Alfonso Aníbal Guijarro Rodríguez
Mirella Carmina Ortiz Zambrano
Jéssica Malena Yépez Holgín
Gustavo Fabián Vaccaro Witt

Seguridad Informática

APLICADA A ENTORNOS EMPRESARIALES

ColloQUIUM
Editorial - Centro de Formación

Seguridad Informática

APLICADA A ENTORNOS EMPRESARIALES

Ing. Alfonso Aníbal Guijarro Rodríguez, Mgs. Profesor con nombramiento de la Universidad de Guayaquil, Ecuatoriano, Ingeniero en Computación por la Escuela Superior Politécnica del Litoral, Posgrados: Máster en Docencia y Gerencia en Educación Superior por la Universidad de Guayaquil - Ecuador, Máster Universitario en Modelado computacional en Ingeniería por la Universidad de Cádiz - Escuela Politécnica Superior (Algeciras) – España. Profesor investigador, posee varios artículos regionales y de alto impacto, además desarrolla catedra en asignaturas como; Seguridad Informática, Sistemas Operativos, Sistemas Operativos Distribuidos, Organización y Arquitectura Computacional.

Abog. Mirella Carmina Ortiz Zambrano, MSc. Profesora contratada de la Universidad de Guayaquil, Ecuatoriana, Abogada de los Tribunales de la República del Ecuador por la Universidad de Guayaquil, Master en Administración Pública por la Universidad Tecnológica América de Guayaquil-Ecuador. Profesora investigadora, posee varios artículos científicos regionales y de alto impacto, dicta la asignatura de legislación informática, metodología científica.

Ing. Jéssica Malena Yépez Holguín, MCA. Profesora Contratada de la Universidad de Guayaquil, Ecuatoriana, Ingeniera Comercial por la Universidad de Guayaquil, Posgrados: Máster en Docencia y Gerencia en Educación Superior por la Universidad de Guayaquil, Máster en Contabilidad y Auditaría por la Universidad Laica Vicente Rocafuerte, Diplomado Superior en Docencia y Evaluación en la Educación Superior. Formación adicional: Metodología de la Investigación, Introducción a la Neurociencia y Neuroingeniería.

Dr. Gustavo Fabián Vaccaro Witt, PhD. Odontólogo por la Universidad de Guayaquil, Master en investigación Odontológica por la Universidad de Granada – España, Master en Gerencia Educativa por la Universidad de Guayaquil, Investigador del Instituto de Investigación Biomédica de Málaga-España (ibima), Laboratorio Inteligencia Computacional y Análisis de Imágenes.

Seguridad Informática

APLICADA A ENTORNOS EMPRESARIALES

Alfonso Aníbal Guijarro Rodríguez
Mirella Carmina Ortiz Zambrano
Jéssica Malena Yépez Holgín
Gustavo Fabián Vaccaro Witt

Seguridad Informática

APLICADA A ENTORNOS EMPRESARIALES

ColloQUIUM
Editorial - Centro de Formación

Alfonso Aníbal Guijarro Rodríguez
Mirella Carmina Ortiz Zambrano
Jéssica Malena Yépez Holgín
Gustavo Fabián Vaccaro Witt

Seguridad Informática aplicada e entornos empresariales
Editado por Colloquium
ISBN: 978-9942-814-11-1
Primera edición 2019

La obra fuer revisada por pares académicos antes de su proceso editorial, en caso de requerir certificación debe solicitarla a: sbores@colloquium-editorial.com.

Ecuador 2019

Contenido

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Prefacio

Este libro aborda una serie de temas que se plantean en el pensum que desarrolla la asignatura seguridad informática a nivel de pregrado en la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil. Los ejercicios descritos en esta obra, van en función de la experiencia personal de los autores, con el cual se intenta llevar a los estudiantes a prácticas reales bajo entornos controlados.

Otro motivo, es compartir experiencias profesionales con personas interesadas en afianzar conocimiento en el área de seguridad informática, considerando para ello metodologías probadas que sirvan de guía como es el caso de **defensa en profundidad**, esta metodología aborda la seguridad con un modelo en capas, además se aplica modelos de gestión de infraestructura de red, **modelo jerárquico** difundidos a través de los cursos de formación que ofrece cisco system.

A la espera que esta obra sea de completo agrado para los lectores y que la información descrita en ella se transmita como un valor agregado para los profesionales de IT.

La Unidad 1, define de forma general, varios conceptos de seguridad informática, todos ellos necesarios para comprender los temas de las unidades siguientes. También se describen los campos de acción de la seguridad informática y los mecanismos de seguridad empleados en los tipos de redes LAN Y WAN. Este capítulo concluye determinando el buen uso de las firmas digitales.

La Unidad 2, determina las políticas de seguridad basados en normas internacionales. Así como la implementación de seguridad local en sistemas operativos. Esta unidad aborda el manejo de herramientas de seguridad de mayor demanda del mercado para búsquedas de vulnerabilidades en sistemas operativos, además implementa criterios de seguridad local como implementar hardening en los sistemas Operativos y describe los principales ataques que sufren los sistemas operativos.

La Unidad 3, define tecnologías de seguridad aplicadas en ambientes de red empresarial, además determina la importancia de los protocolos en ambientes controlados, determina la importancia de la calidad de servicio, la disponibilidad en una red convergente, y finalmente se concluye dando a conocer el impacto de la misma en los negocios.

La Unidad 4, trata de evaluar y analizar los métodos de encriptación y la importancia que tienen estos para la seguridad en los correos electrónicos. Esta Unidad se introduce en temas relacionados a los algoritmos apropiados para ejecutar una encriptación, formula y desarrolla sus modelos de encriptación para transmitir los datos. La unidad concluye determinando la importancia de cifrar los datos en un canal seguro.

Introducción

Para los administradores de sistemas, queda claro que la tecnología presenta avances de una manera acelerada, por una parte los fabricantes dan a conocer soluciones integradas en un solo chasis, mientras que otros desarrollan software aplicable bajo plataformas compatible con arquitecturas de hardware y hay quienes llevan todo a la nube de información. Las tecnologías de la información y comunicaciones (TIC´S) al ser un recurso indispensable para una empresa está expuesta a continuas amenazas por ende es necesario aplicar contramedidas que logren mitigar el riesgo. (Rhodes-Ousley & Mark, 2013).

Los TIC´S han sustituido a los sistemas de información (Voutssas M, 2010); las empresas requieren utilizar tecnología actualizada donde intervienen complejas redes empresariales, locales y regionales o internet, siendo una de las principales formas que usa la empresa para realizar sus actividades económicas y empresariales, así como el uso de equipos de cómputos conformados principalmente de estaciones de trabajo y servidores, los cuales cada vez tienen mayor capacidad de procesamiento y de conexión.

Las TIC´S, al ser el activo más importantes de las empresas, son los que proveen los servicios y recursos a sus clientes y proveedores, además de ser la principal forma de administrar la información, estos deben ser preservados y asegurados de principio a fin, debido a que no existe solución (cura) instantánea a la inseguridad informática, sino de diversas formas, estrategias, y metodologías que permiten aplicar correctamente el termino de seguridad informática.

Este libro pretende servir de guía, para personas que deseen introducirse en temas de infraestructuras de redes, abarcando todas las áreas posibles de la seguridad informática, partiendo con conceptos ampliamente usados y pocos conocidos de seguridad informática, así como los mecanismos de seguridad implementados en redes LAN y WAN, políticas de seguridad, herramientas de búsqueda de vulnerabilidades, ataques, Hardening, y la importancia de los protocolos de comunicaciones.

CAPÍTULO 1

Seguridad

Seguridad, considerado un tema controversial, hay quienes se adentran a explorar el término y en su paso logran ver los alcances que este posee, reduciendo la brecha en esta obra, se analizan conceptos relacionados a seguridad informática y términos asociados, se pudo observar que hay una tendencia bien marcada de definiciones asociadas a seguridad informática, cuando se trata de proteger los datos de una empresa.

La seguridad informática (S.I), contempla en la actualidad un importante número de disciplinas y especialidades distintas y complementarias, se ha convertido en una pieza fundamental en el entramado empresarial, industrial y administrativo de los países.
La falta de una figura encargada de coordinar, planear y promover las actividades que tengan que ver con la S.I genera una situación que se ve reflejada en el crecimiento de problemas de seguridad que se presentan dentro de las instituciones, conocidos como incidentes. (Diaz, Perez, & Proenza, 2014)

La seguridad informática, o seguridad de la información, es la preservación de la confidencialidad, integridad y disponibilidad de la información. Esto se logra mediante la implantación de un grupo de controles que incluyen políticas, procedimientos, estructuras organizativas y sistemas de hardware y software. (Montesino Perurena, Baluja García, & Porvén Rubier, 2013).

La seguridad informática: La seguridad informática está relacionada con las metodologías, procesos y procedimientos para mantener salvaguardada la información y los datos confidenciales de una organización, al interior de los sistemas informáticos. Los procesos se estructuran con el uso de estándares, normas, protocolos y metodologías para mitigar y minimizar los riesgos asociados a la infraestructura tecnológica. (Solarte Solarte, Benavides Ruano, & Enriquez Rosero, 2015).

La seguridad de la información tiene por objeto proteger a los sistemas informáticos de las amenazas a los que están expuestos. Sin embargo, se considera un proceso complejo que conlleva tres aspectos: Gente, procesos y tecnología. Si estas variables no se evalúan y resuelven como partes de un todo, se obtiene como producto final un sistema vulnerable.

Seguridad se basa en libertad frente al miedo (conflictos, crímenes, guerras), libertad frente a las carencias (pobreza, degradación ambiental), y libertad para vivir una vida con dignidad (discriminación, intimidación) (Pérez & Castillejo, 2016).

Tendencias

Seguridad se define como un derivado de la inseguridad que percibimos en nuestro entorno que manifiesta la falta de protección contra las amenazas externas que nos privan de necesidades o derechos que nos permiten vivir una vida plena o sin preocupaciones.

UNIDAD 1 - Términos asociados a la seguridad Informática

Es imprescindible que los profesionales de IT conozcan los términos que se mostrarán en esta unidad, para poder identificar de manera correcta a individuos y a que actividades que realicen definiciones debería evitar porque podría repercutir en crímenes, en la actualidad el auge por los delitos informáticos está acompañado por las soluciones de seguridad que todas las empresas adquieren para mantener su activo más valioso los datos. Se presentarán las vulnerabilidades a las que empresas son expuestas por cada término, existen en la actualidad los que no tienen conocimientos de las actividades que se realizan para que tengan seguridad en sus sistemas, los que conocen a fondo los sistemas los atacan con la debida autorización del dueño/os para encontrar fallos o vulnerabilidades para proceder a disminuir la posibilidad a ataques informáticos y los que tienen un amplio conocimiento con todo lo que tenga que ver con hardware y software para lucrarse de ello causando daño a otras personas siendo estos criminales.

1.1 Conceptos básicos de seguridad informática

1.1.1 Luser

Término despectivo con el que los hackers se refieren a los usuarios comunes de los ordenadores en Internet. Proviene de dos palabras inglesas: loser (perdedor) y user (usuario) (J. Steiner, J. Neuman, 1988).

1.1.2 Newbie

Son aquellos usuarios que quieren llegar a ser hackers, pero en realidad solo tienen conocimientos generales sobre los ordenadores y para lograr su objetivo, se valen de tutoriales, sitios sobre hacking, software diseñado, etc. Hacker: es aquel que posee amplios conocimientos de redes (TCP/IP), sistemas operativos (Windows, Linux), programación (Java, ensamblador) (Setfree, 2015).

1.1.3 Geek

Habitualmente padecen de una versión aguda de neofilia es decir, sentirse atraídos, excitados y complacidos por cualquier cosa nueva). La mayor parte de los geeks, son hábiles con los ordenadores y entienden la palabra hacker como un término de respeto, pero no todos ellos son hackers (Pardo, 2013) .

1.1.4 Hacking

Conjunto de técnicas para acceder a un sistema informático sin autorización. Es decir, nombramos a alguien que tiene un amplio conocimientos, sobre técnicas de intrusión de sistemas (Adastra, 2012).

1.1.5 Hacker

Es un pirata informático que se infiltra para robar, modificar o destruir información, de un computador o de una red, posee conocimientos avanzados de sistemas informáticos (Alberto & Quispe, 2009). Es una persona, que se interesa por aprender cada día más sobre los sistemas y la manera de ir innovando las formas de intrusión. Los hackers se clasifican en tres grupos: Grey Hats, Black Hats y White Hats.

1.1.6 Greyhats

Son aquellos que tienen moral ambigua, es decir se encuentra en conflicto sin saber de qué lado de la ley estar, estos son aficionados con conocimientos intermedios (Benitez, 2016).

1.1.7 Blackhats

Es un término utilizado para aquellos que irrumpen la seguridad de la computadora, crean virus, entradas remotas no autorizadas por medio de redes de comunicación como Internet; lo cual hace que colapsen los servidores o los servicios de un sistema informático (Alberto & Quispe, 2009).

1.1.8 Lamer

Carecen prácticamente de conocimientos, se consideran psicológicamente perdidos, por ejemplo ayer quisieron ser 007, hoy hackers. Buscan información para presumir de ella o para plagiarla (Benitez, 2016).

1.1.9 Scriptkiddies

Gente que invade computadoras, usando programas escritos por otros, y que tienen muy poco conocimiento sobre cómo funcionan, causando daños a los sistemas (Alegsa, 2008).

1.1.10 Trashing

(Recogida de basura) Rebuscar en la basura, para encontrar algo que pueda ser útil a la hora de hackea (Seguridad Informática, 2009).

1.1.11 Sniffers o escaneadores de puertos

Son programas que se encargan de buscar claves en puertos que tienen una mínima seguridad (Ares, 2009).

1.1.12 Phreakers

Actividad en la cual están involucradas varias personas que tienen amplios conocimientos de sistemas telefónicos para ejecutar llamadas sin pago (Borghello, 2009b).

1.1.13 Carders

Este es un término que se usa para quienes hacen un uso ilegal de tarjetas de crédito, cuenta bancaria u otra información financiera (Doevan, 2016).

1.1.14 Phreaker

Es una persona que investiga los sistemas telefónicos, mediante el uso de tecnología, por el placer de manipular un sistema tecnológicamente complejo y en ocasiones también para poder obtener algún tipo de beneficio como llamadas gratuitas (Alegsa, 2008).

1.1.15 Cracker

Son aquellos expertos o aficionados en las nuevas tecnologías de la información que de forma consciente y voluntaria usan su conocimiento con fines maliciosos, antimorales o incluso bélicos, como intrusión de redes, acceso ilegal a sistemas gubernamentales, robo de información, distribuir material ilegal o moralmente inaceptable, piratería, fabricación de virus o herramientas de crackeo, es decir, usan sus conocimientos para el beneficio propio, para lucrarse o causar daños a un objetivo("Informática Hoy: Craker," 2010).

1.1.16 Pirata del software

El pirateo está en auge y es la causa más importante para obtener altos beneficios económicos perjudicando a sus autores, el volumen de pérdidas se ha convertido en un serio problema a combatir por ejemplo: el CD-ROM e Internet son dos de las plataformas más utilizadas para piratear (Alegsa, 2008).

1.1.17 Ciberokupa

Este término ha sido ampliamente usado en los medios de comunicación para referirse al registro de dominios de marcas comerciales de forma ilegítima, es una persona que se dedica a comprar y reclamar los derechos de determinados dominios de Internet relevantes o buscados por grandes empresas, celebridades emergentes u otros, con el fin de revendérselos a los interesados a un precio desorbitado, los ciberokupas registran nombres de páginas web muy parecidos a los originales.

1.1.18 Typosquatters

Consiste en prever los errores tipográficos más probables que cometerán los visitantes de direcciones URL famosas: por ejemplo, escribir "microsft" en lugar de "microsoft" (Alberto & Quispe, 2009).

1.1.19 bCiberpunk

Apuestan por aprender a hacer las cosas por sí mismos, llegan a defender la liberta de información a niveles extremos como podría ser la divulgación de manuales de construcción de bombas atómicas caseras o hacking sobre satélites, apoyándose en el principio de que la información en sí no es mala (seguinfo, 2013).

1.1.20 Copyhacker

En cuanto a ingeniería social, se trata del grupo más experto, pues su objetivo es aprovecharse de los propios hackers y que éstos les expliquen cómo crackear cualquier software o hardware.

Después, venden el software a los bucaneros, prácticamente son falsificadores sin escrúpulo que comercializan todo lo copiado, es decir, lo robado. (Borghello, 2009b).

1.1.21 Bucanero

Son peores que los Lamers, ya que no aprenden nada ni conocen la tecnología buscan el comercio negro de los productos entregados por los Copyhackers. Los bucaneros sólo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos "crackeados" pasan a denominarse "piratas informáticos" (Borghello, 2009).

1.1.22 Ingeniería social

Convencer a alguien, por diversos medios, para que nos facilite información útil para hackear, o para que haga algo que nos beneficie (Adastra, 2012).

1.1.23 Phiser

También se le llama Ingeniero Social. Es un hacker que se aprovecha de una de las más grandes vulnerabilidades que poseen los sistemas: los humanos. Habitualmente el Ingeniero Social, consigue contraseñas a través de aprovechar descuidos del personal, tales como dejar contraseñas escritas, llamar por teléfono haciéndose pasar por un servicio técnico, conectarse a puertos con contraseñas “default” o “test” para solicitar servicios o suponiendo contraseñas como “123” o “111” (Borghello, 2009b) .

1.1.24 Spammer

Son los responsables de los millones de correos basura, no solicitados que saturan cada día los buzones electrónicos de todo el mundo. En la actualidad, casi el 70% de todos los correos electrónicos que circulan en el mundo son spam, una auténtica plaga que puede llegar a dificultar el uso del correo electrónico como herramienta útil de comunicación (emred, 2015).

1.1.25 Superzapping

Se denomina superzapping, al uso no autorizado de un programa editor de ficheros para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de un ordenador (Alegsa, 2008).

1.1.26 Whitehats

Son aquellos que se introducen a la seguridad de los sistemas informáticos, normalmente depuran y arreglan errores en los sistemas, son conocidos como especialistas en seguridad de red (Benitez, 2016).

1.1.27 Samurai

Normalmente, es alguien contratado para investigar fallos de seguridad, también investiga casos de derechos de privacidad, está amparado por la primera enmienda estadounidense o cualquier otra razón de peso que legitime acciones semejantes. Los samuráis desestiman a los crackers y a todo tipo de vándalos electrónicos. También se dedican a hacer y decir cómo saber sobre la seguridad con sistemas en redes (Ecured, 2015), (Borghello, 2009b).

1.1.28 Sneaker

Es aquel individuo contratado por las empresas para romper los sistemas de seguridad de ellas, con la intención por parte de las empresas de subsanar dichos errores y evitar posibles ataques dañinos (tugurium, 1997).

1.1.29 Gurú

Se trata del experto en un determinado tema, por ejemplo conoce a profundidad alguna distribución de GNU/Linux. A un Gurú se le puede preguntar, cualquier cosa al respecto: es la opinión y palabra final (Borghello, 2009b).

1.2 Campos de acción de la seguridad informática

En la seguridad, cada día crecen las necesidades de proteger los sistemas informáticos, de tal manera que para cumplir dicho objetivo, se debe diseñar y crear una arquitectura; así mismo diseñar e implementar políticas que conlleven a desarrollar esquemas de seguridad que contribuyan a disminuir el nivel de vulnerabilidad que presentan las organizaciones en una red. Encontramos diferentes campos de acción de seguridad informática (Álvarez & Pérez, 2004).
En la seguridad informática, es importante que se consideren medidas preventivas a nivel de aplicaciones, antivirus, etc. que aseguren el sistema de información de pérdidas, modificación o daños en los sistemas.

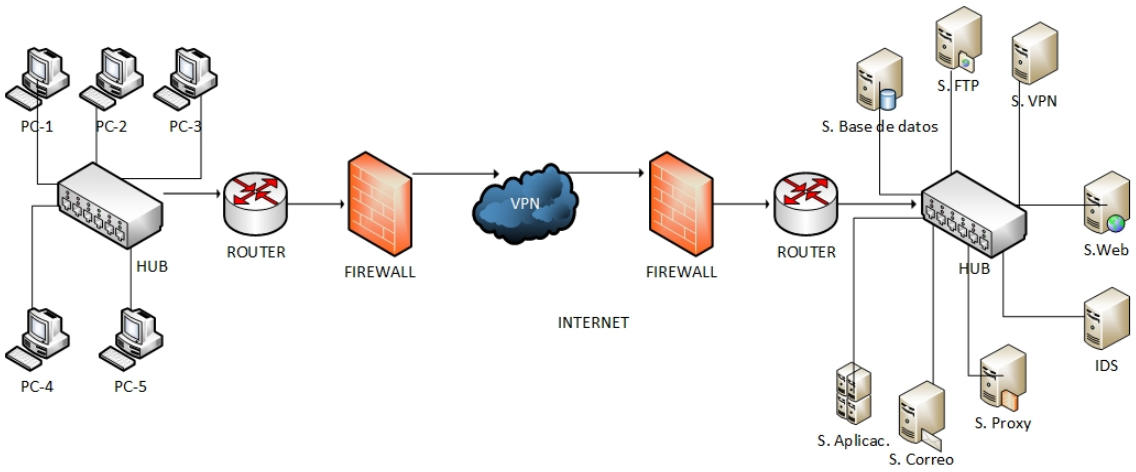


Figura 1. Campos de acción de la seguridad informática

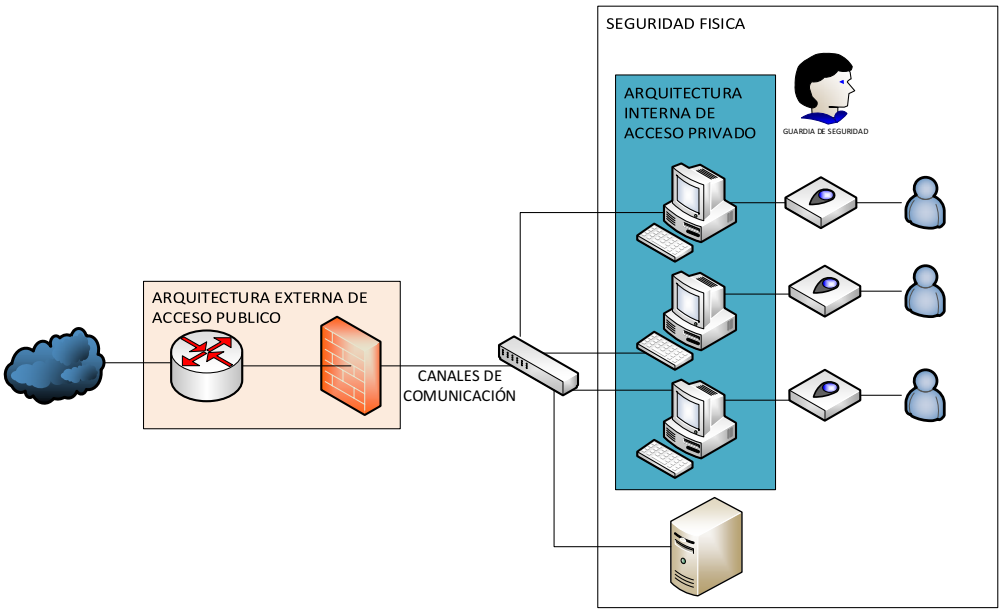


Figura 2. Ubicación de los campos de acción de seguridad informática

1.2.1 Canales de comunicación

El canal de comunicación es el vehículo que transporta loa mensajes de la fuente al receptor (Fernández Collado, 1997).

