Fundamentos de seguridad informática

Eduardo Amable Samaniego Mena
Jéssica Alexandra Ponce Ordóñez

compAs
Grupo de capacitación e investigación pedagógica

Fundamentos de seguridad informática

compAs
Grupo de capacitación e investigación pedagógica

UNIVERSIDAD TECNICA ESTATAL DE QUEVEDO
1984
ECUADOR

Eduardo Amable Samaniego Mena
Jéssica Alexandra Ponce Ordóñez

Fundamentos de seguridad informática

compAS
Grupo de capacitación e investigación pedagógica

UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO
1984
ECUADOR

Fundamentos de seguridad informática

© Eduardo Amable Samaniego Mena
Jéssica Alexandra Ponce Ordóñez

Universidad Técnica Estatal de Quevedo

Una obra de relevancia producto del
4to. Congreso Internacional de Educación Superior
Publicado por acuerdo con los autores.
© 2021, Editorial Grupo Compás
Guayaquil-Ecuador

Grupo Compás apoya la protección del copyright, cada uno de sus textos han sido sometido a un proceso de evaluación por pares externos con base en la normativa del editorial.

El copyright estimula la creatividad, defiende la diversidad en el ámbito de las ideas y el conocimiento, promueve la libre expresión y favorece una cultura viva. Quedan rigurosamente prohibidas, bajo las sanciones en las leyes, la producción o almacenamiento total o parcial de la presente publicación, incluyendo el diseño de la portada, así como la transmisión de la misma por cualquiera de sus medios, tanto si es electrónico, como químico, mecánico, óptico, de grabación o bien de fotocopia, sin la autorización de los titulares del copyright.

Editado en Guayaquil - Ecuador

ISBN:978-9942-33-426-8

compÁs
Grupo de capacitación e investigación pedagógica

UNIVERSIDAD TECNICA ESTATAL DE QUEVEDO
1984
ECUADOR

Cita.
Samaniego, E., Ponce, J. (2021) Fundamentos de seguridad informática. Editorial Grupo Compás.

PREFACIO

Este libro surgió basado en la necesidad de exponer las bases de la seguridad informática, así como sus diversas debilidades para que al conocerlas se puedan aplicar los correctivos necesarios al sospechar sobre vulnerabilidades ya sea en las redes o en los dispositivos informáticos que diariamente son manipulados.

Cuando se trata el tema de la seguridad informática es importante conocer sus fundamentos es decir aquellas definiciones que forman parte de los principios para entender en que consiste, así como las diversas formas de ataques que existen, técnicas de seguridades que se pueden aplicar y las normas aplicadas.

El libro contiene temas que abordan los fundamentos de la seguridad informática como la seguridad visualizada desde la parte económica, de los procesos, el valor de la información, la seguridad implica a las personas, las diversas normativas de seguridad, la seguridad de las redes por medio de firewalls, protocolos, IDS, la criptografía y políticas.

Cada uno de estos temas están desarrollados para que el lector que conoce poco sobre los temas de la seguridad informática conozca los conceptos y los aplique en ejercicios basado en el contexto de las debilidades tecnológicas.

En el capítulo I se abarcan conceptos que permiten realizar una fundamentación de la seguridad informática desde conocer el papel que tiene la seguridad, el valor de la información en la actualidad, se abordan también los conceptos fundamentales de la seguridad informática, también hay una descripción sobre el modelo de seguridad basada en autenticación, autorización y auditoria (AAA), finalmente se describen las políticas de seguridad en el uso de contraseñas.

El capítulo II se centra en la seguridad de redes, se abordan la arquitectura TCP/IP, firewalls en la protección, control de acceso a la red, protocolos de seguridad, ataques en las redes, seguridad en cloud computing y ciberseguridad

El capítulo III contiene aspectos relevantes de criptografía, se describen los algoritmos asimétricos como el DES, AES, MD5 y SHA, finalmente se abarcan los algoritmos simétricos como el RSA y la firma electrónica.

En el capítulo IV se centra en los sistemas de gestión seguridad de la información SGSI, según las Norma ISO 27001 que rigen la. Se abordan aspectos relevantes de la implementación de un Sistema de Seguridad de la Información SGSI según la Norma 27001 y sus beneficios, así como un estudio de caso en una IES.

Contenido

Capítulo I: Introducción a la seguridad informática 1
1.1. ¿Qué es seguridad? 1
1.2. Seguridad informática 2
1.2.1. Tipos de seguridad informática 2
1.2.1.1. Seguridad del hardware 2
1.2.1.2. Seguridad del software 3
1.2.1.3. Seguridad de red 3
1.3. Conceptos básicos en materia de seguridad 4
1.3.1. Amenazas 4
1.3.2. Activos 4
1.3.3. Personas 4
1.3.4. Vulnerabilidades 4
1.3.5. Ataques 5
1.3.6. Riesgos 5
1.3.7. Impacto 5
1.4. Principios de la seguridad de la información 5
1.4.1. Confidencialidad 6
1.4.2. Integridad 6
1.4.3. Disponibilidad 7
1.5. Principio del menor privilegio 7
1.6. Ingeniería social 8
1.7. Tipos de mecanismos 9
1.7.1. Preventivos 9
1.7.2. Correctivos 10
1.7.3. Detectivos 10
1.8. Cifrados en la seguridad informática 11
1.8.1. Encriptación simétrica 12
1.8.2. Encriptación asimétrica 12
1.9. Cifrado WEP y WPA 13
1.10. Modelo de seguridad Autenticación, autorización y auditoria (AAA) 13
1.10.1. Autenticación 13
1.10.2. Autorización 14

1.10.3. Auditoría 15
1.10.3.1. Tipos de auditoría 15
1.11. Políticas de seguridad en contraseñas 18
1.11.1. Crear contraseñas sólidas 18
1.11.2. No usar la misma contraseña 19
1.11.3. Cambiar la contraseña periódicamente 20
1.11.4. Usar gestores de contraseñas 20
Capítulo II: Seguridad en redes 22
2.1. Arquitectura TCP/IP 22
2.2. Firewalls en la protección 24
2.3. Control de acceso a la red 27
2.3.1. Snort 27
2.3.2. Funcionamiento de Snort 28
2.3.3. Requerimientos de Snort 32
2.3.4. Las reglas de Snort 33
2.4. Protocolos de seguridad 35
2.4.1. Tunelización en la red 35
2.4.1.1. Generic Routing Encapsulation (GRE) 35
2.4.1.2. PPTP (Point-to-Point Tunneling Protocol) 36
2.4.1.3. SSL (Secure Socket Layer) 37
2.4.1.4. SSH (Secure Shell) 38
2.4.1.5. TLS (Transport Layer Security) 39
2.5. Ataques en las redes 40
2.5.1. Amenazas en redes inalámbricas 40
2.5.2. Ataque Man-in-the middle (hombre en medio) 40
2.5.3. Denial of service (DoS) denegación de servicio 42
2.5.4. Network injection o inyección en red 45
2.5.5. Identity theft (MAC spoofing) 47
2.5.6. Amenazas de seguridad en móviles 48
2.5.6.1. Ataques de Ingeniería Social 48
2.5.6.2. Malware 50
2.6. Seguridad en redes inalámbricas 51
2.6.1. Medidas de seguridad inalámbricas 51
2.6.1.1. Ocultar señales inalámbricas 52
2.6.1.2. Cifrado 52
2.6.1.3. Otras medidas de seguridad 52

2.6.2. Privacidad equivalente a cableado (WEP) 52
2.6.3. Acceso protegido a wifi WPA y WPA2 52
2.7. Seguridad en dispositivos móviles 53
2.8. Seguridad en Cloud Computing o Computación en la Nube 54
2.8.4. Amenazas en Cloud Computing 56
2.9. Ciberseguridad 57
2.9.3. El desafío de la ciberseguridad 59
Capítulo III: Criptografía 60
3.1. Concepto de criptografía 60
3.2. Importancia de la criptografía 61
3.3. Criptoanálisis 61
3.4. Criptosistemas básicos 62
3.4.1. Tipos de criptosistemas 63
3.4.1.1. Criptosistema simétrico 63
3.4.1.2. Criptosistema asimétrico 63
3.5.1. Algoritmos simétricos 64
3.5.1.1. Data Encryption Standard (DES) 65
3.5.1.2. Advanced Encryption Standard (AES) 67
3.5.1.3. Message Digest 5 (MD5) 71
3.5.1.4. Secure Hashing Algorithm (SHA) 71
3.5.2. Algoritmos asimétricos 72
3.5.2.1. Algoritmo RSA (Rivest, Shamir, Adleman) 72
3.5.3. Firma electrónica 73
Capítulo IV: Seguridad de la Información 75
4.1. Seguridad de la Información según la Norma ISO 27001 75
4.2. Beneficios de los SGSI 75
4.3. Importancia de la implementación de un SGSI 76
4.4. Implementación de la Norma Técnica Ecuatoriana NTE-INEN ISO 27001: 2015 77
4.5. Implementación de un SGSI en Universidades 83
4.5.1. Beneficios que aporta a las Universidades la certificación de la norma ISO-27001 83
4.5.2. Estudio de caso. La Seguridad de la Información en una IES 84
Glosario de términos claves 85
Bibliografía. 93

Capítulo I: Introducción a la seguridad informática

1.1. ¿Qué es seguridad?

La seguridad es una condición que permite tener libertad ante el peligro, su principal objetivo es la protección contra los adversarios, por ejemplo, en la seguridad de un estado se debe proteger su soberanía, sus activos y su gente para que estos no sean atacados.

En una organización alcanzar un nivel de seguridad adecuado requiere de la implementación de un sistema de varias capas estratégicamente relacionadas con elementos en común, por lo tanto, es deber de la organización asegurarse de contar con estrategias debidamente planificadas y organizadas.

Las áreas de seguridad son:

- Área física: Encargada de proteger a las personas, activos físicos, el lugar de trabajo.
- Seguridad en las operaciones: Asegura la capacidad de las organizaciones para llevar a cabo sus actividades operativas sin interrupciones.
- Seguridad en las comunicaciones: Protege a los medios de comunicación, la tecnología de una organización.
- Seguridad en red: Protege los dispositivos de red de datos, conexiones y contenidos.

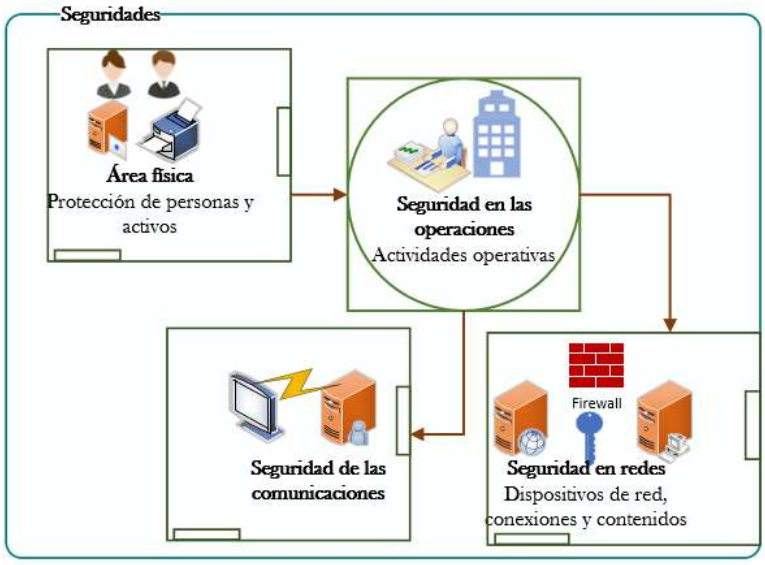

Figura 1.1: Áreas de la seguridad

Fuente: Autores

1.2. Seguridad informática

En el siglo XXI los gobiernos despliegan tecnologías avanzadas e inteligentes en todos los sectores que conforman su territorio incluida áreas como la salud, la educación, el medio ambiente, el transporte y la energía, su objetivo es la utilización de tecnología que promueva el crecimiento de sus ciudades.

El espectacular crecimiento de internet y de los servicios telemáticos (comercio electrónico, servicios multimedia de banda ancha, administración electrónica, herramientas de comunicación como el correo electrónico o la videoconferencia…) ha contribuido a popularizar aún más, el uso de la informática y de las redes de ordenadores, hasta el punto de que en la actualidad no se circunscriben al ámbito laboral y profesional, sino que incluso se han convertido en un elemento cotidiano en muchos hogares, con un creciente impacto en las propias actividades de comunicación y de ocio de los ciudadanos.

Concepto: Es cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

Objetivos de la seguridad informática:

- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos.

1.2.1. Tipos de seguridad informática

1.2.1.1. Seguridad del hardware

Protege los elementos físicos de cualquier daño, proporciona seguridad un poco más robusta por lo que es importante proteger los sistemas de alimentación ininterrumpida (SAI), los corta fuegos, entre otros. Para conocer si el hardware es seguro hay que tomar atención a los problemas de vulnerabilidades en la fabricación, los dispositivos de entrada y salida de datos que permiten la navegación en la red.

1.2.1.2. Seguridad del software

Protege al software de amenazas que pueden ser producidas por un cracker u otras potenciales vulnerabilidades que ponen en peligro a los principios de la seguridad de la información como la confidencialidad, integridad y disponibilidad de los datos. En el software se pueden encontrar diversas formas de vulnerarlo por ejemplo a partir de los errores de implementación, defectos presentes en la fase del diseño, por medio de un desbordamiento de buffer, la falta de seguridad en el código, mal manejo de errores, entre otros.

1.2.1.3. Seguridad de red

Permite la protección de los datos y la red por lo que evita que los datos puedan ser modificado o robados, para proteger la red es necesario contar con varios niveles de seguridad ya que si uno es vulnerado los demás siguen trabajando, entre los componentes de seguridad en una red hay las redes privadas virtuales (VPN), Sistemas de prevención de intrusos (IPS), cortafuegos, entre otros, ver figura 1.2.

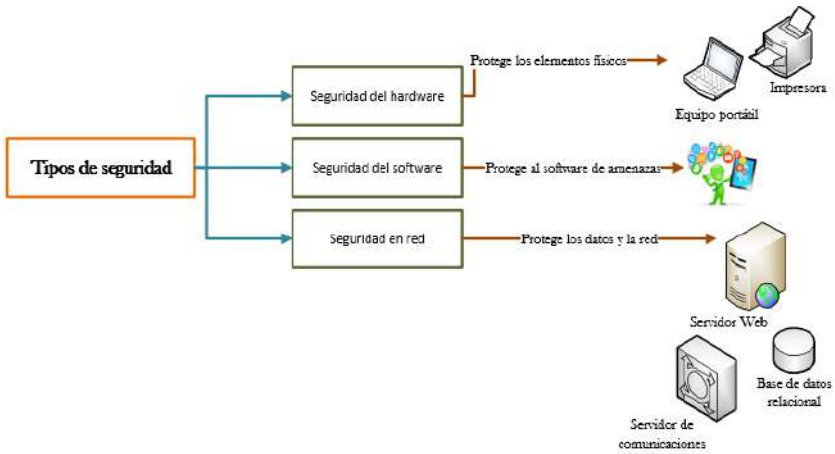

Figura 1.2: Tipos de seguridad informática
Fuente: Autores

1.3. Conceptos básicos en materia de seguridad

1.3.1. Amenazas

Una amenaza es una acción que podría resultar en la violación, interrupción o corrupción de un sistema mediante la explotación de vulnerabilidades conocidas o desconocidas. Las amenazas las podemos encontrar de dos tipos: las amenazas accidentales y las deliberadas.

- Amenazas accidentales son los desastres naturales como tormentas, inundaciones, incendios, cortes de energía, terremotos, entre otros. En la parte tecnológica este tipo de amenaza incluyen interrupciones por fallas que se presenten en el equipo, problemas de software y otros problemas no planificados del sistema, la red o el usuario.
- Amenazas deliberadas se relacionan con interrupciones que resultan de la explotación de una vulnerabilidad del sistema, este tipo de amenazas se encuentran en los ataques de denegación de servicio que impactan la disponibilidad.

1.3.2. Activos

Es un recurso del sistema informático o no necesario para que la organización alcance los objetivos propuestos; es decir, todo aquello que tenga valor y que deba ser protegido frente a un eventual percance, ya sea intencionado o no, ejemplo los trabajadores, el software, los datos, los archivos, el hardware, las comunicaciones, etc.

1.3.3. Personas

La mayoría de los ataques a nuestro sistema van a provenir en última instancia de personas que intencionada o inintencionadamente, pueden causarnos enormes pérdidas.

1.3.4. Vulnerabilidades

Es cualquier debilidad de un activo que pueda repercutir de alguna forma sobre el correcto funcionamiento del sistema informático. Estas debilidades, también

conocidas como “agujeros de seguridad”, pueden estar asociadas a fallos en la implementación de las aplicaciones o en la configuración del sistema operativo.

1.3.5. Ataques

Es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él e incluso tomar el control de este. Se trata de acciones tanto intencionadas como fortuitas que pueden llegar a poner en riesgo un sistema.

1.3.6. Riesgos

Es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

1.3.7. Impacto

Una organización se ve afectada cuando se produce una situación que atenta contra su funcionamiento normal; estas consecuencias para la empresa reciben el nombre de impacto. Dicho de otra forma, el impacto sería el alcance producido o daño causado en caso de que una amenaza se materialice.

1.4. Principios de la seguridad de la información

Los pilares de la información se fundamentan en la necesidad que los datos sean confiables, íntegros y estén disponibles para obtener el máximo rendimiento con un mínimo de riesgo. Si la información que es vital para la toma de decisiones estuviera en manos equivocadas, perdería su valor con lo que se perderá la capacidad de maniobra, la reputación, además de sufrir daños por la cantidad de información a la que se puede acceder.

En el proceso de gestión de la seguridad informática es necesario contemplar una serie de servicios o funciones de seguridad de la información, como la confidencialidad, integridad y disponibilidad, ver figura 1.3.

Figura 1.3: Los tres pilares de la seguridad
Fuente: Autores

1.4.1. Confidencialidad

La confidencialidad asegura que sólo el personal autorizado accede a la información que le corresponde para usar los recursos que necesita en la realización de sus tareas, por lo tanto, para asegurar la confidencialidad deben existir tres recursos:

a) Autenticación de usuarios: Permite identificar quién accede a la información es quien dice ser.
b) Gestión de privilegios: Permite que la información pueda ser operada por quienes se les ha autorizado y en la forma en que se le haya autorizado.
c) Cifrado de información: Evita que la información sea accesible a quien no está autorizado, para ello se transforma la información intangible en una no legible.

Este principio de seguridad permite estar protegido contra la divulgación de información a personas o sistemas no autorizados, por tanto, solo aquellos con los privilegios y derechos pueden acceder a la información requerida.

1.4.2. Integridad

consiste en asegurarse que la información no se pierda ni este comprometida, ya que el hecho de trabajar con información errónea puede acarrear que se forme una cadena de errores y se tomen decisiones equivocadas. Para garantizar la información se debe tomar en consideración los siguientes puntos:

a) Monitorear la red para descubrir posibles intrusos.

b) Implementar políticas de auditorías a fin de auditar los sistemas.
c) Implementar sistemas de control de cambios.
d) Copias de seguridad que permitan respaldar la información.

La información tiene integridad cuando es completa y sin corrupción es así que el daño, o alteración de su estado auténtico puede ocurrir en el proceso de almacenamiento o transmisión por medio de virus y gusanos informáticos diseñados para corromper los datos. Por esta razón, un método clave para detectar un virus o gusano es buscar cambios en la integridad del archivo como el tamaño.

1.4.3. Disponibilidad

La disponibilidad permite que la información esté disponible para quien la necesita, para ello hay que implementar las medidas necesarias para que tanto la información como los permisos estén disponibles, por ejemplo, un DDOS (Ataque de denegación de servicios) puede dejar inutilizada una tienda online, los correos spam pueden impedir que los destinarios legítimos no reciban sus emails.
Para que estas acciones no sucedan se deben implementar acuerdos de nivel de servicios, balanceadores de tráfico que minimicen el impacto del DDoS, copias de seguridad y disponer de recursos alternativos ante posibles eventualidades que perjudiquen la disponibilidad de la información.

1.5. Principio del menor privilegio

El principio del menor privilegio es aquel donde se da acceso a un sujeto a los módulos del sistema únicamente donde estos realizan sus actividades y si en algún momento este sujeto debe controlar la asignación de derechos específicos a otros módulos del sistema, estos tienen que abandonarse de manera inmediata una vez se haya completado la acción. Por lo tanto, una regla fundamental debe ser que, si el sujeto no necesita acceso a un objeto para realizar su tarea, no debería tener derecho a acceder a ese objeto.

En la práctica, a la mayoría de los sistemas de alguna manera les falta fortalecer los controles de privilegios y permisos necesarios para aplicar este principio con precisión.

Los diseñadores de mecanismos de seguridad aplican este principio lo mejor que pueden debido a que las consecuencias de los problemas de seguridad son a menudo más graves que las consecuencias para los sistemas que se adhieren a este principio.

1.6. Ingeniería social

Vivimos en un mundo donde el gran avance tecnológico ha facilitado la comunicación esto ha llevado a que cada día sea más difícil darnos cuenta cuando alguien está usando habilidades de conversación en nuestra contra. El uso de las redes sociales ha creado una nueva conciencia social donde decirle a todos todo sobre nosotros es aceptable e incluso promovido. A partir de estos argumentos se puede mencionar que la ingeniería social es la práctica de obtener información sin ser detectados, se consideran los siguientes métodos para su implementación.

Phishing por SMS

Este método de ingeniería social se realiza por medio de SMS o mensajes de texto desde donde se pretende obtener información sin que la víctima se dé por enterada, en la figura se visualiza su práctica, por medio de un supuesto mensaje informativo que describe no haber tener éxito el pago de un cliente y a partir de un enlace debe terminar con su proceso dicho enlace será la forma de obtener información de la persona que realiza la ingeniería social.

Figura 1.4: Phishing por SMS
Fuente: Autores

Phishing por llamadas

Esta práctica en los últimos años ha ido en aumento ya que para el atacante es fácil y seguro realizar llamadas desde países del exterior para cometer el delito sin poder ser detectado.

Suplantación de identidad

Dentro de la ingeniería social la suplantación de identidad o Phishing que consiste en tomar una identidad que no corresponde es uno de los ataques más peligrosos, este se ha utilizado para piratear información, cerrar grandes fábricas, cometer crímenes que son altamente perjudiciales.

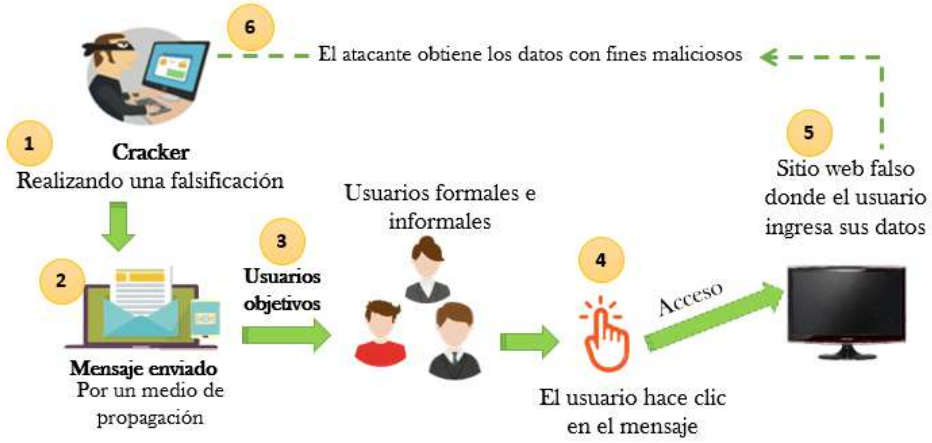

Figura 1.5: Pasos llevados a cabo en la realización de un Phishing.
Fuente: Autores

En la figura se puede visualizar el proceso para realizar un Phishing que inicia con la falsificación de un contenido de confianza por parte de un cracker enviado a través de un medio de propagación como un email a algunos usuarios sin importar que sean formales e informales, estos usuarios hacen clic en el contenido e ingresan información personal pata luego ser usado por el cracker y así cometer su delito.

