información realizan fuertes inversiones en hardware y nuevas tecnologías, pero se han olvidado de las personas y sin querer han provocado que ellas sean el eslabón más débil en lo que respecta a seguridad de la información dentro de una empresa (Álvarez, 2017).

En virtud a lo anteriormente expuesto y a los resultados de los ataques de pishing realizados, se hace necesario establecer un plan de capacitación a los empleados del GADPO que mitigue el riesgo de que puedan ser víctimas de ataques de pishing.

Tomando como punto de partida la "Guía para la Elaboración de un Plan de Concientización y Entrenamiento, sobre Seguridad de la Información" desarrollada por Diego Álvarez de la Universidad Piloto de Colombia se propone el siguiente plan de concientización y entrenamiento sobre seguridad de la información para el GADPO.

A. Diseño

1. Estructura del programa de concientización y entrenamiento

Se plantea un programa de concientización y capacitación centralizado, en el cual el responsable de su ejecución sea la JIT, ya que cuenta con personal afines a los temas de capacitación a tratarse. Además, cabe indicar que se debe asignar el debido presupuesto para una adecuada ejecución del programa de capacitación.

2. Evaluación de necesidades

Con base a los resultados anteriormente expuestos en la presente investigación, donde se pudo determinar con la ayuda de la metodología MAGERTI v3.0 que una vez realizados los ataques de pishing existe en el GADPO un 67.94% de vulnerabilidad y un impacto de nivel alto. El cálculo de los riesgos indicó un nivel de riesgo para la confidencialidad de la información de 22.42%, un riesgo de 44.84% a la integridad de la información y un riesgo de 67.26% de la disponibilidad.

Por lo expuesto se hace necesario establecer un plan de capacitación para los usuarios del GADPO en materia de ataques de Ingeniería Social, específicamente el pishing, ataque que se ha venido estudiando a lo largo de esta investigación.

3. Desarrollo de estrategias y planes

- **Alcance del plan**

El presente plan de concientización y capacitación se enfoca en cómo actuar ante los ataques de pishing y está dirigido a los funcionarios del GADPO.

- **Objetivos del plan**

- Capacitar a los usuarios del GADPO en temas relacionados con la protección frente a los ataques de pishing.
- Mitigar los riesgos que pueda provocar un ataque de pishing a la seguridad de la información en el GADPO.

- **Roles y responsabilidades**

Tabla 32. Roles y responsabilidades en el plan de capacitación

Rol	Responsabilidad
Jefe de Sistemas	- Gestionar la asignación de presupuesto para el plan de concientización y entrenamiento de funcionarios del GADPO en materia de seguridad de la información - Coordinar con Talento Humano las fechas en las que se dictarán los cursos de capacitación al personal. - Revisar y aprobar el material elaborado para las capacitaciones.
Profesional Informático	- Investigar sobre nuevos posibles ataques informáticos que puedan afectar a los usuarios del GADPO - Elaborar el material para las capacitaciones a los usuarios sobre seguridad de la información. - Actualizar el material de capacitación en base a las investigaciones realizadas sobre ataques informáticos - Capacitar a los usuarios del GADPO.
Administrador de Redes	- Garantizar el acceso a Internet o a cualquier servicio tecnológico requerido en el lugar donde se realizarán las capacitaciones.

Elaborado por: Investigador

- **A quien va dirigido**

El presente plan de concientización y capacitación va dirigido a los funcionarios del GADPO y que interactúan a diario con dispositivos informáticos.

- **Temas a tratar**

- Seguridad de la información
- Ataques informáticos: Pishing
- Ataque informático de pishing al GADPO
- Como protegerse del pishing

- **Frecuencia de las capacitaciones**

La frecuencia de las capacitaciones estará determinada por los nuevos ataques informáticos que puedan surgir y que se considere puedan afectar gravemente la seguridad de la información del GADPO.

- **Evaluación y renovación del material creado**

A partir de la determinación de nuevos ataques informáticos que puedan afectar a la seguridad de la información del GADPO, será necesario actualizar los contenidos elaborados para las capacitaciones.

4. Definición de prioridades

Como prioridad se estableció capacitar a los usuarios del GADPO en lo que respecta a los ataques informáticos de pishing.

5. Aprobación

La aprobación del presente plan de concientización y capacitación estuvo a cargo del Jefe de Informática y Tecnología.

6. Financiamiento

Para llevar a cabo el presente plan de capacitación se contó con el apoyo del GADPO quien financió el total de los recursos utilizados. Para futuros planes de capacitación, en caso de requerir algún otro recurso, se deberá hacer constar en el plan anual de contratación para el respectivo financiamiento.

Los recursos utilizados en el presente plan se detallan en la siguiente tabla:

Tabla 33. Recursos utilizados en el plan de capacitación

Recurso	Costo/hora	Cantidad horas	Subtotal
Jefe de Sistemas	8	3	24
Profesional Informático	6	64	384
Administrador de Redes	6	2	12
Internet	0.50	40	20
TOTAL			440USD

Elaborado por: Investigador

B. Desarrollo de material de concientización

El material para realizar la capacitación, se puede obtener a partir de diversas fuentes como (Álvarez, 2017):

- Organizaciones profesionales y proveedores de seguridad de la información.
- Periódicos

- Conferencias
- Seminarios online
- Boletines sobre seguridad en la web

A continuación, se desarrollan los temas definidos en la fase de diseño del presente plan:

1. Seguridad de la información

La seguridad de la información abarca tres dimensiones, que son los pilares sobre los que se aplica las medidas de protección de la información (Liras, 2015):

Figura 72. Dimensiones de la seguridad de la información

Fuente: (Liras, 2015)

- La disponibilidad de la información, se refiere a que la información esté accesible cuando se la requiera. Un ejemplo de falta de disponibilidad de la información sería cuando se intenta acceder a una página web y nos es imposible hacerlo debido a algún error de configuración.
- La integridad de la información, hace referencia a que la información no haya sido alterada intencionalmente y se encuentre libre de errores. Por ejemplo, la alteración de un reporte de ventas por parte de un empleado malintencionado o por error sería un ataque a la integridad.
- La confidencialidad implica, que la información debe estar accesible únicamente para las personas autorizadas. Ejemplos de falta de confidencialidad, sería la publicación en redes sociales de información confidencial.

2. Ataque informático

Un ataque informático es un método por el cual un individuo, a través de un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (Guamán, 2014).

3. Phishing

Según el Instituto Nacional de Ciberseguridad de España (INCIBE), una de las amenazas de ciberseguridad que afectan frecuentemente a las pymes es el phishing. El término phishing viene del inglés fishing y significa pescar. Para este caso no se pescan peces, sino datos personales como por ejemplo usuarios, contraseñas o datos de cuentas bancarias.

INCIBE define al pishing como una forma de ingeniería social, en la cual un atacante intenta adquirir información confidencial de forma fraudulenta de una víctima, haciéndose pasar por un tercero de confianza.

3.1. Ataque de pishing a funcionarios del GADPO

Se efectuaron cuatro ataques de pishing a los usuarios del GADPO. A través del sistema de mensajería Spark se les hizo llegar un mensaje, el mismo que tenía como finalidad engañar al usuario para obtener las credenciales de acceso del sistema atacado. La siguiente figura muestra uno de los mensajes enviados a los usuarios:

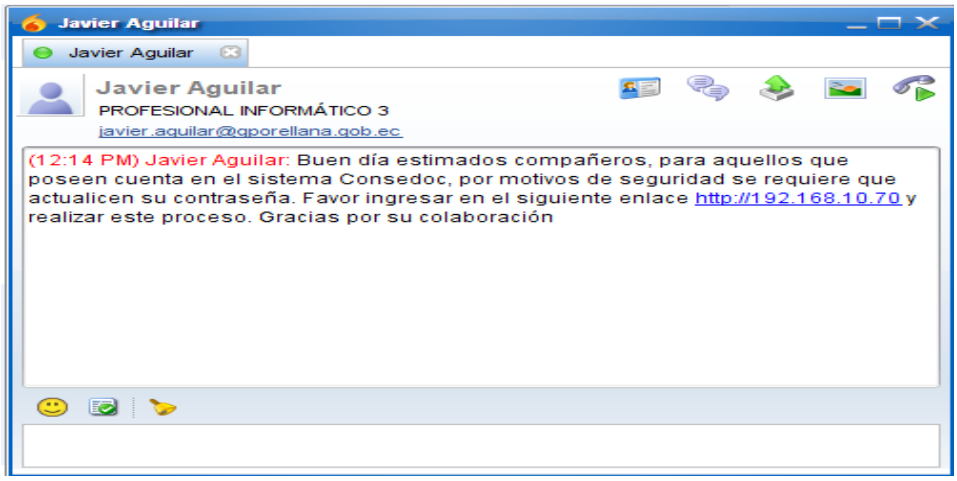


Figura 73. Mensaje de engaño enviado

Elaborado por: Investigador

El usuario al abrir el enlace enviado, pudo observar una página web idéntica al sitio web del servicio atacado.