En esta área, se debe proteger los canales de comunicación externos, a través de cifrado de información, firmas digitales, VPN, entre otros, para lograr que los datos se transmitan de forma íntegra.

1.2.1.1 Arquitecturas externas de acceso público

Es importante proteger los sistemas de acceso público, como servidores web, correo, DNS, aplicaciones, entre otros. Estos servicios, se los protege mediante políticas de seguridad aplicada en servidores, routers, firewalls, IDS.

1.2.1.2 Arquitecturas internas de acceso privado

Protección de sistemas, redes y aplicaciones, implementando seguridad para host, redes, políticas de usuario, acceso a los datos de manera segura, protección mediante antivirus, etc.

1.2.2 Seguridad física de los sistemas informáticos

Punto considerado de mayor importancia debido a que permite implementar seguridad a los sistemas, se puede utilizar gabinetes cerrados, candados físicos a los escritorios, así como un control de acceso a los centros de datos con lectores biométricos con reconocimiento de voz, huellas, patrones oculares, etc.

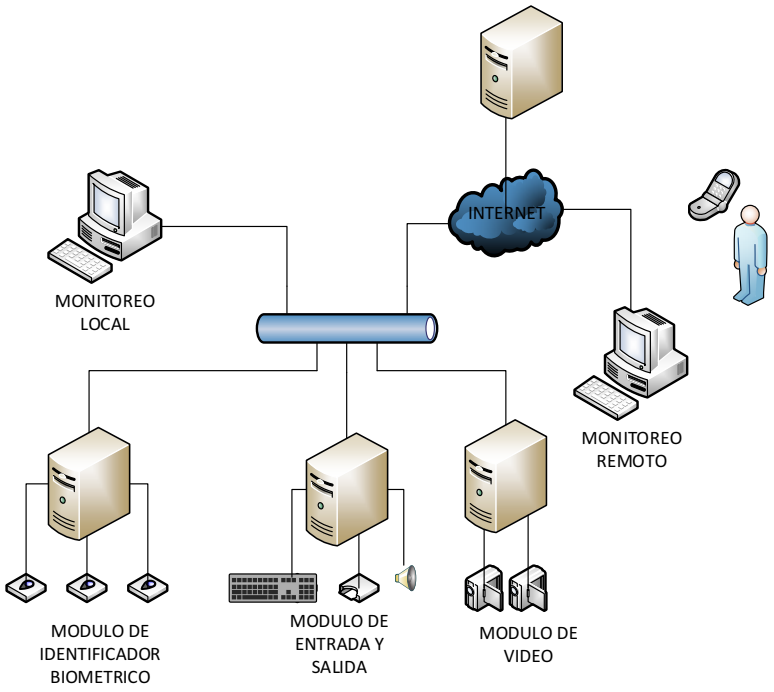


Figura 3. Ejemplos de seguridad física

En otro caso, es importante recalcar que las infracciones de seguridad afectan a las organizaciones de diversas formas:

- Pérdida de beneficios.
- Perjuicio de la reputación de la organización.
- Pérdida o compromiso de la seguridad de los datos.
- Interrupción de los procesos empresariales.
- Deterioro de la confianza del cliente.
- Deterioro de la confianza del inversor.
- Consecuencias legales: en muchos estados o países, la incapacidad de proteger un sistema tiene consecuencias legales.

1.2.3 Aspectos de seguridad

Tabla 1 Aspectos comunes a proteger

TIPO	EJEMPLOS
HARDWARE	Computadoras de escritorio y móviles. Routers y switches. Medios de Backup.
SOFTWARE	CD´s de instalación de Software. Imágenes de sistema operativo. Código de software propio.
DOCUMENTACIÓN	Políticas y procedimientos de seguridad. Diagramas de Red y edificios. Secretos.
DATOS	Información de empleados. Información de clientes.

1.2.4 Tipos de seguridad informática

1.2.4.1 Seguridad de Hardware

La seguridad de hardware, se puede relacionar con un dispositivo que se utiliza para escanear un sistema o controlar el tráfico de red. Los ejemplos más comunes incluyen cortafuegos o firewalls de hardware y servidores proxy. Otros ejemplos menos comunes incluyen módulos de seguridad de hardware (HSM), como se muestra en la Fig. 4, los cuales suministran claves criptográficas para funciones críticas tales como el cifrado, descifrado y autenticación para varios sistemas. De entre los diferentes tipos de seguridad informática, son los sistemas de hardware, los que pueden proporcionar una seguridad más robusta, además pueden servir como capa adicional de seguridad para los sistemas importantes (Valencia, 2016).

Figura 4. Asegurar los dispositivos de hardware

1.2.4.2 Seguridad de Software

La seguridad de software se utiliza para proteger los programas de ataques maliciosos de hackers y otros riesgos, de forma que siga funcionando correctamente. Esta seguridad de software es necesaria para proporcionar integridad, autenticación y disponibilidad (Valencia, 2016).

Los defectos de software tienen diversas ramificaciones de seguridad, tales como errores de implementación, desbordamientos de buffer, defectos de diseño, mal manejo de errores, etc. Con demasiada frecuencia, intrusos maliciosos pueden introducirse en los sistemas mediante la explotación de algunos de los defectos de software denominados vulnerabilidades.

1.2.4.3 Seguridad de red

La seguridad de red, se refiere a cualquier actividad diseñada para proteger la red. En concreto, estas actividades protegen la facilidad de uso, fiabilidad, integridad y seguridad de su red y datos. La seguridad de red efectiva se dirige a una variedad de amenazas y la forma de impedir que entren o se difundan en una red de dispositivos (Valencia, 2016).

Muchas amenazas a la seguridad de la red se propagan a través de Internet. Los más comunes incluyen:

- Virus, gusanos y caballos de Troya.
- Software espía y publicitario.
- Ataques de día cero, también llamados ataques de hora cero.
- Ataques de hackers.
- Ataques de denegación de servicio.
- Intercepción o robo de datos.
- Robo de identidad.

1.2.5 Amenazas de seguridad

1.2.5.1 Suplantación

La suplantación ocurre, cuando algún usuario logra falsificar su identidad haciendo pasar por otro usuario. Casos más usuales suelen ser la falsificación de mensajes de correo electrónico, reproducir paquetes de autenticación. (Chicanos, 2014)

1.2.5.2 Alteración

La alteración está basada en la modificación o cambios de datos, registros e información relevante de un sistema de información. Tales como reproducir paquetes de autenticación, alterar datos durante la transmisión, cambiar datos en archivos. (Chicanos, 2014)

1.2.5.3 Repudio

Esta amenaza procede de la negación de un empleado con respecto algún suceso. Eliminación de un archivo importante y denegar lo ocurrido, adquisición de un producto y denegar su adquisición. (Dussan, 2006)

1.2.5.4 Divulgación de información

La divulgación de información confidencial hacia personas ajenas a ella, terceras personas que no deberían poseer esa información. Mostrar la información en mensajes errados, divulgar el código de los sitios web. (Chicanos, 2014)

1.2.5.5 Denegación de servicio

Esta amenaza sucede cuando se nos imposibilita el acceso a los servicios de nuestro sistema de información, se lo relaciona con la saturación de datos. Sobrecargar una red con el envío excesivo de paquetes de sincronización, o con paquetes ICMP falsificados. (Dussan, 2006).

1.2.5.6 Elevación de privilegios

La elevación de privilegios hace referencia al uso de niveles superiores a usuarios que no deberían tener acceso. Usuarios finales con acceso a base de datos, Lograr la saturación de un búfer y conseguir accesos exclusivos en el sistema, obtener privilegios de administrador de un sistema de forma ilegítima. (Chicanos, 2014)

Hay que entender que no existe una solución única, para proteger los sistemas de una variedad de amenazas que existen, para esto, es necesario implantar varios niveles de seguridad, es decir, si uno falla, los demás siguen en pie. La seguridad de la red, se lleva a cabo a través del reforzamiento del hardware y software, para lo cual, se debe mantener actualizado los productos de software constantemente para lograr protegerlos de amenazas emergentes.

Un sistema de seguridad de la red, por lo general, se compone de muchos elementos todos ellos trabajan juntos, lo que minimiza el mantenimiento y mejora la seguridad.

1.2.5.6.1 Los componentes de seguridad de red incluyen:

- Antivirus y antispyware.
- Cortafuegos, para bloquear el acceso no autorizado a su red.
- Sistemas de prevención de intrusiones (IPS), para identificar las amenazas de rápida propagación, como el día cero o cero horas ataques.
- Redes privadas virtuales (VPN), para proporcionar acceso remoto seguro.

1.2.6 Defensa en profundidad

Se utiliza el término defensa en profundidad para denotar el uso de varias líneas de defensa consecutivas, en lugar de una única barrera muy fuerte (Benchimol, 2011).

Para reducir riesgo en un ambiente, se debe utilizar una estrategia de la defensa-en-profundidad para proteger recursos contra amenazas externas e internas, como podemos observar en la Fig. 5 que la red interna está protegida por un firewall de las amenazas externas. Este término es usado para describir las contramedidas de la seguridad para formar un ambiente cohesivo de seguridad, sin un solo punto de falla. Las capas de la seguridad que forman la estrategia de defensa-en-profundidad deben incluir medidas protectoras que implementen desde sus routers externos completamente a la localización de los recursos y a todos los puntos entre ellos (Álvarez & Pérez, 2004).

Se implementa seguridad, y se debe ayudar a asegurar una capa si se compromete la misma, Las otras capas proporcionarán la seguridad necesaria para proteger los recursos. Por ejemplo, el compromiso del firewall de una organización no debe proporcionar acceso del atacante a los datos más sensibles de la organización. Cada capa debe proporcionar idealmente diversas

formas de contramedidas para evitar que el mismo método de ataque sea utilizado en las diferentes capas.
Se debe invertir en una protección multi-vendor contra virus si es posible. También es necesario asegurarse de que la protección de virus esté configurada en diversos puntos como gateway, server, clientes etcétera.

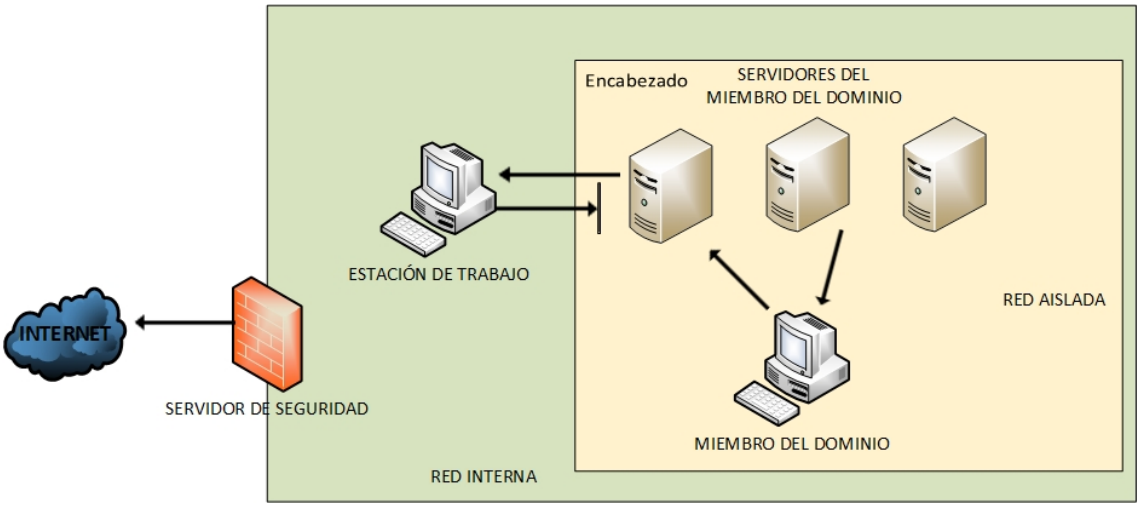


Figura 5. Diagrama de red de defensa en profundidad

1.2.6.1 Estructura de organización de la seguridad

Para reducir al mínimo la posibilidad de que un ataque contra una organización tenga éxito, se debe utilizar el mayor número posible de niveles de defensa. Defender una organización en profundidad implica el uso de varios niveles de defensa como se muestra en la Fig. 6. Si un nivel se ve comprometido, ello no conlleva necesariamente que también lo esté toda la organización. Como directriz general, se debe diseñar y crear cada nivel de la seguridad bajo el supuesto de que se ha conseguido infringir la seguridad.

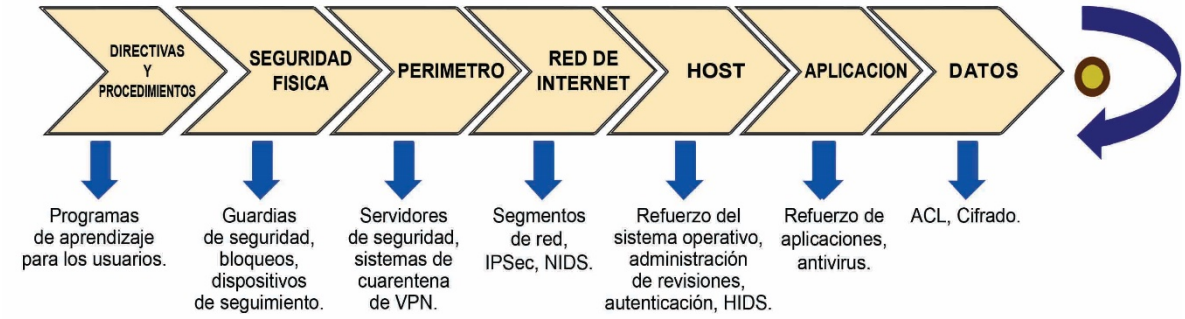


Figura 6. Organización de seguridad por niveles

1.2.6.1.1 Nivel de directivas, procedimiento y concientización

Siendo el primer nivel de la metodología de defensa en profundidad, es importante definir el interior de las empresas las políticas a seguir, todas ellas con la finalidad de definir reglas.

- Procedimiento a seguir para reparar equipo.
- Capacitación al personal no informático para crear conciencia, que permita elevar los niveles de seguridad por ejemplo: aumentar el nivel de complejidad de las contraseñas.

1.2.6.1.2 Nivel de seguridad física

Se puede utilizar una amplia variedad de técnicas para proteger una instalación. El grado de seguridad física disponible depende del presupuesto. Es fácil mantener estándares elevados cuando se trabaja con un modelo hipotético. Sin embargo, en el mundo real, las soluciones deben idearse en función del sitio, los edificios y las medidas de seguridad empleadas.

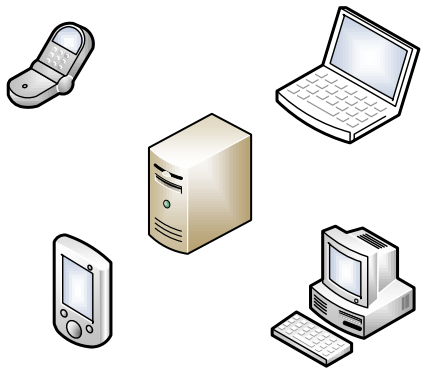


Figura 7. Descripción de la protección en el nivel de Seguridad Física

Muchas empresas toman como principal refuerzo de seguridad en los servidores, y dispositivos que pueden ser víctimas de ataques como se muestra en la Fig. 7 y no implementan un perímetro físico no tan seguro (Paloma, 2007).

¿Sabias que?

Toda señal de comunicación para propagarse necesita de un medio físico, sin este sería imposible establecer una comunicación.

A continuación, encontramos diferentes medidas de seguridad física que se deben tomar en cuenta:

- La defensa en profundidad comienza por aplicar una seguridad física a todos los componentes de la infraestructura. Si algún individuo no autorizado tiene acceso físico al entorno, éste no se puede considerar seguro. Por ejemplo, un técnico de mantenimiento podría cambiar un disco con errores en una matriz RAID1 que contenga datos de clientes. Es posible que el disco se pueda reparar. Los datos están ahora en manos de un tercero.

- El primer paso es, separar los servidores de los operadores humanos y los usuarios. Todas las salas de servidores deben estar cerradas con llave. El acceso a las salas de servidores debe estar controlado y registrado estrictamente. Algunos de los mecanismos de control de acceso que pueden aplicarse incluyen el uso de placas de identificación y sistemas biométricos. Un empleado de confianza debe organizar de antemano el acceso y autorizarlo. Si no existen salas especiales para los servidores, éstos se deben proteger en cabinas o, al menos, cerrarse bajo llave en los armarios. La mayor parte de los armarios de servidores se puede abrir con una llave estándar de modo que no debe confiar únicamente en las cerraduras que vengan de fábrica.

- Todas las salas de servidores deben disponer de algún tipo de mecanismo contra incendios: los incendios provocados constituyen una amenaza que requiere una medida preventiva.

- Utilizar dispositivos como candados magnéticos, camas de seguridad puertas de seguridad, etc. (Martinez, 2014).

- El acceso físico, se extiende a las consolas de administración remotas, además de a los servidores. No tiene sentido proteger directamente el acceso a los monitores y los teclados si los servicios de terminal pueden tener acceso a los servidores desde cualquier lugar de la red interna. Esta directriz, se aplica a las soluciones de monitor de vídeo de teclado (KVM, Keyboard Video Monitor) IP y también al hardware de administración remota.

  Existen tecnologías como DASH que son apropiadas para la administración remota de dispositivos de hardware (Sierra, 2017).

- Igualmente, es importante limitar las oportunidades que puedan facilitar que los usuarios, con buenas intenciones o no, infecten o pongan en peligro un sistema. Quitar los dispositivos de entrada de datos como las unidades de disquete y de CDROM de los sistemas que no los requieran.

- Por último, comprueba que todo el hardware de red está físicamente protegido. Si los servidores están protegidos en una sala o armario con cerradura, los enrutadores y conmutadores adjuntos también deben estar protegidos físicamente. De lo contrario, un intruso puede llegar fácilmente hasta un equipo portátil o de escritorio, y atacar a los servidores desde dentro del perímetro. Una vez más, se debe controlar la administración de los dispositivos de red; de lo contrario, pueden utilizarse para perpetrar un ataque contra el resto de la infraestructura (Coronel, 2014).

1.2.6.1.3 Nivel de perímetro

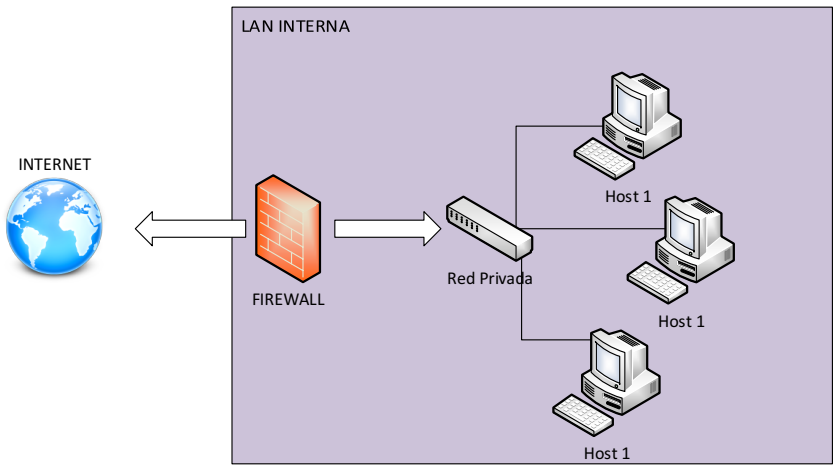


Figura 8. Seguridad Perimetral

La protección de los perímetros se puede llevar a cabo principalmente con servidores de seguridad de detectan ataques a la LAN como se muestra en la Fig. 8. La configuración de un

servidor de seguridad puede ser difícil desde el punto de vista técnico. Por lo tanto, los procedimientos deben detallar claramente los requisitos.

Los sistemas operativos recientes tanto de código libre y propietario facilitan el bloqueo de los puertos de comunicación innecesarios para reducir el perfil de ataque de un equipo.