1.7. Tipos de mecanismos

1.7.1. Preventivos

La prevención implica que se implementen mecanismos que los usuarios no puedan anular siendo estos correctos e inalterables, de modo que un cracker o

atacante no pueda cambiarlo. Los mecanismos preventivos suelen interferir con el uso del sistema impidiendo su normal funcionamiento en algunas ocasiones.

Aunque es importante recalcar que estos mecanismos evitan que parte del sistema se encuentre comprometido, entre uno de los mecanismos comunes de prevención se puede mencionar a las contraseñas que impiden el acceso a usuarios no autorizados. En teoría se puede mencionar que cuando se aplican estos tipos de mecanismos el sistema no necesita ser protegido, aunque esto no siempre es así.

Según Romero Castro et al. (2018) menciona que la mayoría de los ataques se pueden evitar o disminuir su impacto mediante la aplicación de los mecanismos preventivos aunque estos representen una gran barrera por parte de los involucrados al momento de comprometerse. Entre los mecanismos preventivos que se pueden aplicar están: actualización del sistema, antivirus, corta fuegos, contraseñas, navegación por internet accesos remotos, cifrar información confidencial en reposo, verifique la identidad de la información, entre otros.

1.7.2. Correctivos

Los mecanismos de seguridad correctivos ayudan a mitigar o disminuir los efectos de un evento que afecta a los sistemas, corrigiendo brechas de seguridad por medio del bloqueo de direcciones IP que representan amenazas a partir de acciones detectadas, así como el bloque de acciones sospechosas, el requerir que haya un desbloqueo por parte del administrador entre otros.

Entre los pasos en los mecanismos de ejecución tenemos realizar un inventario donde se detallen los problemas en la seguridad informática ya que esto permitirá buscar posibles soluciones, se debe también estudiar el o los posibles problemas encontrados para plantear una solución y por último hay que documentar todos los procesos realizados.

1.7.3. Detectivos

El mecanismo de detección determina el momento en que ocurre un ataque monitoreando varios aspectos del sistema que le ayuda a obtener información

para poder informarlo, es importante mencionar que los mecanismos detectivos no evitan que algunas partes del sistema se comprometan.

Entre los mecanismos detectivos que se pueden aplicar está la tecnología CAPTCHA y la implementación de controles que emitan alertas sobre intentos fallidos al intentar usar funcionalidades del sistema que no le competen y otras actividades irregulares.

1.8. Cifrados en la seguridad informática

La encriptación transforma la información de tal modo que solo las partes autorizadas saben como leerlo, usar este método es importante debido a que en el peor de los casos si alguien no autorizado llega a obtener la información se le haga difícil conocer su contenido. Entre los ejemplos de encriptación implementados en el pasado está la cifra ADFGVX usada en la primera guerra mundial por los alemanes en 1918 que consistía en un método de sustitución y otro de transposición donde su mensaje final se emitía por medio de código Morse y la máquina enigma que empleaba un cifrado rotativo usada en la segunda guerra mundial por el ejército alemán.

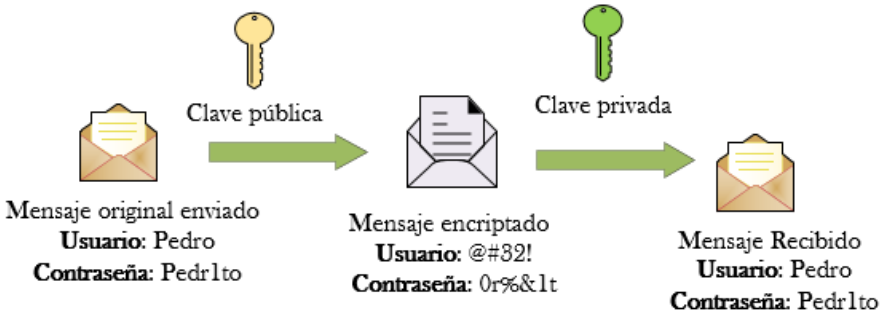

Figura 1.6: Ejemplo de encriptación
Fuente: Autores

En la figura anterior se visualiza que al enviar un mensaje este pasa por una clave pública donde posteriormente se encripta el mensaje para ser enviado a través de la clave privada llegando el mensaje seguro a su destino. Entre los métodos de encriptación están el simétrico con una única clave y el asimétrico que tiene clave

pública y privada, WPA, WEP y firma digital a continuación se detallan cada uno de ellos.

1.8.1. Encriptación simétrica

Este tipo de encriptación usa un mismo método para cifrar y descifrar un mensaje en donde el remitente cifra su contenido y el destinario lo descifra. Entre los cifrados simétricos está el DES con claves de 56 bits, el 3DES que usa claves de 128 bits y los algoritmos R5 y AES.

Figura 1.7: Cifrado simétrico.
Fuente: Autores

1.8.2. Encriptación asimétrica

En esta encriptación si el emisor cifra la información el receptor puede descifrarla o viceversa usando dos tipos de claves la pública que es conocida por los usuarios y la privada que es conocida por el propietario donde únicamente él tiene acceso sin que nadie tengo conocimiento de esta clave.

Figura 1.8: Cifrado asimétrico
Fuente: Autores

1.9. Cifrado WEP y WPA

Estos algoritmos de encriptación están creados para las conexiones inalámbricas y se basan en protocolos para conexión wifi. El cifrado WEP fue el primero en aplicarse para proteger las redes wifi sin embargo en la actualidad es muy débil y cualquier programa puede romper su seguridad, para mejorar los problemas de seguridad se crea WPA que usa una contraseña donde todos los usuarios pueden conectarse con ella.

Figura 1.9: Cifrado WEP y WPA
Fuente: Autores

1.10. Modelo de seguridad Autenticación, autorización y auditoria (AAA)

1.10.1. Autenticación

La autentificación se refiere a la confirmación de algo verdadero es decir corroborar si un dato o cambio es correcto, no está siempre relacionada con los usuarios también puede existir autenticación a un sistema que requiere permisos de ejecución o un dispositivo**.** La misma puede considerarse como un método de control de acceso, ya que en la actualidad el control de los sistemas se vuelve complejo.

Según (Instituto Nacional de Ciber Seguridad (INCIBE), 2019) menciona que la autenticación es la encargada de comprobar que quien o quienes acceden a los sistemas es realmente quien dice ser.

El proceso de autenticación está dado por **lo que sabemos** es decir una contraseña o un PIN que se solicita cuando ingresamos al sistema operativo por

medio de una computadora, un servidor o un teléfono celular, por **algo que tenemos** como un token que es un dispositivo físico con acceso a un recurso protegido o por una tarjeta magnética y por **algo que somos** en otras palabras lo que me identifica como persona en el caso de la biometría para los procesos de autenticación como el uso de huellas dactilares, reconocimiento facial, entrada de voz, escaneo de retinas entre otros.

Figura 2: Procesos de autenticación.
Fuente: Autores

Por tal motivo es importante que los métodos de autenticación sean robustos sin afectar negativamente el trabajo de los usuarios. Cuando se trate del acceso a servicios críticos es recomendable utilizar el doble factor de autenticación que consiste en aplicar por ejemplo **algo que sé** con **algo que soy**, teniendo con ellos una capa extra de seguridad frente a los accesos no autorizados.

1.10.2. Autorización

La autorización permite acceder a los recursos según los permisos asignados ya sea a la red o a los sistemas de información en función a su identidad. Este puede variar dependiendo de lo que se protege por ejemplo en el caso de los datos, la autorización debe asegurar la confidencialidad e integridad, dando los permisos necesarios entre ellos el borrado, la lectura y la eliminación.

En la siguiente figura se visualiza que los usuarios tienen acceso con un inicio de sesión que permite ingresar a un conjunto de carpetas alojadas en la computadora, pero no a los datos ubicados en la base de datos, por otra parte, vemos que estos usuarios también acceden a los archivos del servidor de datos, pero no a la configuración del servidor ya que cuando quieren acceder a estas opciones hay un proceso que les termina el acceso.

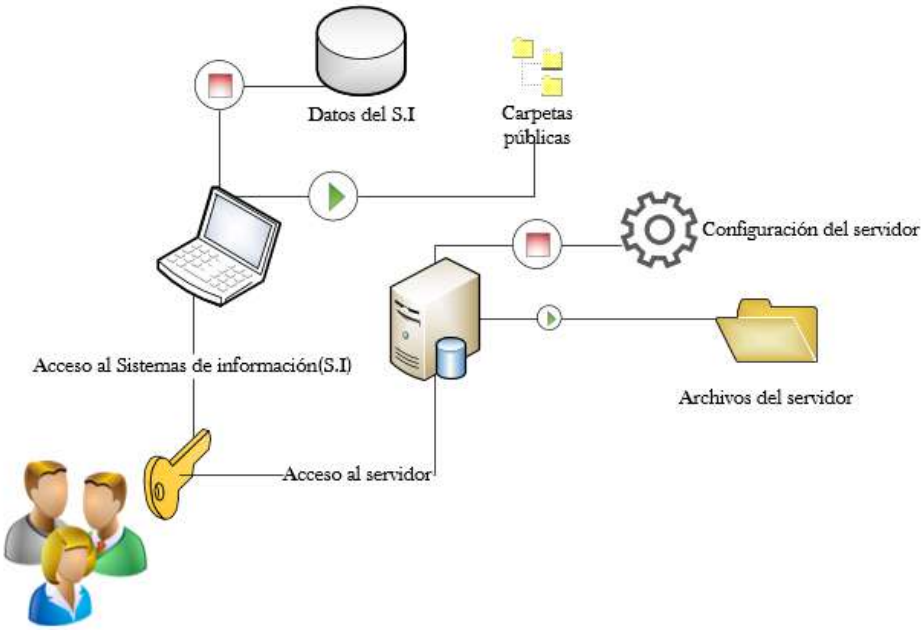

Figura 3: Autorización de usuarios
Fuente: Autores

1.10.3. Auditoría

La auditoría se basa en identificar problemas de seguridad en estaciones de trabajo, redes de comunicaciones, servidores o aplicaciones desde el análisis y gestión de las tecnologías de la información (TI) realizando un seguimiento a las acciones de los usuarios en un determinado tiempo, a los servicios accedidos, así como a los datos manipulados y transferidos.

Para realizar una auditoría se debe identificar los activos de la información que queremos revisar, los activos a revisar pueden ser ficheros, las bases de datos, equipos o programas, sistemas de red entre otros.

1.10.3.1. Tipos de auditoría

En la auditoría informática existe tipos de auditorías como: test de penetración, auditorías basadas en red, auditoría forense entre otros, para la verificación de los activos críticos.

Test de penetración

Los test de penetración son un grupo de ataques realizados a los sistemas informáticos con el objetivo de descubrir debilidades que luego deben ser corregidas para que no sean explotadas. Este tipo de auditoría inicia con la obtención de información sobre los sistemas y equipos. Luego se realiza la explotación de las vulnerabilidades simulando ataques que llevarían a cabo los ciberdelincuentes para obtener acceso a la información o al control de los sistemas. En la fase final se realiza un informe donde consta el detalle de los ataques que pueden tener éxito.

Los pentesting o test de penetración son llevados a cabo por pentesters quienes utilizan diversas técnicas y procedimientos usados por los atacantes a fin de conocer las brechas de seguridad en los sistemas o equipos informáticos.

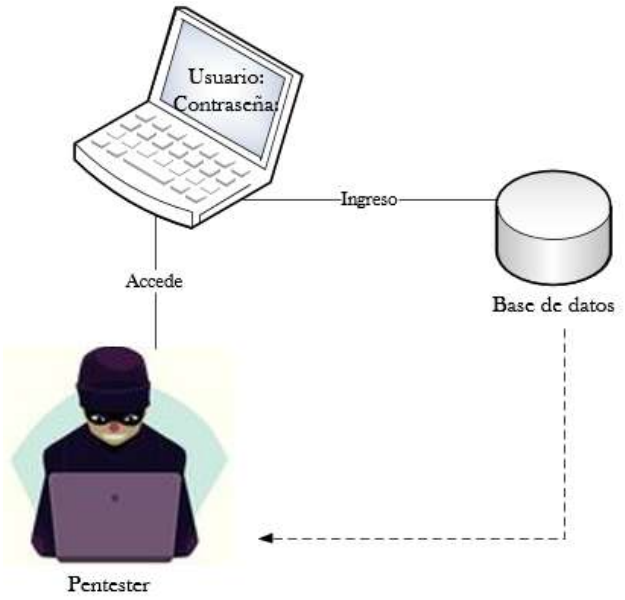

Figura 4: Pentester ingresando a los datos de un sistema
Fuente: Autores

Auditorías basadas en red

La auditoría de redes se realiza para conocer el estado de las conexiones, esta debe iniciar con la revisión física del estado de las redes como el cableado el sistema de ventilación entre otros, luego continua con la auditoría basada en la ciberseguridad donde se realiza un sin número de prueba en las direcciones IP, las reglas de ingreso, los puertos abiertos. En la imagen se visualiza las pruebas realizadas a la red mediante un ataque a la configuración del firewall que si tiene

éxito puede acceder al router y con esto tener acceso al servidor y al sistema de información.

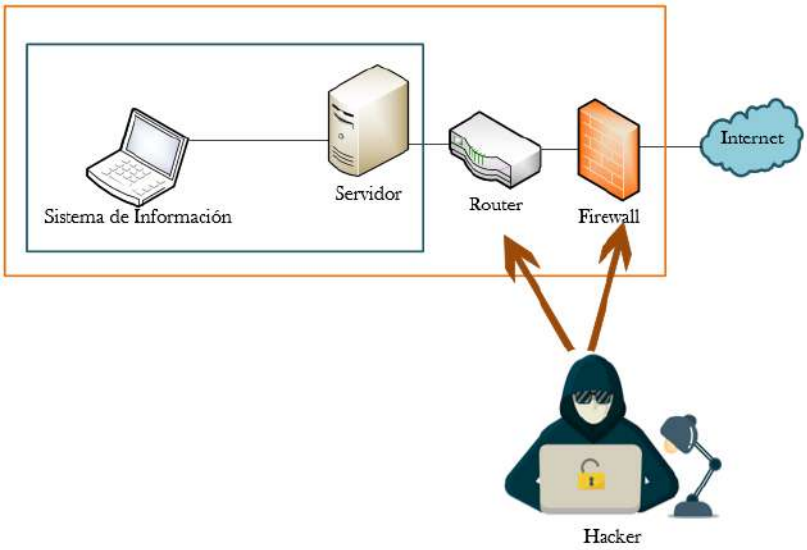

Figura 5: Pruebas a la seguridad de la red
Fuente: Autores

Auditoría forense

La auditoría forense es la encargada de recabar pruebas que luego serán analizadas por medio de técnicas de investigación criminalística para ayudar a resolver delito, esta auditoría está destinada asegurar evidencias encontradas sobre datos ocultos, dañados o eliminados garantizando su validez.

Para realizar una auditoría forense se debe realizar el estudio de las evidencias, para emitir un informe final sobre las novedades encontradas en la examinación de las pruebas y finalmente acudir a un juicio civil donde se pone en evidencia los resultados a las pruebas, en la siguiente imagen se ilustra el proceso.

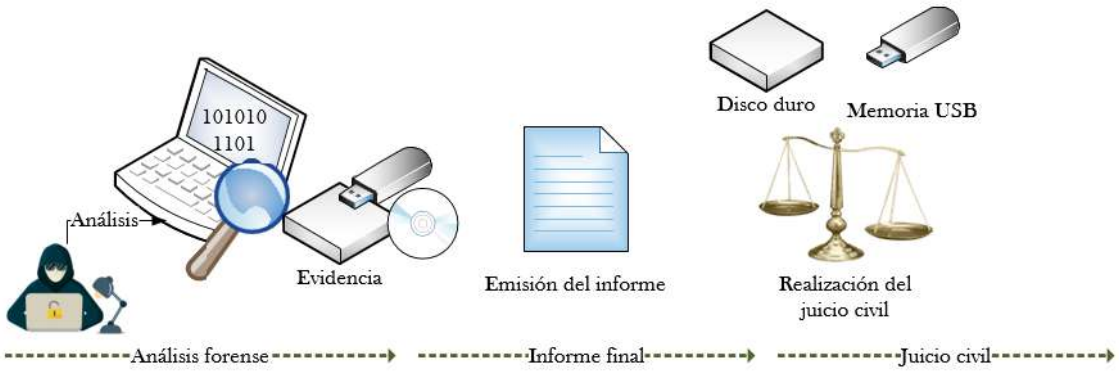

Figura 6: Proceso de la auditoría forense
Fuente: Autores

1.11. Políticas de seguridad en contraseñas

1.11.1. Crear contraseñas sólidas

Para crear una contraseña segura y compleja esta debe tener mínimo 8 caracteres, contener caracteres en mayúsculas y en minúsculas, números del 0 al 9 y caracteres no alfanuméricos como: !, @, #, $, %, ^, &, entre otros. Uno de los principales problemas radica en que se crean contraseñas débiles que contiene solo caracteres en mayúsculas, minúsculas o número por ejemplo 123, OSITO, otras de las contraseñas que deben evitarse son los nombres, número de placa, fecha de nacimiento, ubicaciones geográficas este tipo de contraseñas son fáciles de usar.

Para crear contraseñas seguras y recordarlas puede pensar en una frase, luego recortarla por números que representen palabras, ubicar iniciales usando letras en minúsculas con mayúsculas por ejemplo la frase ¿Cómo te va mi amor? Al momento de convertirla en una contraseña quedaría de la siguiente manera Cot3VM14Mor

Si ponemos a prueba las contraseñas OSITO, Cot3Vm14Mo? y Cot3Vm14Mo?1*2JE# en la siguiente dirección https://howsecureismypassword.net/ esta nos daría como resultado que la primera contraseña OSITO muestra después de la revisión un color naranja que

significa una contraseña débil, luego está la contraseña C0t3Vm14M0? con color azul que simboliza nivel medio en la fortaleza de la contraseña y la última C0t3Vm14M0?1*2JE# de color verde que identifica a una contraseña de nivel alto la página web también muestra el tiempo que invierta una computadora en revelar las contraseñas.

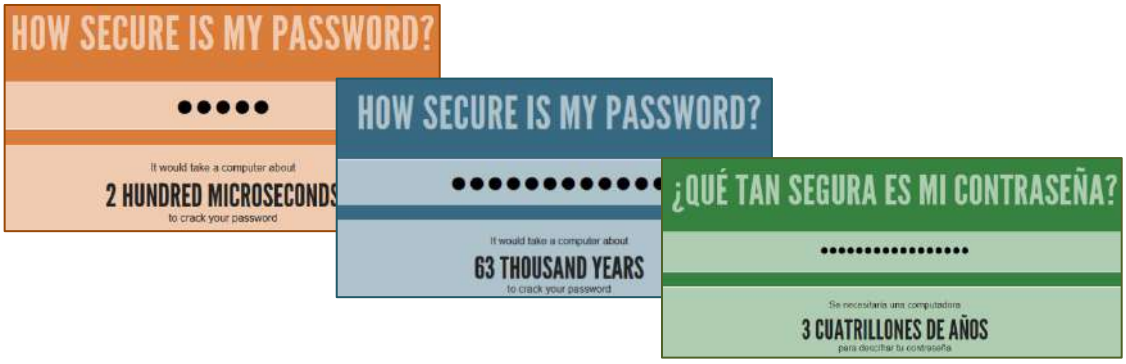

Figura 7: Verificación de contraseña
Fuente: Autores

Otra de las observaciones importantes al momento de usar contraseñas es que no se debe usar la misma contraseña en diferentes servicios como correos, redes sociales; las contraseñas deben tener como mínimo 8 caracteres; no haga uso del recordatorio de contraseñas ya que un cracker puede obtener su contraseña sin mucho esfuerzo si hace uso de este servicio, cambie las contraseñas periódicamente este cambio dependerá de la criticidad de la información.

1.11.2. No usar la misma contraseña

No se debe usar la misma contraseña para todos los servicios que usamos en el internet, esto significa tener contraseñas distintas para las redes sociales, correos electrónicos, aplicaciones empresariales en la nube, entre otros, de esta manera no corremos el riesgo de comprometer la información que gestionamos en los otros servicios si una de nuestras contraseñas fue descubierta.

Si usted es una de las personas con el criterio que está es una recomendación imposible de seguir porque tiende a olvidar contraseñas, puede aplicar la técnica de usar una única frase transformarla en una contraseña sólida e ir agregando caracteres que le recuerde algo.

De esta manera la frase !la vida es color de rosai al transformarla en una contraseña sólida queda como L4V1D3ColRoi esta contraseña puede ser usada en Facebook de la siguiente manera **F3&**L4V1D3ColRoi donde se ha agregado F3 para recordar la palabra Facebook y el & como separación, para el correo electrónico se puede crear la siguiente contraseña L4V1D3ColRoi**co***, de esta manera se puede conseguir variedad en las contraseñas y no olvidarlas fácilmente.

1.11.3. Cambiar la contraseña periódicamente

Las contraseñas deben ser cambiadas constantemente para esto es conveniente que haya una jerarquización de la información en relación a la criticidad en el acceso, con la finalidad de definir periodos de cambio. Es importante que la contraseña a cambiar no se haya usado con anterioridad ya que se corre el riesgo que esta sea vulnerada.

1.11.4. Usar gestores de contraseñas

Los gestores de contraseña son herramientas que almacenan las contraseñas de nuestras diversas cuentas protegiéndolas por medio de una contraseña sólida que sólo conoce el dueño de las contraseñas, por ello es importante memorizar bien la contraseña que permite el ingreso a la herramienta ya que si la olvidamos no tendremos acceso el resto de las contraseñas, finamente hay que realizar copias de seguridad para evitar perder las contraseñas almacenadas.

Entre las herramientas de gestión de contraseñas están Password Boss disponible para sistemas operativos como IOS, Android y Windows, implementa protección anti robo borrando las contraseñas en caso de que un intruso acceda sin permiso. Cuenta con una versión free trial y de pago.

Keeweb es otro gestor de contraseña gratuito disponible en versión de escritorio y web, incluye un generador de contraseñas para sistemas operativos como Mac OS X, Windows, Linux.

LastPass Manager disponible para sistemas operativos iOS, Linux, Android, Windows, Mac OS X este gestor está enfocado en la administración de

contraseñas provenientes de páginas web, por lo que permite instalar la herramienta como un plugin en su navegador.

Capítulo II: Seguridad en redes

2.1. Arquitectura TCP/IP

Uno de los mayores obstáculos para que la redes pudieran desarrollarse era el de encontrar lenguajes comunes para que las computadoras de diversos tipos pudieran comunicarse, aquí es donde TCP/IP se ha instaurado como el modelo a seguir por todos.

Los protocolos de la arquitectura TCP/IP cuentan con una gran ventaja, funcionan con independencia del hardware y el software subyacente, no importa qué sistema operativo o dispositivo se use para la comunicación a través de la red, porque los protocolos están estandarizados de tal forma que funcionan en cualquier contexto.

Se divide en 4 capas:

- Aplicación.
- Transporte.
- Internet.
- Acceso a la red.

Capa física (acceso a la red): Esta capa depende de la tecnología de red utilizada y no se especifica en TCP/IP, es la responsable de la colocación y recepción de paquetes en la red, además de crear una interfaz entre el dispositivo terminal y el hardware de la red, de tal manera que se logre tener acceso al medio de transmisión sobre el cual viajarán los datos, por ejemplo, el protocolo Ethernet, ect.