Haciendo referencia al mensaje mostrado en la figura anterior en el que se solicita actualizar la contraseña del sistema Consedoc, la página que se le mostró en este caso al usuario fue la siguiente:

Figura 74. Sitio web falso mostrado al usuario

Elaborado por: Investigador

Una vez que el usuario accedió al sitio, ingresó sus credenciales y posteriormente hizo clic en el botón ingresar, el atacante pudo obtener el usuario y contraseña de acceso al sistema.

En los ataques realizados los resultados obtenidos fueron los siguientes:

Ataque 1: Ataque realizado al servidor de correo electrónico institucional. Los usuarios atacados fueron los siguientes:

Tabla 34. Resultados obtenidos en el ataque de pishing 1

Coordinación	Usuarios atacados	Ataques satisfactorios
Administrativo	9	8
Financiero	13	7
Talento Humano	10	5
Planificación Técnica	10	9
Turismo	6	6
Fomento Productivo	7	4
Gestión Ambiental	10	6
Imagen Institucional	3	2
Nacionalidades	5	5
TOTAL	73	52

Elaborado por: Investigador

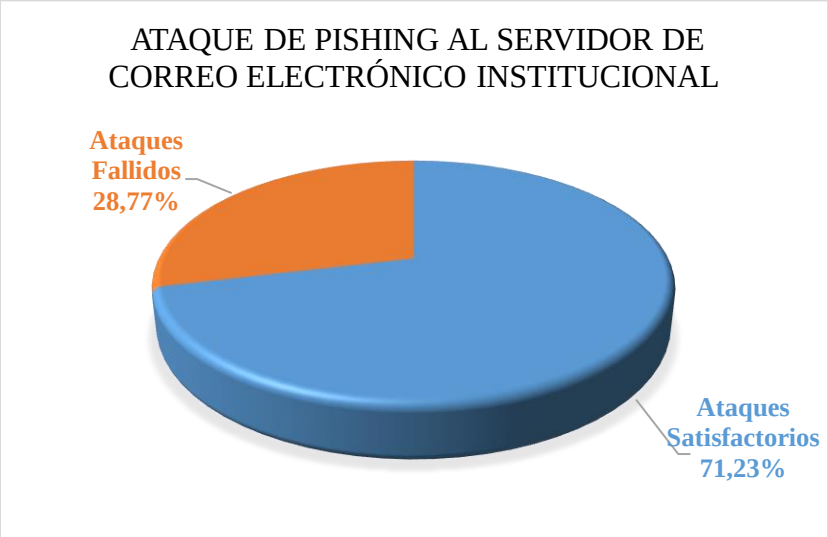


Figura 75. Resultados obtenidos en el ataque de pishing 1
Elaborado por: Investigador

Como resultado final del primer intento de ataque de pishing efectuado mediante la clonación del acceso web del servicio de correo electrónico institucional, de los 73 usuarios a los cuales se les envió el mensaje de engaño, 52 correspondiente a un 71.23% cayeron en la trampa y otorgaron sus credenciales de acceso al correo electrónico, mientras que 21 usuarios correspondiente a un 28.77% del total de usuarios atacados ignoraron el mensaje.

Ataque 2: Se realizó un segundo ataque al servidor de correo electrónico institucional, obteniendo los siguientes resultados:

Tabla 35. Resultados obtenidos en el ataque de pishing 2

Coordinación	Usuarios Atacados	Ataques Satisfactorios
Compras Públicas	4	4
Participación Ciudadana	3	1
Financiero	6	3
Fomento Productivo	6	3
Obras Públicas	2	1
TOTAL	21	12

Elaborado por: Investigador

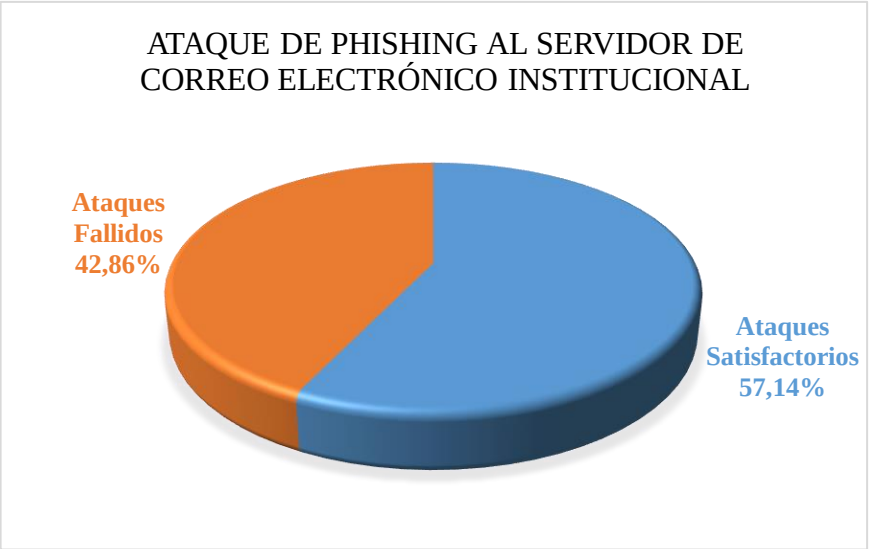


Figura 76. Resultados obtenidos en el ataque de pishing 2
Elaborado por: Investigador

En el segundo intento, de los 21 usuarios atacados, 12 correspondiente al 57.14% entregaron sus credenciales de acceso al correo electrónico institucional, mientras que los 9 restantes correspondiente a un 42.86% hicieron caso omiso del mensaje.

Ataque 3: Ataque de pishing realizado al servidor de trámites en línea Consedoc. Se obtuvieron los siguientes resultados:

Tabla 36. Resultados obtenidos en el ataque de pishing 3

Coordinación	Usuarios atacados	Ataques satisfactorios
Gestión Ambiental	6	5
Fomento Productivo	5	3
Participación Ciudadana	5	2
Financiero	5	5
TOTAL	21	15

Elaborado por: Investigador

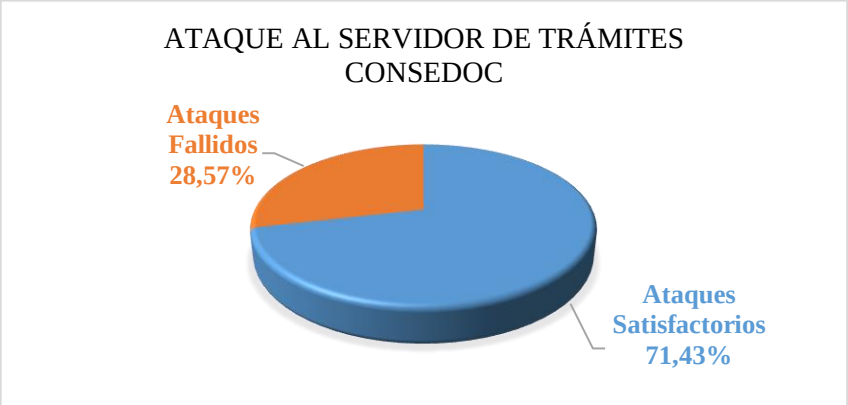


Figura 77. Resultados obtenidos en el ataque de pishing 3

Elaborado por: Investigador

De 21 usuarios atacados, se obtuvo las credenciales de acceso de 15 usuarios correspondiente a un 71.43%, mientras tanto que los 6 restante correspondiente a un 28.57% no entregaron sus claves de acceso.

Ataque 4: Se realizó un nuevo intento de ataque de pishing al servidor de trámites en línea Consedoc. Los resultados obtenidos fueron los siguientes:

Tabla 37. Resultados obtenidos en el ataque de pishing 4

Coordinación	Usuarios atacados	Ataques satisfactorios
Turismo	3	2
Nacionalidades	2	1
Planificación	3	1
Obras Públicas	3	1
Administrativo	5	5
TOTAL	16	10

Elaborado por: Investigador

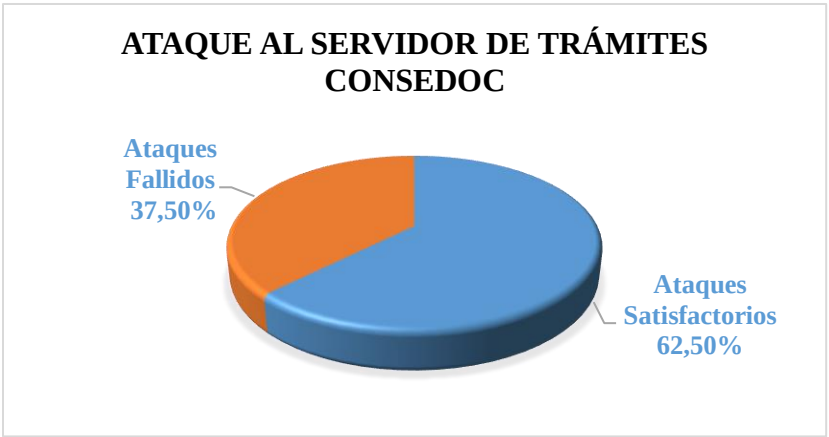


Figura 78. Resultados obtenidos en el ataque de pishing 4

Elaborado por: Investigador

Como resultado final de los distintos ataques de pishing realizados se tiene que 89 ataques correspondiente a un 68% fueron satisfactorios, mientras que 42 correspondientes a un 32% fueron ataques fallidos.