- La traducción de direcciones de red (NAT, Network Address Translation) permite a una organización disimular las configuraciones de direcciones IP y de puertos internos para impedir que usuarios malintencionados ataquen los sistemas internos con información de red robada. Los mecanismos de seguridad del perímetro pueden ocultar también los servicios internos, incluso aquellos que están disponibles externamente, de modo que un intruso nunca se comunique de forma directa con ningún sistema que no sea el servidor de seguridad desde Internet.

Cuando los datos salen del entorno que está bajo la responsabilidad de uno, es importante que se encuentren en un estado que garantice su seguridad y que lleguen intactos a destino. Esto se puede conseguir mediante protocolos de túnel y cifrado, con el fin de crear una red privada virtual (VPN, Virtual Private Network).

El protocolo de túnel que emplean los sistemas de Microsoft, es el Protocolo de túnel punto a punto (PPTP, Point-to-Point Tunneling Protocol), que utiliza Cifrado punto a punto de Microsoft (MPPE, Microsoft Point-to-Point Encryption), o Protocolo de túnel de nivel 2 (L2TP, Layer 2 Tunneling Protocol), que utiliza el cifrado de IPSec.

Cuando los equipos remotos establecen comunicación a través de una VPN, las organizaciones pueden seguir pasos adicionales para examinar esos equipos y garantizar que cumplan una directiva de seguridad predeterminada. Los sistemas que establecen la conexión se aíslan en un área independiente de la red hasta que se completan las comprobaciones de seguridad.

Los sistemas del perímetro también deben tener usos claramente definidos. Bloquear o deshabilitar cualquier otra funcionalidad.

- Un ejemplo de firewall de perímetro es el Firewall de Windows, que se incluye desde las versiones de inicio, con la cual se puede extender la protección del perímetro a los usuarios remotos.
- La protección del perímetro de una red, es el aspecto más importante para parar un ataque del exterior. Si un perímetro sigue siendo seguro, la red interna se debe proteger contra ataques externos. Se enumeran abajo algunas maneras de implementar la defensa del perímetro: Packet Filtering es una técnica que se implementa en los firewall para controlar el Acceso de paquetes, Inspección de paquetes, Intrusion Detection como se muestra en la Fig. 9,10.

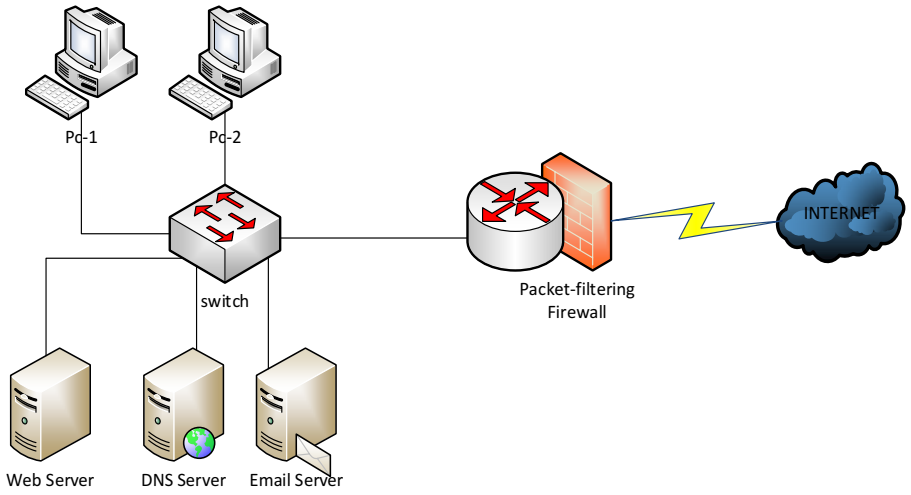


Figura 9. Ejemplo Packet Filtering

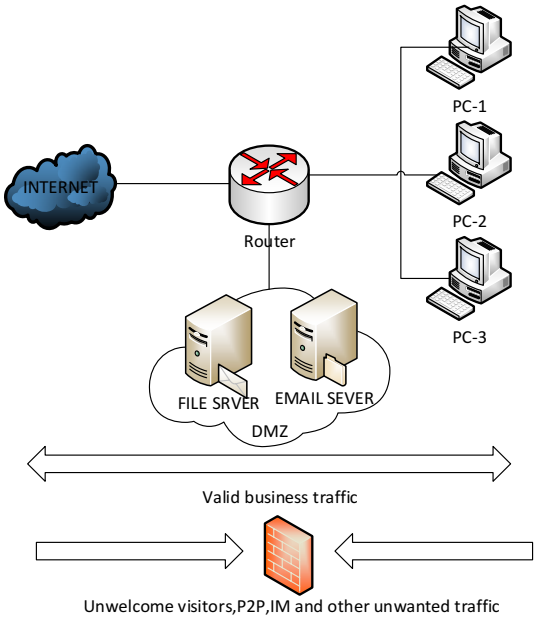


Figura 10. Inspección de paquetes con firewall

1.2.6.1.4 Nivel de red interna

Uno puede tener una serie de redes en su organización y debe evaluar cada una individualmente para asegurarse de que está asegurada apropiadamente como se muestra en la Fig. 11.

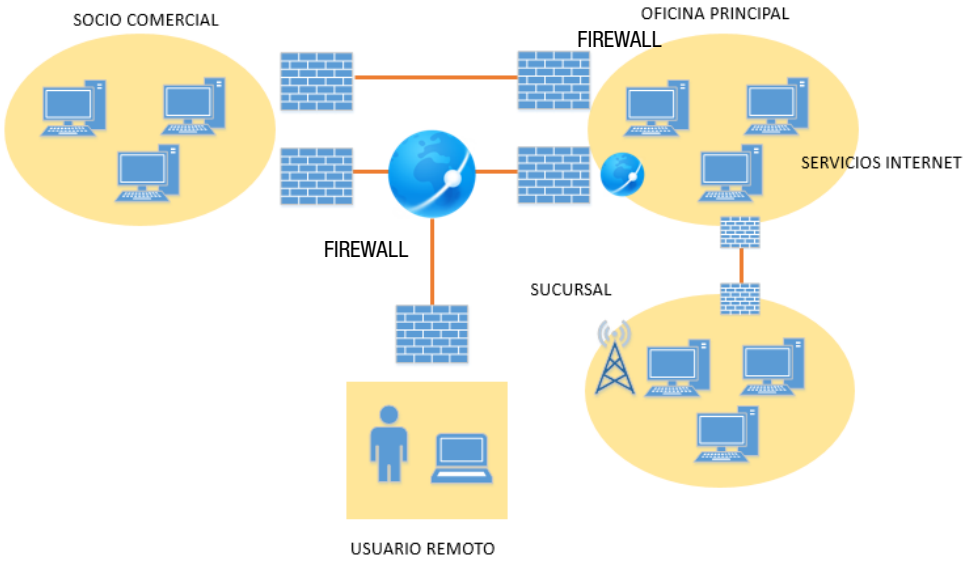


Figura 11. Seguridad de red interna

Se enumeran abajo algunas maneras de implementar defensas de red:

- VLAN, Access Control Lists, Internal Firewall, Auditing, Intrusion Detection.

- Para proteger el entorno de la red interna, se debe requerir que cada usuario se autentique de forma segura en un controlador de dominio y en los recursos a los que tenga acceso. Utilizar la autenticación mutua, de modo que el cliente también conozca la identidad del servidor, con el fin de impedir la copia accidental de datos a los sistemas de los intrusos.

- Segmentar físicamente los switch o conmutadores, es decir, crear particiones de la red para impedir que toda ella esté disponible desde un único punto. Se puede crear particiones si se utilizan enrutadores y conmutadores de red independientes o si crean varias redes virtuales de área local (VLAN, Virtual Local Área Network) en el mismo conmutador físico como se muestra en la Fig.12.

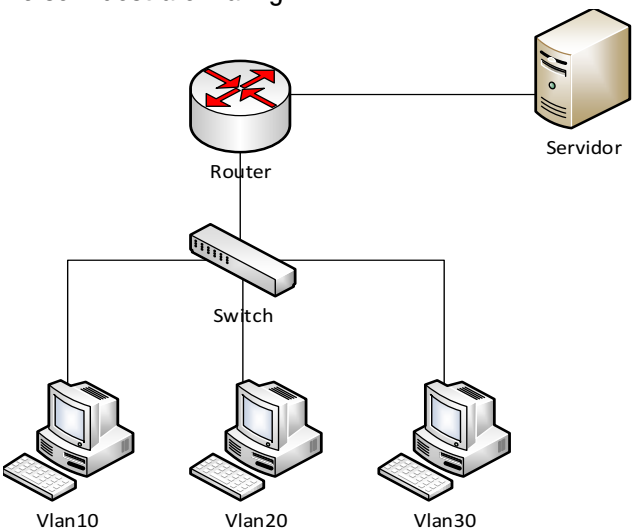


Figura 12. Ejemplo de una Vlan Segmentada y enrutamiento

- Considerar cómo se van a administrar los dispositivos de red, como los conmutadores. Por ejemplo, el grupo de trabajo de red podría utilizar Telnet para tener acceso a un conmutador o enrutador y realizar cambios de configuración.

> **¿Sabias que?**
> Telnet pasa todas las credenciales de seguridad en texto sin cifrar. Esto significa que los nombres y las contraseñas de los usuarios son accesibles para cualquiera que pueda rastrear el segmento de red. Esto puede constituir una debilidad importante de la seguridad.

- Considerar permitir únicamente el uso de un método seguro y cifrado, como SSH de shell o acceso de terminal serie directo.

1.2.6.1.5 Nivel de host

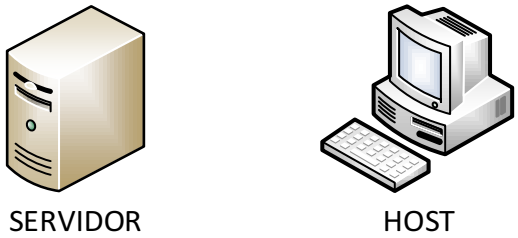


Figura 13. Protección nivel de host

En la Fig. 13 se muestra un servidor que debe crear las políticas que limitan las tareas que se tienen que realizar y cada Host se debe evaluar en su ambiente. Esto crea otra barrera de seguridad que un atacante necesitaría evitar antes de hacer cualquier daño. Server Hardening, Host Intrusion Detection, IPSec Filtering, Auditing (Álvarez & Pérez, 2004).

- Tanto en los sistemas cliente como en los servidores, las técnicas de refuerzo dependerán de la función del equipo. En cada caso, se pueden utilizar plantillas de seguridad y plantillas administrativas con directivas de grupo para proteger estos sistemas.

- En los sistemas cliente, también se pueden utilizar directivas de grupo, para restringir los privilegios de los usuarios y controlar la instalación de software. El uso de directivas de grupo para limitar las aplicaciones que un usuario puede ejecutar impide que éste, ejecute de forma inadvertida código de tipo Caballo de Troya.

- En los sistemas de servidor, las técnicas de refuerzo también incluyen la aplicación de permisos NTFS, la configuración de directivas de auditoría, el filtrado de puertos y la realización de tareas adicionales según la función del servidor.

- Mantener el servidor y el cliente actualizados con respecto a las actualizaciones mejora la seguridad. Microsoft proporciona varias formas de aplicar revisiones a los sistemas, por

ejemplo, mediante Windows Update, Software Update Service y Microsoft Systems Management Server (SMS).

- La utilización de un paquete antivirus y de un servidor de seguridad personal, como Firewall de Windows, disponible con los sistemas operativos, puede reducir la parte expuesta a un ataque de un equipo cliente.

1.2.6.1.6 Nivel de aplicación

Como capa de defensa, Application Hardening, es una parte esencial de cualquier modelo de seguridad. Cada aplicativo en una organización debe ser probado a fondo para la conformidad de seguridad en un ambiente de prueba antes de que se permitir su puesta en producción como se muestra en la Fig. 14.

Validation Checks, Verify HTML / Cookies Source, Secure IIS.

¿Sabías que?

La capa de aplicación tal vez sea el nivel donde mayor cantidad de protocolos existen.

- Las instalaciones de las aplicaciones sólo deberían incluir los servicios y funcionalidad requeridos.

- Las aplicaciones desarrolladas internamente, se deben evaluar para descubrir vulnerabilidades en la seguridad de una forma continuada y deben desarrollarse e implementarse revisiones para cualquier vulnerabilidad que se identifique.

- Las aplicaciones que se ejecutan en la red se deben instalar de forma segura y se les deben aplicar todas las revisiones y Service Packs correspondientes.

- Debe ejecutarse software antivirus para ayudar a impedir la ejecución de código malintencionado.

- Si una aplicación se ve comprometida, es posible que el intruso pueda tener acceso al sistema con los mismos privilegios con los que se ejecuta la aplicación. Por lo tanto, ejecutar los servicios y aplicaciones con el menor privilegio necesario.

- Al desarrollar nuevas aplicaciones personalizadas, implementar las recomendaciones más recientes de ingeniería de seguridad.

Figura 14. Protección a Nivel de aplicación

1.2.6.1.7 Nivel de datos

- EFS permite el cifrado de los archivos cuando residen en el sistema de archivos. Se basa en el formato NTFS del disco, que está disponible desde Windows 2000. Es importante entender que EFS no cifra los archivos mientras se están transmitiendo a través de una red. El proceso de cifrado utiliza una clave para cifrar el archivo y la tecnología de claves pública y privada para proteger dicha clave.

- NTFS también proporciona seguridad en los archivos y en las carpetas. De este modo, se permite la creación de listas de control de acceso para definir quién ha obtenido acceso a un archivo y qué acceso tiene.

- El aumento de la protección del nivel de datos debe incluir una combinación de listas de control de acceso y cifrado. Al cifrar un archivo, únicamente se impide la lectura no autorizada; no se evita ninguna acción que no requiera la lectura del archivo, como la eliminación. Para impedir la eliminación, utilice listas de control de acceso.

- Puesto que los datos son esenciales en muchos negocios, es importante que su recuperación sea un proceso conocido y probado. Si se realizan copias de seguridad con regularidad, cualquier alteración o eliminación de datos, ya sea accidental o malintencionada, puede recuperarse a partir de las copias de seguridad cuando corresponda. Un proceso confiable de copia de seguridad y restauración es vital en cualquier entorno.

- Proteger las cintas de copia de seguridad y restauración. Las copias de las cintas de copia de seguridad y restauración se deben mantener en otro lugar, en una ubicación segura. El acceso no autorizado a las cintas de copia de seguridad es igual de dañino que infringir la seguridad física de la infraestructura.

- Las listas de control de acceso sólo funcionan en documentos dentro del sistema de archivos para estos se habiliten. Una vez que se han copiado los documentos a otra ubicación (disco local de un usuario), no se sigue controlando el acceso. Windows Rights Management Services (RMS), que se incluye con Windows Server 2003, mueve la función de control de acceso al propio objeto de forma, que dicho control se aplica independientemente de dónde se almacene el documento físico como se muestra en la Fig. 15. RMS también ofrece a los creadores de contenido un mayor control sobre las acciones particulares que un usuario tiene permitido llevar a cabo; por ejemplo, el destinatario puede tener concedido acceso para leer un documento, pero no para imprimir, copiar o pegar; en

el correo electrónico enviado por Microsoft Outlook, el remitente del mensaje puede impedir que los destinatarios reenvíen el mensaje.

Figura 15. Protección a Nivel de datos

1.3 Mecanismos de seguridad empleados en redes lan y wan

En esta sección se describirá las herramientas técnicas que se utilizan para implementar seguridad.

1.3.1 Protección de los dispositivos de interconexión

Switch

- Los switch de gama media-alta en adelante ofrecen la creación de redes virtuales dentro de un único dispositivo, esta opción permite evitar crear ataques de MAC Spoofing (Álvarez & Pérez, 2004).
- Además, permite activar opciones de prevención de crear de direcciones falsas.
- Utilizando tablas caché ARP de manera estáticas, de forma que no existe caché dinámica, cada entrada de la tabla mapea una dirección MAC y su debida dirección ip.
- Pueden interconectar dos o más segmentos de red en base a una dirección física de origen y destino.
- Permiten configurar y administrar VLANs, Port Mirroring, QoS (IEEE 802.1p).

En la Fig. 16 se muestra un switch que permite interconectar redes operando en la capa 2 o nivel de enlace de datos.

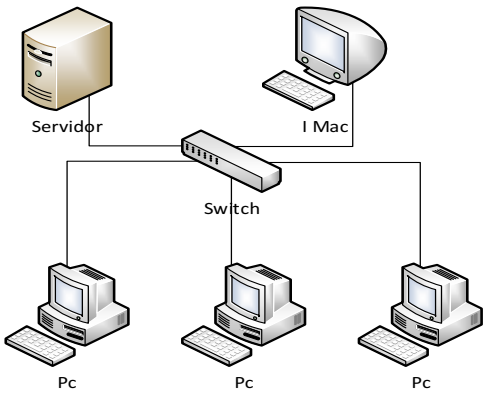


Figura 16. Conexión de un switch

Router

Los routers tienen las características de un computador, porque cuentan con memoria, procesador y se pueden ir ampliando sus interfaces a medida que se las requiere(Vázquez, 2005), no todos cuentan con toda esta funcionalidad, pero esto depende de su uso.

Según afirma (Álvarez & Pérez, 2004), los routers nos permiten direccionar el tráfico entre diferentes redes como se muestra en la Fig. 17. A continuación, se da relevancia a varios parámetros.

- Protocolos de routing seguros.
- Entrada de redes de manera estática para evitar ser engañados.
- Permite filtrar tráfico por dirección IP y puerto no deseados.

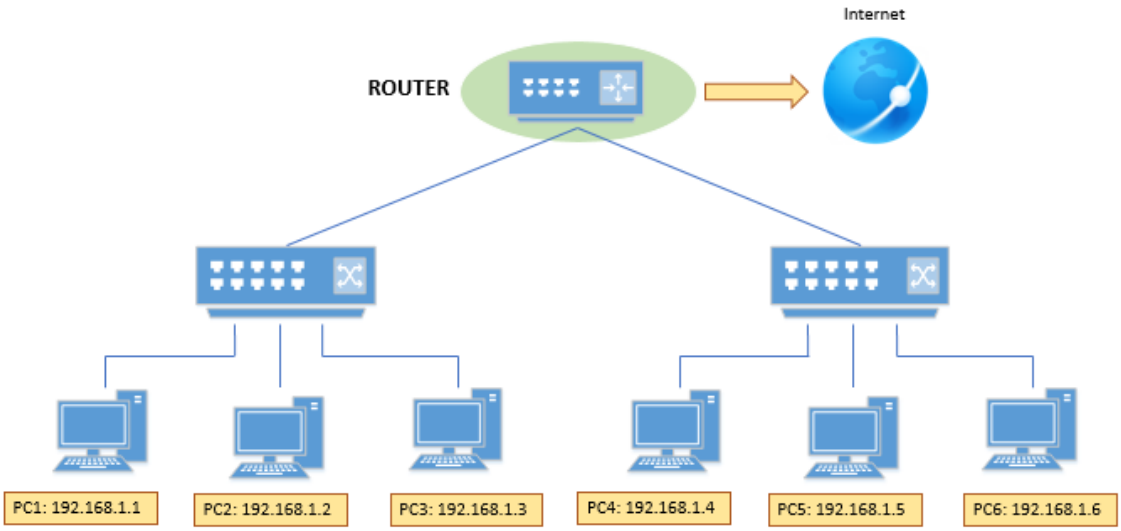


Figura 17. Conexión de un Router

1.3.2 Protección de redes inalámbricas

Implementar políticas de bloqueo a un sistema protegido por PIN, ante un número reiterado de intentos fallidos.

También se puede destacar que el límite de perímetro de protección, se debe proteger el acceso a los sistemas asegurando todo el cableado en las redes físicas, y en las redes inalámbricas se debe proteger el aire(Álvarez & Pérez, 2004).

1.3.3 Redes privadas virtuales

Las redes privadas virtuales, nos permite acceder a un servidor que se encuentra en una red privada empleando una infraestructura adecuada, lo cual la tiene que proporcionar una red pública como se muestra en la Fig. 18 (Microsoft, 2012).

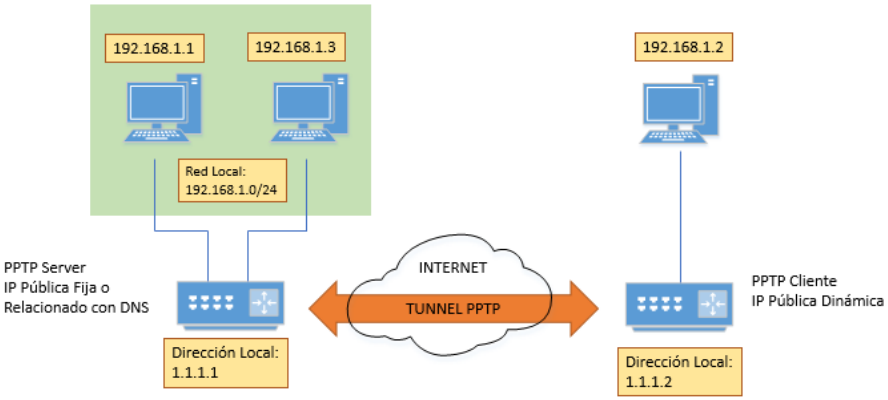


Figura 18. Diseño de redes privadas virtuales

1.3.4 Filtrado mediante firewall

Según (Pello Altadill, 2003), un firewall es un dispositivo que filtra el tráfico entre redes, como mínimo dos. Este puede ser físico o un software sobre un sistema operativo.

Además, este un mecanismo de seguridad indispensable en todo sistema de seguridad ya que ofrece los siguientes servicios como se muestra en la Fig. 19 (Álvarez & Pérez, 2004).