Capa de red (internet): Se encarga de direccionar y guiar los datos desde el origen al destino a través de la red o redes intermedias, las funciones de esta capa son de direccionamiento, empaquetado y enrutamiento. Existen protocolos como Internet Protocol (IP) encargado de transmitir y encaminar los paquetes de datos del origen al destino, protocolo Internet control message (ICMP) este es de control y notificación de errores. Además, se utiliza herramientas como ping, traceroute, ipconfig, etc.

Capa de transporte: Se encarga de establecer una conexión lógica entre el dispositivo transmisor y el receptor, los protocolos de transporte segmentan los datos en el origen para que las capas inferiores realicen el envío, y una vez que llegan a su destino, son ensamblados para recuperar el mensaje original, brindando de esta manera un transporte de extremo a extremo**.** Se utiliza Trasmision Control Protocol (TCP) orientado a conexión es confiable y asegura la recepción de los paquetes, así como que preserva el orden de cada paquete. También se usa User datagram protocol (UDP) este no tiene un mecanismo que le permite corregir errores, no es confiable con conexiones de un gran intercambio de paquetes.

Capa de aplicación: Ofrece a las aplicaciones la capacidad de acceder a los servicios de las otras capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, ejemplo Tenet, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), etc.

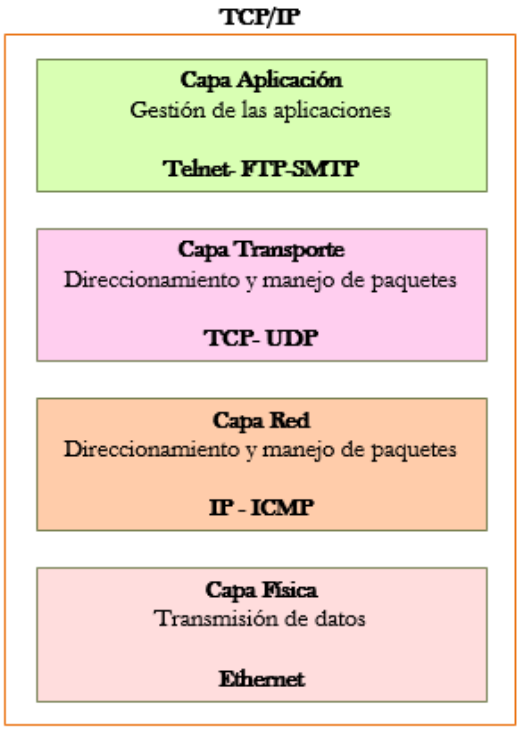

Figura 2.1: Capas de la arquitectura TCP/IP
Fuente: Autores

2.2. Firewalls en la protección

El firewall o cortafuego representa una línea de defensa en el sistema de red que de manera gráfica es simbolizado como una puerta de ladrillo en el perímetro de la red. Tiene como objetivo filtrar el tráfico de red a partir de un conjunto de reglas.

Un firewall es un sistema diseñado para proteger una computadora o una red de computadoras de los ataques basados en la red.

Por lo tanto, los firewalls protegen a los hosts de una red a otra, dividiendo y aislando las áreas de redes, por ejemplo, se divide la red interna que puede ser la de una organización compuesta de manera local con la red externa que es la internet denominada remota.

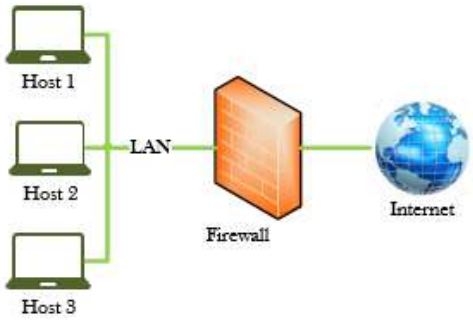

Figura 8: Implementación del Firewall
Fuente: Autores

Los firewalls presentan una gran variedad de uso en las redes de ahí que existen algunos tipos según la acción a realizar.

2.2.1. Tipos de firewalls

- Firewall de filtrado de paquetes
- Pasarelas a nivel de aplicación
- Pasarelas a nivel de circuito

Firewall de filtrado de paquetes

A menudo llamado enrutadores de filtrado**,** implementa filtrado de paquetes a nivel de un enrutador, filtra los paquetes según la información de la cabecera de red (IP) y transporte (TCP) proporcionando un grado inicial de seguridad en la capa de red, lo que imposibilita el uso de modelos sofisticados basados en reglas**.**

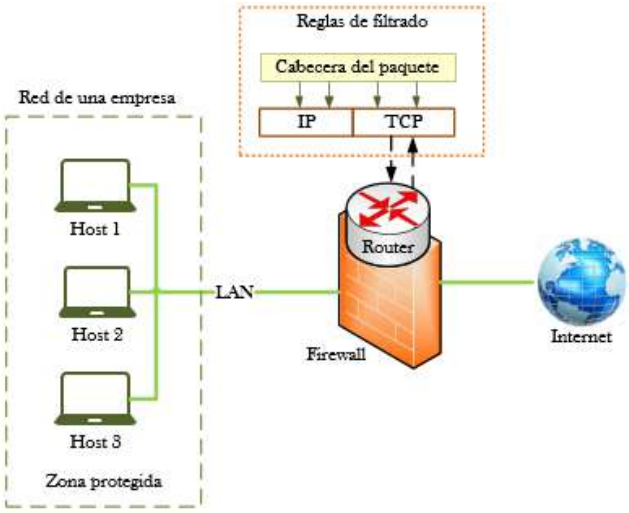

Figura 9: Tipología de defensa en el Firewall de filtrado de paquete
Fuente: Autores

Este tipo de firewall inspecciona el encabezado del paquete entrante y pueden filtrar de forma selectiva los paquetes según la información del encabezado, como la dirección de destino, la dirección de origen, el tipo de paquete y otra información clave.

Las políticas predeterminadas del firewall son:

- Políticas restrictivas es decir todo aquello que no se está permitido en las reglas de filtrado está descartado
- Política permisiva donde todo el tráfico no prohibido en la regla de filtrado está permitido.

La mayoría de estos firewalls admiten la tecnología TCP/IP, son fáciles, sencillos de implementar, de bajo costo, tiene poco impacto en el rendimiento de la red, entre una de las desventajas en este tipo de firewall es que no llevan a cabo el filtrado a nivel de aplicación, se considera difícil mantener reglas coherentes entre muchos cortafuegos de filtrado de paquetes diferentes.

Pasarelas a nivel de aplicación

Las pasarelas de nivel de aplicación, también llamadas proxys filtran paquetes en la capa de aplicación, los paquetes entrantes o salientes no pueden acceder a servicios para los que no haya un proxy, lo que permite el filtro en todo el tráfico de la red. Debido a que examinan los paquetes en la capa de aplicación, pueden filtrar comandos específicos en esta capa.

Una pasarela a nivel de aplicación está configurada para ser un proxy web que permitan aplicaciones FTP, Telnet u otro tráfico.

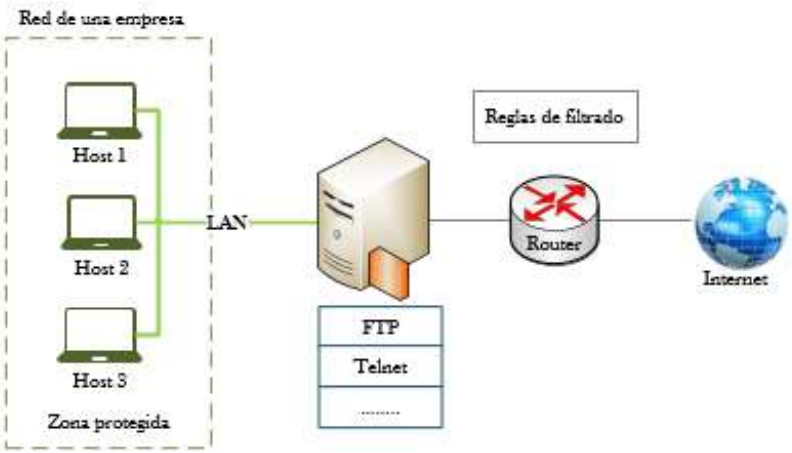

Figura 10: Tipología de defensa en el Firewall de pasarela a nivel de aplicación
Fuente: Autores

Este firewall es más seguro que el de filtrado de paquetes debido a que no se especifican reglas para la capa de red, ya que deben detallarse las aplicaciones admitidas, por otra parte, es posible mantener un LOG para registrar el tráfico entrante, entre los problemas que se pueden presentar es que el proxy sufra una caída.

Pasarelas a nivel de circuito

Este tipo de firewall valida las conexiones que serán permitidas para la transmisión de datos. Se puede considerar un híbrido entre el firewall de filtrado de paquetes y el de pasarela a nivel de aplicación.

Su función inicia cuando el usuario establece la conexión con la pasarela comportándose como un firewall de filtrado de paquetes dirigiendo las tramas entre los extremos sin analizar el contenido a nivel de aplicación.

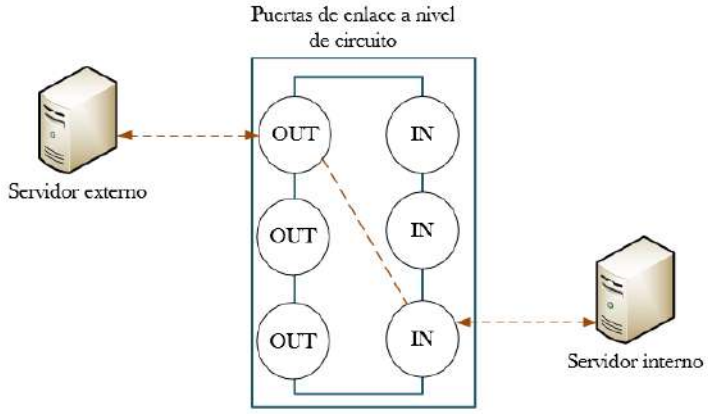

Figura 11: Firewall de pasarelas a nivel de circuito
Fuente: Autores

En las pasarelas a nivel de circuito existe la ventaja que una vez realizada la conexión se revisa la cabecera del paquete, sin tener la necesidad de examinar el contenido del paquete lo que reduce la carga del sistema.

2.3. Control de acceso a la red

No todos los usuarios deben tener acceso a la red. Para evitar posibles ataques, debe reconocer a todos los usuarios y dispositivos. Es decir, se podrá aplicar las políticas de seguridad. Puede bloquear dispositivos de EndPoint que no cumplen las políticas o proporcionarles acceso limitado. Este proceso se denomina control de acceso a la red (NAC).

La protección de los recursos de la red es de carácter urgente para todo administrador de red, en los servidores Linux existe el sistema de detección de intrusos llamado Snort que puede obtenerse desde la página oficial https://www.snort.org/, este IDS permite mediante líneas de comandos rastrear los paquetes que transitan por la red y al encontrar paquetes sospechosos los bloquea.

2.3.1. Snort

Snort es un IDS (Sistema de detección de intruso) libre y gratuito, cuyo propósito principal es vigilar el tráfico de la red a fin determinar comportamientos extraños

que puedan comprometer la seguridad de la red, este IDS se basa en definir reglas creadas por el usuario cuya función es detectar ataques y al momento de hacerlo emitir alertas.

Originalmente estaba diseñado para usarse en sistemas Linux en los momentos actuales funciona en varios sistemas operativos como Windows que utiliza una carga útil hexdump, mostrando los diferentes paquetes de red de la misma manera.

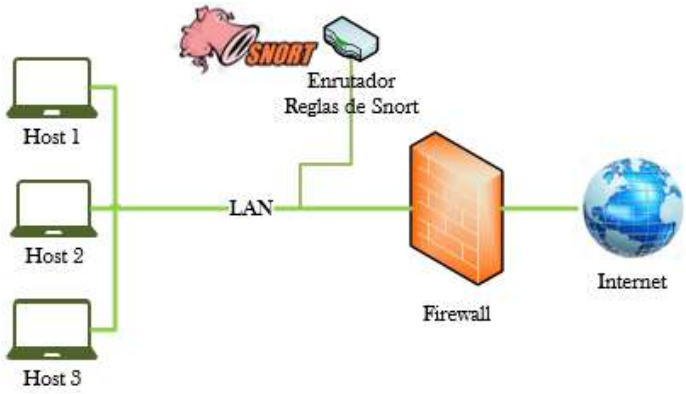

Figura 126: Tipología sobre el uso de Snort en la red
Fuente: Autores

En la versión 3.0 se han agregado varias características como el procesamiento múltiple de paquetes, una configuración compartida con la tabla de atributos, detección automática sin puertos, compatible con más de 200 complementos, analizador nuevo de las reglas y su sintaxis, manejo de TCP, reglas con alerta HTTP, eventos de inspección, documentación autogenerada, uso de un mapa de red compartido, soporte de Windows, detección de anomalías, entre otros.

2.3.2. Funcionamiento de Snort

Snort permite controlar todos los paquetes que atraviesan la red en la cual se ha instalado, estos paquetes son analizados y es posible determinar qué acciones se llevarán a cabo a partir de reglas.

Tipos de modos que puede ser configurado Snort:

- Sniffer
- Modo de registro de paquetes
- Modo de sistemas de detección de intrusos en la red.

Modo Sniffer

Este modo permite la captura del tráfico en la red y muestra los resultados, el modo Sniffer también muestra una gran cantidad de información en la pantalla lo que permite guardar la información para posteriormente realizar un estudio sobre estos datos. La información que se visualiza en este modo son las direcciones IP, y las cabeceras TCP/UDP/ICMP, este modo se activa por medio del comando snort –v.

En la figura 2.7, se muestra la ejecución del comando snort -v desde una terminal de Kali Linux, los resultados de dicha ejecución son las IP que para seguridad se han ocultado con el color gris, por último, se visualizan las cabeceras UDP y TCP.

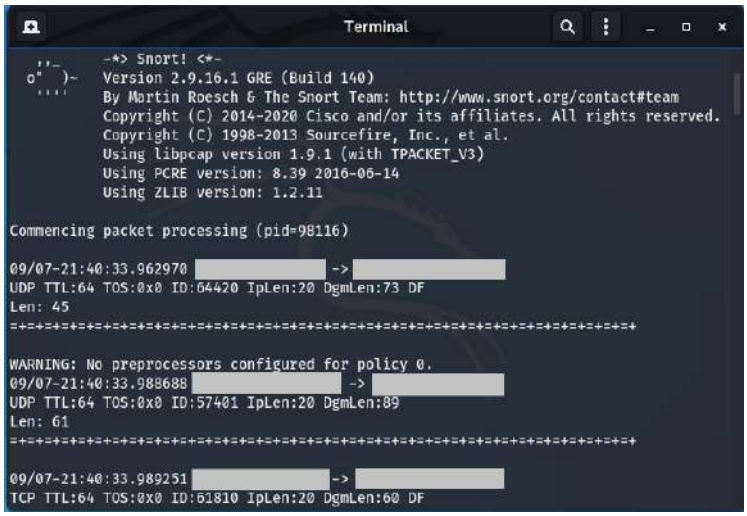

Figura 13: Encabezados de IP y TCP / UDP / ICMP
Fuente: Autores

En la figura 2.8, se visualiza los campos de los datos que pasan por la interfaz que se está usando estos datos pueden ser guardados para su posterior análisis, el comando snort -vd sirve para este propósito.

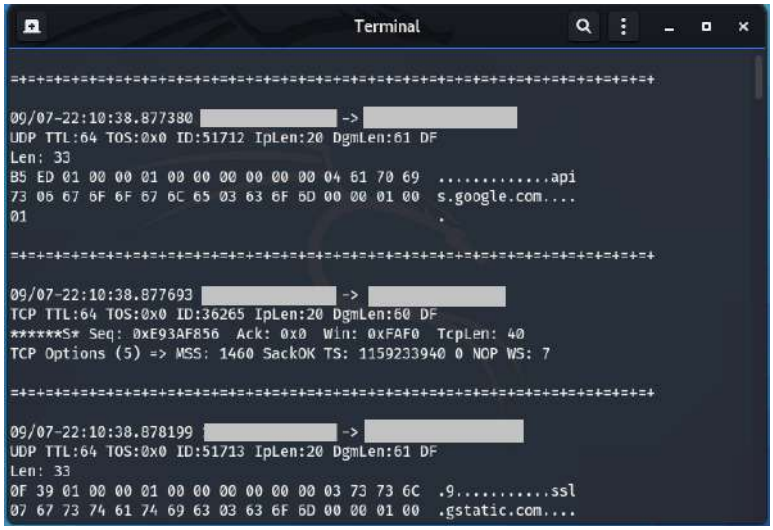

Figura 14: Ejecución del comando snort -vd
Fuente: Autores

En la figura 2.9, se visualiza el escaneo general de la red por medio de snort -v -i eth0, el comando v permite que Snort muestre un resumen de las notificaciones y el parámetro i señala la interfaz de red a monitorear.

Snort realizará el proceso de monitoreo en la interfaz eth0 para este ejemplo, para culminar con este proceso hay que pulsar la combinación de las teclas control+c, seguidamente se puede visualizar un resumen de la monitorización.

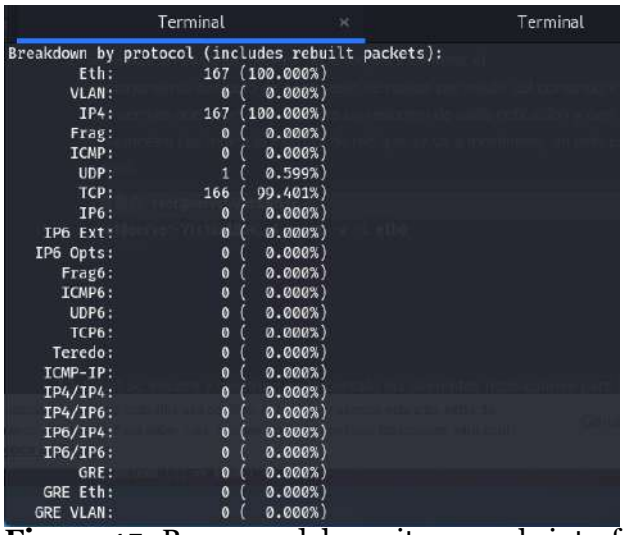

Figura 15: Resumen del monitoreo en la interfaz eth0
Fuente: Autores

Modo de registrador de paquetes

Este modo guarda los paquetes de la red configurada guarda los detalles de configuración en ficheros con un formato que permita un análisis posterior. Se puede volver a reproducir el tráfico almacenado en los ficheros. Para activar el modo de registrador de paquetes se escribe el siguiente comando snort –l /etc/snort/log

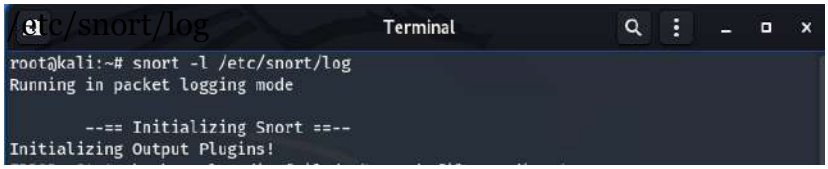

Figura 16: Ejecución del comando snort –l /etc/snort/log
Fuente: Autores

Modo de sistema de detección de intrusiones en la red

Este modo también llamado NIDS compara las tramas de cada paquete con el conjunto de reglas que el usuario haya configurado, los resultados son mostrados por pantalla o a su vez se almacenan en un sistema basado en registros. Los comandos para usar y aplicar este modo es snort –dev –c /etc/snort/snort.conf

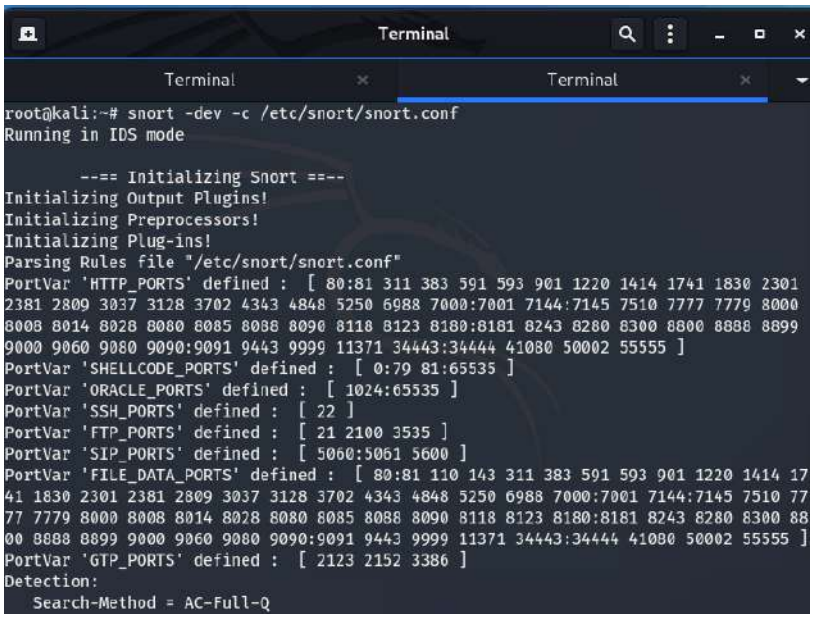

Figura 17: Ejecución del comando snort –dev –c /etc/snort/snort.conf
Fuente: Autores

2.3.3. Requerimientos de Snort

Para la instalación de Snort en un sistema operativo es importante conocer los requerimientos de hardware y software así tendremos al IDS operativo realizando las funciones necesarias en la administración de la red.

Requerimiento de hardware

Para instalar Snort hay que tener en cuenta que los datos generados pueden necesitar mucho espacio en el disco, así como monitorear el sistema de manera remota. Por otra parte, también se debe tomar en cuenta las necesidades de hardware que van a hacer variables dependiendo del tráfico en la red y cuanto de ese tráfico se almacena y procesa.

En un nivel mínimo por ejemplo usado para administrar una red doméstica no se necesita ningún requisito de hardware que el sistema operativo no requiera para ejecutarse. Sin embargo, es importante tener en cuenta que la conexión a la red y el disco duro limitarán los datos que pueden recopilar.

Cuando Snort se instala para usarse en modo NIDS se debe contar con un disco grande y rápido, para almacenar los datos que el motor de detección de Snort utilice para detectar problemas de instrucciones por medio de la violación a las reglas aplicadas.

Se debe considerar tener una tarjeta de interfaz de red (NIC) más rápida que el resto de la red para recopilar todos los paquetes. Dada las nuevas características de Snort ocupa mucha memoria por lo que es importante asegurarse de que sus sensores tengan suficiente RAM para manejar el volumen de tráfico que está recibiendo.

Requerimiento de software

Snort puede ejecutarse en sistemas Windows, Linux y compatibles con sistemas operativos como Spare Solaris, x86 Mac OS X, PowerPC Mac OS X y MkLinux y PA-RISC HP-UX. Es decir, Snort se ejecutará en casi cualquier sistema operativo moderno.

Adicional a los sistemas operativos se pueden instalar aplicaciones como: MyQL, Postgres, Oracle todos ellos gestores de base de datos, Apache, PHP.

2.3.4. Las reglas de Snort

Snort posee reglas creadas y pueden ser instaladas en el proceso de instalación del IDS, estas reglas comparan los paquetes recibidos y emiten las alertas, para visualizar y activar las reglas según la necesidad se debe digitar en la terminal de Kali Linux con el usuario root la ruta donde está el directorio de las reglas que es etc/snort luego mediante un editor de texto visualizarlas.