3.2. ¿Cómo actuar ante los ataques de pishing?

El INCIBE a través de su kit de concienciación pishing brinda los siguientes consejos de que se puede hacer ante un ataque de este tipo:

- Ante cualquier duda sobre un mensaje recibido, no facilitar información confidencial.
- Mantenerse informado sobre las últimas noticias en materia de seguridad de la información.
- Utilizar un antivirus y mantenerlo actualizado. En caso de alguna sospecha realizar un análisis del ordenador.
- Si se tiene dudas de la información recibida ponerse en contacto por otros medios para realizar la respectiva verificación.
- Prestar atención a la redacción, sospechar si la redacción no tiene sentido o existen errores ortográficos o gramaticales.
- Utilizar el sentido común cuando se vaya a realizar alguna transacción por internet, si le ofrecen algo que es demasiado bueno para ser cierto, simplemente es que no es cierto.
- Nunca proporcionar datos confidenciales como usuarios, contraseñas, número de cuentas bancarias, números de tarjetas de crédito, cédula, número de celular, a menos que esté pagando por algún servicio en un sitio seguro y reconocido.
- Si ha sido víctima de pishing, informar inmediatamente a la empresa suplantada. Informar además en caso de que suceda en su trabajo al responsable de tecnologías de la información.
- Cuando tenga que introducir información confidencial en una página web, verifique que el sitio es seguro. Ha de empezar con <<https://>> y tener un candado cerrado en el navegador.
- Una variante del pishing es el smishing, que se realiza a través de mensajes de texto en los cuales se intenta convencer de que se visite un enlace fraudulento.

- El vishing se realiza a través de una llamada telefónica que simula proceder de una entidad bancaria solicitando la verificación de datos.

C. Implementación del plan

La técnica utilizada en el presente proyecto para difundir la información sobre los ataques de pishing a los usuarios fue una charla de concientización, dicha charla fue realizada en el Auditorio del GADPO.

D. Mantenimiento del plan

Indicadores

En la presente investigación, luego de realizada la capacitación, se volvieron a efectuar ataques informáticos de pishing a los usuarios del GADPO para verificar el comportamiento de los indicadores que se determinaron en la evaluación de necesidades de la fase de diseño.

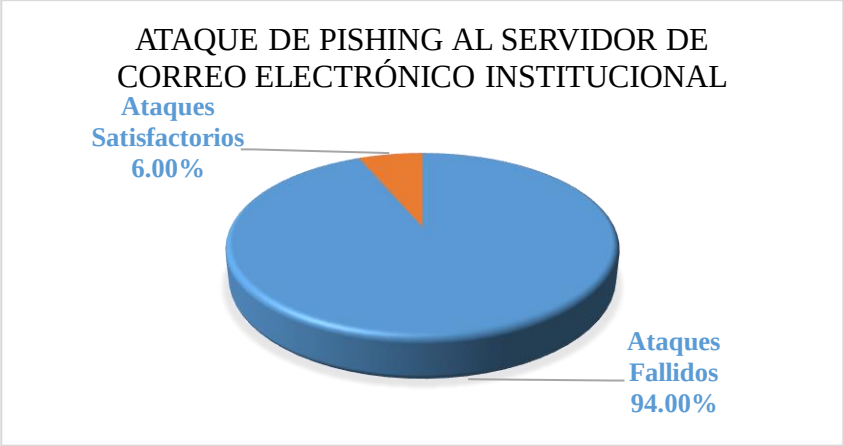
Los resultados obtenidos fueron los siguientes:

Ataque 1: Ataque realizado al servidor de correo electrónico institucional. Los usuarios atacados fueron los siguientes:

Tabla 38. Resultados ataque phishing 1 luego de la capacitación

Coordinación	Usuarios atacados	Ataques satisfactorios
Administrativo	9	1
Financiero	13	0
Talento Humano	10	0
Planificación Técnica	10	2
Turismo	6	1
Fomento Productivo	7	0
Gestión Ambiental	10	1
Imagen Institucional	3	0
Nacionalidades	5	0
TOTAL	73	5

Elaborado por: Investigador



Elaborado por: Investigador

Figura 79. Resultados ataque pishing 1 luego de la capacitación

De 73 usuarios atacados, tan solo 5 usuarios correspondiente al 6.00% cayeron en la trampa, mientras que los 68 restantes correspondiente a un 94.00% ignoraron el mensaje.

Ataque 2: Se realizó un segundo ataque al servidor de correo electrónico institucional, obteniendo los siguientes resultados:

Tabla 39. Resultados ataque phishing 2 luego de la capacitación

Coordinación	Usuarios atacados	Ataques satisfactorios
Compras Públicas	4	0
Participación Ciudadana	3	0
Financiero	6	0
Fomento Productivo	6	1
Obras Públicas	2	0
TOTAL	21	1

Elaborado por: Investigador

Figura 80. Resultados obtenidos en el ataque de pishing 2 luego de la capacitación

Elaborado por: Investigador

En este ataque realizado se logró un ataque satisfactorio correspondiente al 4.55%, mientras que el 95.45% restante correspondió a los ataques fallidos.

Ataque 3: Ataque de pishing realizado al servidor de trámites en línea Consedoc. Se obtuvieron los siguientes resultados:

Tabla 40. Resultados obtenidos en el ataque de pishing 3 luego de la capacitación

Coordinación	Usuarios atacados	Ataques satisfactorios
Gestión Ambiental	6	2
Fomento Productivo	5	0
Participación Ciudadana	5	0
Financiero	5	1
TOTAL	21	3

Elaborado por: Investigador

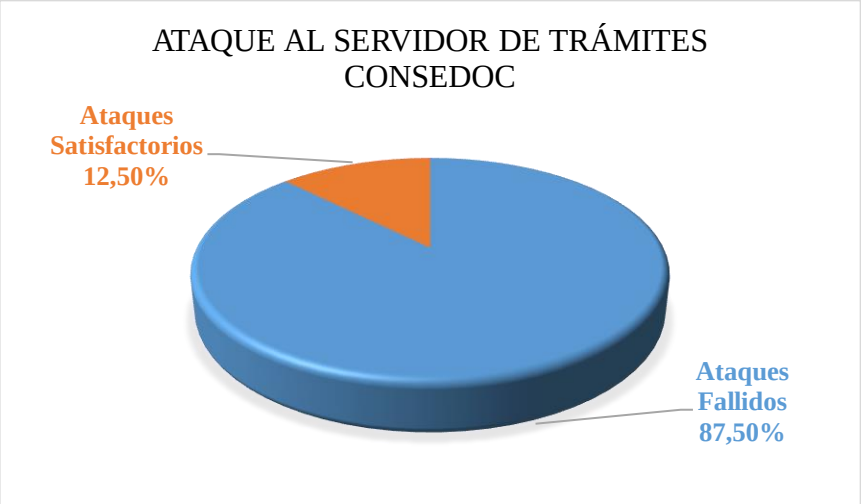


Figura 81. Resultados obtenidos en el ataque de pishing 3 luego de la capacitación
Elaborado por: Investigador

De 21 usuarios atacados, 3 ataques correspondientes a un 12.50% fueron satisfactorios, mientras que los 18 restantes correspondientes a un 87.50% fueron ataques fallidos.

Ataque 4: Se realizó un nuevo intento de ataque de pishing al servidor de trámites en línea Consedoc. Los resultados obtenidos fueron los siguientes:

Tabla 41. Resultados obtenidos en el ataque de pishing 4

Coordinación	Usuarios atacados	Ataques satisfactorios
Turismo	3	0
Nacionalidades	2	0
Planificación	3	0
Obras Públicas	3	0
Administrativo	5	0
TOTAL	16	0

Elaborado por: Investigador

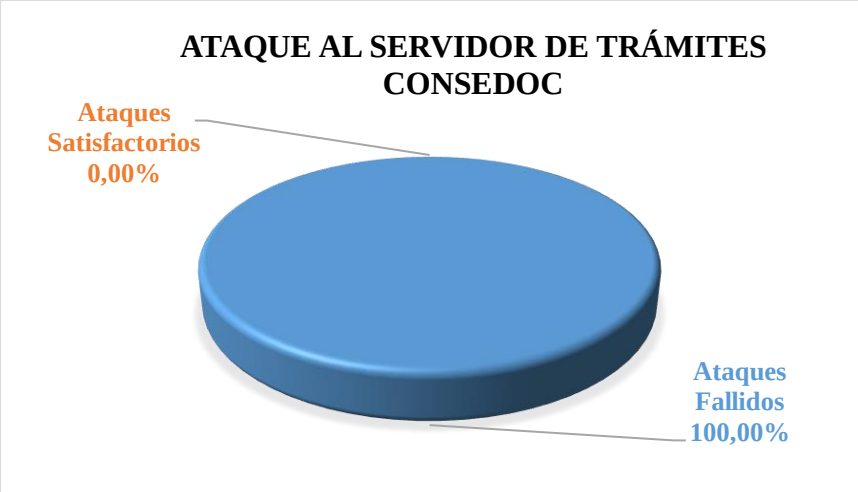


Figura 82. Resultados obtenidos en el ataque de pishing 4 luego de la capacitación
Elaborado por: Investigador

De los 16 ataques efectuados, ningún usuario accedió al engaño, obteniendo de esta forma un 100.00% de ataques fallidos.