- Mediante el Aislamiento de internet, se restringe el acceso hacia/desde su red sólo a ciertos servicios, se analiza todo el tráfico que pasa a través de él.
- A través de un sistema de detección de intrusos, ayudará a alertar cuando se detecta conexiones anomalías.
- Auditar todos los registros de actividad entre la red exterior y la interior.

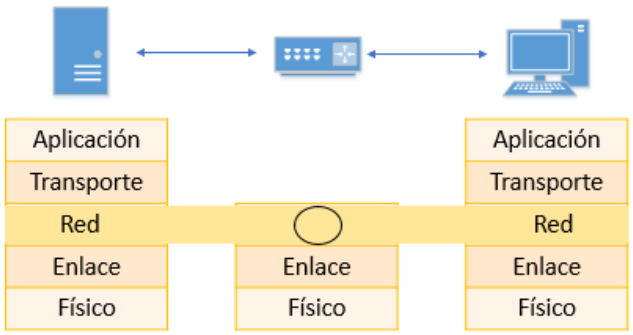


Figura 19. Filtrado de paquetes a nivel de red

Los cortafuegos de filtrado de paquetes se comportan como dispositivos de encaminamiento de paquetes entre las máquinas internas y externas, pero de forma selectiva.

- Dirección IP de origen del paquete.
- Dirección IP destino del paquete.

- El tipo de tráfico: TCP, UDP, ICMP, etc.
- Algunas características del nivel de transporte, como el número de puerto de origen o de destino.
- Propiedades internas de los paquetes
- Filtrado de contenido en páginas web
- Bloqueo de todos los archivos adjuntos o de algunas extensiones en los mensajes de correo electrónico, tanto entrantes como salientes.
- Escaneo y borrado de virus.
- Bloqueo de comandos y contenido específicos de las aplicaciones.
- Bloqueo de contenidos Web: páginas de ocio, entretenimiento, entre otros.

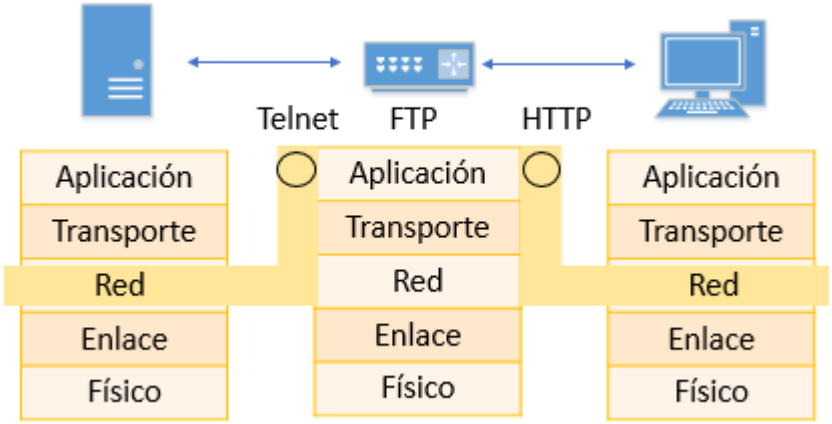


Figura 20. Filtrado a nivel de aplicación

1.3.5 Sistema de detección de intrusos

Es un sistema que permite la detección de accesos no autorizados a un determinado host o a una red, en el siguiente listado se describen el funcionamiento.

- Realizan en inspección permanente identificando posibles ataques.
- Detectan acciones sospechosas contra los servidores.
- Permiten mantener en estado exacto de los registros de la base de datos (Integrity Check), para de esta manera, poder identificar si los datos han sido modificados.
- Todos los archivos que ingresan tienen un control alto de examinación para identificar si no se trata de algún virus.

Además podemos destacar que los sistemas detección de intrusos los podemos clasificar de la siguiente manera(Borghello, 2009b).

1. Detector de intrusos basado en un host.
2. Detector de intrusos basado en red.
3. Detector de intrusos basados en conocimiento.
4. Detector de intrusos basados en la conducta.

Los IDS detectan, cuáles son las posibilidades de infiltraciones, que se pueden encontrar en el núcleo del Sistema Operativo, para de esta manera salvaguardas los recursos de una red.

HIDS (Host IDS)
Protege contra un Host (Servidor o PC). Posibilita la monitorización de gran cantidad de eventos para un posterior análisis detallado de las actividades sospechosas de manera que se determina con precisión cuan involucrados se encuentran los usuarios en una determinada acción. Todo ello ocurre en modo local, dentro del propio sistema.
NIDS (Net IDS)
Protege un sistema basado en red. Son sniffers del tráfico de red, ya que capturan los paquetes de red y los analizan, normalmente en tiempo real, según las reglas con las que ha sido configurado en busca de algún tipo de ataque.
DIDS (Distributed IDS)
Protege un sistema con una arquitectura basada en cliente-servidor formada por un conjunto de NIDS que actúan recopilando toda la información en una base de datos central como se muestra en la Fig. 21. La ventaja de este sistema es que cada NID se puede configurar con las reglas específicas de control que se aplicarán a un determinado segmento de red.

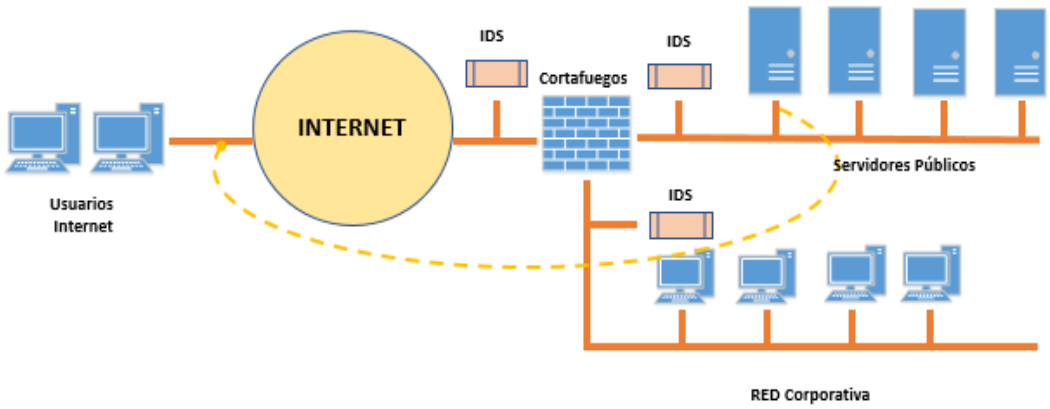


Figura 21. Detector de intrusos

1.3.6 Sistemas anti-sniffers

Estos programas sirven para verificar el estado actual de la placa de red, para detectar de qué manera está actuando y todo el tráfico que pasa sobre ella como se muestra en la Fig. 22 (Borghello, 2009b).

Además evita que estos programas evitar que se chequee todo lo que va dirigido a una dirección MAC(Semanat, 2008).

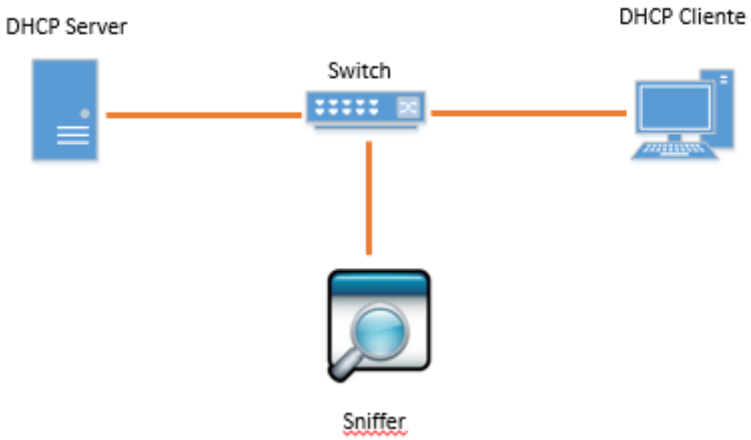


Figura 22. Detector de Sniffer

1.3.7 Gestión de claves

Las claves se deben proteger y toda la responsabilidad recae sobre el administrados debido a que este debe implementar diferentes políticas para que no se comprometa todo el sistema de red (Klein, 1999).

Así también como incorporar gestión y protección de las contraseñas, por ejemplo, número de intentos fallidos, longitud mínima, restricciones de formato, expiración de contraseñas y ataque preventivo.

1.3.8 Seguridad de protocolos y servicios

El adecuado uso de los protocolos de comunicaciones de acuerdo al objetivo y su funcionamiento. Verificar las posibles puertas de entrada como fuentes de ataque.

1.3.9 Cifrado de datos

Transformar un mensaje inteligible en otro que no lo es, para después devolverlo a su forma original, sin que nadie vea el mensaje cifrado sea capaz de entenderlo.

La importancia del uso de basa en la mantener la privacidad, la integridad, la autenticidad de los datos (Lucena López, 1999).

A continuación, presentamos un ejemplo del sistema de Criptografía Simétrica AES como se muestra en la Fig. 23.

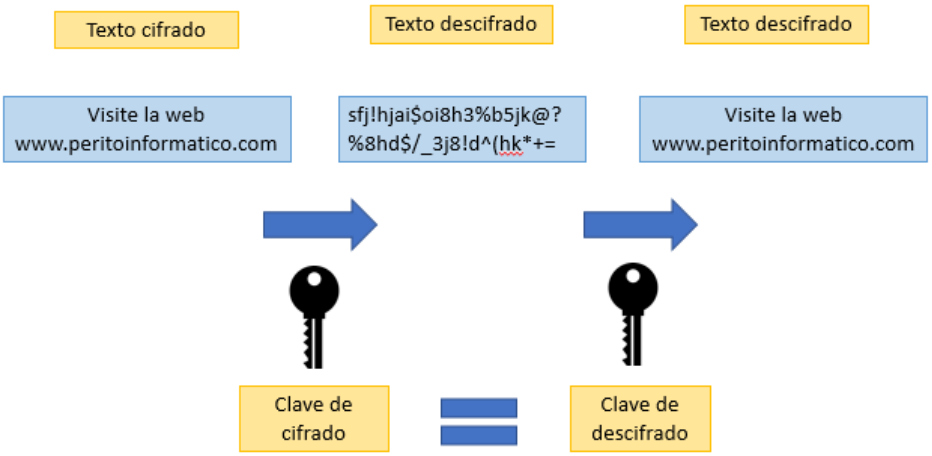


Figura 23. Funcionamiento de Criptografía Simétrica AES

1.3.10 Access control list (acl)

Permiten definir permisos a usuarios y grupos concretos. Por ejemplo, pueden definirse sobre un Proxy una lista de todos los usuarios (o grupos de ellos) a quien se le permite el acceso a Internet, FTP, etc. También podrán definirse otras características como limitaciones de anchos de banda y horarios (Lucena López, 1999).

Las listas de acceso estándar se deben colocar cerca del destino y colocar cerca de la fuente como se muestra en la Fig. 24.

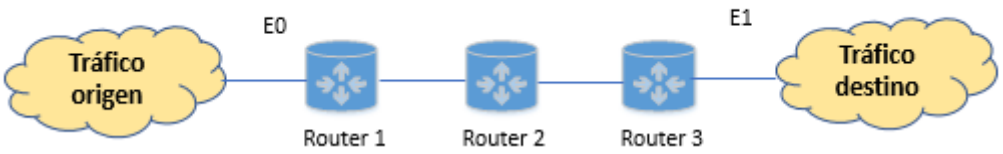


Figura 24. Lugar donde se aplican las ACL

En este caso es bloquear el tráfico del origen al destino, mejor aplicar una ACL entrante a E0 en el router 1 en vez de una lista saliente a E1 en el router 3.

1.4 Buen uso de firmas digitales

Primeramente, explicaremos que es una firma digital. Es una reducida cantidad de datos que fue creada utilizando para ello una clave privada, y donde puede ser utilizada una clave pública para verificar que dicha firma fue realmente generada utilizando la clave privada correspondiente(Álvarez & Pérez, 2004). El algoritmo a utilizar para generar la firma, debe funcionar de manera que sin conocer la clave privada sea posible verificar su validez como se muestra en la Fig. 25.

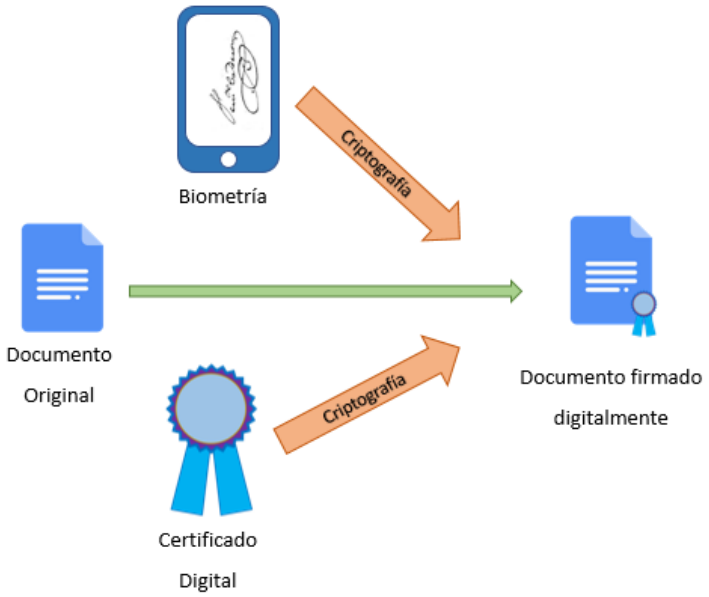


Figura 25. Esquema simple de firma digital

Uso de las firmas digitales

- Por medio de la autentificación nos permite verificar que el mensaje recibido viene realmente de quien dice ser el remitente (asumiendo que el remitente conoce la clave privada) que se corresponde a la clave pública utilizada para la verificación.

- Certificar que una clave pública pertenece a una entidad en particular. Esto se hace firmando con una combinación de la clave pública y la información sobre su propietario, a la estructura de datos resultante se la llama frecuentemente **Certificado de Clave-Pública (o simplemente Certificado)**.

La firma digital de un documento cualquiera es generalmente generada calculando un mensaje resumido de que se desprenda del documento y concatenándolo con información sobre el firmante, sello de momento, etc. Esto puede ser hecho aplicando la función de hash a los datos. La cadena resultante se encuentra entonces encriptada utilizando la clave privada del firmante utilizando un algoritmo adecuado. El bloque de bits resultante es la firma. Generalmente se distribuyen en conjunto con la información de la clave pública que fue utilizada para firmarlo (Álvarez & Pérez, 2004).

Para verificar una firma, el receptor primero deberá determinar si la clave pertenece a la persona que se supone debe pertenecer (utilizando un certificado o conocimiento previo), y luego desencripta la firma utilizando la clave pública de la persona. Si la firma se desencripta debidamente y la información concuerda con la del mensaje (resumen de mensaje apropiado) la firma es aceptada como válida. Además de la autentificación, esta técnica provee integridad de datos, lo que significa que cualquier alteración de la información durante su transmisión es detectada (Álvarez & Pérez, 2004).

1.4.1 Certificado digital

Se trata de documentos electrónicos cuya misión consiste en garantizar la identidad de su titular, los certificados digitales contienen de forma estructurada información relevante acerca de su portador y de la entidad que lo emitió.

A continuación, nombraremos los tipos de certificados:

1.4.1.1 Certificado de servidor

Permiten la identificación de los servidores que utilizan canales de comunicaciones seguras con SSL. Mediante la presentación del certificado, los servidores garantizar la autenticidad, integridad y confidencialidad de la comunicación entre el navegador del cliente y el servidor (MARKUP, 2017).

1.4.1.2 Certificados personales

Sirven para validar la identidad de los individuos en sus operaciones, dentro de una institución a la que pertenece y se incluye una tarjeta de con chip criptográfico (CSCU, 2017) .

1.4.1.3 Certificados de explorar Web

Aunque poco usado en la actualidad en internet, sirven al propósito de autenticar a sus titulares ante servidores Web remotos a través de canales SSL. Antes de crearlos, la autoridad verifica que los solicitantes son quienes dicen ser, además de cumplir con una normativa estricta en el proceso de estos certificados (Osi, 2012).

1.4.1.4 Certificados de correo electrónico

Estos certificados son la identidad digital en internet, ya que permiten autentificar, firmar y encriptar emails y documentos electrónicos, garantizando así la confidencialidad de sus mensajes (MARKUP, 2017).

1.4.1.5 Certificados de edición de software

Se utilizan para la firma de software distribuida a través de internet. Su objetivo es resolver el grave problema de inseguridad y desconfianza al que se enfrentan los usuarios cuando adquieren software, gratuito o de pago, a través de internet. Este certificado se emite a personas jurídicas responsables de la edición, publicación o distribución digital de software (*applets, scripts,* etc.) para su firma (CSCU, 2017).

1.10.1.6 Certificados de entidad emisora de certificados

Aquí trabajan dos tipos de certificados digitales como, las autoridades raíz y las autoridades subordinadas; las autoridades raíz se certifican a sí mismo y las autoridades subordinadas solamente pueden emitir certificados a otra entidad subordinada.

1.4.2 Canales seguros

La protección de las comunicaciones que se realiza mediante cliente y servidor, es por canales seguros entre las partes que realiza la comunicación (S.Kent, 1983).

Los datos se los puede cifrar de acuerdo al medio que se van transportar, como por ejemplo, en el navegador, correo o también cuando se va a acceder a datos de un servidor. Por lo tanto hay varios protocolos de comunicaciones que no soportan el cifrado de forma nativa como: telnet, rlongin, FTP, NNTP y otros más. De hecho hoy en día en la práctica no se utilizan (Álvarez & Pérez, 2004).

1.4.2.1 SHH (Secure Shell)

Proporciona conexiones seguras a terminales remotos gracias al uso de criptografía de clave pública como se muestra en la Fig. 26. SSH no se limita a proteger sesiones de terminal remotas, también proporciona seguridad para FTP y permite redirigir puertos TCP/IP a través de un canal cifrado en ambas direcciones, al estilo de lo que se hace con los túneles SSL(Álvarez & Pérez, 2004).

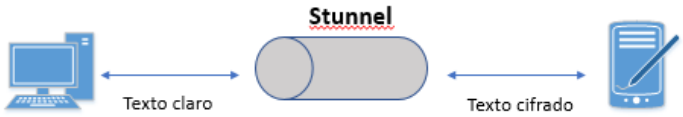


Figura 26. Funcionamiento de Stunnel

1.4.2.2 IPSEC

Es una versión segura del protocolo IP, de ahí su nombre IP Security. Las limitaciones de la suite de protocolos TCP/IP son conocidos porque no proporcionan ni autenticación, ni autorización, ni confidencialidad ni integridad, como consecuencia a esto pueden ser falsificados, manipulados, interceptados, causando fallos a servidores. Por tal motivo, se creó IPSec para ofrecer protección a los datos y a la red contra estos ataques, por tal motivo cubre las siguientes cuestiones de seguridad principales (IBM, 2017).

- Autenticidad de origen de datos.
- Integridad de datos.
- Confidencialidad de datos.
- Protección de reproducción.
- Gestión automatizada de claves criptográficas y asociaciones de seguridad.

1.4.2.3 Kerberos

Un sistema importante a menudo utiliza, el cual es Kerberos un protocolo de autenticación (J. Steiner, J. Neuman, 1988).

Utilizando una biblioteca extensa y compleja de claves cifradas propia de la plataforma de Kerberos identifica a usuarios. Estas claves no pueden ser leídas o exportadas fuera del sistema; ya que los usuarios y los servicios de la infraestructura de red que requieren acceso a un dominio, solo les permite autentificarse por medio de Kerberos, es decir que el sistema verifica la autenticidad del usuario y automáticamente le da. Para seguir explicando este tipo de sistema podemos decir que el usuario si necesita acceder a otro servicio, lo normal es que sea necesaria otra autenticación (Tanenbaun & M. Van Steen, 2008).

De tal modo, para el uso de Kerberos se debe utilizar dos credenciales, como se muestra en la Fig. 25 podemos observar cómo funciona la obtención de acceso a un servicio mediante Kerberos.

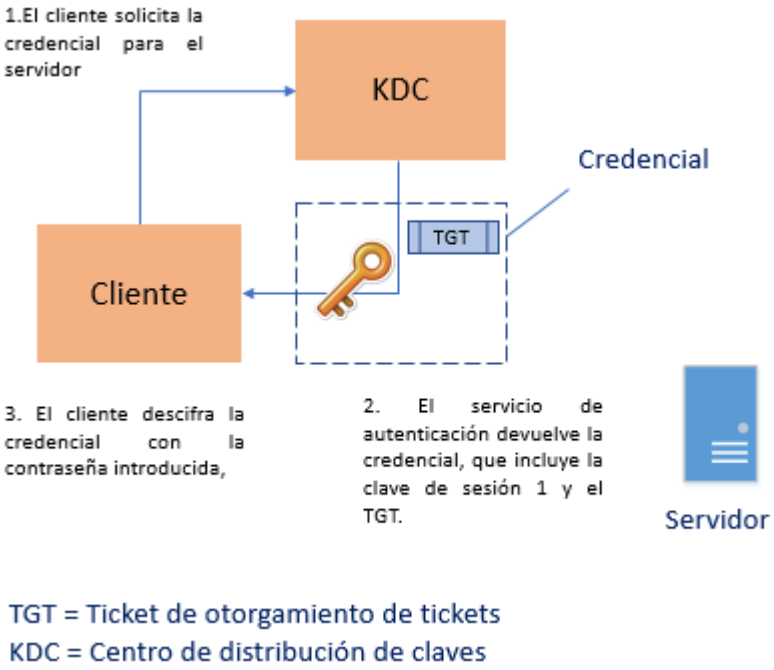
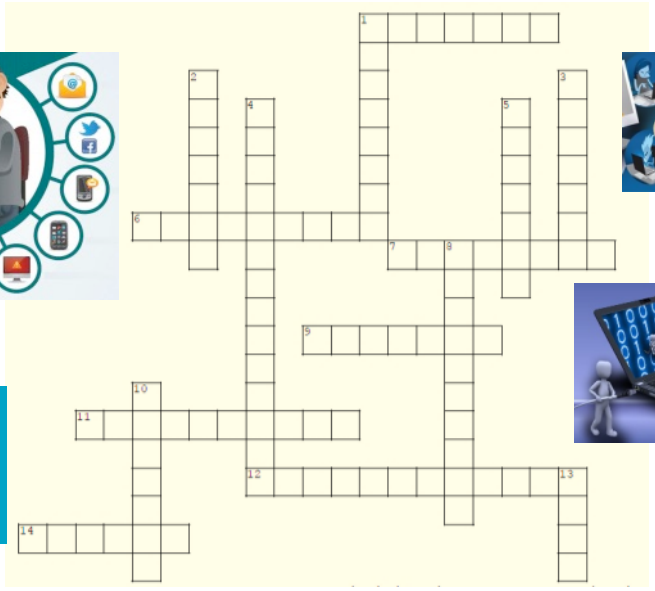


Figura 27. Otorgación de credencial. Fuente: www.docs.oracle.com

Analiza y resuelve



Completar el siguiente crucigrama contestando las preguntas que están a continuación.