Figura 18: Acceso a las reglas de Snort
Fuente: Autores

La visualización de las reglas en Snort se realiza mediante gedit que es un editor de texto compatible con Linux, que permite visualizar las reglas descrita en el archivo snort.conf, además, Snort también permite la creación de nuestras propias reglas según sea la necesidad en la red administrada.

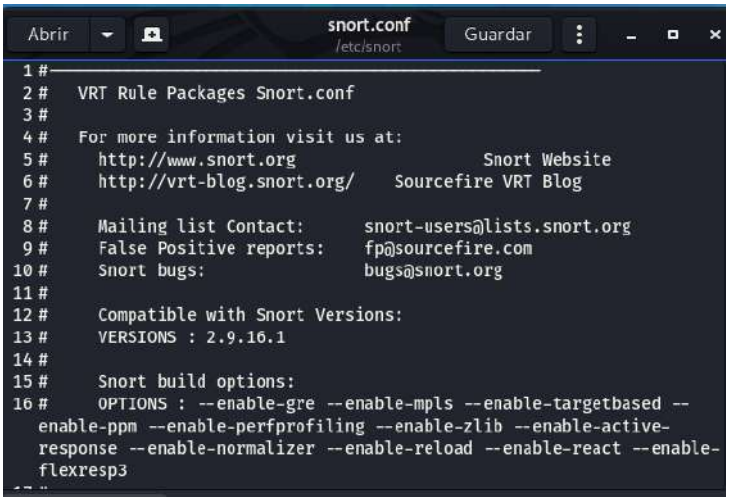

Figura 19: Contenido del archivo snort.conf donde están las reglas de Snort
Fuente: Autores

Una regla en Snort está compuesta por la cabecera que tiene acciones como alert que genera alertas, log de los paquetes, pass que ignora el paquete, active activa la regla, y dynamic que es una regla dinámica activada o llamada por la acción

active, en la cabecera también están los protocolos involucrados (UDP, TCP/IP), la dirección IP de origen y destino, el número de puertos y dirección de la operación dado por el símbolo ->.

Por último, están las opciones donde se describe el mensaje y las opciones de decisión como flags:A que establece el contenido de las bandera TCP , ack:0 caso particular para ACK=0 valor de nmap quien realiza el rastreo de los puertos, entre otros.

Ejemplo una regla en Snort para alertar de un escaneo nmap puede estar diseñada de la siguiente manera: alert tcp 192.16.1.0 any -> 191.16.1.4 any (msg: "Escaneo de nmap";ack:0) a continuación se muestra el análisis de la regla.

Cabecera:

- Acción de la regla: alert
- Protocolo: tcp
- Dirección IP origen: 192.16.1.0
- Puerto IP origen: any (cualquier puerto).
- Dirección IP destino: 192.16.1.4
- Puerto IP destino: any (cualquier puerto)

Opciones:

- Mensaje: msg
- Opciones: ack:0

La siguiente regla permite detectar el patrón GET en los paquetes TCP que abandonan la red 184.11.23.0/255.255.255.0 y van hacia una dirección distinta de la ip 194.11.23.0 cuando hay una detención del patrón indicado se debe lanzar una alerta con el mensaje "GET detectado".

alert tcp 184.11.23.0/255.255.255.0 80 -> 194.11.23.0 any (content: "GET"; offset:0;msg:"GET Detectado";sid:101;)

Cabecera:

- Acción de la regla: alert
- Protocolo: tcp
- Dirección IP origen: 184.11.23.0/255.255.255.0

- Puerto IP origen: 80.
- Dirección IP destino: 194.11.23.0
- Puerto IP destino: any (cualquier puerto)

Opciones:

- Mensaje: msg
- Opciones: ack:0, contect(Busca un patrón), offset:0(Donde inicia la búsqueda)
- La regla a continuación configura una regla para alertar el tráfico del protocolo TCP, que previene de cualquier puerto y cuyo puerto destino varía entre 80:110 a la red 172.18.1.0/24
- log tcp any any -> 172.18.1.0/24/24 80:110

2.4. Protocolos de seguridad

Son un tipo de protocolo de red que garantiza la seguridad y la integridad de los datos en tránsito a través de una conexión de red como internet. Esto se aplica a prácticamente todos los tipos de datos, independientemente del medio de red utilizado.

2.4.1. Tunelización en la red

La tunelización encapsula varios protocolos de red o en ruta de forma segura en el tráfico a través de una red insegura también permite la creación de redes privadas. Algunos de los protocolos de tunelización son:

- Generic Routing Encapsulation (GRE)
- PPTP (Point-to-Point Tunneling Protocol)
- SSL (Secure Socket Layer)
- SSH (Secure Shell)
- TLS (Transport Layer Security).

2.4.1.1. Generic Routing Encapsulation (GRE)

Es un protocolo que posibilita el transporte de paquetes de una red por medio de otra red diferente. GRE está diseñado para ser un protocolo que permite la encapsulación de propósito general simple reduciendo la sobrecarga de

proporcionar encapsulación, puede que no siempre se ajuste a la necesidad de encapsular un protocolo sobre otro.

En la tipología se visualiza que el túnel GRE crea un enlace virtual entre dos redes distintas estas son la red 10.1.1.0/24 y la 10.9.2.0/24 para que las subredes 10.1.1.1 y 10.9.2.1 tengan salida a internet, el túnel utiliza el protocolo IPSEC para encriptar el tráfico y que haya seguridad en el envío de datos, este túnel posibita correr protocolos de routing como BGP para la parte exterior y RIP para la interior.

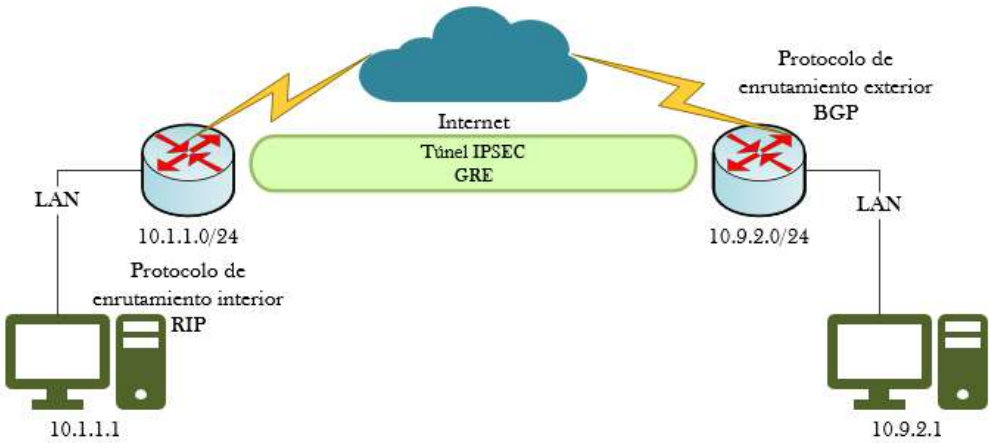

Figura 20: Tipología de un túnel GRE
Fuentes: Autores

2.4.1.2. PPTP (Point-to-Point Tunneling Protocol)

Este protocolo posibilita extender las redes por medio de un túnel privado a una red pública como la de internet, patrocinado por Microsoft y otras empresas, está basado en el protocolo punto a punto (PPP) y también permite encapsular el tráfico de red a través del internet. Este protocolo posibilita tener redes virtuales que canalizan el tráfico TCP / IP a través de Internet.

PPTP permite la tunelización por medio del uso de VPN, muy común, fácil de configurar y rápido, por tal motivo cuando se quiere rapidez en un protocolo es conveniente su uso. Es importante recalcar que el protocolo está expuesto a vulnerabilidades siendo esto una gran desventaja en la seguridad.

En la figura 2.15 se puede visualizar un túnel con el protocolo PPTP que se enlaza a los router con dirección local 1.1.1.1 y 1.1.1.2 respectivamente para distribuir la señal de internet a las redes 172.16.2.0/24 y 172.16.3.0/24.

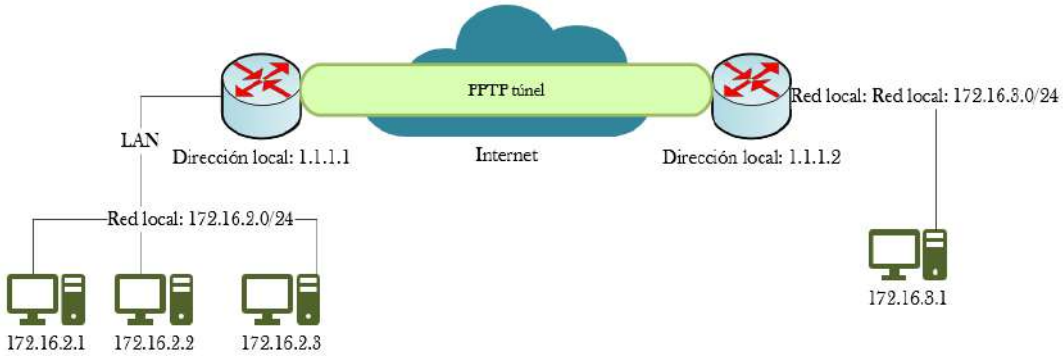

Figura 21: Tipología de un túnel PPTP
Fuentes: Autores

2.4.1.3. SSL (Secure Socket Layer)

Es un protocolo usado en navegadores web y servidores basados en autenticación, encriptación y desencriptación de los datos que navegan en internet. SSL es un protocolo estándar usado para la transmisión segura de documentos a través de una red.

Es desarrollado por Netscape, este protocolo crea un vínculo seguro entre un servidor web y un navegador para garantizar la transmisión de datos de forma privada e integral. Además de utilizar (TCP) para la comunicación.
Convirtiéndolo en un protocolo que brinda seguridad en el transporte de los datos por medio de la red, ya que proporciona una ruta de datos cifrada de un extremo a otro entre un cliente y un servidor, independientemente de la plataforma o el sistema operativo en uso.

La figura 2.16 muestra a un usuario enviado una petición de ingreso a un servidor web a través del navegador Google Chrome, el servidor a su vez envía un certificado digital SSL para autenticar la identidad la página, una vez autenticada la identidad se acepta el certificado y el usuario puede visualizar la información. Este proceso cifra el tráfico impidiendo que un cracker pueda tener acceso a los datos.

Figura 22: Tipología sobre el uso de SSL
Fuentes: Autores

Entre las ventajas de usar el protocolo SSL está la seguridad en las conexiones del cliente con el servidor, también ofrece confianza mediante el uso de certificados SSL y tiene mayor seguridad en la protección a los ataques realizados por los crackers.

Las desventajas son su alto costo debido al uso de certificados por lo que se debe implementar una infraestructura, otra desventaja es que el certificado SSL no está capacitado para la protección de todas las vulnerabilidades presentes en la web.

2.4.1.4. SSH (Secure Shell)

SSH es un poderoso protocolo usado para dar seguridad a la red, por medio de la encriptación (codificación) automática, cuando los datos llegan a su destinatario, desde donde los descifra o en otras palabras muestre el mensaje entendible al usuario.

SSH proporciona una sesión autenticada y encriptada entre el cliente y los equipos host utilizando criptografía de clave pública. SSH proporciona un reemplazo más seguro para la utilidad común de terminal de línea de comandos telnet.

Utiliza el algoritmo de criptografía asimétrica RSA que proporciona conexión y autenticación. Además, el cifrado de datos se logra mediante uno de varios algoritmos de cifrado simétrico disponibles.

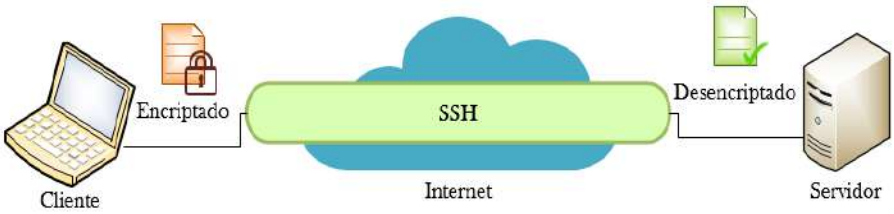

Figura 23: Tipología de un túnel SSH
Fuentes: Autores

Este protocolo también se puede utilizar para crear túneles seguros para otros protocolos de aplicación, además de administrar sistemas y aplicaciones de forma remota lo que posibilita el inicio de sesión a través de una red.

2.4.1.5. TLS (Transport Layer Security)

El TLS es la continuación del protocolo SSL, ya que permite la seguridad de la capa de transporte y protege la comunicación en la red entre los socios al cifrar los datos transmitidos, logrando tener integridad, autenticación y confidencialidad en los datos. TLS utiliza firmas digitales, certificados PKI y funciones hash seguras para evitar que los mensajes se camuflen, las contraseñas sean pirateadas y las transacciones sean denegadas.

Por lo que es un protocolo usado en la trasmisión de información de correos electrónicos.

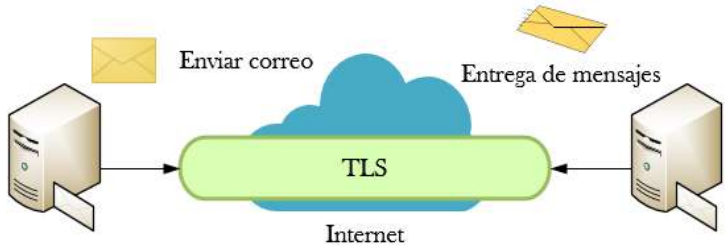

Figura 24: Envío de correo por medio de TLS
Fuentes: Autores

TLS suele ser usado en la mayoría de los navegadores, ya que posee una función de degradación que permite al protocolo SSL ejecutarse según sea necesario. Una de las ventajas de este protocolo es la capacidad de abrir canales seguros en los

servidores de correo electrónico y entre sus desventajas está el no ofrecer seguridad que el mensaje ha llegado al servidor de destino.

2.5. Ataques en las redes

Consiste en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, programa de software o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causan un daño.

2.5.1. Amenazas en redes inalámbricas

A menudo existe el pensamiento que para proteger una red lo principal es conocer los mecanismos de protección existentes, aunque esa idea no está muy lejana a la realidad lo primero a realizar para proteger una red es conocer las amenazas a las que está pueda estar expuesta, así como sus mecanismos de ataques.

2.5.2. Ataque Man-in-the middle (hombre en medio)

En español es llamado hombre de en medio, este es uno de los ataques más peligrosos y afectivos que se llevan a cabo en una red. La manera de explotar esta amenaza es por medio de una conexión a la red utilizando un flujo de paquetes desde cualquier cliente a un dispositivo.

Esto significa que cualquier paquete que se envíe hacia o desde el cliente tendrá que pasar por nuestro dispositivo, y como hay conocimiento de la contraseña, de la clave de red, se pondrán a leer estos paquetes, por lo que podemos modificarlos, eliminarlos o simplemente leerlos para ver si contienen contraseñas o información importante ya que no están encriptados. Este ataque es tan efectivo porque es muy difícil protegerse contra él.

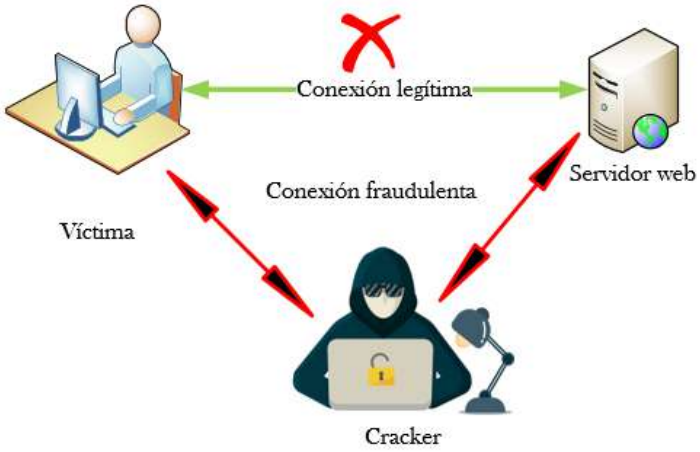

Figura 25: Ataque Man-in-the middle
Fuentes: Autores

En la figura 2.20 se visualiza que un usuario llamado victima tiene una conexión legitima con el servidor web, pero el cracker interrumpe la conexión realizando el ataque man-in-the middle y de esta manera obtener la información de la víctima, así el flujo de paquete llega hasta su dispositivo y puedo manipularlo para sus fines maliciosos.

Para realizar el ataque de hombre en medio Kali Linux cuenta con la herramienta Ettercap que permite obtener las direcciones IP y las máscaras de red desde donde se inicia el ataque y la IP del ataque objetivo.

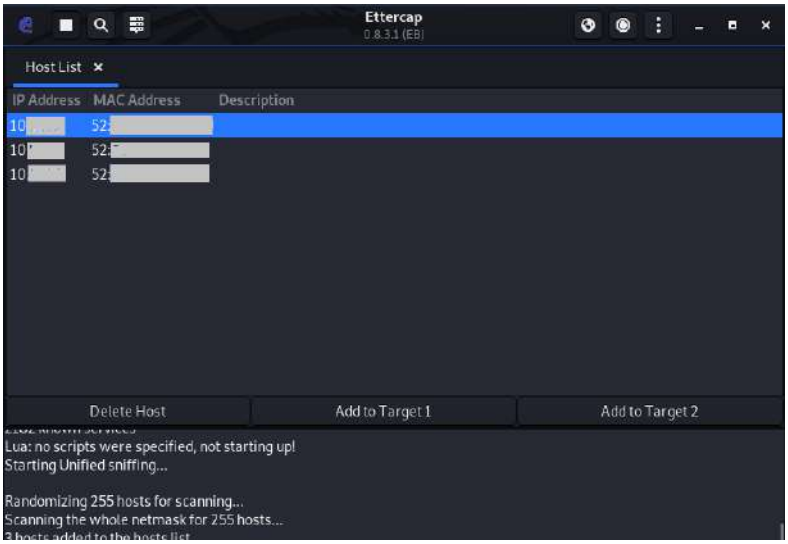

Figura 26: Escaneo de direcciones IP con las direcciones MAC en Ettercap
Fuentes: Autores

Una vez obtenida la lista de direcciones IP y MAC agregamos aquella desde donde se va a escuchar (obtener los datos) a la IP objetivo desde la opción Add to Target 1 y Add to Target 2.

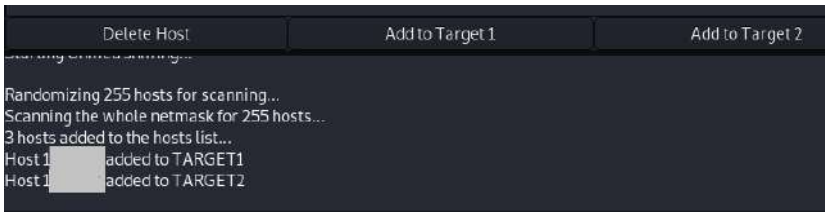

Figura 27: Host para el target 1 y Target 2 en Ettercap
Fuentes: Autores

Con la IP origen y destino se procede a realiza el ataque man-in-the middle desde ettercap eligiendo la opción MITM y luego ARP poisoning seguidamente se visualiza una pantalla donde hay que seleccionar la sniff remote connections para iniciar el ataque.

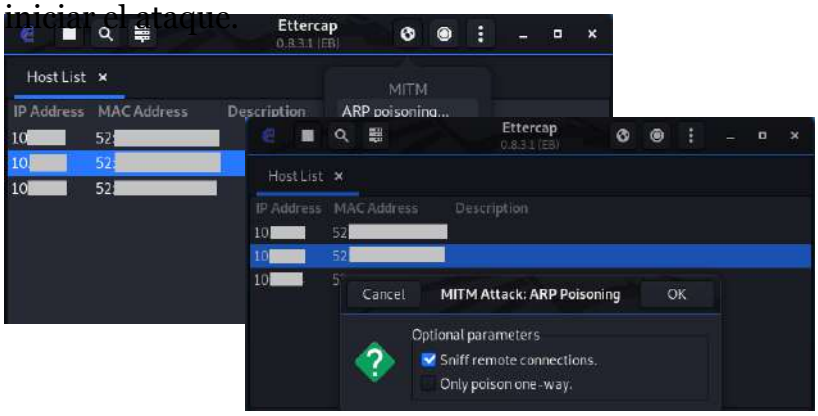

Figura 28: Ataque man-in-the middle desde Ettercap
Fuentes: Autores

2.5.3. Denial of service (DoS) denegación de servicio

La denegación de servicio es un ataque que no le permite a un usuario legitimo tener acceso a un recurso (Özçelik & Brooks, 2020) menciona que un ataque de denegación de servicio (DoS) inhabilita los recursos de la red.

Este tipo de ataque es grande ya que básicamente equivale a todos los componentes de hardware y software conectados a Internet. El DoS se puede realizarse alterando los archivos de configuración de los recursos comprometidos, dañando físicamente los componentes de la red o consumiendo recursos.

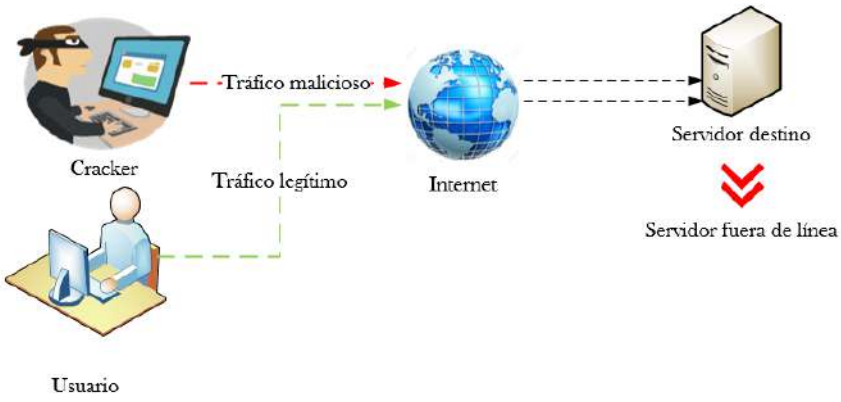

Figura 29: Ataque Denial of service (DoS)
Fuentes: Autores

Para realizar un ataque de denegación de servicio existen herramientas como las de Ettercap en Kali Linux, también están dos herramientas de código abierto creadas para realizar pruebas de seguridad por lo que permiten realizar ataques de denegación de servicios estas herramientas son Hight Orbit Ion Cannon (HOIC) y Low Orbit Ion Cannon (LOIC)

Un ataque con HIOC inicia con la ejecución de la herramienta, para seguidamente ingresar la dirección del sitio web a atacar, luego en la opción power se debe elegir High, para agregar la dirección a la lista y elegir el número de ataques a realizar que pueden ser 4, dar clic en Fire teh lazer.

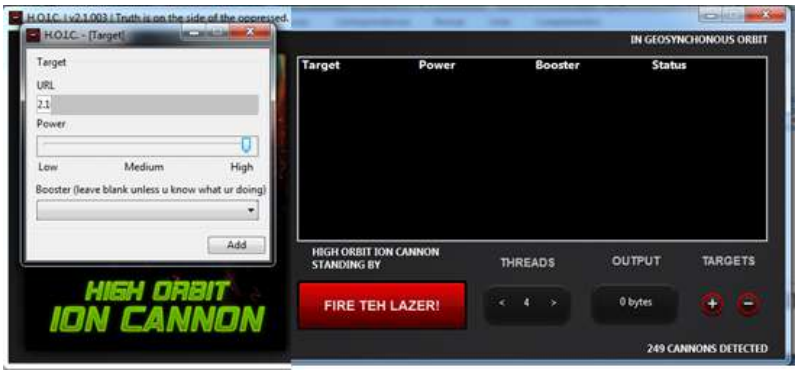

Figura 30: Configuración en la herramienta H.O.I.C para realizar ataques de DoS
Fuentes: Autores

El ataque desde la herramienta hará que en cuestión de minutos que inunde al servidor con peticiones haciendo que los servicios brindados en un sitio web no estén disponibles al usuario final.