Figura 83. Resultado final de los ataques de phishing luego de la capacitación
Elaborado por: Investigador

Como resultado de los cuatro ataques informáticos de phishing efectuados luego de la capacitación, se obtuvo que de los 131 usuarios atacados 9 usuarios correspondiente al 6.43% cayeron en la trampa, mientras que el 93.57% restante ignoraron el mensaje de engaño.

Tabla 42. Indicadores para el mantenimiento del plan de capacitación

Indicador	Diseño (Evaluación de Necesidades)	Luego de la capacitación
Vulnerabilidad	67.94%	6.43%
Impacto	Alto	Bajo
Riesgo (Confidencialidad)	22.42%	2.12%
Riesgo (Integridad)	44.84%	4.24%
Riesgo (Disponibilidad)	67.26%	6.37%

Elaborado por: Investigador

Con los resultados obtenidos se pudo evidenciar que el presente plan de capacitación tuvo un impacto positivo, ya que se pudo reducir la vulnerabilidad de, impacto y riesgo de los ataques de pishing a la seguridad de la información del GADPO.

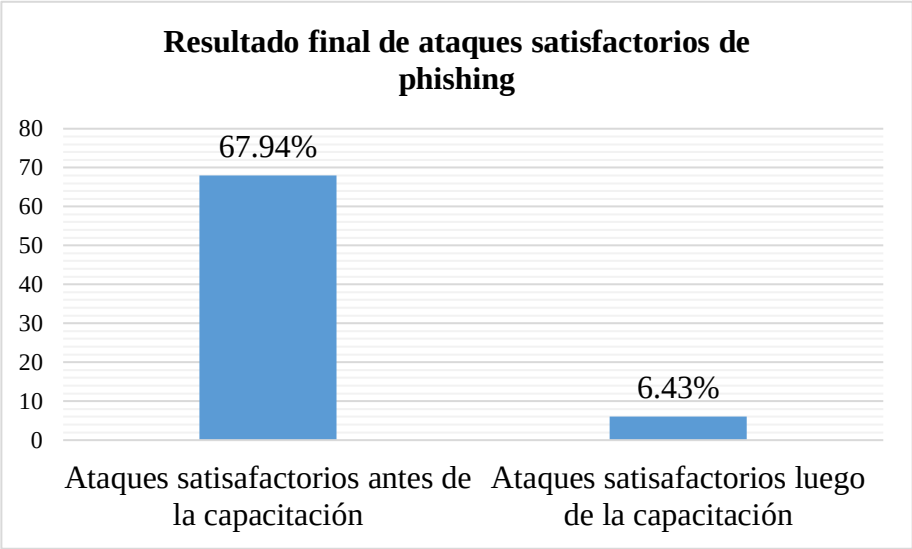


Figura 84. Resultado final ataques satisfactorios de phishing

Elaborado por: Investigador

Una vez aplicado el plan de capacitación sobre los ataques informáticos de phishing a los funcionarios del GADPO, se logró reducir el porcentaje de ataques satisfactorios de 67.94% a 6.43%.

6.7.2. Protección contra ataques DDoS SYN Flood

Los ataques DDoS son un tipo de ataque informático que busca reducir la capacidad de un servidor o recurso informático de ofrecer un servicio. La mayoría de las veces este tipo de ataque supone un gran problema porque no solo se ven afectados los clientes, sino también los administradores ya que serían incapaces de acceder al recurso para administrarlo y tratar de impedir o mitigar el incidente.

6.7.2.1. Configuraciones en el kernel de Linux para mitigar los ataques DDoS

Para activar en Linux las SYN Cookies debemos realizar lo siguiente(Bogdanoski, 2013):

Editamos el archivo /etc/sysctl.conf y añadimos lo siguiente:

#Habilitar syncookies

net.ipv4.tcp_syncookies = 1

#Aumentar tamaño de cola SYN de 1024 a 2048

net.ipv4.tcp_max_syn_backlog = 2048

Además de habilitar las SYN Cookies, para mitigar los efectos de un ataque SYN Flood es necesario usar iptables.

Existen tres tablas en iptables, cualquier regla que se cree irá a una de estas tablas. La tabla por defecto y la más utilizada es Filter. Esta tabla contiene las siguientes cadenas:

INPUT: Procesa los paquetes entrantes

FORWARD: Procesa los paquetes que pasan a través del host.

OUTPUT: Procesa los paquetes salientes.

Para la creación de las reglas de mitigación con iptables, se utilizó la cadena FORWARD, debido a que se trabajó en un servidor firewall y es por donde pasan los paquetes de datos de los distintos servicios que se ofrecen en la red.

A continuación, se muestran las reglas utilizadas para la mitigación del ataque (Qasim & Musawi, 2012) (RedHat, 2014):

#iptables –N syn_flood

#iptables –A FORWARD –p tcp –syn –j syn_flood

#iptables –A syn_flood –m limit –limit 1/s –limit-burst 3 –j RETURN

#iptables –A syn_flood –j DROP

#iptables -A INPUT -i $DEV -p tcp -m tcp --dport $PORT \ -m state --state INVALID, UNTRACKED \ -j SYNPROXY --sack-perm --timestamp --wscale 7 --mss 1460

Las opciones utilizadas se describen en la siguiente tabla:

Tabla 43. Comandos utilizados en reglas iptables

OPCIONES DE COMANDOS IPTABLES	
-N	Crea una nueva cadena con un nombre definido por el usuario
-A	Permite añadir una regla de iptables.
FORWARD	Cadena que procesa los paquetes de datos que pasan a través del firewall
-p	Establece el protocolo para la regla
-j	Salta a un objetivo particular como ACCEPT, DROP, QUEUE, RETURN y una cadena definida por el usuario.
-m	Indica el estado de una conexión.
--syn	Provoca que los paquetes TCP, comúnmente llamados SYN cumplan esta regla.
--limit	Especifica el número de coincidencias en un intervalo de tiempo especificado con un número y un modificador de tiempo <número>/<tiempo>
--limit-burst	Configura un límite en el número de paquetes capaces de cumplir una regla en un determinado tiempo. Se usa conjuntamente con –limit
DROP	Deja caer el paquete sin responder al solicitante
RETURN	Verifica el paquete contra las reglas de la cadena actual.

Elaborado por: Investigador

Una vez aplicadas las reglas de mitigación se procedió a realizar nuevamente ataques DDoS SYN Flood para evaluar la efectividad de las mismas frente a este tipo de ataques.

Se procedió a efectuar nuevamente ataques DDoS de tipo SYN Flood, luego de haber implementado las medidas de mitigación obteniendo los siguientes resultados

Ataque 1: hping3 -V -c 4500 -d 800 -S -p 8443 --flood --rand-source 192.168.10.55

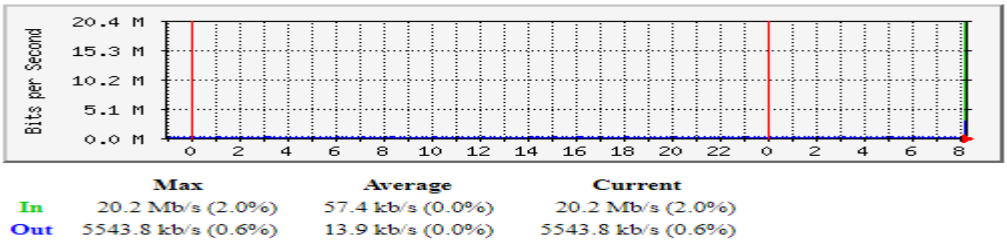


Figura 85. Uso de ancho de banda ataque 1 DDoS

Elaborado por: Investigador

El ancho de banda utilizado por el ataque DDoS efectuado fue de 20.2 Mb/s correspondiente a un 2.0% del ancho de banda disponible.

Ataque 2: hping3 -V -c 1500 -d 200 -S -p 8443 --flood --rand-source 192.168.10.55

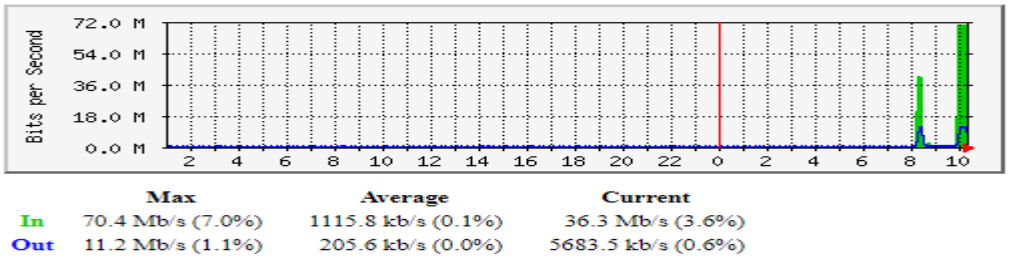


Figura 86. Uso de ancho de banda ataque 2 DDoS

Elaborado por: Investigador

El ancho de banda alcanzado fue de 36.3 Mb/s correspondiente a un 3.6% del ancho de banda disponible.