HORIZONTAL

1. Sabe lo que busca donde encontrarlo y como logarlo.
Hace su trabajo por encargo y a cambio de dinero.
6. Se llama así a quien investiga y practica el arte de pasearse por las redes telefónicas.
7. Son comerciales sucios que venden los productos crackedos por otros.
9. Aquel individuo contratado para romper los sistemas de seguridad por las empresas e instituciones.
11. Literalmente son falsificadores sin escrúpulos que comercializan todo lo copiado (robado).
12. Uso no autorizado de un programa editor de ficheros para alterar borrar, copiar los datos almacenados.
14. Es una persona con un conocimiento importante de sistemas operativos redes protocolos lenguajes de programa.

VERTICAL

1. Permite capturar los paquetes que viajan por una red.
2. Realizar transacciones con tarjetas de creadas o adulteradas.
3. Personas que desproteger programas los modifica para obtener determinados privilegios, etc.
4. Software incrustados en otros códigos para realizar un ataque malicioso ala parte lógica del ordenador.
5. un conjunto de técnicas para acceder a un sistema informático sin autorización.
8. Personas que ocupan dominios por internet para luego venderlas a buenos precios.
10. Persona o grupo dedicados a la distribución de correo electrónicos no deseados.
13. Son considerados los maestros y los encargados de forma al os futuros hacker.

1.5 Actividades

Verifica conceptos

1.Realizar la siguiente encuesta para determinar el nivel de conocimiento sobre seguridad informática.

1. **¿Qué es un virus informático?**
   a. Una enfermedad que afecta al computador
   b. Un código malicioso cuyo fin es dañar
   c. Un código malicioso cuya finalidad es robar información
   d. Un programa maligno que se propaga

2. **¿Qué es un programa malicioso del tipo troyano?**
   a. Un programa malicioso que se 'disfraza' para pasar desapercibido
   b. El primer virus que se creó en la época de Troya
   c. Un virus tipo caballo
   d. Un virus muy dañino

3. **¿Qué es el malware?**
   a. Un software que busca infiltrarse o dañar al computador
   b. Un programa malo
   c. Un software defectuoso
   d. Un tipo de virus

4. **¿Qué es un hacker?**
   a. Un criminal cibernético
   b. Persona apasionada por los lenguajes de programación
   c. Un ingeniero que trabaja en campañas políticas
   d. Un ladrón tecnológico

5. **¿Qué es firewall?**
   a. Un muro de fuego
   b. Una pared segura
   c. Un programa que impide accesos no autorizados
   d. Un antivirus de fuego

6. **¿Qué es ransomware?**
   a. Un sistema de cifrado
   b. Un código aleatorio
   c. Un programa malicioso que cifra información y pide un rescate
   d. Un videojuego con virus

7. **¿Qué es el phishin'?**
   a. Una red social
   b. Una red social para pescadores
   c. Una estrategia de engaño informático
   d. Una aplicación para Android
   e. Una publicación falsa

8. **¿Qué es el hacking ético?**
   a. Un ataque hecho por una buena causa
   b. Un ataque informático que no roba dinero
   c. Descubrir vulnerabilidades y reportarlas
   d. Ninguna de las anteriores

9. **¿Qué es un ataque de día cero?**
   a. El primer día de un ataque informático
   b. Un ataque de virus que tiene una fecha puesta por los delincuentes informáticos
   c. El primer día de un ataque informático
   d. Un ataque que inicia el primero de enero.

10. **¿Qué es un gusano?**
    a. Código malicioso que se propaga por una red
    b. Un virus con forma de gusano
    c. Tipo de virus que pesca a sus víctimas
    d. Ninguna de las anteriores

11. **¿A qué se refiere la ingeniería social?**
    a. A las estrategias usadas para engañar a usuarios
    b. A un nuevo pregrado de ingeniería
    c. A un hacker con conocimientos en comunicación social
    d. Obras de ingeniería con propósito social

12. **¿Cuál contraseña es recomendable?**
    a. Qwert
    b. 123456
    c. Ert&yumIU8Po#2
    d. BarcelonaCampeoN

Verifica conceptos

2. Complete las siguientes Normas y Estándares aplicables a la Seguridad Informática.

1. _____ Estándar de cableado de telecomunicaciones en edificios comerciales.

2. _____ Estándar de cableado de telecomunicaciones en edificios comerciales para rutas y espacios.

3. _____ Estándar de administración de infraestructura de comunicaciones de edificios comerciales.

4. _____ Requerimientos de tierra y protección para infraestructura de telecomunicaciones en edificios comerciales.

5. _____ Estándar de Infraestructura de Telecomunicaciones para Centros de Cómputo.

6. _____ Estándar para protección ante incendios.

7. _____ Powering and Grounding Electronic Equipment.

8. _____ Requerimientos de tierra y protección para infraestructura de telecomunicaciones en edificios comerciales.

3. Subraye las etapas que forman parte de la Planeación de la capacidad de la red

Definición de índices de servicio

Enlaces de comunicaciones

Acceso Remoto

Redes WAN

Definición de arquitectura y topología

Definición de capacidad

Caracterización de aplicaciones (tráfico)

4. Escriba un ejemplo que permita identificar las amenazas de seguridad según su tipo.

a) Suplantación:

_____

_____

b) Elevación de privilegios:

_____

_____

c) Divulgación de información:

_____

_____

d) Denegación de servicio:

_____

_____

e) Repudio:

_____

_____

f) Alteración:

_____

_____

Problemas básicos

5. Resuelva la siguiente sopa de letras y complete la definición de Seguridad de la Información.

Seguridad-proteger-conocimiento-asegurar-informacion-secuencial-ordenado-disminuir-proceso-amenazas

I	D	Y	I	D	U	X	E	J	F	O	O	L	R
C	O	N	O	C	I	M	I	E	N	T	O	O	U
C	O	K	I	D	I	O	V	O	J	V	S	O	I
S	E	C	U	E	N	C	I	A	L	R	G	I	Z
Z	O	R	D	E	N	A	D	O	E	U	V	Y	X
E	A	P	R	O	T	E	G	E	R	Q	E	I	I
J	M	Q	B	Y	S	I	Y	H	K	V	X	D	A
C	A	S	E	G	U	R	A	R	E	D	N	E	B
I	N	F	O	R	M	A	C	I	O	N	O	E	F
P	R	O	C	E	S	O	W	A	P	F	N	O	B
A	K	I	Q	L	U	C	O	T	A	O	W	E	Q
S	E	G	U	R	I	D	A	D	T	Z	O	Y	O
D	I	S	M	I	N	U	I	R	R	I	Y	O	F
W	R	B	A	M	E	N	A	Z	A	S	O	Q	Y

"Es un _____ que busca proteger la _____, contra un compendio de _____, en pro de _____ la continuidad del negocio, _____ los posibles daños y maximizar el retorno de la inversión de la organización.

La Seguridad de la Información se tiene que preocupar por crear estrategias que permitan _____ la información y el _____ de la organización, bajo el control de un proceso _____ y _____ que muestre un indicador positivo que refleje el aumento del nivel de _____."

6. Complete:

Según las recomendaciones de mejores prácticas dadas por el estándar ISO/IEC 17799 la seguridad de la información se dedica a proteger:

La _____, asegurando que sólo quienes estén autorizados pueden acceder a la información; la _____, asegurando que la información y sus métodos son exactos y completos y la _____, asegurando que los usuarios tengan acceso a la información cuando lo requieran.

7. Enliste cinco dominios principales del estándar **ISO/IEC 17799.**

_____

_____

_____

_____

_____

_____

_____

_____

1.6 Resumen de Unidad 1

- La seguridad informática conlleva conceptos básicos que ayudarán a identificar la clase de delitos que se pueden cometer, con o sin conocimiento previo.
- Nos permitirá brindar una mayor protección a la empresa, y evitar ser víctima de ataques informáticos.
- Proteger nuestro sistema se convierte en la prioridad debido a que el atacante encuentra complejo el acceso.
- Se utilizan términos para identificar los delitos que se pueden cometer.
- La defensa en profundidad protege los recursos de una empresa, entidad u organización con si defensa exhaustiva de cada capa. Por lo que el firewall de una empresa no debe permitir el acceso a información propia, se debe denegar el acceso a terceras personas.

CAPÍTULO 2

1.1. Políticas de seguridad basado en normas internacionales
2.2 Implementar seguridad local a sistemas operativos
2.3 Herramientas de mayor demanda del mercado para búsquedas de vulnerabilidades en los sistemas implementar seguridad local a sistemas operativos
2.4 Hardening en los sistemas operativos
2.5 Principales ataques a sistemas
2.6 Actividades

UNIDAD 2

2.1 Políticas de seguridad basada en normas internacionales

La información que cada día se despliega en una empresa, tiene un gran valor como cualquier activo, por tal motivo debe ser protegida, las políticas de seguridad de los recursos informáticos tienen el propósito de administrar adecuadamente la seguridad de la información.

Estas políticas protegen a los recursos de información dentro de una gama amplia de amenazas internas y externas, tal sean, accidentales o de manera directa, con el fin de garantizar la integridad de los recursos informáticos y que los usuarios tengan en cuenta para su total cumplimiento (Yrigoyen, 2008).

- ISO 17.799

Es un estándar para la administración de la seguridad de la información, e implica la implementación de toda una estructura documental que debe contar con un fuerte apoyo de la alta dirección de cualquier organización. Este estándar fue publicado por la International Organization for Standardization (ISO) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones. Esta norma internacional ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

- COBIT

Acrónimo de "Control Objectives for Information and related Technology" (Objetivos de Control para la Información y Tecnologías Relacionadas), es un estándar desarrollado por la Information Systems Audit and Control Foundation (ISACA), la cual fue fundada en 1969 en EE.UU., y que se preocupa de temas como gobernabilidad, control, aseguramiento y auditorias para TIC. Actualmente tiene más de 60.000 miembros en alrededor de 100 países. Esta organización realiza eventos y 239 conferencias, y desarrolla estándares en TI de gobierno, aseguramiento y seguridad, siendo COBIT el más importante. En los últimos 5 años ha cobrado fuerza debido a que fue desarrollado en específico para el ámbito de las TIC.

- ITIL

Acrónimo de "Information Technology Infrastructure Library", ITIL es una norma de mejores prácticas para la administración de servicios de Tecnología de Información (TI), desarrollada a finales del año 1980 por entidades públicas y privadas con el fin de considerar las mejores prácticas a nivel mundial. El organismo propietario de este marco de referencia de estándares es la Office of Government Commerce, una entidad independiente de la tesorería del gobierno británico. ITIL fue utilizado inicialmente como una guía para el gobierno de británico, pero es aplicable a cualquier tipo de organización.

- LEY SOX

La Ley Sarbanes-Oxley (SOX), de EE.UU., nombrada así en referencia de sus creadores, obliga a las empresas públicas nacionales de dicho país, o extranjeras inscritas en la Securities and Exchange Comission a llevar un control y almacenamiento informático estricto de su actividad. La ley nace producto de grandes escándalos financieros ocurridos en compañías norteamericanas como Enron y Worldcom, durante el año 2002, en los cuales se comprobó que información financiera fue falsificada. Esta ha tenido un alto impacto a nivel mundial en empresas que transan sus valores en la bolsa de EE.UU.

- COSO

La normativa COSO, acrónimo de The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework, está principalmente orientada al control de la administración financiera y contable de las organizaciones. Sin embargo, dada la gran cercanía que hoy existe entre esta área y los sistemas de información computarizados, es que resulta importante entender el alcance y uso de esta norma. Junto a esto son muchas otras las normas que 240 están directa o indirectamente relacionadas con ésta como por ejemplo COBIT.

En síntesis, el Informe COSO es un documento que contiene directivas e indicaciones para la implantación, gestión y control de un sistema de Control Interno, con alcances al área informática.

- ISO Serie 27000

A semejanza de otras normas ISO, la 27000 es una serie de estándares, que incluye (o incluirá, pues algunas partes aún están en desarrollo), definiciones de vocabulario (ISO27000), requisitos para sistemas de gestión de seguridad de la información (ISO 27001), guía de buenas prácticas en objetivos de control y controles recomendables de seguridad de la información (ISO 27002), una guía de implementación de SGSI (Sistema de Gestión en Seguridad de la Información) junto a información de uso del esquema PDCA (Plan, Do, Check, Act) (ISO 27003), especificación de métricas para determinar la eficacia de SGSI (ISO 27004), una guía de técnicas de gestión de riesgo (ISO 27005), especificación de requisitos para acreditación de entidades de auditoria y certificación de SGSI (ISO 27006), una guía de auditoria de SGSI (ISO 27007), una guía de gestión de seguridad de la información para telecomunicaciones (ISO 27011), una guía de continuidad de negocio en cuanto a TIC (ISO 27031), una guía de ciber-seguridad (ISO 27032), una guía de seguridad en redes (ISO 27033), una guía de seguridad en aplicaciones (ISO 27034), y una guía de seguridad de la información en el sector sanitario (ISO 27799).

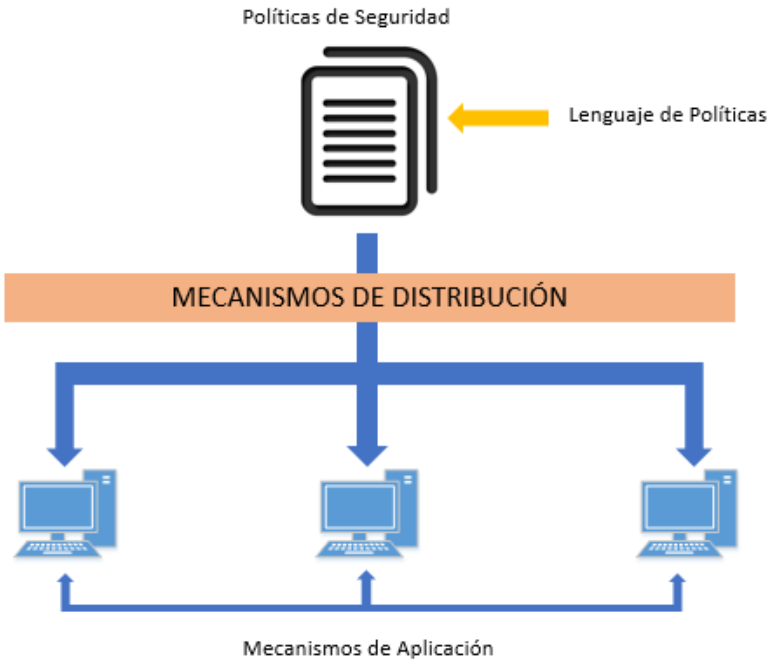


Figura 28. Políticas de Seguridad

Las aplicaciones se ejecutan dentro de un entorno llamado sistema operativo, donde cualquier tipo de vulnerabilidad puede comprometer la seguridad de la aplicación. Por ellos la seguridad que se implemente dentro del sistema operativo, va a garantizar la estabilidad del entorno, además de mantener controlado los accesos a todos los recursos internos y externos que se encuentran dentro en él como se muestra en la Fig. 28.

Otro punto de seguridad muy importante es la seguridad física, donde las amenazas para vulnerar pueden ser lógicas o físicas.

A continuación se dictan políticas de seguridad y recomendaciones para sistemas operativos (IBM Knowledge Center, 2016).

- Deshabilitar el acceso a los puertos USB y gestor de CD.
- Bloqueo de la BIOs.
- No abrir documentos adjuntos o hacer clic en enlaces de mensajes no solicitados.
- Bloqueo que páginas web (no permitidas).
- No utilizar la misma contraseña en diferentes páginas web o compartirlas.
- Ocupación de memoria y demás recursos para fines personales.
- Transmisión a terceros de información confidencial.
- Identificar y priorizar los recursos informáticos.
- Establecer condiciones de uso del correo y de navegación.
- Disponer de un plan de contingencia que contemple copias de resguardo, autenticación de usuarios, integridad de datos, confidencialidad de la información almacenada y control de acceso.
- Actualización permanente y observancia de las normas laborales.
- Educación y capacitación constante sobre las políticas de seguridad.

2.1.1 Cuentas de usuario

Los usuarios deberán tener una cuenta para poder acceder a un sistema informático y así mismo poder tener acceso a los recursos compartido dentro de una red.

Además, es importante destacar que los usuarios comunes no deberán tener permisos de administración. Es decir, que sólo unos cuantos usuarios de confianza tengan acceso administrativo a los sistemas servidores (IBM Knowledge Center, 2016).

Por otra parte asignar los permisos mínimos a los usuarios que utilicen un aplicativo, se considera una buena práctica, porque en caso de que el atacante obtenga acceso a la aplicación, tendrá los mismos permisos de aquel usuario que solo utilice el aplicativo.

2.1.2 Políticas de las cuentas

Cuando se trate de registrar la contraseña, no se deberá hacer referencia a conceptos, objetos o idea reconocible del usuario, ejemplo fechas significativas, nombres, meses del año, etc. Para ello, se debe utilizar un software para descifrar las contraseñas para comprobar su verdadera fortaleza (Velasco, 2016), en caso de que no cumpla con estas reglas los usuarios deberán recibir una notificación de cambiar las contraseñas por una que sea más robusta.

En caso de que el sistema, no solicite automáticamente la contraseña, lo recomendable es que el usuario cambie la contraseña en la primera vez que haga el acceso al sistema; así mismo debe actualizarla cada cierto periodo de tiempo.

En caso de que use un sistema basado en UNIX, se debe activar el archivo de contraseña duplicado. En UNIX las contraseñas se guardan en el archivo /etc/passwd, por lo tanto este archivo está abierto para que cualquier persona tenga acceso, lo que representa un riesgo de seguridad. Para la mejorar la seguridad de la contraseña, se debe activar el archivo de contraseña duplicado llamado /etc/shadow, donde los permisos para este archivos son más restrictivos (“IBM Knowledge Center,” 2016).

2.1.3 Servicios de red

Reducir el nivel de permisos de los usuarios registrados en los servidores de red debido a que estos están expuestos al público.

Así mismo asegurar que los usuarios que tienen el acceso al servidor web no tengan acceso al Shell.

Proporcionar el número mínimos de servicios necesarios en el sistema servidor. Solo utilizar los servicios que necesite el servidor.

Proteger el sistema frente a las amenazas de NetBIOS asociadas con los puertos 137, 138, 139. Estos puertos se los enumeran en el archivo /etc/services.

Utilizar servicios como iptables, más adelante se explicará más a fondo este tema.

Evitar los servicios que tengan interfaz gráfica de usuarios.

2.1.4 Sistemas de archivos

Otorgar a los usuarios permisos de sólo lectura para directorios necesarios.

Denegar permisos de lectura y escritura para todas las estructuras de directorios a todos los usuarios y después otorgar permisos explícitamente necesarios.

2.1.5 Actualización e instalación de sistemas

Se debe planificar el mantenimiento regular de las actualizaciones de seguridad.

Ejecutar parches recomendados de seguridad del sistema operativo o así mismo actualizaciones de las aplicaciones que se ejecuten.
Para poder instalar un programa adicional, el usuario deberá presentar una solicitud para su respectiva instalación, para ello deberá ser comprobado su requerimiento, de tal manera que deberá ser instalado por el personal de sistema.

2.1.6 Minimización del sistema operativo

Se debe eliminar aplicaciones que no son necesarias con el objetivo de reducir vulnerabilidades del sistema.

Además, restringir los servicios locales a los servicios necesarios para la operación.

Se debe implementar un sistema de protección para el desbordamiento de búfer (Ramos, 2012).

2.1.7 Usos indebidos por partes de los usuarios

Los usuarios no podrán modificar o reubicar equipos de computación, software, información, periféricos, redes sin la debida autorización del departamento o área de sistema.

Así mimo como borrar información o configuraciones en los sistemas operativos, de la misma manera para las respectivas configuraciones de la red.

Alterar o falsificar de manera fraudulenta los archivos o permisos, documentos de identificación.

Intentar descifrar claves, sistemas o algoritmos cifrados y cualquier otro componente de seguridad que tenga que ver con los procesos diarios de una empresa.

Sustracción de equipos informáticos.

Grabar, modificar o borrar información o algún software que no estén incluidas dentro de las tareas del usuario

Acceder a los sistemas de información sin autorización.

Revelar o compartir contraseñas de acceso, propias o de terceros, así mismo como una firma digital o identificación de otro usuario.