Figura 31: Sitio web afectado por el ataque DoS desde H.O.I.C.
Fuentes: Autores

Al visualizar el log del servidor atacado se muestra el detalle del ataque donde menciona la dirección que fue afectada junto el servicio denegando el ingreso al cliente por medio de servidor apache.

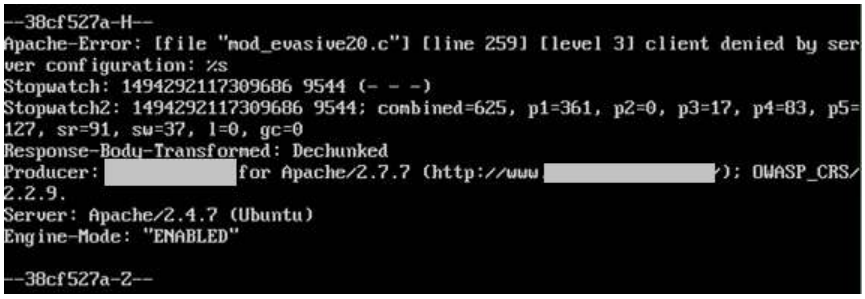

Figura 32: Log sobre el ataque de DoS
Fuentes: Autores

Para realizar un ataque DoS con la herramienta LOIC se configura mediante el ingreso de la dirección IP en el sitio web, agregando el tiempo, el puerto, el método y los hilos de ataques.

Figura 33: Datos ingresados en la herramienta LOIC
Fuentes: Autores

Este ataque al igual de HIOC lo que hace es que el servicio no esté disponible y cuando el cliente hace uso de este se muestra una página donde menciona que no tiene permiso a visualizar sus servicios.

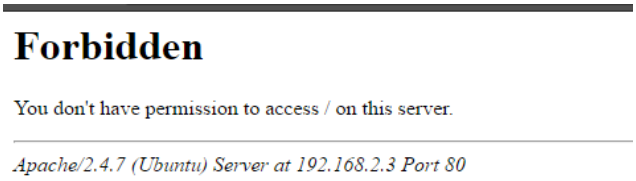

Figura 34: Visualización de la página tras el ataque de LOIC
Fuentes: Autores

En el servidor donde se encuentra alojado el sitio web hay una gran cantidad de ataques generándose con una gran rapidez y al parar muestra las líneas de error que ha generado el ataque**.**

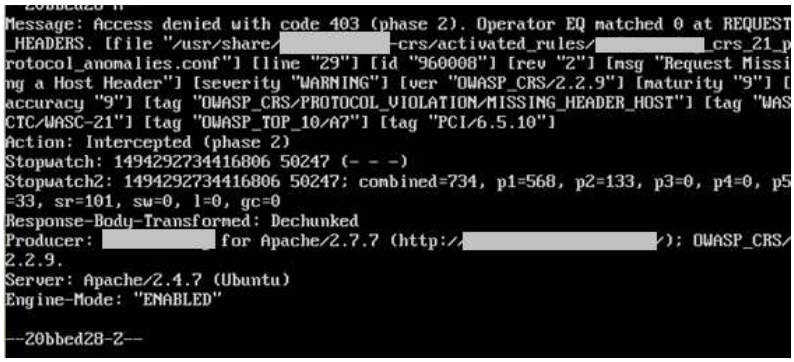

Figura 35: Log tras el ataque con LOIC
Fuentes: Autores

Las herramientas LOIC y HOIC debe usarse bajo responsabilidad de los riesgos que pueden adquirirse tras el uso de estas, ya que los autores y los colaboradores no son responsables de los daños ocasionados por el uso de las herramientas.

2.5.4. Network injection o inyección en red

Un ataque de inyección de red hace uso de puntos de acceso que están expuestos a tráfico de red no filtrado, este ataque posibilita la inyección de falsos comandos que afectan al buen desenvolvimiento de la red.

Entre los ataques por inyección están los de SQL injection o inyección de SQL, en este tipo de ataque se ejecuta sentencias SQL maliciosas que controlan un servidor de base de datos de aplicaciones web. Esta es una de las vulnerabilidades más antiguas, debido a que los sitios web utilizan bases de datos basadas en SQL. A partir de esta vulnerabilidad y dadas las circunstancias adecuadas, un atacante

puede usarla para eludir los mecanismos de autenticación y autorización de una aplicación web y obtener el contenido de una base de datos completa.

En la figura 2.30 se muestra el proceso que realiza un atacante para obtener información de los datos de la tabla usuario contenida en una base de datos por medio del código 100 OR 1=1 que normalmente siempre es verdadero, una vez obtenida la información el cracker puede manipular los datos.

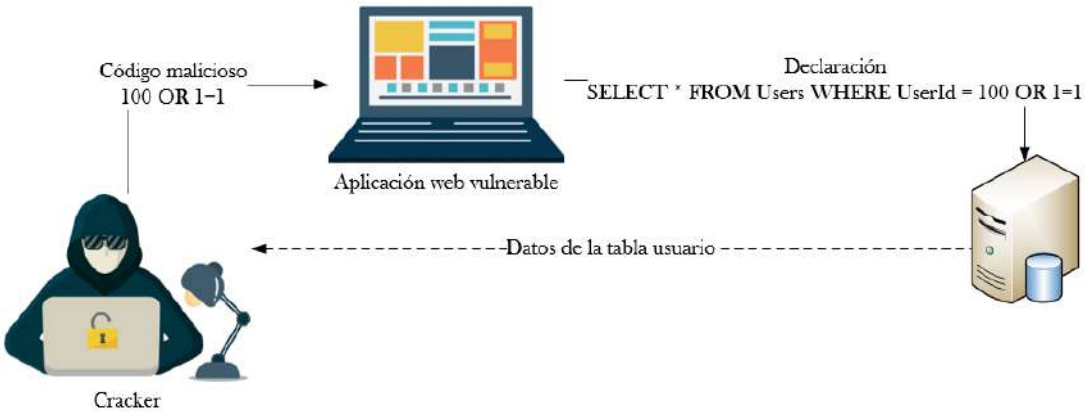

Figura 36: Ataque SQL Injection
Fuentes: Autores

Para realizar ataques de SQL injection existe la herramienta de código abierto llamada Sqlmap que sirve para explotar fallas de inyección SQL y tomar el control del servidor de base de datos a partir de a información que se encuentra en la base de datos. La siguiente figura muestra la pantalla de inicio de Sqlmap en Kali Linux.

Figura 37: Pantalla de inicio de Sqlmap en Kali Linux
Fuentes: Autores

El ataque Cross-site scripting (XSS) es otro de los ataques usados en las inyecciones a la red este consiste en una secuencia de comandos maliciosos en

forma de un script del lado del navegador y es realizada entre sitios que son inyectados en una página web y que al momento que el usuario ingresa a la página son ejecutados. ocurren cuando una aplicación web usa la entrada de un usuario dentro de la salida que genera sin validarla o codificarla.

La figura 2.32 presenta el proceso que tiene un ataque Cross-site scripting (XSS), que inicia cuando un cracker envía un script malicioso a una aplicación web que no está protegida contra estos ataques, llegando al servidor web quien se conecta con el servidor de base de datos quien por medio del script malicioso publica información sensible en el dispositivo del cracker.

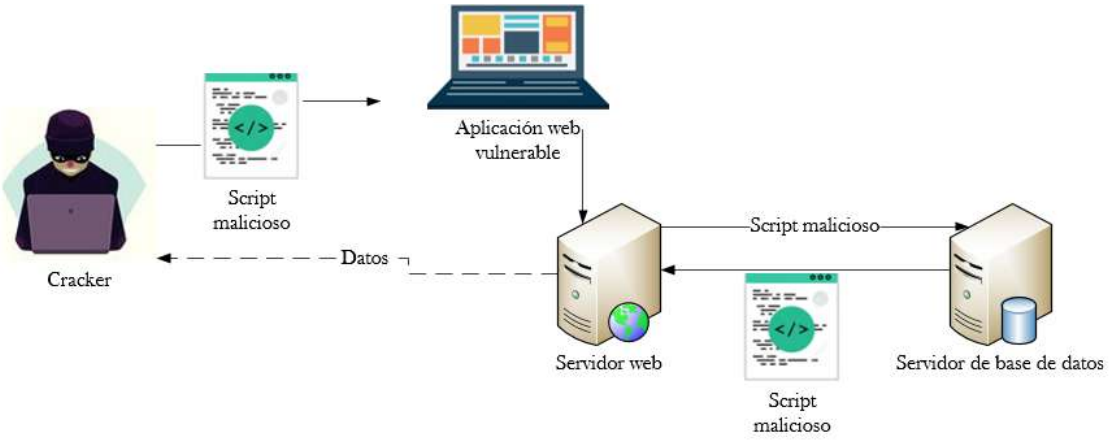

Figura 38: Ataque Cross-site scripting (XSS)
Fuentes: Autores

2.5.5. Identity theft (MAC spoofing)

El ataque identify theft enmascara la dirección MAC de un dispositivo, lo que permite evitar los mecanismos de seguridad encargados de proteger la información y los dispositivos o imitar la identidad de un usuario dentro de la red.

Este ataque permite que un cracker o intruso se haga pasar por un dispositivo legítimos de la red robando las credenciales, para lo cual el atacante debe realizar un cambio en la identidad de la MAC que ha sido asignada por el fabricante de su NIC por el valor de un usuario legítimo de la red; asumiendo la identidad de este usuario falsificando su dirección MAC.

Una vez obtenida la dirección MAC el cracker puede analizar el tráfico de los usuarios autorizados, lo mismo que es similar a realizar un ataque Man-in-the middle, donde un dispositivo se hace pasar por alguien que no es.

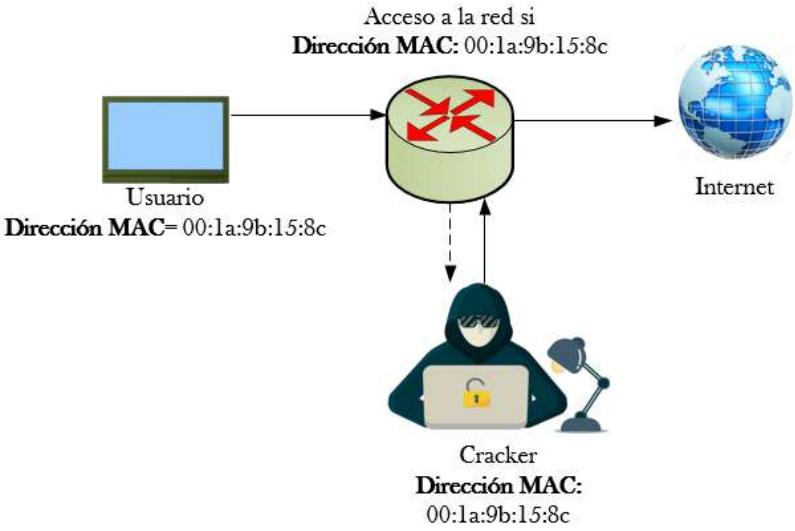

Figura 39: Ataque MAC spoofing
Fuentes: Autores

En la imagen se visualiza que un usuario legítimo intenta acceder al internet con una dirección MAC en el proceso un atacante se adueña de esta dirección teniendo con este acto acceso a la red.

2.5.6. Amenazas de seguridad en móviles

Los problemas de seguridad en los dispositivos móviles se dan por la falta de controles en la seguridad física.

2.5.6.1. Ataques de Ingeniería Social

Entre los ataques que puede tener los dispositivos móviles se encuentra el *phishing* que permite engañar al usuario para obtener información y los *ataques dirigidos* que se realizan en función de un objetivo.

Ataque Phishing

El Phishing utiliza el fraude para manipular a la víctima y de esa manera obtener información del usuario por ejemplo inicios de sesión, cuentas bancarias, número de tarjeta de crédito, este tipo de ataques puede causar mucho daño a la víctima.

El phisher o también conocido como el atacante, intenta pescar víctimas potenciales. Esencialmente, es un enfoque de engaño en línea que se dirige a usuarios en línea desprevenidos, engañándolos para que revelen información confidencial. (Dalkir & Katz, 2020).

El ataque inicia en el móvil al momento de acceder a los correos electrónicos o sitios web, estos inician por medio de una planificación sobre la manera de atacar, luego se redacta el correo electrónico, se envía a posibles víctimas para realizar el ataque y recopilar los datos que pueden usar para cometer el fraude.

El Instituto de Ciberseguridad de España (INCIBE) fomenta la investigación en ciberseguridad (https://www.incibe.es), mencionan que uno de los *correos maliciosos tiene como remitente* ***nuevo paquete***. Y en el *asunto envío* ***Nº ES/2938456*** que intenta suplantar la identidad del servicio del correo electrónico.

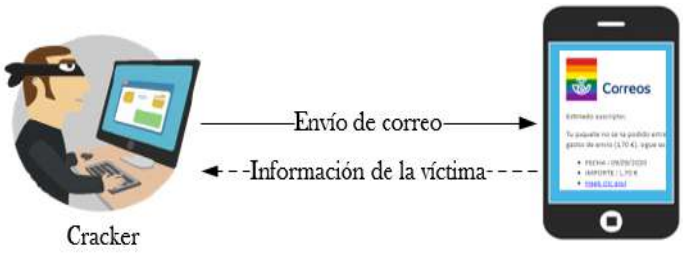

Figura 40: Phishing por medio de correos
Fuentes: Autores

Ataques dirigidos

Los ataques dirigidos se los realiza especialmente a los altos directivos, personas famosas, entre otras con el fin de acceder a la información confidencial, este tipo de ataque también se llama *whaling* la diferencia con el *Phishing* es que se conoce a la víctima.

El ataque *whaling* está dirigidos a los que toman decisiones en las empresas, ya que son ellos quienes tienen información confidencial como contraseñas usadas en cuentas para administradores, secretos comerciales entre otros.

Diversos ataques

Entre los ataques también están aquellos que se realizan explotando los huecos de seguridad en el firmware lo que permite dañar los circuitos electrónicos de los dispositivos móviles, esto es posible por las fallas de hardware que presentan los dispositivos móviles.

También se realizan ataques a las fallas provenientes del sistema operativo por ejemplo la vulnerabilidad CVE-2020-0074 en sistemas Android con una puntuación alta de ataque, consiste en que una aplicación puede controlar dominios arbitrarios, lo que puede conducir a una escalada local de privilegios con los privilegios de ejecución del usuario necesarios.

Por último, es importante mencionar que los dispositivos móviles también pueden ser atacados por las aplicaciones que se instalen, porque no siguen estándares de seguridad. Como los fallos de seguridad en la función de llamadas WhatsApp VOIP en la aplicación de WhatsApp con un nivel alto de explotación permitía a un atacante instalar software malicioso para borrar datos de las llamadas. Otra aplicación vulnerable es la Bluetooth que posibilitaba a un atacante la intercepción de datos transmitidos por usuarios legítimos.

2.5.6.2. Malware

El malware es un código malicioso que realiza acciones dañinas en los sistemas informáticos, a continuación, se detallan los siguientes malwares: LeifAccess o Shopper, Dropper y Emotet.

LeifAccess: Este malware permite aprovechar las funciones de Android para crear cuentas, descargar aplicaciones y realizar advertencias de manera fraudulenta como *"el sistema debe actualizarse su decodificador de video"*. Una vez instalado el malware en el dispositivo crea una carpeta llamada System Security Service sin mostrar ningún icono o acceso directo ganando legitimidad con el usuario para este no borre los archivos ya que piensa que es del sistema.
Este tipo de malware fue identificado en el año 2019 desde entonces está activo especialmente en Estados Unidos y Brasil. Se distribuye por medio de redes sociales, plataformas de juego, puede usar inicios de sesión de terceros que

permite engañar a los sistemas de clasificación de aplicaciones y causar varios estragos en los dispositivos de las víctimas.

Dropper: Es un malware que contiene archivos ejecutables como *.exe, .msi, .docm*, entre otros que instala otro malware. El directorio de activos es un directorio opcional que se puede agregar a un APK para almacenar archivos de activos sin procesar. En el caso de un Dropper troyano móvil, contiene un APK malicioso.

Emotet: Este malware fue desarrollado inicialmente en forma de troyano bancario, permite acceder a los dispositivos y espiar datos privados confidenciales. Emotet engaña a los programas antivirus básicos y se esconde de ellos. Una vez infectado, el malware se propaga como un gusano informático e intenta infiltrarse en otros equipos de la red.

Su mayor propagación es por medio de correos electrónicos no deseados que contiene un enlace malicioso o un documento infectado, si se descargar el documento o se da clic en el enlace inmediatamente hay una descarga del malware. Sus objetivos de ataques normalmente son las empresas, organizaciones y autoridades.

2.6. Seguridad en redes inalámbricas

Las redes inalámbricas son ampliamente usadas en la actualidad en los negocios, parques, hogares, entre otros. Por tal motivo tiene un carácter de importancia conocer las medidas de seguridad que se deben aplicar, para no ser víctimas de la ciberdelincuencia. En esta sección se abordarán algunos temas que nos pueden ayudar a la protección de las redes inalámbricas.

2.6.1. Medidas de seguridad inalámbricas

Las amenazas de las redes inalámbricas son muy variadas como las hemos podido conocer en los temas abordados anteriormente**,** para poder hacer frente a las amenazas se deben tomar en cuenta las siguientes contramedidas.

2.6.1.1. Ocultar señales inalámbricas

Consiste en aplicar una serie de medidas para que a los atacantes les resulte difícil poder encontrar los puntos de accesos inalámbricos, donde se debe incluir la desactivación del identificador de conjunto de servicios (SSID) mediante puntos de acceso inalámbricos, asignar nombres difíciles de descifrar, reducir la señal a nivel bajo, ubicar puntos inalámbricos lejos de ventanas y aplicar técnicas de blindaje de señal.

2.6.1.2. Cifrado

Aplicar medidas de cifrado en la transmisión inalámbrica siempre será eficaz para proteger a la red contra los ataques que pretenden escuchar la información que se transmite, al aplicar claves de cifrado estas deben estar protegidas. El uso de los protocolos de encriptación son buenos aliados para contrarrestar los intentos de escuchar la información en la red, también existen enrutadores inalámbricos equipados con mecanismos de cifrado para el tráfico de red.

2.6.1.3. Otras medidas de seguridad

Usar un antivirus, antispyware y un firewall para los puntos finales de la red, cambie el identificador predeterminado del enrutador, cambiar las contraseñas por defecto de los enrutadores, configure la red inalámbrica para que dispositivos específicos ingresen a la red, configurar el enrutador para aceptar direcciones MAC aprobadas, deshabilitar la administración remota, use el IDS Snort.

2.6.2. Privacidad equivalente a cableado (WEP)

WEP tiene una falla de mecanismo en el cifrado, lo que posibilita que un cracker de manera fácil descifre el cifrado y acceda a la red inalámbrica, por lo que WEP se usa solo si está tratando con dispositivos antiguos como PDA, una de las utilidades que posee WEP y de la que se puede sacar ventaja es que evita que los vecinos se conecten a la WLAN doméstica.

2.6.3. Acceso protegido a wifi WPA y WPA2

WEPA fue diseñado para reemplazar a WEP implementa en su mayoría el estándar IEE 802.11i, garantizando la compatibilidad con versiones anteriores y abarca problemas relacionadas a WEP, es importante mencionar que a pesar de

las mejoras en WEPA este sigue siendo vulnerables a varios ataques, aunque en menor escala que WEP.

WEPA2 es la versión mejorada de WEPA. WEPA/WEPA2 funciona en dos modos el primero es WEPA de clave compartida en este modo hay que ingresar una clave para el cliente y para la red inalámbrica, destinado usualmente para usuarios domésticos. El segundo modo es IEE 802.1x que usa un servidor de autenticación externo con el protocolo de autenticación extensible (EAP) para habilitar autenticación en extensiones WLAN, la autenticación IEE 802.1x está generalmente destinado a grandes entornos que soporte servidores adicionales, por último, cuando se usa token posibilita una autenticación de WLAN muy segura.

2.7. Seguridad en dispositivos móviles

Para asegurar los dispositivos móviles es necesario contar con políticas de seguridad propias, se debe inspeccionar cada dispositivo antes de permitir que accedan a la red. Hay que realizar configuraciones para aplicaciones que van a hacer instaladas. Para el uso de dispositivos móviles se deben aplicar los siguientes controles de seguridad:

- Habilitar el bloqueo automático para bloquear en caso de no usar durante un tiempo determinado, el bloqueo se puede realizar por medio de un PIN o contraseña que reactivan el dispositivo.
- Configurar el dispositivo para que el correo electrónico y otros datos se cifren por medio de la contraseña o el PIN.
- Evitar usar las opciones de autocompletar para no recordad usuarios y contraseñas.
- Habilitar la limpieza remota.
- Habilitar la protección SSL en caso de estar disponible.
- Asegurarse que el sistema operativo y las aplicaciones que se usan estén activos hasta la fecha.
- Prohibir el almacenamiento de datos confidenciales en el móvil, caso contrario deben ser encriptados.
- Tener cuidado cuando se instalan aplicaciones de terceros.

2.8. Seguridad en Cloud Computing o Computación en la Nube

El Instituto Nacional de Estándares y Tecnologías (NIST) define el Cloud computing como un modelo para hacer posible el acceso a la red y bajo demanda a un conjunto de recursos de computación configurables y compartidos (redes, servidores, almacenamiento, aplicaciones, servicios, etc.). (INTECO-CERT, 2011)

El origen del término del cloud computing está en la representación del Internet como si fuera una nube (*cloud*). Y para (*computing*) por los recursos de computación del hardware y software que están disponibles a través de Internet.

Los sistemas de computación en la nube funcionan en un servidor remoto. Esto implica que para interactuar con ellos debemos conectarnos a este dispositivo a través de una conexión a Internet y abrir una interfaz, que en la mayoría de casos será un navegador web o una app específica. La infraestructura en la nube se pueden distinguir tres tipos de infraestructuras cloud: privada, pública y comunitaria.

2.8.1. Características de la computación en la nube

La computación en la nube se caracteriza por tener herramientas de alta innovación, la monitorización en tiempo real, dinámica y agilidad de las aplicaciones. En la actualidad una de las tendencias del mercado de los sistemas de información es la proliferación de los servicios operando en la nube.

Estos servicios permiten la asignación dinámica de recursos en función de las necesidades de los clientes y reducen considerablemente los costos en las infraestructuras. Sin embargo, la rápida migración a la nube está introduciendo una serie de nuevas amenazas y desafíos de seguridad. Proteger estos activos significa que las organizaciones deberán centrar sus esfuerzos en mejorar sus programas de seguridad en la nube.

Los entornos cloud proliferan de forma exponencial obligando a los posibles usuarios a comprender mejor estos entornos y sus principales problemáticas como son:

- Ataques a la nube a través de Credenciales robadas,
- Phishing,
- Explotación de configuraciones incorrectas en la nube,
- Almacenamiento en la nube mal configurado.
- La visibilidad, el control reducidos y la eliminación incompleta de datos.
- Hackeo de aplicaciones vulnerables en la nube.

Las estrategias de prevención y detección serán decisivas para que todas las organizaciones se protejan contra estas amenazas. La expansión del uso de la nube requerirá que las organizaciones mejoren la visibilidad de su presencia en la nube; los activos; y las relaciones con los proveedores para gestionar los riesgos.

En este contexto, se requiere el estudio de las amenazas, riesgos y aspectos a considerar en la seguridad en cloud. Las preocupaciones se centran en aspectos la gestión de los datos, fundamentalmente en la propiedad de los mismos y la forma de operarlos y tratarlos por parte de los proveedores, así como en la identificación y control de acceso a los recursos.