Ataque 3: hping3 -V -c 2000 -d 300 -S -p 8443 --flood --rand-source 192.168.10.55

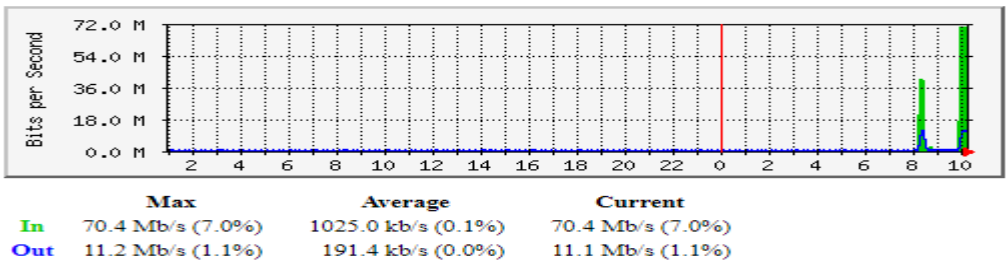


Figura 87. Uso de ancho de banda ataque 3 DDoS

Elaborado por: Investigador

El ancho de banda alcanzado fue de 70.4 Mb/s, es decir un 7.0% del total del ancho de banda de 1 Gb/s.

Ataque 4: hping3 -V -c 2500 -d 400 -S -p 8443 --flood --rand-source 192.168.10.55

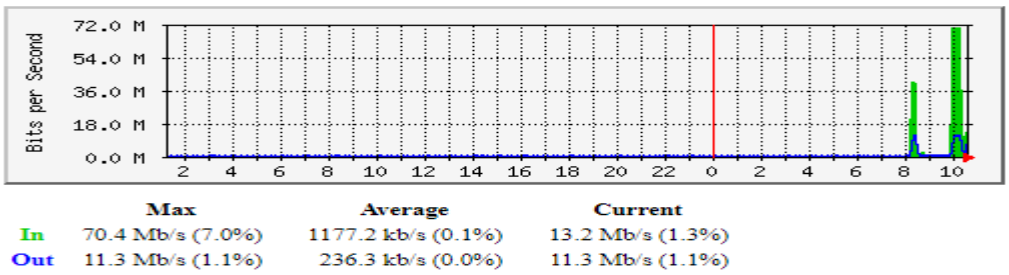


Figura 88. Uso de ancho de banda ataque 4 DDoS

Elaborado por: Investigador

El ancho de banda alcanzado por el ataque informático fue de 13.2 Mb/s correspondiente a un 1.3%.

Ataque 5: hping3 -V -c 3000 -d 500 -S -p 8443 --flood --rand-source 192.168.10.55

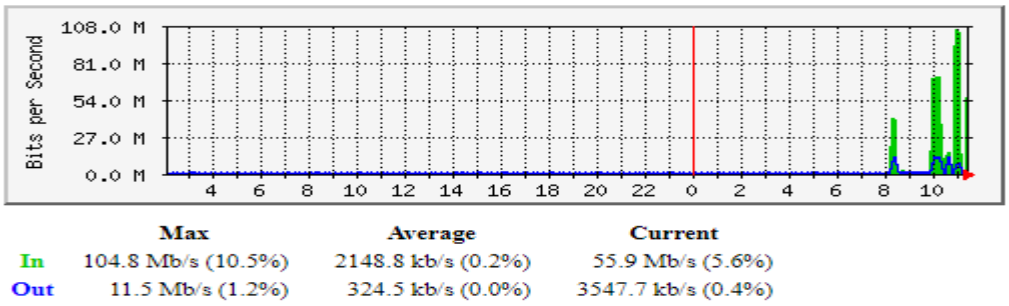


Figura 89. Uso de ancho de banda ataque 5 DDoS

Elaborado por: Investigador

El ancho de banda alcanzado fue de 55.9 Mb/s correspondiente a un 5.6%.

Ataque 6: hping3 -V -c 3500 -d 600 -S -p 8443 --flood --rand-source 192.168.10.55

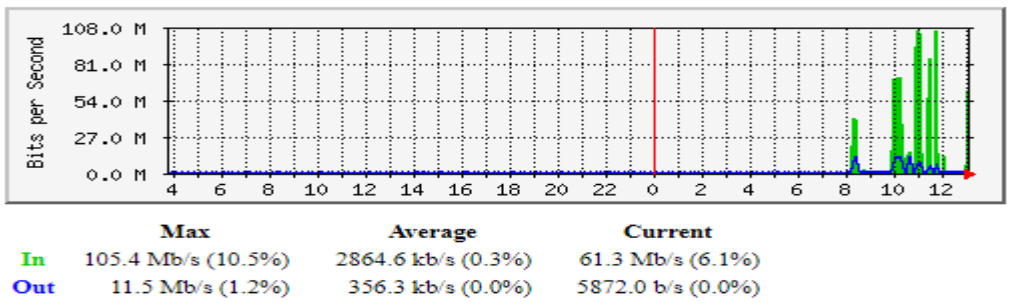
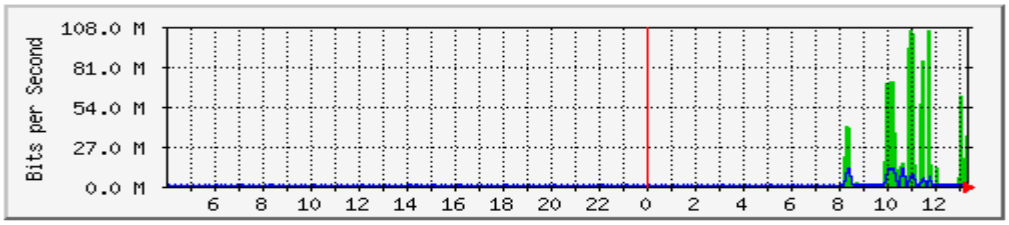


Figura 90. Uso de ancho de banda ataque 6 DDoS

Elaborado por: Investigador

El ancho de banda utilizado por el ataque informático fue de 61.3 Mb/s, es decir un 6.1% del total de ancho de banda disponible.

Ataque 7: hping3 -V -c 4000 -d 700 -S -p 8443 --flood --rand-source 192.168.10.55



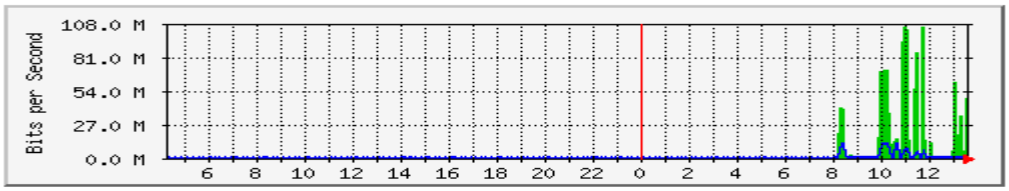
	Max	Average	Current
In	105.4 Mb/s (10.5%)	2996.9 kb/s (0.3%)	33.7 Mb/s (3.4%)
Out	11.5 Mb/s (1.2%)	356.3 kb/s (0.0%)	1200.0 b/s (0.0%)

Figura 91. Uso de ancho de banda ataque 7 DDoS

Elaborado por: Investigador

El ancho de banda utilizado por el ataque informático fue de 33.7 Mb/s correspondiente a un 3.4% del ancho de banda disponible.

Ataque 8: hping3 -V -c 4500 -d 800 -S -p 8443 --flood --rand-source 192.168.10.55



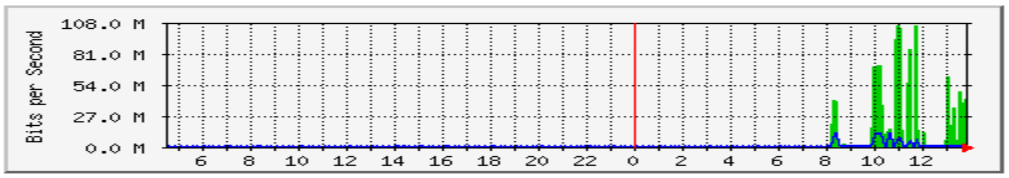
	Max	Average	Current
In	105.4 Mb/s (10.5%)	3131.3 kb/s (0.3%)	48.0 Mb/s (4.8%)
Out	11.5 Mb/s (1.2%)	356.3 kb/s (0.0%)	3976.0 b/s (0.0%)

Figura 92. Uso de ancho de banda ataque 8 DDoS

Elaborado por: Investigador

El ancho de banda alcanzado en este ataque informático fue de 48 Mb/s, es decir un 4.8% del total de ancho de banda.