Introducir cualquier virus, gusano, macros, applets o cualquier amenaza lógica que altere el funcionamiento correcto de un sistema informático.

2.1.8 Políticas enmarcadas dentro de los sistemas operativos

Las siguientes políticas pueden ser aplicadas para para los usuarios de diferentes áreas (Sarba, 2013).

- Determinar un periodo de tiempo para el logeo de los usuarios dependiendo al departamento que corresponden, ejemplo, usuarios de del departamento de contabilidad su horario es de 08H00 a 17H00, esta política se la aplica directamente a una cuenta creada en Directorio Activo o dependiendo del sistema operativo se busca restringir de acuerdo el horario.

- Determinar un tiempo de retardo luego de que un usuario realiza un intento fallido al logearse.

- Limitar el uso de servicios que no tengan nada que ver con la actividad que realice el usuario.

- Establecer días permitidos para que un usuario vuelva a cambiar la contraseña.

- Mantener bloqueadas las cuentas que no requieran autenticación.

- Cuando exista una inactividad en una cuenta, se deberá inhabilitar.

- Desactivar instalaciones de software de terceros para usuarios, tener en cuenta que pueden ser software para ocio o también que maliciosos.

- Prohibir el acceso a las configuraciones del sistema operativo o panel de control.

- Desactivar reproducción automática de dispositivos, si bien es cierto, esto ayuda a agilizar los que hacemos, pero esto puede infectar nuestro sistema con algún virus.

- Monitorizar los archivos de registros, en cuentas de administradores para su debido análisis, utilizando herramientas confiables; así mismo para detectar si han sufrido algún cambio.

2.2 Implementar seguridad local a sistemas operativos

Los sistemas operativos es un entorno donde se ejecuta un conjunto de aplicaciones (Tanenbaum, 2009). Cualquier vulnerabilidad en el sistema operativo puede comprometer los datos que se manejen dentro de las aplicaciones.

La implementación de seguridad global ayuda a los controladores de dominio y, clientes y de una organización, tener en cuenta que las configuraciones de seguridad son reglas que se puede configurar en un equipo o varios equipos, con el único objetivo de proteger los recursos de un equipo o red(Microsoft, 2015).

2.2.1 Características a implementar en seguridad local

2.2.1.1 Complemento Directiva de seguridad Local

A esto se le llama complemento MMC (Microsoft Management Console) diseñado para administrar la configuración de directiva de seguridad solo. Este complemento también restringe la vista de objetos a las siguientes directivas y características.(Microsoft, 2015).
Lógicamente este enfoque es aplicable a servidores Windows Sever.

- Directivas de cuenta.
- Directivas locales.
- Firewall de Windows con seguridad avanzada.
- Directivas del administrador de listas de redes.
- Directivas de clave pública.
- Directivas de restricción de software.
- Directivas de control de aplicaciones.
- Directivas de seguridad IP en equipo Local.
- Configuración de directiva de auditoría avanzada.

2.2.1.2 Herramienta de línea de comandos

Podemos utilizar es comando **secedit.exe** debido a que este configura y analiza la seguridad del sistema y hace una comparación actual haciendo referencia a las plantillas se seguridad especificadas(Bonnet, 2012). Aquí podemos citar las funcionalidades principales como observamos en la tabla 2 (Microsoft, 2015).

Tabla 2. Herramientas de línea de comandos

PARAMETROS	FUNCIÓN
Configure	Ayuda a resolver discrepancias de seguridad entre servidores, mediante la aplicación de la plantilla de seguridad correcta para el servidor errónea.
Analyze	Compara la configuración de seguridad del servidor con la plantilla seleccionada.
Import	Permite crear una base de datos de una plantilla existente. La herramienta de configuración de seguridad hace el análisis hace esto también.
Export	Permite exportar la configuración de una base de datos en una plantilla de configuración de seguridad.
Validate	Parámetro le permite validar la sintaxis de cada o las líneas de texto que creen o agreguen a una plantilla de seguridad. Esto garantiza qué si se produce un error en la plantilla, el problema no estará listo.

2.2.1.3 Administrador de cumplimiento de seguridad

Ayuda a planear, implementar, operar y administrar la seguridad básica para el cliente de Windows y sistemas operativos de servidor y aplicaciones de Microsoft. Contiene una base de datos completa de la configuración de seguridad recomendada, métodos para personalizar sus líneas de base y la opción de implementar dicha configuración en varios formatos.

2.2.1.4 Administración de configuración de seguridad

Este conjunto de configuraciones permite crear, aplicar y modificar la seguridad de un equipo local, unidad organizativa o dominio(Microsoft, 2015).

En la siguiente tabla 3 se enumera las características de administración de la seguridad.

Tabla 3. Administración de seguridad

PARAMETROS	FUNCIÓN
Configuración de seguridad y análisis	Define una directiva de seguridad en una plantilla.
Plantillas de seguridad	Estas plantillas se pueden aplicar a directiva de grupo o en el equipo local.
Extensión de configuración de seguridad de directiva de grupo	Modifica la configuración de seguridad individual en un dominio, sitio o unidad organizativa.
Directiva de seguridad local	Modifica la configuración de seguridad individual del equipo local.
Secedit [LH]	Automatiza las tareas de configuración de seguridad en un símbolo del sistema.

En esta sección encontramos varias secciones que nos ayudaran a determinar los pasos que se debe seguir para una correcta administración.

2.2.1.5 Aplicar configuración de seguridad

Una vez que se ha modificado la configuración de la seguridad, se actualiza en los equipos la unidad organizativa vinculada a su objeto de directiva de grupo(Microsoft, 2015):

- Cuando se reinicia un equipo, se actualizará la configuración en ese equipo.
- Para forzar un equipo a actualizar su configuración de seguridad, así como la configuración de directiva de grupo, consulte el Gpupdate (CLH)herramienta de línea de comandos.

Se determina la prioridad de una directiva, cuando se aplica a más de una directiva a un equipo. En la tabla 4 se muestran las prioridades de la Directiva.

Tabla 4. Prioridad de directiva

N	PRIORIDAD
1	Directiva de unidad organizativa
2	Directiva de dominio
3	Directiva de sitio
4	Directiva de equipo local

2.2.1.6 Importar y exportar plantillas de seguridad

Configuración de seguridad y análisis proporciona la capacidad de importar y exportar plantillas de seguridad en una base de datos.
Si los cambios realizados en la base de datos de análisis, puede guardar esta configuración mediante su exportación a una plantilla. La característica de exportación proporciona la capacidad para guardar el análisis de la configuración de base de datos como un nuevo archivo de plantilla. Este archivo de plantilla, a continuación, puede utilizarse para analizar o configurar un sistema, o se puede importar a un objeto de directiva de grupo.

¿Sabías que?

La capacidad de importar y exportar plantillas de seguridad en una base de datos. https://msdn.microsoft.com/es-es/library/jj966254(v=ws.11).aspx

2.2.1.7 Analizar la seguridad y ver los resultados

La configuración realiza un análisis de seguridad mediante la comparación del estado actual de seguridad del sistema con una *base de datos analysis*. Durante la creación de la base de datos de análisis utiliza al menos una plantilla de seguridad. En la tabla 5 se muestra la importancia de prioridades de indiciador visual.

¿Sabías que?

Si elige importar más de una plantilla de seguridad, la base de datos se combinará las distintas plantillas y creará una plantilla compuesta.

Resuelve los conflictos en orden de importación; la última plantilla importada tiene prioridad.

Tabla 5. Importancia de prioridad

INDICADOR VISUAL	SIGNIFICADO
X roja	La entrada está definida en la base de datos de análisis y en el sistema, pero no coinciden con los valores de configuración de seguridad.
Marca de verificación verde	La entrada está definida en la base de datos de análisis y en el sistema y coinciden con los valores de configuración.
Signo de interrogación	La entrada no está definida en la base de datos de análisis y, por lo tanto, no se ha analizado. Si no se analiza una entrada, es posible que no se ha definido en la base de datos de análisis o que el usuario que ejecuta el análisis no puede tener permisos suficientes para realizar análisis en un objeto o área específicos.
Signo de exclamación	Este elemento se define en la base de datos de análisis, pero no existe en el sistema real. Por ejemplo, puede haber un grupo restringido que se define en la base de datos de análisis, pero en realidad no existe en el sistema analizado.
Sin resaltar	El elemento no está definido en la base de datos de análisis o en el sistema.

2.2.1.8 Resolver discrepancias de seguridad

Se puede resolver las discrepancias entre la configuración de base de datos y del sistema de análisis por ejemplo:

- Aceptando o cambiando algunos o todos los valores que se marcan o no se incluye en la configuración, si determina que los niveles de seguridad del sistema local están válidos por el contexto (o roles) de ese equipo(IBM, 2010).

- Configuración del sistema con los valores de base de datos de análisis, si determina que el sistema no es conforme a los niveles de seguridad válido.

- Importar una plantilla más adecuada para la función de ese equipo a la base de datos como la nueva configuración básica y aplicarla al sistema.

Los cambios realizados en la base de datos de análisis se realizan en la plantilla almacenada en la base de datos, no el archivo de plantilla de seguridad. El archivo de plantilla de seguridad sólo se modificará si vuelve a plantillas de seguridad y modifica la plantilla o exportar la configuración almacenada en el mismo archivo de plantilla(Microsoft, 2015).

2.2.1.9 Automatizar las tareas de configuración de seguridad

Al llamar a la herramienta Secedit.exe en un símbolo del sistema desde un archivo por lotes o programador de tareas automático, puede usarlo para crear y aplicar plantillas

automáticamente y analizar la seguridad del sistema. También puede ejecutarla dinámicamente desde un símbolo del sistema.

Secedit.exe resulta útil cuando dispone de varios equipos en el que debe analizar o configurar la seguridad, y tendrá que realizar estas tareas de horas de trabajo.

2.3 Herramientas de mayor demanda del mercado para búsquedas de vulnerabilidades

Actualmente los directores de seguridad, necesitan permiso de su empresa para probar redes en vivo y necesitan herramientas de pruebas de penetración adecuadas para el trabajo. La detección de vulnerabilidades en las redes consta de tres pasos mediante las cuales se busca obtener las respectivas vulnerabilidades. En el siguiente Fig. 29 muestra las fases que de manera estándar se utilizan (Franco & Perea, 2012).

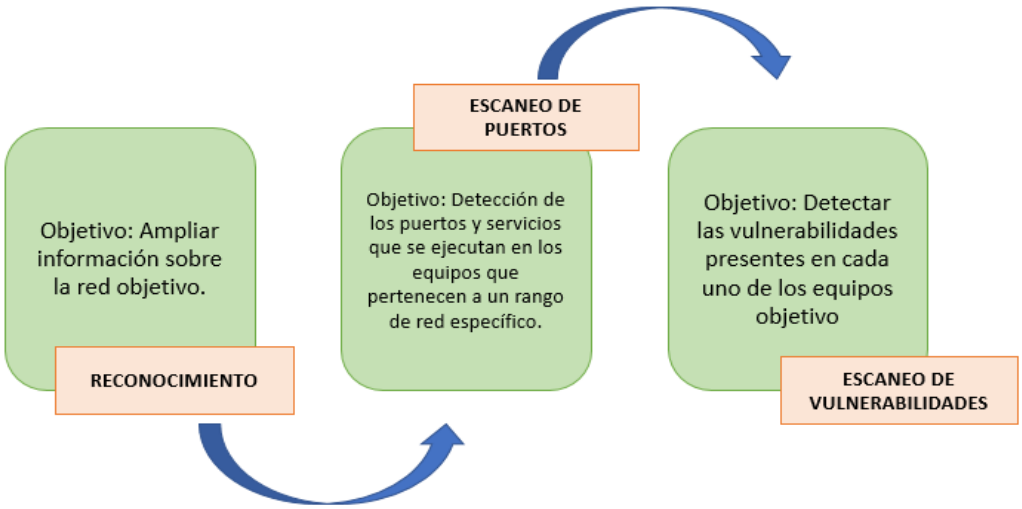


Figura 29. Fases de detección de vulnerabilidades. Fuente: (Franco & Perea, 2012).

La primera fase, trata de obtener información de la red objetivo (Franco & Perea, 2012), además de recolectar la mayor parte de cantidad de evidencia sobre la empresa donde se van implementar las pruebas (Ardita, 2001).

En la segunda fase, se realiza la ejecución de la fase de anterior, donde se examinará los puertos y servicios de cada uno de los equipos, además se realiza la evaluación de los segmentos de red (Hernández, 2015).

Y por último, se someterá a evaluación las vulnerabilidades y la detección de los equipos expuestos, y se generan reportes de las soluciones que se deben presentar para evitar ataques.

Una vez explicadas las fases de exploración de vulnerabilidades, vamos a nombrar herramientas para poder mitigar ataques.

2.3.1 Nmap

Sin duda alguna, es un escáner de puertos más popular entre profesionales de redes en la informática, primero por su fácil uso y segundo por versatilidad para escanear puertos (Astudillo, 2013). Sin embargo, esto hecho a base de scripts, permite identificar versiones de

software en remoto, vulnerabilidades, enumeración de usuarios, directorios y otras opciones más (Duarte, 2012).

2.3.2 Openvas

Es un framework de diversos servicios y herramientas que ofrecen una solución completa y potente de análisis y gestión de vulnerabilidades de red (Cedeño, 2015).

2.3.3 Advancep ip scanner

Es una herramienta gratuita que permite hacer exploraciones en una red de área local y recopilar información sobe los dispositivos conectados. Con esta herramienta se puede acceder fácilmente a recursos como carpetas compartidas servidores HTTP y servidores FTP.

2.3.4 Dsniff

Este programa que monitoriza datos de red, que se suele utilizar examinando el tráfico copiando los datos sin alterarlos, captura las claves que circulan por la red de protocolos ftp, telnet, smtp, http, pop y otros (Hernández, 2015).

2.3.5 Nessus

Esta herramienta presenta una arquitectura modular, cliente – servidor, ya que posee una base de datos de patrones de ataques para de esta manera poder lanzar ataques a un conjunto de máquinas y así poder detectar vulnerabilidades (Carvajal, 2007). Esta aplicación por lo general la utilizan las organizaciones como una aplicación de auditoria de sistemas de información para las búsquedas de fallas críticas de seguridad.

2.3.6 Jhon the ripper

Esta herramienta sirve para descifrar contraseñas, es compatible tanto para un ataque basado en diccionario y ataque de fuerza bruta(“Hacking Ético,” 2008). Para realizar un ataque los realizamos con los siguientes pasos (Hernández, 2015).

1. Copiar los archivos.
2. Fundir los archivos en uno.
3. Crackear las claves.
4. Mostrar las claves .

2.4 Hardening en los sistemas operativos

Para su definición técnica, se tomará la expresión por dos expertos:

Escrito por el envangelista en seguridad Roberta Bragg:

- Adoptar un enfoque proactivo para la seguridad de la red por el endurecimiento de un sistema Windows contra ataques antes de que ocurran.

Por Luis Montenegro, Windows y Security MVP (Most Valuable Professiona) 2007:

- Haciéndole la vida difícil al atacante. Ese es el concepto que está detrás del hardening de sistemas operativos. Hardening es una acción compuesta por un conjunto de actividades que son llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo posible la seguridad de su equipo (Borghello, 2009).

Además, las configuraciones adecuadas para los usuarios domésticos no son suficientemente seguras como para ser aplicadas en redes corporativas como se muestra en la Fig. 30. Los siguientes recursos ofrecen orientación sobre las configuraciones de seguridad y los procedimientos de endurecimiento para la mayoría de las aplicaciones conocidas:

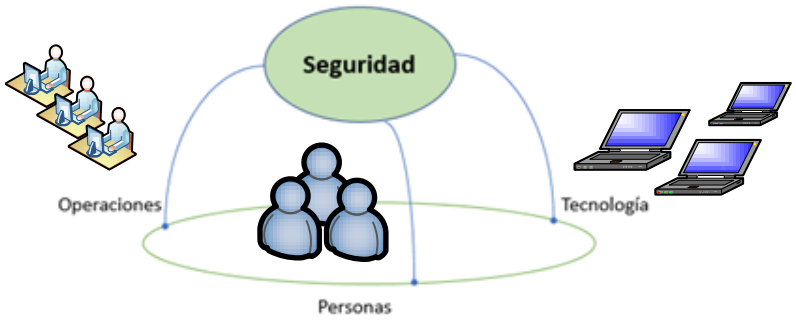


Figura 30. Seguridad en una organización

Debemos destacar que si existe acceso físico al equipo, este es un punto crítico de falla(Callejas, 2015), por ejemplo:

- Acceso al servidor.
- Proteger el BIOS/UEFI.
- Deshabilitar periféricos no utilizados.
- Fuentes redundantes.
- RAID.

2.4.1 Técnicas de hardening para Linux

2.4.1.1 Permisos

Linux es un sistema multiusuario, lo que conlleva a mantener la privacidad de estos y un control general para que no todos puedan hacer lo que quieran y comprometer así el sistema. Es por eso que vamos describir los permisos que se deben aplicar.

Si usamos el comando “ls -l” veremos una cadena parecida a la siguiente.

```
-rwx------
```

Estos permisos indican que el usuario propietario tiene permisos de lectura (r), escritura (w) y ejecución(x), que no es un directorio y que los miembros del grupo y el resto de usuarios del sistema no pueden hacerle nada.

Para poder interpretar esta cadena se debe entender que cada espacio corresponde a bit de permisos, y estos se agrupan en la siguiente tabla.

Indicador	Descripción
-	Indica si es o no un directorio.
Rwx	Permisos para el propietario del Fichero.
---	Permisos para los usuarios del grupo del Fichero.
---	Permisos para el resto de los usuarios.

2.4.1.2 SUIDS (s)

Este bit es un flag que sirve para modificar temporalmente los privilegios del usuario que ejecuta un programa (Llaquet, 2011).

```
-rwsr-xr-x
```

Este bit se puede asignar para que al ejecutar la aplicación se cambie el usuario, el grupo o ambas características del usuario que ejecuta.

2.4.1.3 Configuración del gestor de arranque

Cuando el sistema operativo arranca, cualquier persona podría acceder a los parámetros de arranque de gestor y forzar un inicio en modo de recuperación del sistema, por lo tanto tendría el control total del sistema (Llaquet, 2011).

Otro escenario que nos planteamos que de seguro un atacante lo conoce es la funcionalidad de edición añadida cuando se muestra el menú, si esta opción no se encuentra protegida bajo contraseña, sería una puerta abierta para un atacante para tomar el control del sistema.

Supongamos el caso de un gestor de inicio GRUB que permite arrancar diferentes tipos de sistemas operativos libres, así como sistemas operativos privativos (Mifsud, 2007), en el que añadimos una entrada configurada de la siguiente manera:

```
title Linux
root (hd0,0)
kernel /vmlinuz root=/dev/hda4 ro quiet splash
boot
```

En caso de que no estuviera protegido con contraseña, al iniciar GRUB se presiona la tecla 'e' y editar estas líneas, con la siguiente modificación se tiene el control total toral del sistema.

```
kernel /vmlinuz root=/dev/hda4 ro quiet splash init=/bin/bash
```

Los siguientes pasos conllevan a activar al gestor de arranque GRUB.

1. Acceder al fichero de configuración. p.e. '/boot/grub/menu.lst'

2. Activar la opción de contraseña añadiendo una de estas líneas:
    a. En claro (inseguro y totalmente desaconsejable):
    password <CONTRASEÑA>
    b. Encriptada en md5 (recomendado):
    password –md5 <HASH MD5 de la Contraseña>

2.4.1.4 Seguridad del sistema de fichero

Asignar permisos adecuados a los directorios sensibles del sistema. Con los siguientes comandos aseguramos privacidad a los usuarios.

```
# chmod 700 <fichero>                          (permisos)
# chown <usuario>:<grupo><fichero>             (propietario)
```

Se puede utilizar aplicaciones de cifrado como las siguientes:

Aplicación	Descripción
Enc FS	Creación de directorios cifrados
Loop AES	Creación de particiones cifradas.
GNU Privacy Guar (GPG)	Versión de PGP libre
OPEN SSL	Versión Abierta de SSL

Veamos un ejemplo con la aplicación OPEN SSL.
Primero creamos un archivo:

```
# openssl enc –e –bf –in texto_plano.txt –out texto_cifrado.sec
enter bf-cbc encryption password: <contraseña>
Verifying - enter bf-cbc encryption password: <contraseña>
```

Una vez hecho esto el fichero cifrado es "texto_cifrado.sec". En este caso se ha usado "blueFis." (-bf) como algoritmo de cifrado. A continuación, se muestra como descifrar el fichero:

```
# openssl enc –d –bf –in texto_cifrado.sec –out texto_original.txt enter bf-cubic encryption
password: <contraseña>
```

2.4.1.5 Actualización completa

- Actualización completa del sistema
  yum update
- Revisión de erratas
  yum check – update --security
- Instalación de erratas
  yum update –security

2.4.1.6 Limitar información sobre el equipo

- Modificar /etc/banner y /etc/banner.issue
- /etc/motd --- Política de uso de información y del sistema

2.4.1.7 Determinar servicios

Tener en cuenta los servicios necesarios

- ntsysv
- chkconfig
- systemctl

2.4.1.8 Limitar recursos

- Limitar el acceso como root a las terminales
  /etc/securetty
- Forzar el logout de los usuarios
  .bashrc ó /etc/profile
  TMOUT=360
- Limitar el acceso a los recursos
  /etc/security/limits.conf

2.4.2 Técnicas de hardening para Windows

2.4.2.1 Deshabilitar los usurarios invitados

En algunas versiones de sistemas operativos los usuarios invitados vienen por defecto deshabilitadas, pero esto no se cumple en todos. Por ello es importante verificar una vez finalizada la instalación en que estatus se encuentra este usuario.