2.8.2. Modelos de servicio de la computación en la nube

Los modelos de servicio de la computación en la nube son de Software, Plataforma y de Infraestructura.

Software de Servicio o Software as a Service (SaaS): Son proveedores que ofrecen aplicaciones para los usuarios de la nube, los proveedores tienen control total sobre los recursos virtuales.

Plataforma como Servicio o Platform as a Service (PaaS): en el que se ofrece la capacidad de computación en la nube y la posibilidad de usar paquetes de aplicaciones usando el entorno y el apoyo del proveedor.

Infraestructura como Servicio o Infrastructure as a Service (IaaS): permite crear los servidores en un entorno virtualizado sin las restricciones que se utilizan con el hardware físico. Para los usuarios de la nube, ya que mantienen el control de sus recursos usando la máquina virtual suministrada por el proveedor para instalar su propio sistema.

2.8.3. Principales características de los sistemas en las nubes

Las principales características de los sistemas en las nubes son: Elástica, Móvil, Rápida

Elástica: Adaptable rápidamente a negocios en crecimiento o de picos estacionales, ya que el sistema en nube está diseñado para hacer frente a fuertes aumentos en la carga de trabajo.

Móvil: El sistema en nube está diseñado para ser utilizado a distancia, así que el personal de la empresa tendrá acceso a la mayoría de los sistemas en cualquier lugar donde se encuentre.

Rápida: Los servicios más básicos de la nube funcionan por sí solos. Para servicios de software y base de datos más complejos, la computación en nube permite saltarse la fase de adquisición de hardware y el consiguiente gasto, por lo cual es perfecta para la creación de empresas.

Además, los sistemas en la nube generan dependencia de la conexión, dependencia del proveedor de servicios, dependencia tecnológica, dependencia de seguridad ajena, gran cantidad de datos en la misma ubicación.

2.8.4. Amenazas en Cloud Computing

La Cloud Security Alliance (CSA) se define como una organización internacional sin ánimo de lucro para promover el uso de mejores prácticas para garantizar la seguridad en cloud, que ha definido las mayores amenazas cloud computing: abuso y mal uso del cloud computing, interfaces y API poco seguras, amenaza interna, problemas derivados de las tecnologías compartidas, pérdida o fuga de información, secuestro de sesión o servicio, riesgos por desconocimiento

Para la creación de un servicio cloud interviene multitud de software de distintos proveedores. Es decir, son entornos complejos por lo que se ha de poner especial atención a las posibles vulnerabilidades del mismo e implantar procedimientos de parcheado.

Otro de los aspectos considerados importantes es la identidad y el control de acceso. Por lo general, la mayoría de las infraestructuras son compartidas por

múltiples empresas o usuarios y la mala definición de los controles de acceso puede provocar accesos no autorizados a datos confidenciales.

La definición de una buena política de identidad y control de acceso basada en políticas de mínimo privilegio es esencial en entornos cloud.

La seguridad y la propiedad de los datos es uno de los aspectos clave. Existe actualmente una gran preocupación por la propiedad y el tratamiento de los datos dado que estas infraestructuras pueden gestionar los datos en múltiples países lo que puede generar conflictos en cuanto al marco legal en el que son tratados.

Estos entornos, al manejar gran cantidad de datos, pueden ser objeto de fugas de información, ya sean intencionadas o fortuitas. El cumplimiento normativo también es uno de los pilares de la seguridad en entornos cloud.

En este caso el problema se presenta debido a la falta de transparencia de estas infraestructuras, por lo que es muy recomendable que el suscriptor del servicio se informe claramente de cómo se gestiona el entorno.

Por último, existe un denominador común a todos estos aspectos mencionados. Se trata de los contratos de acuerdo de servicio. Todas las recomendaciones en cuanto a este asunto indican que éstos deben de ser revisados y creados específicamente, detallando los controles, las normativas, las medidas de protección, los plazos de recuperación del servicio.

2.9. Ciberseguridad

La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes. Advierte en tiempo real las amenazas que provienen de los códigos abiertos o las aplicaciones de terceros. (Kaspersky, 2021)

Las herramientas de seguridad en el internet son:

- La autoprotección de la aplicación en tiempo de ejecución (RASP)

- Firewall de aplicación web (WAF)

2.9.1. La autoprotección de la aplicación en tiempo de ejecución o Runtime Application Self-Protection (RASP)

Los RASP son herramientas informáticas de soporte que funcionan cuando se ejecuta una aplicación y cuando inicia la ejecución. Su función es proteger, supervisar y detectar continuamente los ataques y además de mitigar de inmediato sin la intervención humana.

La protección se realiza principalmente para una variedad de riesgos como:

- Las diez principales vulnerabilidades de OWASP
- Inyecciones
- Deserialización insegura
- Aleatoriedad débil
- IDOR
- SSRF / CSRF
- RPC o XML
- Actividad de cliente sospechoso entre otras.

Las aplicaciones RASP más utilizadas son:

- Fortify (https://www.microfocus.com/en-us/cyberres/application-security)
- Sqreen (https://www.sqreen.com/runtime-application-self-protection)
- Jscrambler (https://jscrambler.com/code-integrity)
- Imperva (https://www.imperva.com/products/runtime-application-self-protection-rasp/)

2.9.2. Firewall de aplicación web o web application firewall (WAF)

Es una aplicación web que detecta las amenazas de la capa de aplicación y protege de malware, SQLi, XSS, CSRF, mitigando los ataques de denegación de servicio de distribución (DDoS) por un monitoreo continuo, las vulnerabilidades OWASP,

exploits y proporciona reglas administradas de forma continua para mantenerse al día con los nuevos riesgos y vectores de amenazas.

Las principales aplicaciones WAF disponibles son:

- Sucuri (https://sucuri.net/)
- AppTrana (https://www.indusface.com/web-application-firewall.php)
- WAF de Cloudflare (https://www.cloudflare.com/es-es/waf/)
- AWS WAF (https://geekflare.com/es/cloud-load-balancer/)

2.9.3. El desafío de la ciberseguridad

La Ciberseguridad se ha convertido en uno de los mayores desafíos para las empresas en los últimos años. En el 2019, las filtraciones de datos expusieron 4.100 millones de registros. En ese mismo año, el coste promedio global de una violación de datos alcanzó los 3,92 millones de dólares. Teniendo en cuenta estos datos, no es difícil entender por qué se espera que el gasto global en Ciberseguridad alcance los 110,99 mil millones de dólares para 2025.

La pandemia de la COVID-19 se ha convertido en un catalizador para que las amenazas de Ciberseguridad aumenten exponencialmente y las empresas sean susceptibles. De hecho, los ciberataques en FinTech se han incrementado con la llegada de la pandemia; los ataques relacionados con el coronavirus han aumentado; además, los ataques de phishing y ransomware han crecido.

Sin embargo, todo esto ha provocado que el 80% de las empresas en todo el mundo aumenten sus infraestructuras de seguridad digital. También han cambiado sus estrategias y han educado en seguridad a sus empleados. Todo para intentar hacer frente a este aumento de las ciberamenazas.

Las organizaciones deben prepararse mejor para los años siguientes, preparándose para reducir los riesgos de seguridad, Además considerar las tendencias y predicciones de Ciberseguridad. (Martínez, 2021)

Capítulo III: Criptografía

3.1. Concepto de criptografía

La Criptografía es la disciplina que estudia los principios, métodos y medios de transformar los datos para ocultar su significado, garantizar su integridad, establecer su autenticidad y prevenir su repudio. Así pues, es una disciplina cuyo fin último es garantizar la confidencialidad de la información.

Al proceso consistente en encubrir la información (que requiere del conocimiento de una información secreta denominada clave de cifrado) se le denomina cifrado, conociéndose como descifrado al proceso inverso (que igualmente precisa del conocimiento de una clave de descifrado, igual o distinta de la anterior).

Los sistemas criptográficos garantizan mediante la complejidad de sus sistemas la seguridad absoluta en las comunicaciones incluso si todo lo relacionado con el sistema es de conocimiento público con excepción de la clave secreta, por lo tanto, estos deben ser seguros inclusive si los crackers conocen los algoritmos de encriptados, desencriptados y la manera de implementarlos.

La criptografía comprende sistemas complejos donde el mensaje pasa encriptado a través de las personas que no les corresponde obtener la información hasta llegar a desencriptado a las personas que le corresponde el mensaje.

En la siguiente figura 3.1 se puede visualizar dicho concepto.

Figura 41: Comunicación usando criptografía
Fuente: Autores

La criptografía se centra en la confidencialidad de los datos cuando estos se encuentran en los estados de datos en reposo, datos en tránsito y datos en uso.

Datos en reposo: Datos que no se usan y se encuentran en dispositivos de almacenamientos como discos duros, memorias flash, discos extraíbles, entre

otros. En este estado se aplica la encriptación para mantener los datos privados si los dispositivos llegan a ser robados.

Datos en tránsito: Los datos se mueven entre dispositivos siendo muy vulnerables a los ataques informáticos como el ataque del hombre en medio.

Datos en uso: Los datos son accedidos por varios usuarios encontrándose muy vulnerables debido a que no están encriptados.

3.2. Importancia de la criptografía

A medida que se realizan las comunicaciones desde diferentes medios tecnológicos por ejemplo usando teléfonos inteligentes o computadoras para compartir información a partir de las redes sociales los mensajes que se envían y reciben pueden ser interceptados por personas que no están autorizadas para leerlos.

Por estas razones la criptografía se hace indispensable al momento de transmitir información por la red para que puedan ser encriptadas convirtiéndolas en seguras y llegue a la persona indicada de forma desencriptada. Del lado de las organizaciones estas se han visto beneficiadas con la criptografía ya que por medio de algoritmos y tecnologías adecuadas pueden proteger los datos de clientes, proveedores, entre otros.

3.3. Criptoanálisis

Es la disciplina contraria a la criptografía, es aquella que investiga los métodos de descubrir informaciones cifradas sin el conocimiento de la clave de descifrado, constituyendo el proceso de intentar descubrir el texto claro o la clave a partir de la información disponible.

Un esquema de cifrado es computacionalmente seguro si el texto cifrado generado por el esquema cumple uno o ambos de los siguientes criterios:

- El coste de romper el cifrado excede el valor de la información
- El tiempo requerido para romper el cifrado excede la vida útil de la información

Tipos de criptoanálisis

Los ataques se clasifican en función del tipo de información disponible para el atacante, asumiendo que el algoritmo de cifrado es conocido:

- **Solo texto cifrado:** El atacante solo tiene acceso al texto cifrado.
- **Texto claro conocido:** El atacante tiene acceso a un conjunto de textos cifrados de los cuales se conoce el correspondiente texto claro.
- **Texto claro elegido:** El atacante puede obtener los textos cifrados correspondientes a textos claros arbitrarios.
- **Texto cifrado elegido:** El atacante puede obtener los textos claros correspondientes a textos cifrados arbitrarios.

3.4. Criptosistemas básicos

En general, un criptosistema consta de tres tipos de protocolos que permiten realizar las siguientes funciones: primero generar las claves para la encriptación, segundo encriptar que consiste en transformar un texto en claro en uno indescifrable y tercero el desencriptado que transforma un texto encriptado en un texto en claro.

De manera general los criptosistemas emplean un conjunto de acciones para transformar el texto en claro en un texto que únicamente pueda ser entendido por la persona que contenga la clave para poder leerlo y de esta manera evitar que existan claves débiles que puedan ser accedidas con facilidad. La siguiente figura 3.2 muestra un criptosistema básico.

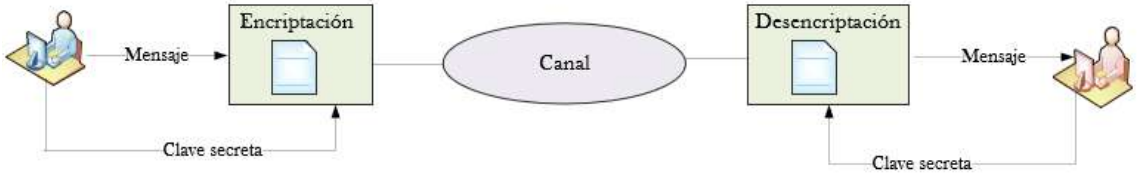

Figura 42: Criptosistema básico
Fuente: Autores

3.4.1. Tipos de criptosistemas

Algunos expertos mencionan que existen varios tipos de criptosistemas, pero de manera formal en la criptografía se mencionan dos, el primero es el criptosistema simétrico y el segundo es el criptosistema asimétrico.

3.4.1.1. Criptosistema simétrico

En este tipo de criptosistema, el remitente y el receptor comparten la clave secreta, por lo que la clave es conocida por las partes que se comunican. Los criptosistemas simétricos suelen ser denominados esquemas de clave secreta o clave simétrica, siendo estos protocolos los que utilizan la misma clave para el cifrado y también para el descifrado.

En la figura 3.3 se puede visualizar como Rosa envía un mensaje a Pedro a partir de una clave secreta compartida entre ambos usuarios (Rosa y Pedro) la misma que sirve para encriptar y desencriptar el mensaje.

Figura 43: Criptosistema simétrico
Fuente: Autores

Este tipo de criptosistema supone un gran problema ya que bastaría con que un intruso descubra la clave simétrica usada por ambos usuarios para tener total control sobre el mensaje que circula por el internet. Entre una de las ventajas está que estos tipos de criptosistemas suponen ser más rápidos.

3.4.1.2. Criptosistema asimétrico

En el cifrado asimétrico, se utilizan dos claves independientes, una para los datos cifrado (clave pública) y otro para el descifrado (clave privada). Por tanto, si una de las llaves se pierde o robado, el mensaje no se ve comprometido.

En la figura 3.4 se puede visualizar como Rosa envía un mensaje a Pedro a partir de una clave pública que cifra el mensaje antes de que Pedro lo lea, cuando Pedro recibe el mensaje para poder leerlo usa una clave privada para descifrar el mensaje.

Figura 44: Criptosistema asimétricos
Fuente: Autores

Los criptosistemas asimétricos, aunque poseen claves distintas, en su gran mayoría depende de algoritmos donde no existen soluciones eficientes. Con el intercambio de claves el destinatario debe conocer la clave secreta y mientras muchos compartan esta clave más vulnerable se vuelve el intercambio de mensajes.

En la práctica se emplea una combinación de estos dos tipos de criptosistemas, puesto que los criptosistemas asimétricos presentan el inconveniente de ser computacionalmente mucho más costosos que los primeros.

En el mundo real se hace uso de la criptografía asimétrica para codificar las claves simétricas y poder así enviarlas a los participantes en la comunicación incluso a través de canales inseguros.

Después se codificarán los mensajes (más largos) intercambiados en la comunicación mediante algoritmos simétricos, que suelen ser más eficientes.

3.5. Algoritmos criptográficos

3.5.1. Algoritmos simétricos

Los algoritmos simétricos son aquellos que comparten la misma clave en esta sección se describen la funcionalidad de los algoritmos DES, AES, Md5 y SHA, además se realizan unas prácticas con los algoritmos haciendo uso de herramientas informáticas.

3.5.1.1. Data Encryption Standard (DES)

Sugiere que el estándar de cifrado de datos o DES por sus siglas en inglés se ha utilizado desde mediados de los 70, fue el principal estándar del gobierno y la industria hasta ser remplazo por el AES, tiene varios modos que ofrecen seguridad e integridad. DES genera una clave de 64 bits, pero 8 de esos bits son solo para la corrección de errores y solo 56 bits son para la clave real, en la actualidad se considera inseguro.

El algoritmo DES utiliza la misma clave para cifrar y descifrar datos, este proceso lo hace por cifrar un bloque de 64 bits usando una clave de 56 bits, es importante mencionar que el tamaño de la clave marca la diferencia en la fuerza del cifrado, por lo tanto, cuanto menor sea la clave más débil y vulnerable se vuelve el cifrado.

Cifrado y descifrado con DES

El cifrado y descifrado con DES se lo realiza por medio de algoritmos matemáticos y el segundo haciendo uso de herramientas informáticas, para la práctica en este libro se usará la herramienta informática SafeDes.

Cifrar el siguiente texto en claro ASCII con la siguiente clave en hexadecimal de 64 bits. La salida cifrada debe estar en hexadecimal y ASCII.

Texto en claro: La vida es un mensaje oculto. (30 caracteres, con punto incluido)

Clave: 74617061646F736F

Para realizar el proceso se debe ejecutar SafeDes, el siguiente paso es elegir en el menú DES la opción cifrar/descifrar.

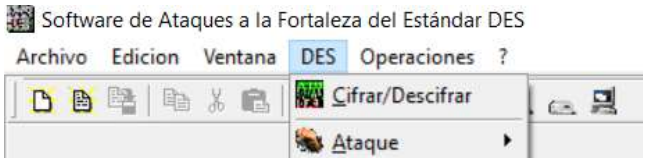

Figura 45: Menús DES para cifrar y descifrar
Fuente: Autores

Elegir en la pantalla que se visualiza la opción teclado, en la entrada de texto en modo elegir ASCII y escribir el texto en claro.

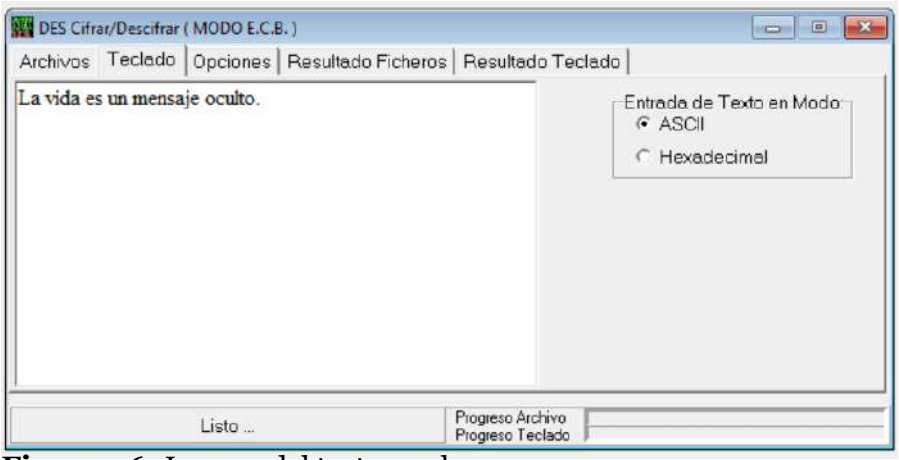

Figura 46: Ingreso del texto en claro
Fuente: Autores

Luego elegir en la viñeta opciones, clic en la opción hexadecimal y escribir la clave en hexadecimal.

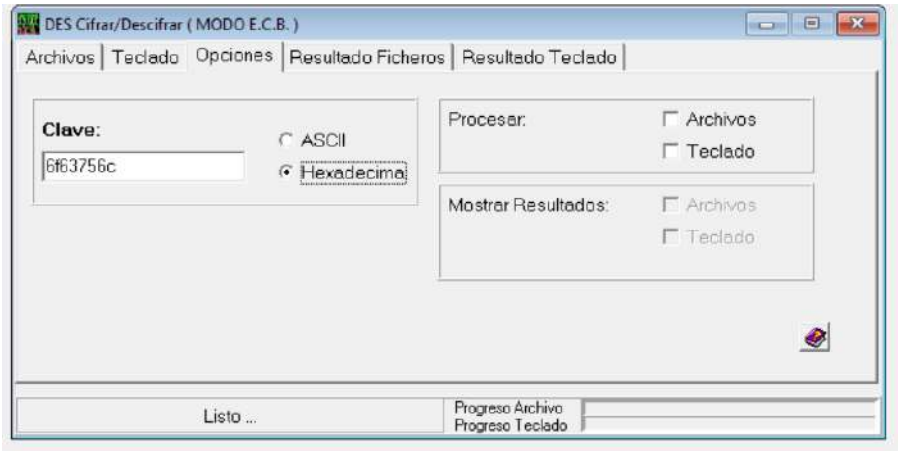

Figura 47: Ingreso de la clave en hexadecimal
Fuente: Autores

Para realizar el proceso de cifrado se debe elegir el menú operaciones y la opción comenzar así el programa realizará sus procesos matemáticos y presentará el resultado.

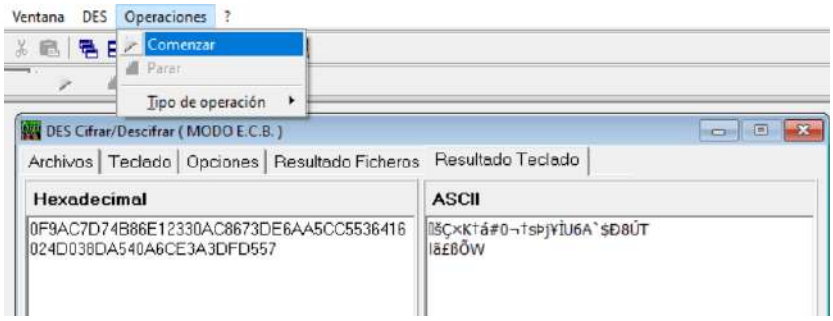

Figura 48: Generación de resultados
Fuente: Autores

Respuesta del texto cifrado en Hexadecimal:

0F9AC7D74B86E12330AC8673DE6AA5CC5536416024D038DA540A6CE3A3DFD557

Respuesta de texto cifrado en ASCII:
_šÇ×K†á#0¬†sÞj¥ÌU6A`$Ð8ÚT
lã£ßÕW

El texto en claro se lo puede cifrar en SafeDes haciendo uso de una clave ASCII por ejemplo una clave “todoso” eligiendo en la clave la opción ASCII daría como resultado un texto cifrado en hexadecimal y ASCII.

3.5.1.2. Advanced Encryption Standard (AES)

El Estándar de cifrado avanzado o AES por sus siglas en inglés tiene claves de cifrado muy fuertes y una gran capacidad de cifrar grandes bloques de datos de una sola vez. Entre los tamaños de claves que usa AES están las de 128 bits, 192 bits, 256 bits siendo esta última (256 bits) una de las más seguras en la actualidad y el tamaño de bloque es de 128 bits

AES fue estandarizado por NIST en remplazo del DES en el año 2000 momento que se convirtió en el estándar más usado en el mundo, la mayoría de los productos de cifrados admiten AES, y la NSA lo ha aprobado para proteger información secreta. AES es tan seguro como puede serlo un cifrado en bloque, y algunos mencionan que nunca se romperá, debido a que todos los bits de salida

dependen de todos los bits de entrada de alguna manera compleja y pseudoaleatoria.

Cifrado y descifrado con AES

El cifrado y descifrado con AES se lo realiza por medio de algoritmos matemáticos y el segundo haciendo uso de herramientas informáticas, para la práctica en este libro se usará la herramienta informática AESPhere.

Cifrar el siguiente texto en claro ASCII con la siguiente clave en hexadecimal de 64 bits. La salida cifrada debe estar en hexadecimal y ASCII.

Texto en claro: La vida es un carnaval lleno de espuma.

Clave: 6361726E6176616C65726F7370617961

Primera cifra en modo: ECB

Segunda cifra en modo CBC

Para realizar el proceso se debe ejecutar AESPhere, el siguiente paso es elegir en el menú la opción cifrar.

Figura 49: Opción cifrar en el menú
Fuente: A

Ingresar el texto en ASCII, ingresar la clave en el apartado clave con las opciones de 128 bits, 192 bits y 256 bits. Elegir el modo de salida y el método de cifrado este puede ser ECB y CBC.