Ataque 9: hping3 -V -c 5000 -d 900 -S -p 8443 --flood --rand-source 192.168.10.55



	Max	Average	Current
In	105.4 Mb/s (10.5%)	3331.5 kb/s (0.3%)	41.5 Mb/s (4.2%)
Out	11.5 Mb/s (1.2%)	356.3 kb/s (0.0%)	280.0 b/s (0.0%)

Figura 93. Uso de ancho de banda ataque 9 DDoS

Elaborado por: Investigador

El tráfico generado por el ataque informático fue de 41.5 Mb/s, ocupando un 4.2% del ancho de banda.

Ataque 10: hping3 -V -c 5500 -d 1000 -S -p 8443 --flood --rand-source 192.168.10.55

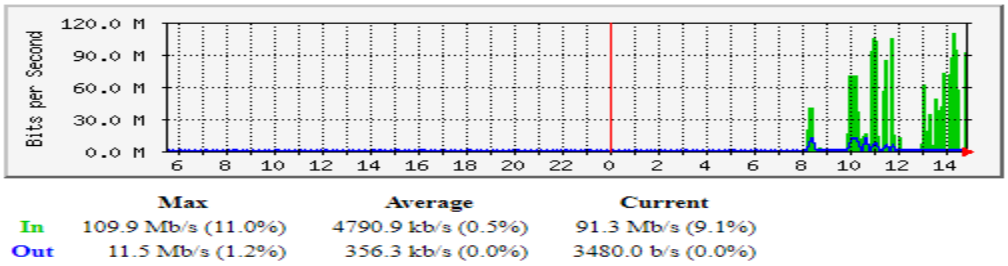


Figura 94. Uso de ancho de banda ataque 10 DDoS

Elaborado por: Investigador

El tráfico generado fue de 91.3 Mb/s, correspondiente a un 9.1% del ancho de banda disponible.

Ataque 11: hping3 -V -c 6000 -d 1500 -S -p 8443 --flood --rand-source 192.168.10.55

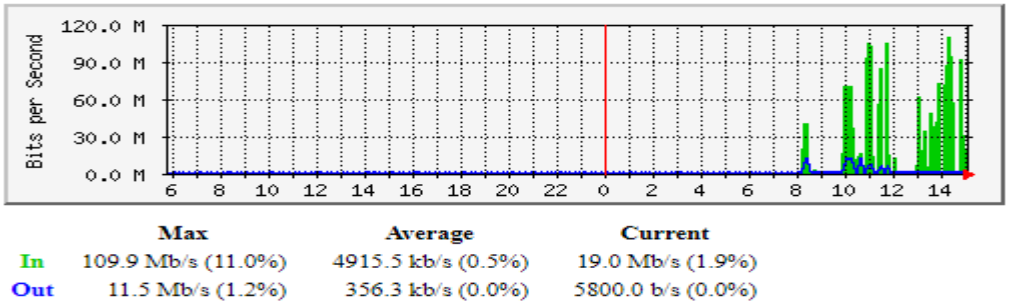


Figura 95. Uso de ancho de banda ataque 11 DDoS

Elaborado por: Investigador

El ancho de banda usado por el ataque informático fue de 19 Mb/s, correspondiente a un 1.9% del total de ancho de banda.

Ataque 12: hping3 -V -c 6500 -d 2000 -S -p 8443 --flood --rand-source 192.168.10.55

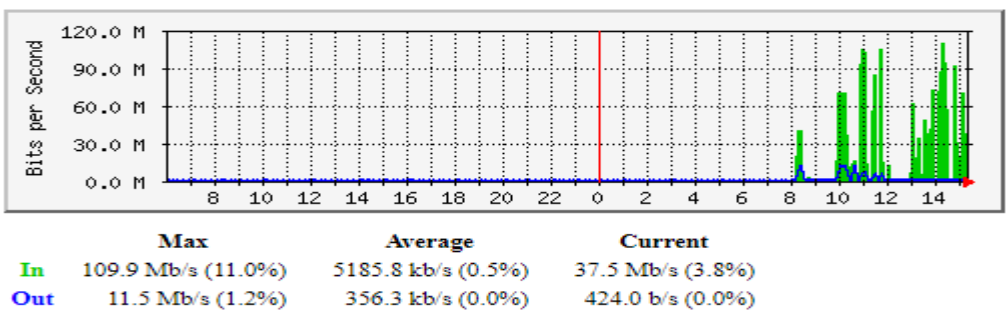


Figura 96. Uso de ancho de banda ataque 12 DDoS

Elaborado por: Investigador

El tráfico generado fue de 37.5 Mb/s, correspondiente a un 3.8% del total de ancho de banda disponible.

Ataque 13: hping3 -V -c 7000 -d 2500 -S -p 8443 --flood --rand-source 192.168.10.55

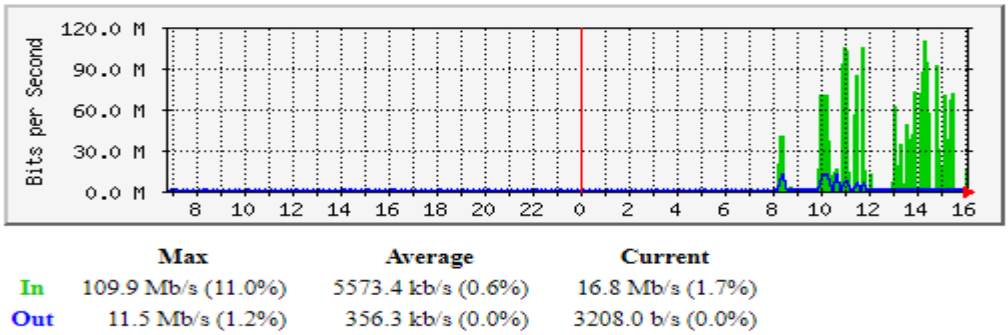


Figura 97. Uso de ancho de banda ataque 13 DDoS

Elaborado por: Investigador

El ancho de banda alcanzado por el ataque informático fue de 16.8 Mb/s, correspondiente a un 1.7% del total de ancho de banda.

Los resultados obtenidos en los distintos ataques informáticos efectuados se resumen en la siguiente tabla:

Tabla 44. Resultados ataques informáticos DDoS después de la mitigación

Número de PCs	Número de ataque	Cantidad de paquetes	Longitud de paquete (bytes)	% Uso de ancho de banda.
1	01	1000	100	2.00
1	02	1500	200	3.6.00
1	03	2000	300	7.00
1	04	2500	400	1.30
1	05	3000	500	5.60
1	06	3500	600	6.10
1	07	4000	700	3.40
1	08	4500	800	4.80
1	09	5000	900	4.20
1	10	5500	1000	9.10
1	11	6000	1500	1.90

1	12	6500	2000	3.80
1	13	7000	2500	1.70

Elaborado por: Investigador

En base a los resultados de la tabla anterior, se estima el uso de ancho de banda que se alcanzaría al realizar el mismo ataque informático con tres computadores.

Tabla 45. Resultados ataques informáticos DDoS con tres computadores

Número de PCs	Número de ataque	Cantidad de paquetes	Longitud de paquete (bytes)	% Uso de ancho de banda.
3	01	1500	100	6.00
3	02	2000	200	10.80
3	03	2500	300	21.00
3	04	3000	400	3.90
3	05	3500	500	16.80
3	06	4000	600	18.30
3	07	4500	700	10.20
3	08	5000	800	14.40
3	09	5500	900	12.60
3	10	6000	1000	27.30
3	11	6500	1500	5.70
3	12	7000	2000	11.40
3	13	7500	2500	5.10
PROMEDIO USO ANCHO DE BANDA				12.58

Elaborado por: Investigador

Tomando en cuenta que la vulnerabilidad que provocaba este tipo de ataque fue el porcentaje de uso de ancho de banda utilizado, se procede con la ayuda de la metodología MAGERIT a calcular la vulnerabilidad, impacto y riesgo luego de haber aplicado las medidas de mitigación.