> **¿Sabías que?**
>
> Como medida extra de seguridad se puede asignar una contraseña compleja y restringir el número de inicios de sesión por día.

2.4.2.2 Limitar el número de cuentas en el servidor

Cualquier usuario innecesario es potencial candidato para ser eliminado ya que dada la naturaleza de los permisos que estas tienen tienden a utilizar contraseñas débiles y con ellas se puede acceder a múltiples equipos, por lo que representan una seria amenaza.

2.4.2.3 Limitar los accesos de la cuenta de administración

Para actividades regulares de administración del servidor no se recomienda utilizar la cuenta de administrador.

¿Sabías que?

Como parte de una política de acceso más agresiva podríamos con figurar una contraseña compleja con cambio cada 3 meses mínimo y un correo o registro cada vez que se acceda desde esta cuenta al servidor.

2.4.2.4 Renombrar la cuenta de administración

La idea es que el nombre de usuario no indique sus privilegios, y al menos dificulte el trabajo de hackers principiantes.

2.4.2.5 Crear una cuenta falsa de administrador

Es una estrategia alterna, donde creamos una cuenta llamada administrador, pero no le otorgamos privilegios pero si una contraseña de al menos 10 caracteres. Con esto podemos monitorear el acceso a la misma y mantener entretenidas a personas que intenten ingresar.

2.4.2.6 Limitar los privilegios por defecto de ciertos grupos de usuarios

Por defecto existen carpetas compartidas compartidas para los usuarios del sistema operativo, así como grupos como “Everyone” con el cual cualquiera que entre al sistema tendrá acceso a los datos de la red.

2.4.2.7 Formato de particiones con NTFS

El tipo de extensión soporta niveles de seguridad y mayor capacidad de almacenamiento, a diferencia de FAT y FAT32 que muy aparte de tener limitaciones de almacenamiento tampoco soportan buenos niveles de seguridad lo que consituye una puerta trasera ideal para los atacantes.

2.4.2.8 Configurar políticas de seguridad en el servidor y en la red

Definir perfiles de usuarios, horas de acceso, seguridad a nivel físico o lógico en los equipos activos de red.

2.4.2.9 Apagar servicios innecesarios en el servidor

El hecho de que muchos servicios vengan configurados y listos para ser usados constituye de cierto modo una ventaja, pero también una vulnerabilidad. Servicios como: IIS, RAS, Terminal Services. De igual manera pueden existir servicios ejecutándose silenciosamente, por lo cual es necesario auditar periódicamente los servicios en uso por el usuario.

2.4.2.10 Cerrar el acceso a puertos que no están en uso

2.4.2.11 Habilitar la auditoría en el servidor

Esta configuración permite mantenerse informado de intrusiones en el sistema. Esta funcionalidad permite recibir alertas en cambios en varios eventos críticos como en configuraciones centrales.

2.4.2.12 Habilitar la protección de los archivos de registro de eventos

Por defecto este tipo de archivos no se encuentran protegidos, es importante dar permisos de lectura como de escritura a usuarios del sistema y administradores, de lo contrario un atacante podría fácilmente eliminar sus registros luego de un ataque.

2.4.2.13Desactivar la opción del último usuario para desplegarse en la pantalla de inicio o bloqueo del sistema

Esto permite que al presionar Ctrl+Alt+Del no se muestre el último usuario en sesión y permita que el atacante intenté adivinar la contraseña del usuario.

> **¿Sabías que?**
>
> Esto puede modificarse en las políticas de seguridad.

2.4.2.14 Verificar los parches de seguridad

Todo sistema operativo debe ser contantemente actualizado basado en las recomendaciones del fabricante para mejoras de seguridad en pro de evitar ser víctima de ATAQUES.

2.4.3 Firewall

Este tema es de suma importancia, porque nos permite proteger una red local conectada a internet a través de un router (Pello Altadill, n.d.). Un firewall pueden ser dispositivos o sistemas que permiten controlar el tráfico de dos o más sistemas, además que pueden ser router, equipos de bastión, sistemas operativos modificados, normalmente es una mezcla de varios (Sánchez, 2004).

A continuación, se detallan unos conceptos importantes que para poder proseguir con el tema de firewall y en tabla 6 se muestra los firewall comerciales mas usados.

Tabla 6. Firewall Comerciales

Firewall Comerciales
1. Agnitum Outpost Free
2. Comodo Firewall
3. ZoneAlarm Free
4. PC Tools Firewall Plus 7
5. AVS Firewall
6. HandyCafe Firewall
7. PrivateFirewall
8. SoftPerfect Firewall
9. Windows 7 Firewall Control
10. PeerBlook

2.4.3.1 Dual Homed Gateway

Este firewall trabaja dos adaptadores de red. El sistema está configurado para que los paquetes se ejecuten directamente desde una red a otra red intranet como se muestra en la Fig.31 (Ferić, 2006).

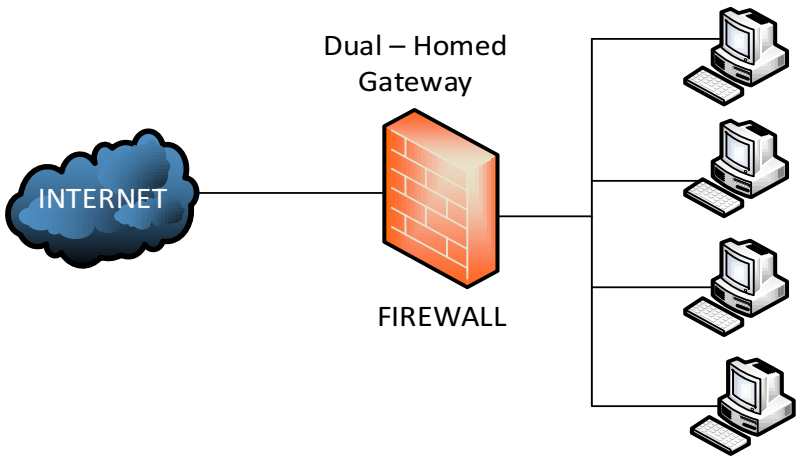


Figura 31. Puerta de enlace dual

2.4.3.2 Screened Host Gateway

Se utiliza un host bastión que se sitúa en la red privada (Sánchez, 2004). Un host bastion es una aplicación que se encuentra en el servidor con el objetivo de brindar seguridad a la red interna como podemos observar en la Fig. 32 (Oviedo, 2005).

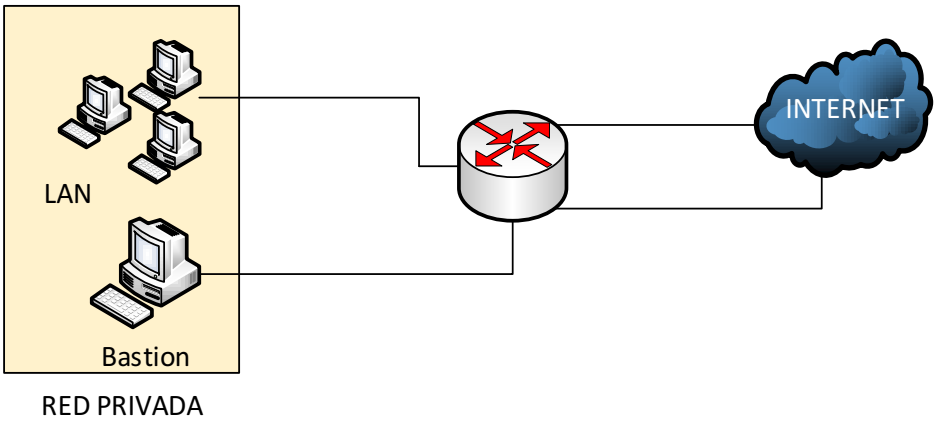


Figura 32. Puerta de enlace seleccionada

2.4.3.3 Screened Subnet

En este caso el host bastion estará ubicado en una red intermedia, se crea una red aislada utilizando dos routers, además, que todos los host pueden acceder a la red intermedia como se muestra en la Fig. 33 (Sánchez, 2004).

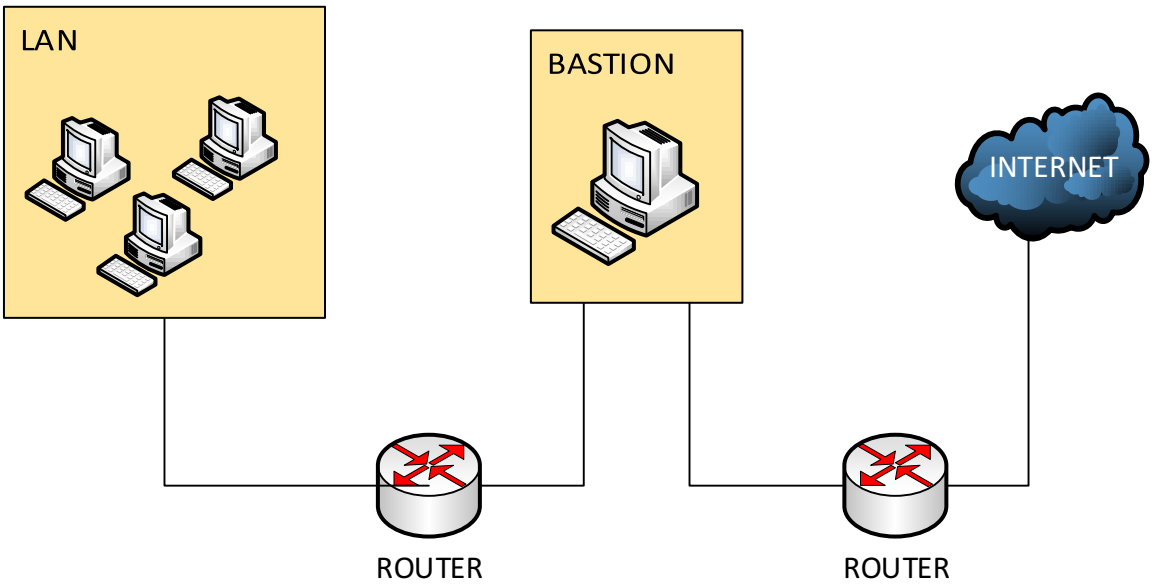


Figura 33. Subred seleccionada

2.4.3.4 DMZ

Una red desmilitarizada es una red separada del resto de servicios para internet, además no permite el tráfico directo entre internet y una red privada como se muestra en la Fig. 34 (Sánchez, 2004).

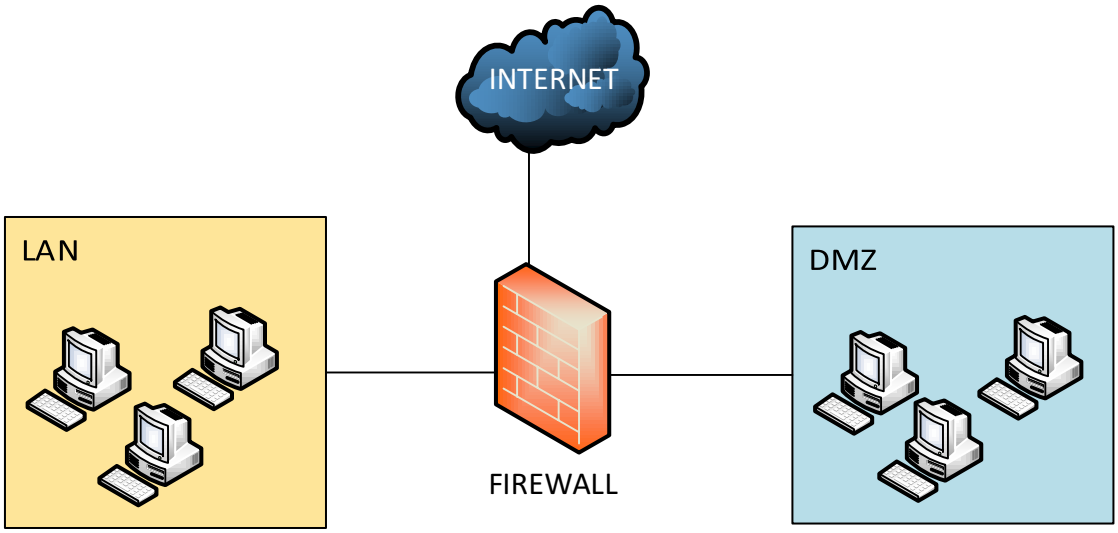


Figura 34. Diseño de una red desmilitarizada

2.4.3.5 Iptables

Es un sistema de firewall vinculado al kernel de Linux, es decir, es parte del sistema operativo. Además, podemos crear un script con un conjunto reglas iptables. Los datagramas deben ir probando regla tras regla, y paran cuando concuerdan con una de ellas (Sánchez, 2004).

Estructura del comando iptables

$$iptables - t[tabla\ a\ usar] - \begin{bmatrix} parámetro \\ de\ tabla \end{bmatrix} \begin{bmatrix} cadena\ a\ usar \\ en\ la\ tabla \end{bmatrix} - \begin{bmatrix} Caracteristicas\ que\ se\ deesean \\ comparar\ con\ el\ paquete \end{bmatrix} - \begin{bmatrix} Acción\ a \\ ejecutar \end{bmatrix}$$

Tabla 7. Tablas a usar

TABLAS A USAR	
NAT	PARA EL CONTROL DE NATEO
MANGLE	PARA MARCA UN PAQUETE
FILTER	PARA FILTRAR UN PAQUE

Tabla 8. Parametros

PARAMETRO DE TABLA	
-A	Esta opción permite ejecutar la adición de una regla nueva, esta regla quedara de última en el orden de la lista de reglas que se encuentre actualmente en la cadena.

-D	Esta opción le permite eliminar la cadena, esto solo sucede si la cadena no es del sistema y si la cadena está vacía.
-I	Esta opción permite ejecutar la inserción de una regla nueva en el principio de la lista de reglas de la cadena, es de especial cuidado porque al estar de primera si se cumple la comparación no se revisara las demás.
-L	Esta opción le permite visualizar en la consola todas las reglas que pertenezcan a la cadena que le indiques, si no coloca la cadena especifica la opción muestra todas las cadenas posibles de la tabla.
-F	Esta opción le permite borrar todas las reglas que estén contenidas en la cadena que se tenga seleccionada.
-Z	Esta opción permite colocar los contadores de la cadena en ceros, esta opción es útil cuando necesitas verificar la cantidad de tráfico generado en una regla específica.
-N	Esta opción le permite crear una nueva cadena, si el administrador cree necesarias más cadenas que las que por defecto entrega el sistema puede crear acá las que necesite.
-P	Esta opción le permite determinar la política general de la gestión de paquetes, por lo que es una de las más importantes del sistema y siempre debe estar presente, si no lo está el sistema coloca que la política de filtrado de aceptar sin restricciones.

Tabla 9. Cadena a usar

CADENA A USAR EN LA TABLA	
PREROUTING	Cadena donde pasan los paquetes después de que salen de la interfaz
POSTROUTING	Cadena donde pasan los paquetes antes de llegar a la interfaz
FORWARD	Cadena de filtrado una vez ruteado
INPUT	Cadena de filtrado de los paquetes que van a la/s ip/s pertenecientes a la maquina
OUTPUT	Cadena de filtrado de los paquetes que salen de la/s ip/s pertenecientes a la máquina.

2.4.3.6 Políticas por defecto

Son cadenas de filtrado que se utilizan para definir si los paquete o datagramas tienen acceso a un determinado host, teniendo en cuenta los protocolos.

Los paquetes o datagramas que van a la propia maquina se aplican las reglas:

INPUT

OUPUT

Para filtrar paquetes:

FORWARD

Para hacer redirecciones de puertos o cambios de IPS de origen y destino, se utilizan las siguientes reglas:

PREROUTING

POSTROUTING

Condiciones principales para iptables:

-p -protocol	Esta regla se aplica a un protocolo.
-s -src -source	Esta regla se aplica a una IP de origen.
-d -dst -destination	Esta regla se aplica a un IP destino.
-i -in-interface	Esta regla se aplica a una interfaz de origen como eth0.
-o -out -interface	Esta regla se aplica a una interfaz de destino.

Dado los conceptos, comenzaremos a dar ejemplos:

Ejercicio 1

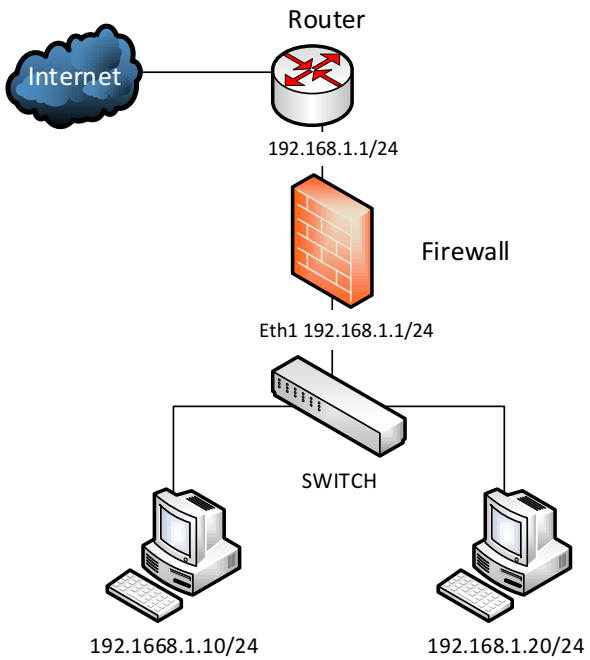


Figura 35. Esquema de una red local con firewall

Establecemos políticas por defecto

```
iptables –P INPUT ACCEPT
iptables –P OUTPUT ACCEPT
iptables –P FORWARD ACCEPT
```

```
iptables –t nat –P PREROUTING ACCEPT
iptables –t nat –P POSTROUTING ACCEPT

## Activamos el reenvío para que FORWARD funcione
echo 1 > /proc/sys/net/ipv4/ip_forward

## Añadimos la cadena de entrada lo que viene de 192.168.1.10/24 cuyo destino sea
192.168.1.1/24

iptables -A INPUT -s 192.168.1.10/24 -d 192.168.1.1/24

## Estamos especificando entradas a través del Puerto SSH
iptables -A INPUT -i eht1 192.168.1.20/24 -d 192.168.1.1/24 -p tcp -dport22 -j ACCEPT

## Con esta línea no permitimos que ninguna dirección ip (0/0) acceda por medio del puerto
ICMP
iptables -A INPUT -i eht1 -s 0/0 -d 192.168.1.1/24 -p tcp -dport7 -j DROP
```

Ejercicio 2

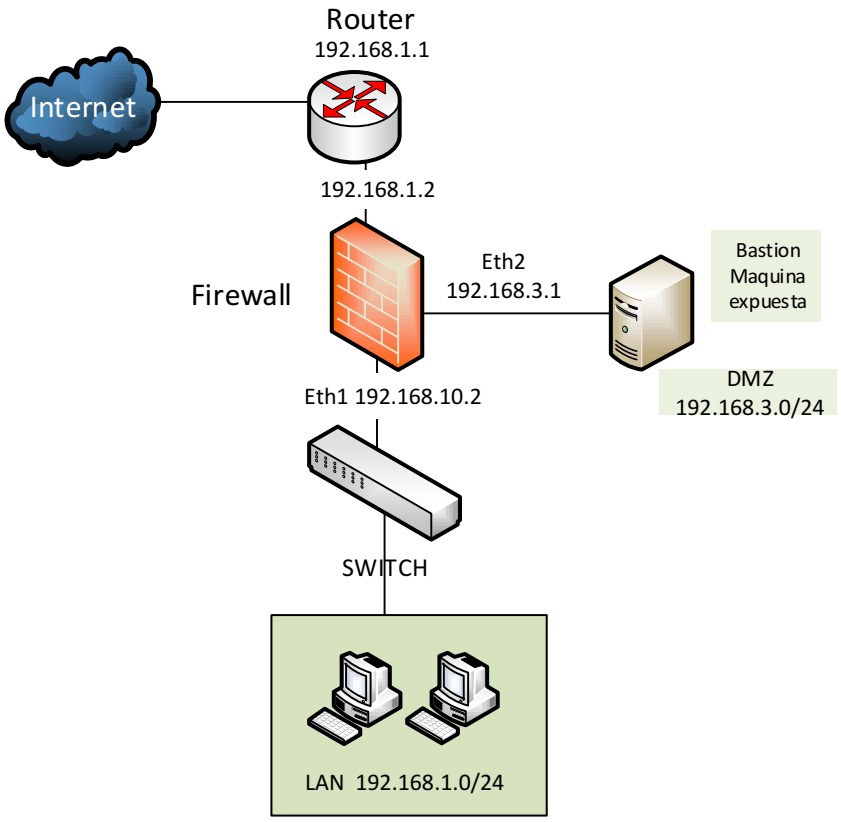


Figura 36. Esquema de firewall entre red local e internet con zona DMZ para servidores expuestos

Ruta por defecto del firewall: 192.168.1.1
Ruta por defecto de la LAN: 192.168.10.1
Ruta por defecto en la DMZ: 192.168.3.1

```
## Activamos el reenvío para que FORWARD funcione
echo 1 > /proc/sys/net/ipv4/ip_forward

## Al firewall tenemos acceso desde la red local
iptables –A INPUT –s 192.168.10.0/24 –i eth1 –j ACCEPT

## Permitimos el paso de la DMZ a una BBDD de la LAN
iptables –A FORWARD –s 192.168.3.2 –d 192.168.10.5 –p tcp ––dport 5432 –j ACCEPT
iptables –A FORWARD –s 192.168.10.5 –d 192.168.3.2 –p tcp ––sport 5432 –j ACCEPT

## Permitimos abrir el Terminal server de la DMZ desde la LAN
iptables –A FORWARD –s 192.168.10.0/24 –d 192.168.3.2 –p tcp ––sport 1024:65535 ––dport
3389 –j ACCEPT 15

## Cerramos el rango de puerto bien conocido
iptables –A INPUT –s 0.0.0.0/0 –p tcp –dport 1:1024 –j DROP
iptables –A INPUT –s 0.0.0.0/0 –p udp –dport 1:1024 –j DROP
```

2.5 Principales ataques a sistemas

Primeramente, para describir los ataques, tenemos que comentar las posibles amenazas que son blanco de ataque en nuestros sistemas (Borghello, 2009b).