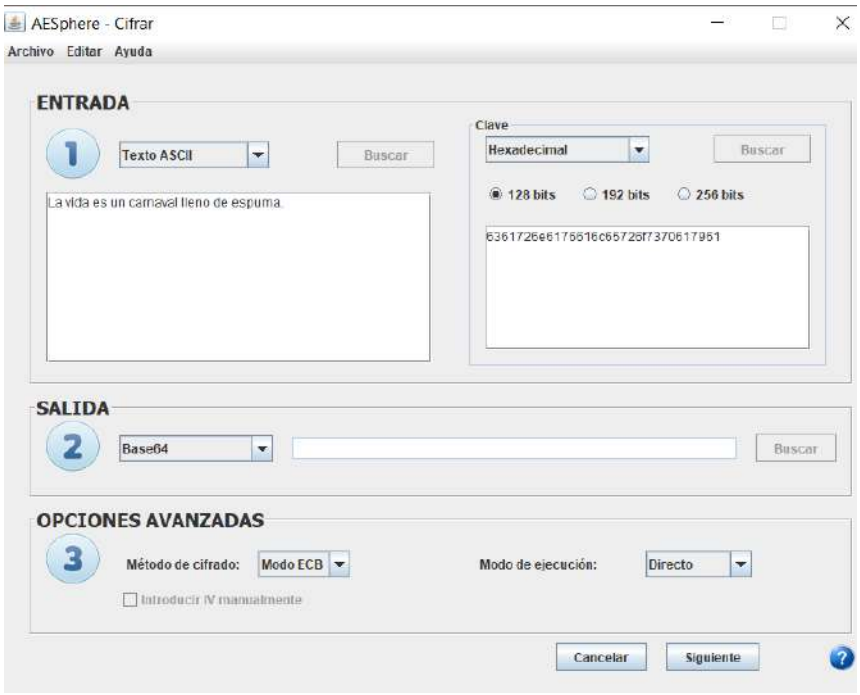

Figura 50: Ingreso de datos para cifrar texto
Fuente: Autores

Para cifrar el texto se da clic en el botón siguiente, finalmente el programa cifra el texto con la clave en hexadecimal.

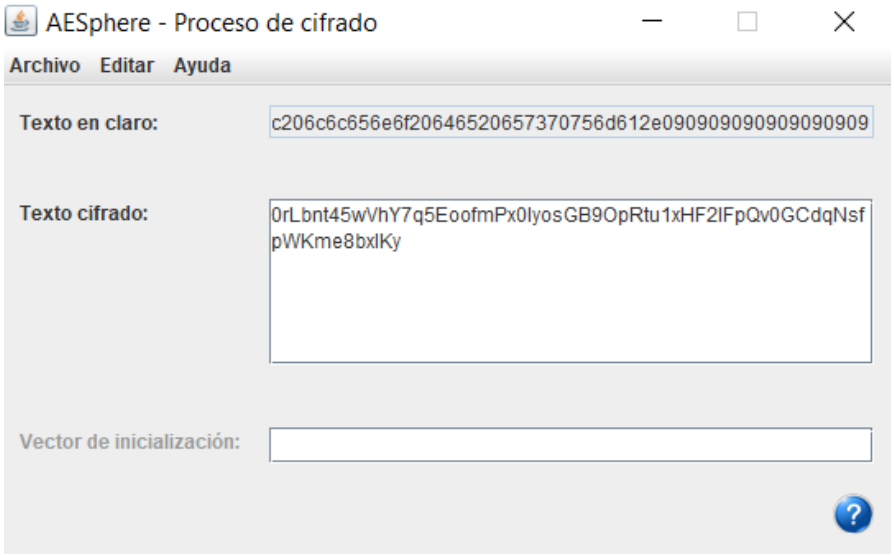

Figura 51: Visualización de resultados en AESPhere con el modo ECB
Fuente: Autores

Para cifrar en modo CBC hay que elegir dicha opción una vez agregados todos los campos se puede visualizar los siguientes datos.

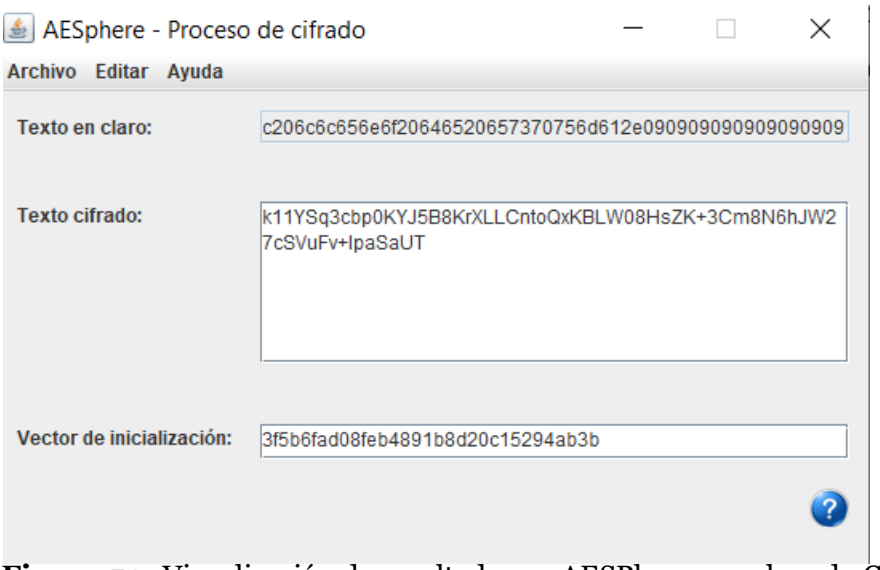

Figura 52: Visualización de resultados en AESPhere con el modo CBC
Fuente: Autores

El Descifrado se lo realiza eligiendo la opción de descifrar en el menú de AESPhere, luego se ingresa la entrada, la clave la salida y el modo de desencriptar (ECB, CBC)

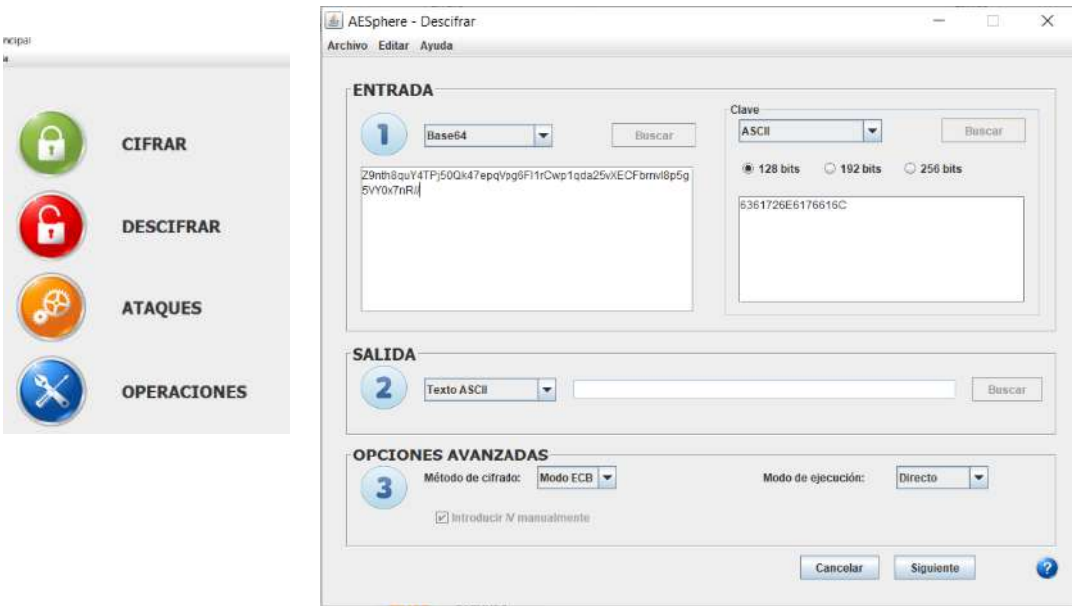

Figura 53: Elección de opciones e ingreso de datos para desencriptar
Fuente: Autores

Para visualizar la respuesta de descifrado en AESPhere se debe dar clic en el botón siguiente, seguidamente se visualiza una pantalla con el texto cifrado y el texto en claro.

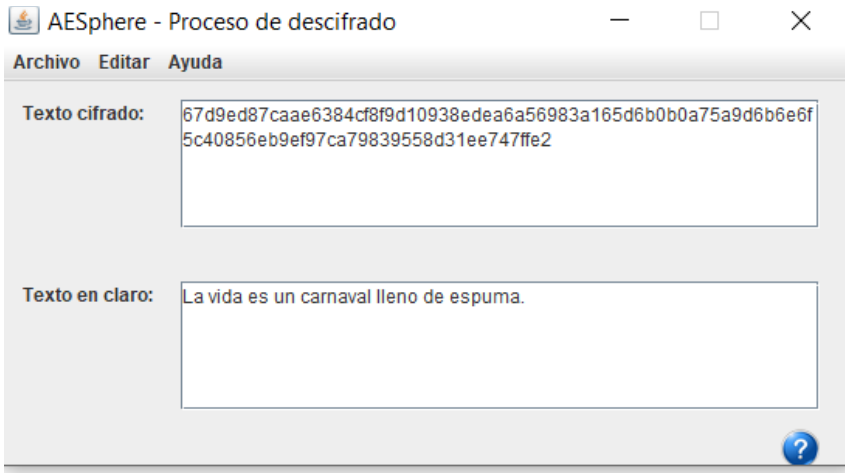

Figura 54: Resultado de descifrado
Fuente: Autores

En este caso funciona la misma clave en hexadecimal para encriptar y desencriptar el mensaje debido a que los algoritmos DES y AES son de criptografía asimétrica es decir comparten la misma clave.

3.5.1.3. Message Digest 5 (MD5)

MD5 crea una cadena criptográfica de tamaño fijo que representa el mensaje. Esta salida se conoce como resumen. El resumen resultante es unidireccional y no se puede revertir. Toma el mensaje, aplica el algoritmo MD5 y genera un valor de 128 bits. Este resumen se envía junto con el mensaje a su destino previsto.

El algoritmo Message Digest 5 es más complejo que sus predecesores, por lo que ofrece una mayor seguridad. Pero su mayor debilidad es que no tiene una fuerte resistencia a las colisiones y, por lo tanto, ya no se recomienda su uso. (Dulaney & Easttom, 2018)

3.5.1.4. Secure Hashing Algorithm (SHA)

El algoritmo de hash seguro (SHA) es otro algoritmo de hash unidireccional que fue publicado por el Instituto Nacional de Estándares y Tecnología como un Estándar de procesamiento de información federal de EE. UU. A diferencia de MD5, SHA crea un resumen de 160 bits.

(Handschuh , 2005) el algoritmo SHA se compone de una familia de seis funciones hash: SHA-0, SHA-1, SHA-224, SHA-256, SHA-384 y SHA-512. Los mensajes de entrada son de longitud variable y los procesan a salidas de longitud fija. Los primeros cuatro operan en bloques de mensajes de 512 bits divididos en palabras de 32 bits y los dos últimos en bloques de 1024 bits divididos en palabras de 64 bits.

3.5.2. Algoritmos asimétricos

Los algoritmos asimétricos son aquellos que tienen claves distintas para las partes que intervienen en el proceso de encriptado en esta parte se detallan la funcionalidad de los algoritmos RSA por medio de su definición y la realización del cálculo de la clave privada, finalmente se menciona el proceso que se lleva a cabo en la firma electrónica.

3.5.2.1. Algoritmo RSA (Rivest, Shamir, Adleman)

RSA utiliza criptografía de clave pública, es decir se usan dos claves diferentes para cifrar y descifrar datos. Entre las características principales de RSA son su capacidad para brindar confidencialidad de los datos mediante el uso de técnicas de cifrado, y autenticación a través de Internet. RSA utiliza tamaños de clave variables que van desde 512 bits hasta 2048 bits, sin embargo, se debe mantener un tamaño de clave mínimo de 1024 bits.

El algoritmo RSA usa exponenciación modular, Las claves públicas y privadas de RSA constan de pares de números. Cada uno contiene dos de los siguientes:

- N-el módulo, parte de ambos pares de claves RSA.
- e-el exponente público, parte de la clave pública RSA.
- d- es el modular inverso (inv), la parte secreta de la clave privada.

Para crear una clave a partir del RSA se obtiene el producto de dos números primos enormes elegidos al azar, que representa un gran problema computacional siempre que se tengan número enormes, es así que la seguridad del algoritmo radica en que no se puede o al menos no se conoce la forma de factorizar números primos enormes.

Para realizar el proceso de cifrado mediante RSA se debe realizar el siguiente proceso:

1. Elegir al azar dos números primos (p y q) lo suficientemente grandes donde:
   $p \neq q$
   $n = p * q$
   $\varphi(n) = (p - 1) * (q - 1)$

2. Se eligen dos exponentes e y d
   ey $\varphi(n)$no tengan números en común que los dividan es decir $mcd[e, \varphi(n)] = 1$
   $e * d = 1 \bmod \varphi(n)$
   $e = 1 < e < \varphi(n), mcd\ [e, \varphi(n)] = 1$
   $d = inv[e, \varphi(n)]$

La clave pública es el número par (e, n) y la clave privada (d, n)o (p, q).

3.5.3. Firma electrónica

Los crecientes avances de la tecnología nos han llevado a vivir en un mundo interconectado que hace necesario el uso de documentación digital que permite el uso de la firma electrónica para garantizar la integridad, autenticidad y no repudio de los documentos.

La firma electrónica es un resumen cifrado o codificado del contenido perteneciente a un documento enviado por un firmante, y que, al tener la totalidad de los requerimientos legales, es garantizada por una Autoridad de certificación. La firma electrónica está basada en la criptografía de clave asimétrica.

Este tipo de firma permite al firmante emplear una clave privada para firmar documentos y quien necesite verificar la autentificación de la firma necesitará poseer la clave pública del emisor o firmante. En la siguiente figura se puede

visualizar Pedro (Firmante) que envía un documento firmado electrónicamente por medio de internet a Rosa quien recibe dicho documento con la firma.

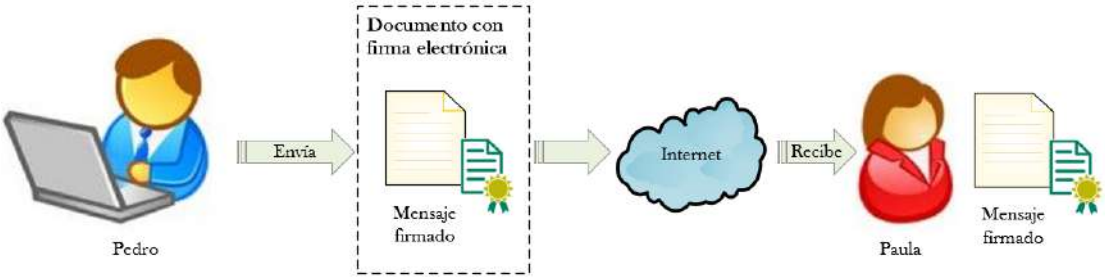

Figura 55: Envío de documento con firma electrónica
Fuente: Autores

La firma electrónica se la puede obtener por medio de un token que es un dispositivo físico que contiene de manera segura certificados digitales, una aplicación para las firmas electrónicas y su validación, se actualiza de forma remota. También puede ser obtenida a partir de un archivo digital que contiene los datos de la persona dueña de la firma electrónica.

Para usar la firma electrónica se necesita de un certificado digital que contiene el nombre del firmante, la clave pública y el tiempo de validez estos son emitidos por medio de una entidad certificadora quien da fe que el firmante es quien dice ser, Las entidades certificadoras emiten distintos tipos de certificados dependiendo del firmante por ejemplo si es una persona natural, jurídica o un funcionario público.

En el caso concreto de no contar con una firma electrónica se debe seguir los siguientes pasos:

1. Buscar la entidad certificadora de su elección
2. Realizar una solicitud online
3. Realizar el proceso a seguir para la obtención del certificado.
4. Realizar el pago adjudicado por la entidad certificadora
5. Descargar el certificado

Capítulo IV: Seguridad de la Información

4.1. Seguridad de la Información según la Norma ISO 27001

Las organizaciones modernas independientemente de su tipo o tamaño almacenan, procesan o transmiten información a través de sus diferentes activos informáticos. Es decir, la información en formato digital cada día juega un papel fundamental en la toma de decisiones para alcanzar los objetivos organizacionales, sin embargo, está sujeta a amenazas constantes de tipo natural o humanos y para las organizaciones es esencial protegerla.

Un Sistema de Gestión de la Seguridad de la Información SGSI o en inglés Information Security Management System, ISMS, según la Norma UNE-ISO/IEC 27001, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. La norma específica que, como cualquier otro sistema de gestión, el SGSI incluye tanto la organización como las políticas, la planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos (Ascanio, J.G.A., R.A.B. Trillos, and D.W.R.J.T. Bautista, 2015).

Los sistemas de gestión que definen las normas ISO siempre están documentados, ya que es la mejor manera de formalizar normas e instrucciones y, por otro, son más fáciles de transmitir y comunicar, donde los sistemas de información, sus datos, estructura pueden ser sujetos a amenazas externas o internas que pueden afectar a la operatividad de los sistemas, para esto se deben identificar los riesgos (Gómez Fernández & Andrés Álvarez, 2012).

4.2. Beneficios de los SGSI

Los principales beneficios de los sistemas de gestión de seguridad de la información son los siguientes:

- Conocimiento profundo a cerca de la organización, cómo funciona y a su vez proporciona un plan de mejoramiento continuo para solucionar las posibles inconsistencias de seguridad de la información.
- Analizar los riesgos, identificando amenazas, vulnerabilidades y su impacto dentro de las actividades de la organización.
- Generar y aplicar planes de mejoramiento continuo en la gestión de la seguridad información.
- Garantizar la continuidad y disponibilidad de las instituciones.
- Reducir los costos vinculados a los incidentes presentados.
- Incrementar los niveles de confianza de los usuarios de los sistemas informáticos.
- Intención de cumplir con la legislación actual para la protección de datos, servicios de la sociedad, propiedad intelectual, comercio electrónico relacionados con la seguridad de la información.

4.3. Importancia de la implementación de un SGSI

La implementación de un SGSI, nos permite proteger la información, junto con los procesos y sistemas que hacen uso de ella. La confidencialidad, la integridad y la disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen de la organización necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Un Sistema de Gestión de Seguridad de la Información, basado en la norma ISO/IEC 27001, es una herramienta o metodología sencilla y de bajo coste que cualquier empresa u organización, independientemente de su tamaño, puede utilizar.

La norma le permite establecer políticas, procedimientos y controles con objeto de disminuir los riesgos de su organización. La implantación y posterior certificación de estos sistemas supone la implicación de toda la empresa,

empezando por la dirección sin cuyo compromiso es imposible su puesta en marcha.

La dirección de la empresa debe liderar todo el proceso, ya que es la que conoce los riesgos del negocio y las obligaciones con sus clientes y accionistas mejor que nadie. Además, es la única que puede introducir los cambios de mentalidad, de procedimientos y de tareas que requiere el sistema.

En primer lugar, obtenemos una reducción de riesgos debido al establecimiento y seguimiento de controles sobre ellos. Con ello lograremos reducir las amenazas hasta alcanzar un nivel asumible por nuestra organización. De este modo, si se produce una incidencia, los daños se minimizan y la continuidad del negocio está asegurada.

En segundo lugar, se produce un ahorro de costes derivado de una racionalización de los recursos. Se eliminan las inversiones innecesarias e ineficientes como las producidas por desestimar o sobrestimar riesgos.

En tercer lugar, la seguridad se considera un sistema y se convierte en una actividad de gestión. La seguridad deja de ser un conjunto de actividades más o menos organizadas y pasa a transformarse en un ciclo de vida metódico y controlado, en el que participa toda la organización.

En cuarto lugar, la organización se asegura del cumplimiento de la legislación vigente y se evitan riesgos y costes innecesarios. La entidad se asegura del cumplimiento del marco legal que protege a la empresa de aspectos que probablemente no se habían tenido en cuenta anteriormente.

Por último, pero no por ello menos importante, la certificación del Sistema de Gestión de Seguridad de la Información contribuye a mejorar la competitividad en el mercado, diferenciando a las empresas que lo han conseguido y haciéndolas más fiables e incrementando su prestigio.

4.4. Implementación de la Norma Técnica Ecuatoriana NTE-INEN ISO 27001: 2015

La Norma Técnica Ecuatoriana NTE-INEN ISO NTE ISO 27001:2015, es una traducción idéntica de la Norma Internacional ISO/IEC 27001, que se aplica a

los sistemas de gestión de la calidad (SGC) y que se centra en todos los elementos de administración de la calidad con los que una organización debe contar para tener un sistema efectivo, que le permita gestionar y mejorar la calidad de sus productos o servicios.

Adicionalmente para la implementación de un SGSI se deben tener en cuenta en Ecuador las normas legales establecidas para la protección de la información:

Constitución política del Ecuador (Asamblea Nacional, 2018) en la que menciona *"Art. 18. Todas las personas, e forma individual o colectiva, tiene derecho a:*

3. *Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en caso expresamente establecidos por la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información".*

El Esquema Gubernamental de Seguridad de la Información (EGSI), tiene su inicio con la Secretaría de la Administración Pública del Ecuador que emite los Acuerdos Ministeriales el 2011, mediante los cuales crea la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación para gestionar de forma eficiente y eficaz la seguridad de la información en las entidades públicas.

Disponiendo a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.

La implementación del EGSI se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información. Basado en la norma técnica ecuatoriana INEN ISO/IEC 27002 para Gestión de la Seguridad de la Información y está dirigido a las Instituciones de la Administración Pública Central, Dependiente e Institucional. Además, establece un conjunto de directrices prioritarias para

Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la Administración Pública. El EGSI no reemplaza a la norma INEN ISO/IEC 27002 sino que marca como prioridad la implementación de algunas directrices.

Normas de control interno de la Contraloría General del Estado, para que la seguridad de información se gestione con transparencia y consistencia en cualquier Institución, es importante siempre considerar los riesgos que se puede generar en cualquier Institución. En este contexto, la Contraloría General del Estado establece las "Normas de control interno para las entidades, organismos del sector público y de derecho privado."

Según (Controlaría General del Estado, 2009), Las Normas de control interno también hacen referencia explícita a la seguridad de información en el siguiente artículo:

Art. 410-10 Seguridad de Tecnología de Información*: La Unidad de tecnologías de la información, establecerá mecanismos que protejan en salvaguarden contra perdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:*

1. *Ubicación adecuada y control de acceso físico a la Unidad de Tecnologías de la información y en especial a las áreas de: servicios, desarrollo y bibliotecas.*
2. *Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado.*
3. *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.*
4. *Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización.*
5. *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.

6. *Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire controlado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros;*
7. *Consideración y disposición de sitios de procesamiento alternativos.*
8. *Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.*

Ley de comercio electrónico, firmas electrónicas y mensajes de datos, Según (Congreso Nacional, 2002), La ley de comercio electrónico regula el uso de sistemas de información y redes electrónicas, como en el internet, desarrollo de comercio tanto en el sector público y privado los puntos más importantes en estas leyes son:

Titulo 1: De los mensajes de datos.

Titulo 2: De las firmas electrónicas, certificados de firma electrónica, entidades de certificación de información, de regulación de entidades de certificación debidamente acreditadas.

Titulo 3: De los servicios electrónicos, la contratación electrónica y telemática, Los Derechos de los Usuarios, e Instrumentos Públicos.

Titulo 4: De la prueba y notificación electrónicas.

Título 5: De las infracciones informáticas.

Ley orgánica de transparencia y acceso a la información pública, tiene como objetivo principal el derecho de las personas a estar informados sobre los procesos de gestión que mantenga cualquier Institución pública ecuatoriana y además de asegurar la información para que no sea mal utilizada. De acuerdo al (Congreso Nacional, 2004) se mencionan los siguientes artículos:

*"**Art. 5. Información Pública.-** Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las*

instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren baso su responsabilidad o se haya producido con recursos del Estado.".