Tabla 46. Cálculo vulnerabilidad luego de la mitigación del ataque DDoS

Ataque	% uso de ancho de banda	Vulnerabilidad
DDoS (SYN Flood)	12.58%	12.58%

Elaborado por: Investigador

Tabla 47. Cálculo vulnerabilidad, impacto y riesgo luego de la mitigación del ataque DDoS

Amenaza	Escala Amenaza	Vulnerabilidad	Impacto	Riesgo
DDoS	Disable Services (0.99)	12.58%	Bajo	12.45%

Elaborado por: Investigador

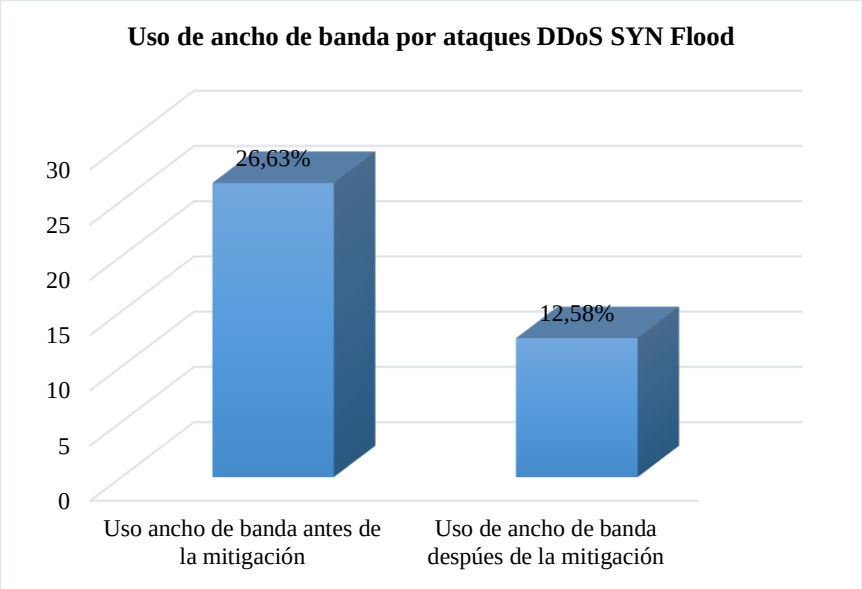


Figura 98. Uso de ancho de banda por ataques DDoS SYN Flood

Elaborado por: Investigador

Una vez implementadas las medidas de mitigación para evitar el uso excesivo del ancho de banda disponible en la red por ataques informáticos DDoS SYN Flood, el porcentaje de uso del ancho de banda paso de un 26.63% inicial a un 12.58%.

Finalmente, luego de haber identificado los ataques informáticos más comunes con base a reportes de importantes empresas de seguridad informática, haber evaluado el riesgo y vulnerabilidad que estos pueden significar para los servidores Linux del GADPO, haber tomado medidas de mitigación para evitar o reducir su impacto y luego haber realizado nuevamente ataques informáticos donde se confirmó que las medidas tomadas redujeron significativamente el impacto que estos ataques podrían provocar en los servidores, se propone una metodología de aseguramiento que para su formulación toma como referencia la metodología de hardening propuesta en la tesis denominada “Diseño e implementación de un proceso de hardening” que fue desarrollada en el año 2017 por Oscar Alonso Cruz Moreno de la Universidad Los Libertadores de Colombia.

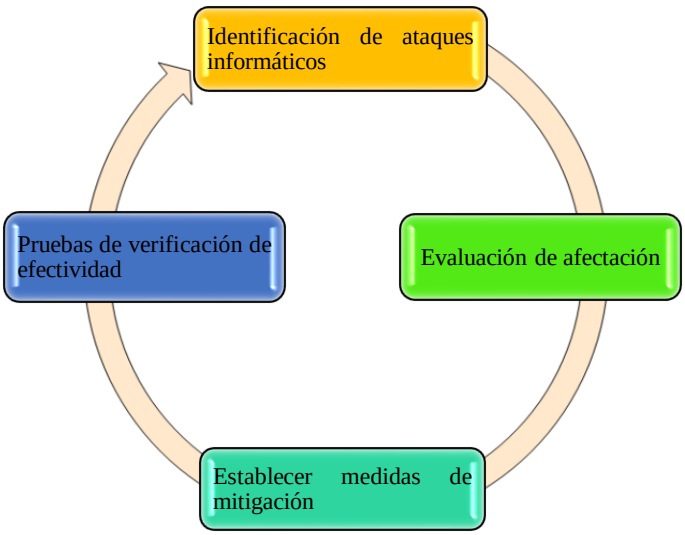


Figura 99. Metodología de aseguramiento de servidores Linux

Elaborado por: Investigador

Las acciones mínimas a realizar en la metodología de hardening propuesta se describen a continuación:

- **Identificación de ataques informáticos**

Determinar los ataques informáticos que están afectando a las infraestructuras de tecnologías de información, tomando en cuenta reportes estadísticos recientes que publican las empresas líderes en lo que respecta a seguridad informática.

- **Evaluación de afectación**

En esta fase utilizando herramientas recomendadas para efectuar ataques informáticos se realizan pruebas de penetración y con la ayuda de una metodología de gestión de riesgos como MAGERIT la utilizada en la presente investigación, se procede a determinar la vulnerabilidad, riesgo e impacto que los ataques informáticos puedan provocar en la infraestructura tecnológica.

- **Establecer medidas de mitigación**

Una vez entendido el funcionamiento de los ataques informáticos y determinados los niveles de afectación en la infraestructura tecnológica, se establecen medidas de protección recomendadas ya sea por artículos científicos, tesis o empresas dedicadas a brindar soluciones de seguridad informática.

- **Pruebas de verificación de efectividad**

Finalmente, luego de implementadas las medidas de mitigación, se debe de realizar nuevamente las pruebas de penetración para evaluar que las acciones llevadas a cabo para proteger nuestra infraestructura funcionan y son realmente efectivas.

El proceso antes descrito debe ser llevado a cabo dentro de la organización de forma continua, dado que cada día surgen nuevas amenazas informáticas que pueden comprometer la confidencialidad, integridad y disponibilidad de la información.

6.8. Administración

La presente investigación fue administrada por el investigador, en donde se empezó por determinar cómo afectaban los ataques informáticos a la seguridad de los servidores Linux del GADPO, y luego se propuso una alternativa de solución para que mitigue los efectos que estos ocasionaban.

6.9. Previsión de la evaluación

Tabla 48. Previsión de la evaluación

Preguntas básicas	Explicación
¿Qué evaluar?	La incidencia de los ataques informáticos a la seguridad de los servidores Linux del GADPO
¿Para qué evaluar?	Para determinar la vulnerabilidad, impacto y riesgo que significan los ataques informáticos para los servidores Linux del GADPO.
¿Indicadores?	Vulnerabilidad, impacto, riesgo
¿Quién evalúa?	El gerente de sistemas
¿Cuándo evalúa?	Despúes de haber aplicado la propuesta
¿Con qué evaluar?	Resultados de los ataques informáticos efectuados, metodología MAGERIT v3.0
¿Fuentes de información?	Funcionarios del GADPO, servidores Linux

Elaborado por: Investigador

6.10. Conclusiones

- Los objetivos planteados fueron cumplidos satisfactoriamente.
- La investigación bibliográfica realizada permitió obtener información relacionada con las mejores prácticas para establecer las medidas de mitigación frente a los ataques informáticos de phishing y DDoS.
- La metodología de gestión de riesgos MAGERIT sirvió como guía para determinar la vulnerabilidad, impacto y riesgo que provocaron los ataques informáticos de phishing y DDoS a los servidores Linux del GADPO.
- Los efectos de los ataques informáticos de phishing fueron mitigados aplicando un plan de capacitación basado en la NIST SP 800-50 a los funcionarios del GADPO, logrando reducir la vulnerabilidad que provocaba el ataque de 67.94% a 6.43%, el impacto de alto a bajo, el riesgo de la confidencialidad de la información de 22.42% a 2.12%, el riesgo de la integridad de la información de 44.84% a 4.24% y el riesgo de la disponibilidad de la información de 67.26% a 6.37%.
- Los ataques informáticos DDoS SYN Flood fueron controlados haciendo uso de Iptables, Syn Cookies, Syn Cache y Syn Proxy, consiguiendo reducir la vulnerabilidad que provocaba el ataque de 26.63% a 12 .58%, el impacto pasó de medio a bajo y el riesgo de 26.36% a 12.45%.
- Se estableció una metodología de aseguramiento de servidores con sistema operativo Linux compuesto de cuatro fases, partiendo de la identificación de ataques informáticos, la evaluación de la afectación, el establecimiento de medidas de mitigación y finalmente las pruebas de verificación de efectividad.

6.11. Recomendaciones

- Utilizar herramientas recomendadas por expertos para la simulación de los ataques informáticos, con el propósito de obtener resultados que se aproximen a un ataque real.
- Capacitar al personal en temáticas que aborden la seguridad informática, con la finalidad de reducir la vulnerabilidad, mitigar el riesgo y el impacto que los

ataques informáticos puedan provocar a la confidencialidad, disponibilidad e integridad de la información.

- Establecer un procedimiento institucional que permita llevar a cabo la aplicación continua de la metodología de aseguramiento de servidores Linux propuesta en la presente investigación.

BIBLIOGRAFÍA

Aguilar, M. (2017). *Plan de seguridad informática basado en estándar ISO-IEC 27001 para proteger la información y activos del Gad cantonal de Pastaza*.

Aguinaga, H. U. C. del P. (2013). *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO / IEC 27001 : 2005 para una empresa de producción y comercialización de productos de consumo masivo*.

Alvarado, J. (2017). Análisis de las vulnerabilidades mediante el uso de phishing para mejorar la seguridad informática de los equipos de cómputo y redes de la municipalidad distrital de Independencia. Retrieved from http://repositorio.unasam.edu.pe/handle/UNASAM/2655

Álvarez, D. (2013). Guía para la Elaboración de un Plan de Concientización y Entrenamiento, sobre Seguridad de la Información. *Universidad Piloto de Colombia*, 7.

Álvarez, D. (2017). *Guía para la Elaboración de un Plan de Concientización y Entrenamiento , sobre Seguridad de la Información*.