*"**Art. 6. Información Confidencial.-** Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimo y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de las Constitución de Política de la Republica"*

*"**Art. 10. Custodia de la información. -** Es responsabilidad de las instituciones públicas y demás entes señalados en el artículo 1 de la Ley, crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción.".*

Ley del sistema nacional de registros de datos públicos, considera como principal objetivo garantizar que la información se maneje de forma eficiente y eficaz en la Instituciones Públicas que manejen recursos públicos como indica en el artículo:

"Art. 26. Seguridad: Toda Base informática de datos debe contar con su respectivo archivo de respaldo, cumplir con los estándares técnicos y plan de contingencia que impida la caída del sistema, robo de datos, modificación o cualquier otra circunstancia que pueda afectar la información pública" (Asamblea Nacional, 2014).

Este artículo hace referencia a la seguridad de la información, gestión de respaldos, planes de contingencia y la protección para robos o alteración de información.

Ley de protección a la intimidad y a los datos personales, El propósito de esta ley es complementar a la ley anterior ya que los datos personales buscan la protección a la intimidad que se encuentren almacenados en lugares físicos y digitales. Estipulan los siguientes aspectos los cuales deben estar debidamente justificados:

- Se permitirá la recolección de información personal siempre y cuando estén claramente especificadas las razones de su uso.
- Se prevé una organización como órgano de control de datos personales de esta manera será únicamente el que controles toda la información personal para que no exista abuso de la misma.

Ley Orgánica de Protección de Datos Personales (Proyecto de Ley), El 19 de septiembre de 2019, la Presidencia de la República envió a la Asamblea Nacional el proyecto de Ley Orgánica de Protección de Datos Personales para Ecuador. El objeto del documento es regular el ejercicio del derecho a la protección de datos personales siguiendo el modelo europeo, adaptando ciertos aspectos a la realidad ecuatoriana.

Los principales puntos del proyecto de ley son:

1. Reconocimiento de diferentes principios para la aplicación de la ley en el tratamiento de datos personales, tales como legalidad, lealtad, legitimidad, finalidad, entre otros.
2. Reconocimiento de derechos a favor de los titulares de los datos, tales como el derecho a la transparencia, derecho al acceso, derecho de eliminación de datos, entre otros.
3. Establece un régimen especial para datos sensibles, datos de niños, adolescentes, etc.
4. Establece un régimen de seguridad y protección de datos personales.
5. Regula la transferencia internacional de datos.

6. Establece obligaciones para los responsables y encargados del tratamiento.

7. Establece un régimen de infracciones tales como la falta de notificación a las vulneraciones de seguridad, utilización de información o datos para fines distintos a los declarados, no implementación de políticas de protección de datos personales en las empresas.

4.5. Implementación de un SGSI en Universidades

Las Instituciones de Educación Superior (IES), públicas y privadas, manejan información sensible de gran importancia para el cumplimiento de sus metas y objetivos, como procesos y almacenamiento de datos de estudiantes, profesores y administrativos, al igual que las instalaciones, aplicaciones y equipos tecnológicos que requieren ser protegidos para garantizar la disponibilidad, integridad y confidencialidad.

Para las universidades se ha convertido en un requisito primordial la gestión de servicios de tecnologías de la información, puesto que requieren que la prestación de sus servicios se realice con la máxima calidad posible.

Gracias a la Norma ISO 27001 se lleva a cabo la implantación de un SGSI de forma eficiente. Su objetivo es otorgar valor a la información, ya que se trata de un activo clave para las universidades, para garantizar la calidad de los procesos académicos (NIEVES, 2017). Además, las universidades, disponer de este SGSI consistiría en la implementación de un marco común de gestión de la seguridad con la finalidad de asegurar la integridad, disponibilidad y la confidencialidad de los datos pertenecientes a la institución.

4.5.1. Beneficios que aporta a las Universidades la certificación de la norma ISO-27001

– Demostración a proveedores, personal, actores productivos y sociales, la realización de buenas prácticas, aprobadas y revisadas internacionalmente.

- Ayuda a la universidad a demostrar que lleva a cabo una gestión de la seguridad de la información de manera eficiente.
- Promueve la participación, motivación e implicación del personal por conservar la política sobre la seguridad de la universidad.
- Se establecen proceso de mejora continua e innovación de las actividades.
- Mejora el desempeño, amplía oportunidades de mercado y suprime la incertidumbre.

4.5.2. Estudio de caso. La Seguridad de la Información en una IES

La metodología PHVA (Planificar, Hacer, Verificar y Actuar), basada en la Norma ISO 27001 y su guía de buenas prácticas ISO 27002, permitirán a la Universidad Técnica Estatal de Quevedo organizar, diseñar y gestionar de manera sistemática su SGSI, plantear estrategias de cambio y mejora de los mismos, verificar las medidas de seguridad aplicadas y los resultados obtenidos, valorar y asegurar sus activos de posibles riesgos y vulnerabilidades presentes, permitiendo la toma de decisiones de manera consecuente, argumentada y documentada, involucrando a todo el personal en un proceso de mejora continua..

Entre los lineamientos para trabajos futuros, se debería considerar la aprobación de políticas de seguridad definidas para la protección, cuidado y continuidad del negocio en caso de materializarse una catástrofe que conlleve a la pérdida de la base de gestión como es la información generada a diario por cada una de las áreas académicas y administrativas involucradas.

Por otra parte, se requiere desarrollar un análisis de riesgos de tipo cuantitativo considerando varios aspectos, como son: las consecuencias económicas de la materialización de una amenaza en cada activo, el costo del despliegue y mantenimiento de las salvaguardas; y estimar la probabilidad de ocurrencia de amenazas basándose en registros reales.

Glosario de términos claves

Activo: El activo es un bien que posee una empresa.

Administradores de red: Encargados de mantener el hardware y el software de red

Administración remota: Permite realizar acciones desde un equipo local hasta un equipo remoto.

Algoritmo: Conjunto de operaciones matemáticas que permite convertir un texto en lenguaje natural para hacerlo ilegible.

APK: Paquete del sistema operativo Android, usados para distribuir e instalar componentes.

Antispyware: software que detecta y elimina programas maliciosos.

Biometría: Área de la ciencia que realiza el estudio del reconocimiento inequívoco de las personas basados en los rasgos físicos o conductuales.

Bits: es un digito de numeración binaria, puede tener solo dos valores ceros y unos.

BS: Estándar Británico.

BSI o BSI group: Institución de estándares británicos en ingles British Standards Institution. (https://www.bsigroup.com/).

CAPTCHA: Es un test controlado por una máquina de Prueba de Turing.

Ciberseguridad: Técnica y métodos que sirven para proteger los sistemas.

Cifrar: el cifrado es un procedimiento que usa algoritmo para enviar un mensaje mediante clave.

Clave pública: Una llave pública puede ser entregada a cualquier persona.

Clave privada: El propietario guarda la clave de manera que nadie tenga acceso a ella.

Clave secreta: es una combinación usada para cifrar y descifrar los mensajes.

Contraseña: Una serie de caracteres secretos que permite al usuario acceder a los distintos servicios asignados a este. Forma de autenticación que usa una combinación secreta para controlar el acceso a un recurso o servicio informático.

Certificado digital: fichero informático firmado de manera electrónica a través de un prestador de servicios electrónicos.

Criptografía asimétrica RSA: sistema criptográfico, sirve para cifrar y para firmar de manera digital.

Cifrado simétrico: es llamada criptografía de clave secreta, usando una misma clave para cifrar y descifrar.

Control de acceso: Restringe el acceso a un recurso que es solo para usuarios, aplicaciones o sistemas informáticos permitidos.

Colisión: Una colisión toma protagonismo cuando dos entradas diferentes a una función de hash producen una misma salida.

Crackers: Experto en técnicas informáticas avanzadas, que usa esas técnicas como medio para realizar delitos informáticos.

Desbordamiento de buffer: es un tipo de vulnerabilidad producida por errores en el código del programa que permite tener acceso remoto en el sistema atacado para lograr que este se cuelgue, uno de los sinónimos para referirse a este tipo de vulnerabilidad es Buffer overflow.

Descifrar: Conocer el mensaje que está en clave.

Desencriptar: Mostrar el contenido de un mensaje que está oculto a partir de una clave.

Direcciones IP: Las direcciones IP (Protocolo de Internet) están dadas por un número único que identifica a los sistemas conectado en la red.

Dirección MAC (Media Access Control): Identificar único de una tarjeta de red o dispositivo que posee 48 bits, también conocida como dirección física.

Drivers: Programa informático con instrucciones precisas para la función correcta de un accesorio o componente del ordenador.

EGSI: El Esquema Gubernamental de Seguridad de la Información.

Emisor: El emisor es quien exterioriza el mensaje en una comunicación

Encriptar: ocultar el mensaje mediante combinaciones de letras, números y símbolos para que no pueda ser interpretado.

Enrutamiento: Buscar un camino entre varios posibles cuando hay una gran conectividad en la red.

Entrada de voz: Identificación de las características como tono, ritmo y volumen únicas de la voz.

Estándar: Las normas que contienen especificaciones técnicas de aplicación voluntaria.

Fichero: Conjunto de información clasificada y ordenada de fácil acceso.

Filtrado de paquetes: Controla en acceso a la red mediante el análisis de paquetes entrantes o saliente.

Funciones hash: usan algoritmos matemáticos, transformando losa datos en código alfanuméricos, el código tendrá siempre el mismo número de caracteres.

Firmware: Programa informático que contiene la lógica a más bajo nivel para el control de los circuitos eléctricos en los dispositivos.

Gestores de bases de datos: Conjunto de programas que almacenan datos a fin de facilitar la administración de los mismos.

Get: usado en el protocolo HTTP para indicar los recursos de descarga.

Herramienta ping: Usada para establecer si un sistema está disponible.

Herramienta traceroute: Facilita conocer los sistemas intermedios que atraviesa un paquete hasta su destino.

Hexdump: Vista hexadecimal del volcado de datos desde la RAM.

Host: computadoras o dispositivos conectados en una red.

Huellas dactilares: La huella dactilar es una característica que tiene lugar en la etapa fetal por lo tanto hace que un individuo sea único distinguiéndonos de una persona a otra.

Industria de la seguridad: encargada de aplicar normas y actividades encargas a prevenir riesgos.

Información: el valor de los datos que aporta conocimiento.

IEC: Comisión Electrotécnica Internacional.

IEE 802.11i: Incluye protocolos que mejoran el cifrado y gestionan las claves.

INEN: Instituto Ecuatoriano de Normalización actualmente se llama Servicio Ecuatoriano de Normalización.

IPS: Es la sigla de Sistemas de Prevención de Intrusiones, este es un software usado para la protección de ataques y abusos a los sistemas, se decir que es una tecnología muy cercana a los corta fuegos.

ISO: Organización Internacional para la Normalización.

ISRM: Gestión de Riesgos de Seguridad de la Información en ingles Information Security Risk Management.

ISRA: Evaluación de Riesgos de Seguridad de la Información en ingles Information Security Risk Assessment.

Kali Linux: es un sistema operativo basado en Debian diseñado especialmente para la auditoría y la seguridad informática.

Método ECB (electronic codebook): es el método más simple de cifrado, el mensaje se divide en bloques en donde cada bloque se cifra de forma separada.

Método CBC (Algoritmo cerrado basado en cifras): Es el modo criptográfico más usado, en donde el bloque cifrado depende de todos los bloques de texto en claro.

Navegador: es una aplicación que posibilita el acceso a la web, interpretando la información para que esta pueda ser visualizada.

Netscape: Es una empresa de software que creo el navegador web Netscape.

Normas: Son documentos que contienen principios, especificaciones, técnicas públicas que se adoptan para la realización correcta de una acción o actividad.

NTE: Norma Técnica Ecuatoriana.

Protocolos de routing: especifican la comunicación entre los enrutadores para distribuir la información.

La protección de los recursos de la red es de carácter urgente para todo administrador de red, en los servidores Linux existe el sistema de detección de intrusos llamado Snort que puede obtenerse desde la página oficial https://www.snort.org/, este IDS permite mediante líneas de comandos rastrear los paquetes que transitan por la red y al encontrar paquetes sospechosos los bloquea.

Protocolo Ipsec: su función es asegurar la comunicación sobre IP, autenticando y cifrando los paquetes, también permite claves de cifrado.

Puertos: Medio por el que un programa cliente se comunica estos van del 0 al 1024 para servicios privilegiados.

Proxy web: es una red informática, servidor, dispositivo o programa que sirve de intermediario en las peticiones que hay entre cliente y servidor.

Protocolo Ethernet: Permite el intercambio de datos entre computadoras, impresoras, servidores, entre otros.

Paquetes: Bloques es que se divide la información para ser enviado por medio de la web.

PDCA: Es un modelo propuesto por Deming (1986) que tiene como estrategia la mejora continua de la calidad realizando cuatro pasos: Planificar, Hacer, Verificar y Actuar. (Plan-Do-Check-Act).

Plugin: Componente de código diseñado para añadir funcionalidades adicionales al software.

PIN: contraseña que se usa en algunos sistemas como tarjetas SIM entre otros y sirven para la identificación.

Pentester: Especialistas informáticos que realizan técnicas avanzadas de explotación para descubrir vulnerabilidades.

PKI (Infraestructura de clave pública): tiene lo necesario tanto en hardware como en software para que las comunicaciones sean seguras por medio de certificado digitales y firmas digitales.

Protocolo IPSEC: conjunto de protocolos, que aseguran las comunicaciones.

Protocolo RIP: Protocolo de enrutamiento interior que hace uso de los vectores a distancia.

Protocolo BGP: Protocolo de enrutamiento exterior.

Pseudoaleatoria: el pseudoaleatorio es un algoritmo que produce un conjunto de números parecidos a los aleatorios.

Receptor: Persona que recibe el mensaje.

Reconocimiento facial: Detección de rasgos faciales únicos de las personas como forma, profundidad, color de piel, cabello.

Red local: interconexiones realizadas entre computadoras y periféricos su extensión es limitada a unos 200 metros.

Red remota: permite conectarse a una red por medio del internet.

Reloj biométrico: recaban la información personal de un usuario mediante un lector digital.

Servidores de correos electrónicos: es una aplicación basada en red ubicada en un servidor de internet, que sirve para brindar servicios de correo electrónico.

Uno de los temas más deficientes para los administradores en red en cuanto a seguridad de la información, son los protocolos de seguridad, ya que estos pueden afectar la seguridad de las redes.

SGSI: Sistema de Gestión de Seguridad de la Información en ingles ISMS (Information Security Management Systems).

Sistema operativo: conjunto de programas y órdenes que controlan los procesos realizados por el hardware y software en las computadoras.

Sistemas operativo Windows: Conjunto de programas que permite la administración de los recursos en las computadoras por medio de distintas ventanas con el fin de ayudar a la interacción con el usuario.

Sistemas operativo Linux: conjunto de programas de software libre es decir que no es propiedad de ninguna persona o empresa tiene una interfaz de comandos y una gráfica.

Sistema operativo iOS: es de uso móvil su dueño es la multinacional Apple usado sólo para dispositivos de la marca.

Sistemas operativo Android: Desarrollado por Google diseñado para dispositivos móviles con pantalla táctil.

Sistemas Operativo Mac OS X: Sistemas gráficos desarrollo por Apple para computadoras Mac.

SSID: es una secuencia de 0-32 octetos que permite identificar los paquetes como parte de una red.

Script: Programa simple que posee una secuencia de comandos.

Tarjeta de red: Permite la conexión del computador al internet.

Terminal de Kali Linux: la terminal o consola en Kali Linux permite ejecutar comandos.

TI: Tecnología de la Información.

Token: dispositivo físico de seguridad usado para acceder a recursos restringidos, usado como complemento o en lugar de contraseña.

Tráfico de red: Datos que se desplazan en la red, a los datos se los representan como paquetes.

Usuario root de Kali Linux: Tiene acceso de administrador en el sistema para ingresar a este se debe agregar el comando sudo -i luego escribir la contraseña y estará activo.

Usuario: un usuario es aquel que usa un servicio con limitaciones determinadas.

Volcado de datos: Registro no estructurado de la información que contiene la memoria.

Vulnerabilidades: Fallos de un sistema que pueden permitir que un usuario sin permisos acceda a la información y realice operaciones no permitidas.

VPN: Es una red privada virtual que permite la extensión segura de una red de área local a una red pública como internet.

Bibliografía.

McAfee. (julio de 2020). *https://www.mcafee.com/*. Obtenido de https://www.mcafee.com/enterprise/es-es/assets/reports/rp-quarterly-threats-july-2020.pdf

Asamblea Nacional. (2014). Obtenido de LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2016/04/Ley-Organica-del-Sistema-Nacional-de-Registro-de-Datos-Publicos.pdf

Asamblea Nacional. (2018). *Constitución de la República del Ecuador*. Obtenido de http://www.estade.org/legislacion/normativa/leyes/constitucion2008.pdf

Ascanio, J.G.A., R.A.B. Trillos, and D.W.R.J.T. Bautista. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. *19 (46)*, Pág 123-134.

Aumasson, J. P. (2017). *Serious Cryptography: A Practical Introduction to Modern Encryption*. San Francisco: No Starch Press.

Baca Urbina, G. (2016). *Introducción a la seguridad informática*. México: Patria.

Barrett, D., Weiss, M., & Hausman, K. (2015). *Exam Cram CompTIA security+ SY0-401*. Indiana: Pearson.

Bolfing, A. (2020). *Cryptographic Primitives in Blockchain Technology: A Mathematical Introduction*. Estados Unidos: Oxford University.

Congreso Nacional. (2002). Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

Congreso Nacional. (2004). Obtenido de Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP): https://www.seps.gob.ec/documents/20181/25522/LEY%20ORG%C3%81NICA%20DE%20TRANSPARENCIA%20Y%20ACCESO%20A%20LA%20INFORMACI%C3%93N%20P%C3%9ABLICA.pdf/57468b59-5cae-4e31-b46c-70f237bae386

Controlaría General del Estado. (2009). *Contraloria General del Esatado*. Obtenido de https://www.contraloria.gob.ec/WFDescarga.aspx?id=53&tipo=nor

Dalkir, K., & Katz, R. (2020). *Navigating Fake News, Alternative Facts, and Misinformation in a Post-Truth World*. Canada: IGI Global.

directory, T. 2. (2018). *http://www.27000.org/*. Obtenido de The 27000.org directory: http://www.27000.org/standards.htm

Dulaney, E., & Easttom, C. (2018). *CompTIA*. Indiana: Wesley.

Fernández Domingo, J. I. (2006). *La firma electrónica: Aspectos de la Ley 59/2003, de 19 de diciembre*. Madrid: Reus.

Gómez Fernández, L., & Andrés Álvarez, A. (2012). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes*. AENOR Ediciones (Asociación Española de Normalización).

Hamid, N. (2007). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*. Estados unidos: IGI Global.

Handschuh , H. (2005). *Familia SHA (algoritmo hash seguro). En: van Tilborg HCA (eds) Enciclopedia de criptografía y seguridad*. Bostón: Springer. doi:https://doi.org/10.1007/0-387-23483-7_388

Instituto Nacional de Ciber Seguridad (INCIBE). (09 de 12 de 2019). *INCIBE*. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/menos-mas-controla-el-acceso-informacion

INTECO-CERT. (2011). *RIESGOS Y AMENAZAS EN CLOUD COMPUTING*. Obtenido de https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

ISO, S. C. (2020). *https://www.iso.org*. Obtenido de ISO: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/fast_forward-es.pdf

Kaspersky. (2021). *Kaspersky*. Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kościelny, C., Kurkowski, M., & Sreb, M. (2013). *Modern Cryptography Primer: Theoretical Foundations and Practical Applications*. New York: Springer Science & Business Media.

Martínez, C. (2021). *Parque Científico y Tecnológo de Castilla - La Mancha*. Obtenido de https://pctclm.com/imediacomunicacion-5/

Migga Kizza, J. (2020). *Guide to Computer Network Security*. Chattanooga: Springer.

Mohamed, E. (2019). *Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments*. Cairo: Springer.

Mora, J. (2020). El Sistema de Gestión de Seguridad de la Información bajo la norma NTE ISO/IEC 27001 en Instituciones de Educación Superior en Ecuador. *ROCA, Vol 16*(1), Págs 546-559 ISSN: 2074-0735. RNPS: 2090. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7414351

NIEVES, A. C. (2017). *DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADOS EN LA NORMA ISO/IEC 27001:2013*. Obtenido de

https://alejandria.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Final.pdf?sequence=1&isAllowed=y

Özçelik, İ., & Brooks, R. (2020). *Distributed denial of service attacks: Real-world Detection and Mitigation*. India: CRC Press.

Romero Castro, M. I., Figueroa, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y al análisis de vulnerabilidades*. Alicante: Ciencias.

Singh, G., Vinod, M., & Anandh, V. (2018). *CCNA Security 210-260 Certification Guide*. Birmingham: Packt Publishing.

Smith, R. E. (2019). *Elementary Information Security*. Estados unidos: Jones & Bartlett Learning.

Whitman, M. E., & Mattord, H. J. (2009). *Principles of Information Security* (Tercera edición ed.). Canadá: Cengage Learning EMEA.

Wilson, A. (2019). *Lo esencial del hackeo: La guía para principiantes sobre hackeo ético y pruebas de penetración*. Estados unidos: Babelcube Inc.

Descubre tu próxima lectura

Si quieres formar parte de nuestra comunidad,
regístrate en https://www.grupocompas.org/suscribirse
y recibirás recomendaciones y capacitación

compAs
Grupo de capacitación e investigación pedagógica

@grupocompas.ec
compasacademico@icloud.com

Jéssica Alexandra Ponce Ordóñez, Ingeniera en sistema por la Universidad Técnica Estatal de Quevedo y Magister en seguridad informática por la Universidad Internacional de la Rioja. Profesora de la Universidad Técnica Estatal de Quevedo en la Facultad de Ciencias Empresariales. de asignaturas como Matemática, Cálculo diferencial e Integral, Estadística, Software para la investigación, Sistemas de información de auditoría, TIC (Tecnología de la información y la comunicación) aplicado a la mercadotecnia. Autora y coautora de varios artículos científicos como Análisis de clustering aplicado a los ataques informáticos en organismos de la salud, Caracterización de factores que influyen en la baja producción científica de las universidades usando análisis de redes sociales entre otros.
Correo electrónico: jponceo@uteq.edu.ec

Eduardo Amable Samaniego Mena, Ingeniería. Ingeniero en sistema por la Universidad Técnica Estatal de Quevedo y Magister en Conectividad y Redes de Ordenadores por la Universidad Técnica Estatal de Quevedo. Profesor de la Universidad Técnica Estatal de Quevedo en la Facultad de Ciencias de la Ingeniería en las asignaturas como Proyectos de Telecomunicación, Sistemas Operativos de Red, Seguridad Informática, Lógica Matemática y Métodos Estadísticos para las Telecomunicaciones. Autor y coautor de varios artículos científicos como Detección de picos de potencia en el consumo eléctrico residencial mediante análisis de datos, Towards measuring effectiveness in dynamic environments, Multimedia interactiva como apoyo para la terapia de infantes con dislalia entre otros, así como autor y coautor de libros como: Fundamento de informática y Fundamento de redes. Profesor Investigador de proyectos de investigación en ingeniería telemática, multimedia, TIC. Investigador acreditado del Senescyt con registro REG-INV-18-02827.
Correo electrónico: esamaniego@uteq.edu.ec

compAs
Grupo de capacitación e investigación pedagógica

@grupocompas.ec
compasacademico@icloud.com

ISBN: 978-9942-33-426-8

@grupocompas.ec
compasacademico@icloud.com

compAs
Grupo de capacitación e investigación pedagógica