Álvaro, G. (2014). *Enciclopedia de la Seguridad Informática. 2ª Edición.pdf*.

Arellano, J. (2017). *ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO CERTIFICACIÓN :*

Avilés, R., & Silva, M. (2017). *Implementación de un modelo de seguridad para control de accesos a la red de datos, evaluando herramientas de hacking ético, en la empresa Blenastor*.

Bani-hani, R. M., & Al-ali, Z. (2013). *SYN Flooding Attacks and Countermeasures : A Survey*. (November 2016).

Bilodeau, O., Pierre, M., Calvet, J., Joncas, D., Étienne, M., Léveillé, M., & Vanheuverzwijn, B. (2014). *Operación Windigo*.

Bogdanoski, M. (2013). *Analysis of the SYN Flood DoS Attack*. (June), 1–11. https://doi.org/10.5815/ijcnis.2013.08.01

Calderón, V. (2015). *Análisis de Riesgos Informáticos y Desarrollo de un Plan de Seguridad de la Información para el Gobierno Autónomo Descentralizado Municipal de Catamayo*.

de la Torre, C., de la Torre, M., de la Torre, M., & de la Torre, A. (2017).

Ciberseguridad normas ISO 27001 - ISO 27002.

Dirección Nacional de Seguridad y Protección de Cuba. (2013). *METODOLOGÍA PARA LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA*.

Esquerra, L. (2014). *Pruebas de penetración con la herramienta Kali Linux en la Universidad Central Marta Abreu de las Villas*.

Gaona, K. (2013). *Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala*.

Garzón, D. S., Ratkovich, J. C., & Vergara, A. (2013). *Metodología de Análisis de Vulnerabilidades para Empresas de Media y Pequeña Escala*. 1–10.

Gil, V., & Gil, J. (2017). *Seguridad informática organizacional : un modelo de simulación basado en dinámica de sistemas*. *22*(2), 193–197.

González, D., & Peña, J. (2013). *Estudio del impacto de la ingeniería social - phishing*.

Guamán, B. (2014). *Anatomía de un ataque Informático*.

Hurtado, L. F. (2017). *Mecanismos para mitigar riesgos generados por la intrusión en routers de frontera basados en resultados de un honeypot virtual*.

INCIBE. (2015). *Gestión de riesgos. Una guía de aproximación para el empresario*.

Jiménez, A. (2010). *myEchelon: Un sistema de Auditoría de Seguridad Informática Avanzado bajo GNU/Linux*.

Joya, J., & Sacristán, C. (2017). *Desarrollo de una Propuesta de Mitigación de Riesgos y Vulnerabilidades en Activos Lógicos*. 1–124.

Julian, V. (2019). *Investigating TCP SYN Flood Mitigation Techniques in the Wild Julian*. https://doi.org/10.2313/NET-2019-06-1

Liras, L. M. (2015). *Protección de la Información*.

Luna, A. (2018). *Modelo conceptual para el uso de componentes electrónicos en el proceso de identificación de un sistema de información*.

Malina, L., Dzurenda, P., & Hajny, J. (2015). *Testing of DDoS Protection Solutions*.

Mieres, J. (2009). *Debilidades de seguridad comúnmente explotadas*.

Moncayo, D. (2014). *Modelo de evaluación de riesgos en activos de tic's para pequeñas y medianas empresas del sector automotriz*.

Montoya, J. P. de C. (2013). *Aseguramiento de infraestructuras de red y de servidores*. 1–5.

Mosquera, A. (2018). *Implementación de mecanismos de defensa en una red de computadores que mitiguen los ataques basados en el protocolo TCP*.

Nieves, A. (2017). *Diseño de un sistema de gestión de la seguridad de la información(SGSI) basados en la norma ISO/IEC 27001:2013*.

Pita, L. (2014). *Métodos de ataque informáticos*.

Portantier, F. (2012). *Seguridad Informática por Fabian Portantier*.

Qasim, B., & Musawi, A. (2012). *MITIGATING DoS / DDoS ATTACKS USING IPTABLES*. (June), 101–111.

RedHat. (2017). *Guía para proteger a Red Hat Enterprise Linux*.

Rico Ávila, L. E. P. de C. (2013). *Defensa en profundidad basada en servidores.* 1–7.

Robayo, H., & Rodríguez, M. (2015). *Aseguramiento de los sistemas computacionales de la empresa sitiosdima.net*.

Robles Tomalá, P. (2015). *ASEGURAMIENTO DE SISTEMA OPERATIVO RED HAT 6.6 ENTERPRISE PARA CUMPLIMIENTO DE NORMATIVA PCI DSS 3.0*.

Rocha, N., & Moreira, R. (2015). *MÉTRICAS PARA A DETECÇÃO DE ATAQUES DDOS*.

Rosety, B. (2016). *Diseño de prototipo de defensa para mitigación de ataques DDoS para PYMES*.

Salgado, O. (2014). *Evaluación de seguridad informática en PYMES*.

Salunkhe, H. S. (2017). *Analysis and Review of TCP SYN Flood Attack on Network with Its Detection and Performance Metrics*.

Samaniego, D. P. N. (2012). *Estudio y Diseño de Comunicaciones Unificadas (UC) para la Compañia MAINT CIA. LTDA*.

Shah, D., & Kumar, V. (2018). *Tcp syn cookie vulnerability*. 3–5.

Sophos. (2006). *El beneficio de proteger Linux*.

Sophos. (2017). *Estado actual de la seguridad para endpoints*.

Soriano, M. (2014). *Seguridad en redes y seguridad de la información*.

Torres, E. (2015). *Políticas de Seguridad de la información basado en la Norma*

ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato.

Torres, G. (2010). *Desarrollo de una guía práctica para la medición del tráfico de red IP y monitoreo de dispositivos en tiempo real mediante herramientas MRTG y PRTG*.

Torres, M. (2015). "Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato (Vol. 5).

Trend Micro. (2015). *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas*.

Vega, C. (2015). *Concienciación en seguridad de la información*. 1–10.

Yánez, E. (2015). *Análisis de las herramientas para el proceso de auditoría de seguridad informática utilizando Kali Linux*.

Anexo 1: Configuraciones en MRTG para monitoreo de tarjeta de red, memoria RAM y CPU

Figura 100. Monitoreo de actividad del CPU

```
#--------------------------------------------------------------
#       PC Alta - total CPU load
#--------------------------------------------------------------

# Enter the following string all on one line.
Target[localhost.cpusum]:ssCpuRawUser.0&ssCpuRawUser.0:public@127.0.0.1+
ssCpuRawSystem.0&ssCpuRawSystem.0:public@127.0.0.1+ssCpuRawNice.0&ssCpuRawNice.0:public@127.0.0.1
RouterUptime[localhost.cpusum]: public@127.0.0.1
MaxBytes[localhost.cpusum]: 100
Title[localhost.cpusum]: CPU LOAD
PageTop[localhost.cpusum]: <H1>Active CPU Load %</H1>
Unscaled[localhost.cpusum]: ymwd
ShortLegend[localhost.cpusum]: %
YLegend[localhost.cpusum]: Uso de CPU
Legend1[localhost.cpusum]: Active CPU in % (Load)
Legend2[localhost.cpusum]:
Legend3[localhost.cpusum]:
Legend4[localhost.cpusum]:
LegendI[localhost.cpusum]:  Usado
LegendO[localhost.cpusum]:
Options[localhost.cpusum]: growright,nopercent
```

Elaborado por: Investigador

Figura 101. Monitoreo de Memoria RAM

```
Target[mem]: .1.3.6.1.4.1.2021.4.6.0&.1.3.6.1.4.1.2021.4.5.0:public@127.0.0.1:::::2
# total memory
MaxBytes1[Mem]: 3772064
# total swap
MaxBytes2[Mem]: 3915772
Unscaled[Mem]: dwmy
Options[Mem]: gauge, growright
YLegend[Mem]: Mem. Disponible(Bytes)
ShortLegend[Mem]: Bytes
kilo[Mem]: 1024
kMG[Mem]: k,M,G,T,P
LegendI[Mem]: Memoria usada
LegendO[Mem]: Total
Legend1[Mem]: Memory Free [MBytes]
Legend2[Mem]: Swap Free [MBytes]
Title[Mem]: Memory Free
PageTop[Mem]: <H1>Memory Free</H1>
```

Elaborado por: Investigador

Figura 102. Monitoreo de tarjeta de red

```
### Interface 2 >> Descr: 'eth0' | Name: 'eth0' | Ip: '192.168.10.55' | Eth: '2c-56-dc-77-38-93' ###

Target[localhost_eth0]: #eth0:public@localhost:
SetEnv[localhost_eth0]: MRTG_INT_IP="192.168.10.55" MRTG_INT_DESCR="eth0"
MaxBytes[localhost_eth0]: 125000000
Title[localhost_eth0]: Traffic Analysis for eth0 -- firewall
```

Elaborado por: Investigador

Anexo 2: Fotografías de la capacitación sobre ataques informáticos de phishing brindada a funcionarios del GADPO.