Los robos de información, sabotajes o accidentes relacionados con los sistemas informáticos son causados por el propio personal de la organización propietaria de dichos sistemas. En la Fig. 37 se muestra los porcentajes de ataques a sistemas internos como externos.

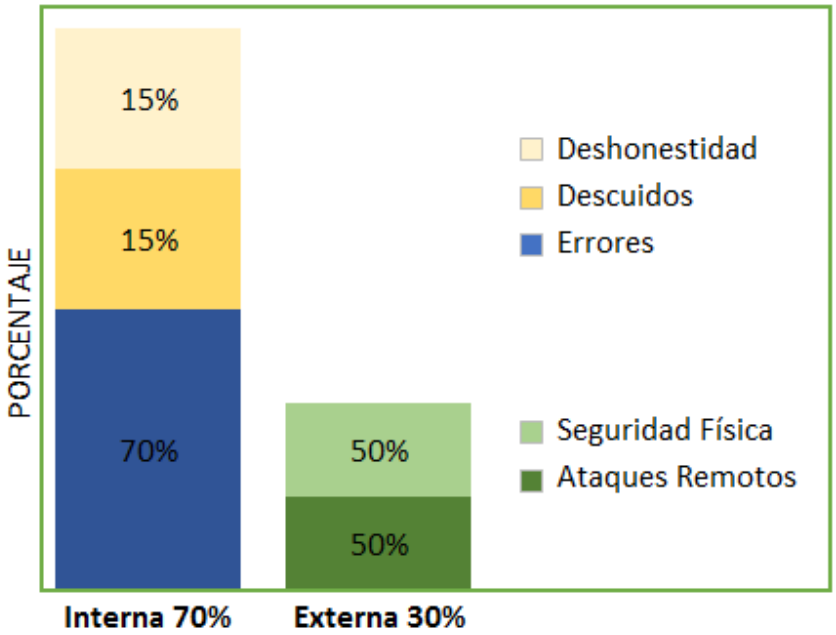


Figura 37. Ataques a sistemas

2.5.1 Amenazas lógicas

Los protocolos de comunicación utilizados carecen (en su mayoría) de seguridad o esta ha sido implementada en forma de "parche" tiempo después de su creación.

- Existen agujeros de seguridad en los sistemas operativos.
- Existen agujeros de seguridad en las aplicaciones.
- Existen errores en las configuraciones de los sistemas.
- Los usuarios carecen de información respecto al tema.

Esta lista podría seguir extendiéndose a medida que se evalúen mayor cantidad de elementos de un Sistema Informático.

Las empresas u organizaciones no se pueden permitir el lujo de denunciar ataques a sus sistemas, pues el nivel de confianza de los clientes (ciudadanos) bajaría enormemente.

2.5.2 Consecuencias de los ataques

- Data Corruption: la información que no contenía defectos pasa a tenerlos.
- Denial of Service (DoS): servicios que deberían estar disponibles no lo están.
- Leakage: los datos llegan a destinos a los que no deberían llegar.

2.5.3 Hacking ético

Son técnicas de intrusión en los sistemas, metodologías sobre los chequeos de seguridad, todo esto para detectar las acciones que los intrusos podrían realizar y las posibles soluciones.

Hay dos tipos de hacking:

2.5.3.1 Hacking ético externo

Este tipo de hacking, se realiza desde internet, sobre la infraestructura de red pública del cliente; es decir, sobre aquellos equipos de la organización que están expuestos a Internet porque brindan un servicio público. Ejemplo: **enrutador, firewall, servidor web, servidor de correo, servidor de nombres de dominio.**

2.5.3.2 Hacking ético interno

Como su nombre lo sugiere, este tipo de hacking se ejecuta en la red interna del cliente, desde el punto de vista de un empleado de la empresa, un consultor, o un asociado de negocios que tienen acceso a red corporativa.

En este tipo de pruebas de intrusión, se suele encontrar más huecos de seguridad que en su contraparte externa, debido a que muchos administradores de sistemas se preocupan por proteger el perímetro de su red y subestiman al atacante interno.

Para continuar con el contenido es importante conocer las siguientes definiciones.

2.5.3.2.1 Exploit

Es un programa o código que explota una vulnerabilidad del sistema o parte de él para aprovechar esta deficiencia en beneficio del creador del mismo(Astudillo, 2013).

2.5.3.2.2 Backdoor

Estos programas son diseñados para abrir una puerta trasera en nuestro sistema de modo tal de permitir al creador del backdoor tener acceso al sistema y hacer lo que desee con él (Quintero, 2011). El objetivo es lograr una cantidad de computadoras infectadas para disponer de ellos libremente hasta el punto de formar redes de botnets.

2.5.3.2.3 Botnets

Los bots son propagados a través de internet utilizando a un gusano como transporte, envíos masivos de ellos mediante correo electrónico o aprovechando vulnerabilidades en navegadores. Normalmente se le conoce como una red de ordenadores zombis infectados por un software malicioso (Inteco, 2010).

2.5.3.2.4 Keylogger

Como su nombre lo indica un Keylogger es un programa que registra y graba la pulsación de teclas (y algunos también clicks del mouse) (Centeno, 2015). La información recolectada será utilizada luego por la persona que lo haya instalado. Actualmente existen dispositivos de hardware o bien aplicaciones (software) que realizan estas tareas.

2.5.3.2.5 Phishing

Es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima (Centeno, 2015).

¿SABIAS QUE?

Las recomendaciones para evitar y prevenir este tipo de estafa son las siguientes:

1. Evite el SPAM ya que es el principal medio de distribución de cualquier mensaje que intente engañarlo. Para ello puede recurrir a nuestra sección de Spam.
2. Tome por regla general rechazar adjuntos y analizarlos aun cuando se esté esperando recibirlos.
3. Nunca hacer clic en un enlace incluido en un mensaje de correo. Siempre intente ingresar manualmente a cualquier sitio web. Esto se debe tener muy en cuenta cuando es el caso de entidades financieras, o en donde se nos pide información confidencial (como usuario, contraseña, tarjeta, PIN, etc.).

Algunas de las características más comunes que presentan este tipo de mensajes de correo electrónico son:

- Uso de nombres de compañías ya existentes. En lugar de crear desde cero el sitio web de una compañía ficticia, los emisores de correos con intenciones fraudulentas adoptan la imagen corporativa y funcionalidad del sitio de web de una empresa existente, con el fin de confundir aún más al receptor del mensaje.
- Utilizar el nombre de un empleado real de una empresa como remitente del correo falso. De esta manera, si el receptor intenta confirmar la veracidad del correo llamando a la compañía, desde ésta le podrán confirmar que la persona que dice hablar en nombre de la empresa trabaja en la misma.
- Direcciones web con la apariencia correcta. Como hemos visto, el correo fraudulento suele conducir al lector hacia sitios web que replican el aspecto de la empresa que está siendo utilizada para robar la información. En realidad, tanto los contenidos como la dirección web (URL) son falsos y se limitan a imitar los contenidos reales. Incluso la información legal y otros enlaces no vitales pueden redirigir al confiado usuario a la página web real.
- Factor miedo. La ventana de oportunidad de los defraudadores es muy breve, ya que una vez se informa a la compañía de que sus clientes están siendo objeto de este tipo de prácticas, el servidor que aloja al sitio web fraudulento y sirve para la recogida de información se cierra en el intervalo de unos pocos días. Por lo tanto, es fundamental para el defraudador el conseguir una respuesta inmediata por parte del usuario. En muchos casos, el mejor incentivo es amenazar con una pérdida, ya sea económica o de la propia cuenta existente, si no se siguen las instrucciones indicadas en el correo recibido, y que usualmente están relacionadas con nuevas medidas de seguridad recomendadas por la entidad.

1. Sepa que su entidad, empresa, organización, etc., sea cual sea, nunca le solicitará datos confidenciales por ningún medio, ni telefónicamente, ni por fax, ni por correo electrónico, ni a través de ningún otro medio existente. Es muy importante remarcar este punto y en caso de recibir un correo de este tipo, ignórelo y/o elimínelo.
2. Otra forma de saber si realmente se está ingresando al sitio original, es que la dirección web de la página deberá comenzar con https y no http, como es la costumbre. La S final, nos da un alto nivel de confianza que estamos navegando por una página web segura.
3. Es una buena costumbre verificar el certificado digital al que se accede haciendo doble clic sobre el candado de la barra de estado en parte inferior de su explorador (actualmente algunos navegadores también pueden mostrarlo en la barra de navegación superior).
4. No responder solicitudes de información que lleguen por e-mail. Cuando las empresas reales necesitan contactarnos tienen otras formas de hacerlo, de las cuales jamás será parte el correo electrónico debido a sus problemas inherentes de seguridad.
5. Si tiene dudas sobre la legitimidad de un correo, llame por teléfono a la compañía a un número que conozca de antemano... nunca llame a los números que vienen en los mensajes recibidos.
6. El correo electrónico es muy fácil de interceptar y de que caiga en manos equivocadas, por lo que jamás se debe enviar contraseñas, números de tarjetas de crédito u otro tipo de información sensible a través de este medio.
7. Resulta recomendable hacerse el hábito de examinar los cargos que se hacen a sus cuentas o tarjetas de crédito para detectar cualquier actividad inusual.

8. Use antivirus y firewall. Estas aplicaciones no se hacen cargo directamente del problema pero pueden detectar correos con troyanos o conexiones entrantes/salientes no autorizadas o sospechosas.

2.5.3.2.6 Framework de Explotación

A diferencia de las aplicación que realizan tareas específicas, son programas que incluyen un conjunto de herramientas que permiten al consultor – dentro de un mismo ambiente – efectuar tareas de reconocimiento, escaneo, análisis de vulnerabilidades y por su puesto hacking (Astudillo, 2013).

El hecho de contar con todo esto en una interfaz facilita el trabajo al auditor, además de proveer un buen punto de inicio para el consultor principiante. Hay varios tipos de framework de explotación comerciales como: Metasploit, Core Impact Pro, Immuny Canvas.

2.5.3.2.7 Metasploit

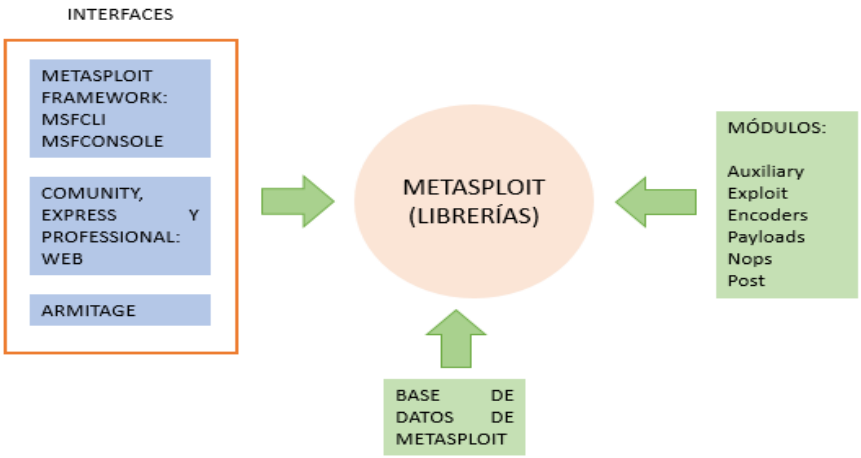


Figura 38. Arquitectura de Metasploit

Este framework está desarrollado en el lenguaje de programación Ruby y está compuesto por librerías, módulos, interfaces y un sistema de archivo proprio. Las librerías se encargan de gestionar la funcionalidad básica de Metasploit, interactuar con los diferentes protocolos soportados y proveer las funciones (API's) que serán a su vez utilizadas por las distintas interfaces disponibles como se muestra en la Fig. 38 (Astudillo, 2013).

Problemas básicos

ACTIVE DIRECTORY

Crear 10 cuentas para el departamento de diseño de una empresa, a las cuales se les deberán aplicar las siguientes.

POLÍTICAS PARA EL DEPARTAMENTO DE DISEÑO:

- Los usuarios deben loguearse solamente de 7:00 am a 8:00 pm
- Los usuarios no deben tener acceso al panel de control
- Debe usarse el papel tapiz de la empresa, no debe poder cambiarse
- Los usuarios deben cambiar su contraseña cada 30 días
- La carpeta documentos de todos los usuarios a apuntará a una carpeta independiente por usuario que esté dentro de la carpeta compartida. \\controladordominio\publica
- Solo los administradores pueden apagar la máquina
- Solo los administradores pueden cambiar la hora del sistema

2.6 Actividades

Analiza y resuelve

Herramienta NMAP

- Instalar NMAP sobre una máquina de Desktop mediante el comando: apt-get install nmap.

- Posteriormente introduciremos las máquinas sobre una misma red, en este caso tres máquinas sobre la red 192.168.50. *, un Windows 7, un Windows 8.

- Comprobamos que los SO de Windows mantienen el Firewall activado.

- Realizado esto y teniendo en cuenta que los Windows por defecto tendrán puertos abiertos, pasaremos a realizar las prácticas siguientes:

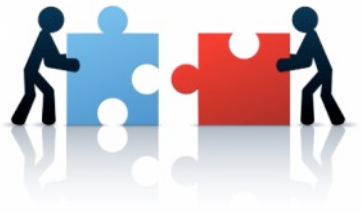
Ejercicio 1

- Extraer las IP de las diferentes máquinas de una misma red. Desde Centos ejecutamos el comando nmap –sP ip de red que deseamos escanear: Comprobando que el nmap devuelve las IPs de las máquinas que están conectadas.
- Mostrar los puertos abiertos en dichas máquinas Utilizando el comando: nmap sT (+ la ip) . El programa realiza un escaneo de los puertos abiertos de la máquina indicada:
- Mostrar los sistemas operativos de dichas máquinas. El comando: nmap -0 (+el número de IP) devuelve el sistema operativo que existe instalado en la máquina escaneada:
- Cualquier otra información que te proporcione NMAP y que consideres de utilidad Los comandos : nmap –sF o –sN o -sX (+la ip). Intentan buscar los paquetes SYN , incluidos en los encabezaros de los paquetes mediante diferentes técnicas; intentando poner al descubierto las máquinas que están detrás del envío de ellos.

Ejercicio 2

1. Direcciones ip de los equipos activos de la red (Ping Scan)
2. Análisis detallados del servidor :S.O y servicios instalados y activos (Intense Scan)
3. Versión del servidor web instalado y estudio de vulnerabilidad.

Problemas de Profundidad



Prueba de penetración: Metasploit

- Instalar una máquina virtual con Kali Linux y otra máquina con Windows 10.
- Verificar que las máquinas tengan visibilidad entre sí, es decir utilizar que puedan comunicarse.
- Luego procedemos a crear un ejecutable, con el cual vamos a tomar el control de una maquina Windows 10, procedemos a utilizar el comando (msfvenom –p) el ejecutable incluirá un payload, el cual será Windows/meterpreter/reverse_ tcp, esto indica que este código malicioso nos dará una sesión inversa para que se conecte con nosotros, posteriormente ingresamos los parámetros para que se conecten con nosotros.
- Le asignamos el nombre WindowsPatch.exe para que sea más atractivo para la víctima.
- Preparar la maquina kali para que este a la escucha de cualquier interacción con el archivo .exe que hemos preparado.
- Luego procedemos a utilizar un handler el servicio que va a estar a la escucha cuando nos llegue la petición de conexión de la maquina víctima.
- Posteriormente especificamos el payload que contiene en archivo con el código malicioso.
- El payload tiene que ser configurado con varias opciones, como el LHOST y el LPORT.
- Ejecutar el payload, pero en el equipo con Kali observaremos que se ha establecido una sesión interprete, desde la cual pedimos obtener el control de la máquina de Windows 10.
- Emplear comandos como hacer una captura de la pantalla.

Visualizar las capturas de pantallas

Verifica conceptos

1. Una con una línea según corresponda.

Nmap	Escáner de vulnerabilidades más popular, herramienta de auditoría de sistemas de información para buscar fallas críticas de seguridad.
Nikto	Herramienta de descifrado de contraseñas que se desarrolló para sistemas tipo UNIX
Nessus	Es un software de código abierto (GPL) para escanear vulnerabilidades en los servidores web
John the Ripper	Herramienta gratuita de código abierto para la exploración de la red o auditoría de Seguridad

2. Escriba verdadero (V) o falso (F):

a) Defensa en profundidad se toma de un término militar usado para describir las contramedidas de la seguridad para formar un ambiente cohesivo de seguridad sin un solo punto de falla. ( )

b) El uso de una solución en niveles aumenta la posibilidad de que se detecten los intrusos y aumenta la posibilidad de que los intrusos logren su propósito. ( )

c) Para reducir al mínimo la posibilidad de que un ataque contra una organización tenga éxito, se debe utilizar el menor número posible de niveles de defensa. ( )

d) La protección a nivel de datos implica listas de control de acceso (ACL) y cifrado. ( )

e) La defensa en profundidad comienza por aplicar una seguridad física a todos los componentes de la infraestructura. ( )

3. Escriba diez acciones que permitan reforzar al máximo posible la seguridad en un sistema operativo:

1) _____
2) _____
3) _____
4) _____
5) _____
6) _____
7) _____
8) _____
9) _____
10) _____

4. Subraya el literal falso:

Las infracciones de seguridad afectan a las organizaciones de diversas formas:

a) Perjuicio a la reputación de la organización.

b) Deterioro de la confianza del cliente.

c) Reanudación de los procesos empresariales.

d) Pérdida o compromiso de la seguridad de los datos.

Problemas básicos

5. Una según corresponda:

Nivel de directivas	Servidores de seguridad de hardware, software o ambos, y creación de redes privadas virtuales con procedimientos de cuarentena.
Nivel de seguridad física	Procedimientos y concienciación: programas educativos de seguridad para los usuarios.
Nivel perimetral	Guardias de seguridad, bloqueos y dispositivos de seguimiento.
Nivel de datos	Prácticas destinadas a reforzar las aplicaciones y el software antivirus.
Nivel de aplicación	Listas de control de acceso (ACL) y cifrado.

6.Subraye las sentencias que correspondan:

La protección en el nivel de seguridad física incluye:

a) Separar los servidores de los operadores humanos y los usuarios.

b) Incluir el uso de placas de identificación y sistemas biométricos.

c) Eliminar todo tipo de mecanismos contra incendios.

d) El acceso debe ser supervisado por guardias de seguridad o mediante un circuito cerrado de televisión.

e) Implementar dispositivos de entrada de datos como las unidades de disquete y de CD-ROM en todos los sistemas.

La protección en el nivel de aplicación incluye:

a) Implementar tecnologías de cifrado y firma con el fin de impedir a los intrusos rastrear los paquetes de la red y reutilizarlos.

b) Las instalaciones de las aplicaciones sólo deberían incluir los servicios y funcionalidad requeridos.

c) Las aplicaciones que se ejecutan en la red se deben instalar de forma segura y se les deben aplicar todas las revisiones y Service Packs correspondientes.

d) Ejecutar los servicios y aplicaciones con el menor privilegio necesario.

e) Se debe requerir que cada usuario se autentique de forma segura en un controlador de dominio y en los recursos a los que tenga acceso.

CAPÍTULO 3

UNIDAD 3

3.1 Tecnologías de seguridad aplicadas en ambientes de red empresarial

3.1.1 Agentes de seguridad de acceso a la nube

El crecimiento de la informática en la nube ha aumentado y ha generado todo un nuevo modelo empresarial. Ofrece a las empresas la posibilidad de modificar la disponibilidad de sus recursos informáticos de manera rápida, fácil, barata y de adaptarse a las exigencias de los recursos informáticos dinámicos (Reis, 2013). En la Fig. 39 se muestra los servicios y dispositivos que se conectan al Cloud Computer

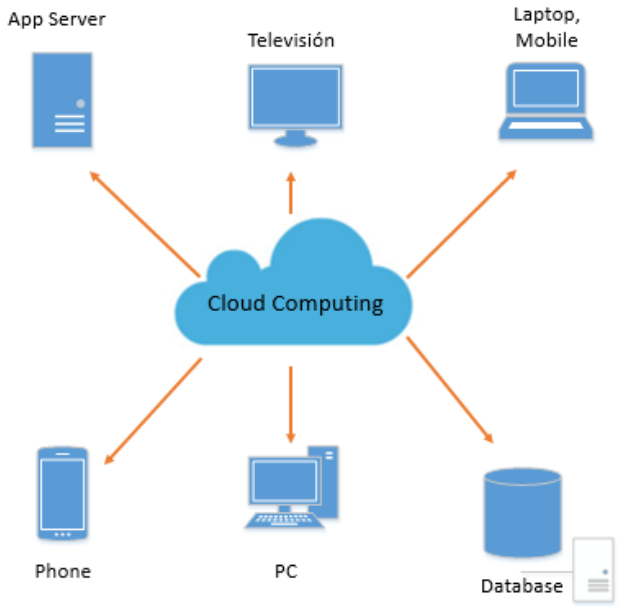


Figura 39. Diagrama de Cloud Computing

Componentes

- **Control de datos.** Se debe hacer un control granular en línea de interacciones de los usuarios con las aplicaciones de la nube, mediante el reconocimiento del uso y la aplicación de políticas para mantener la seguridad de los datos (Sierra, 2017).

- **Control de datos en aplicaciones de la nube y protección contra amenazas.** Proteger las cuentas en la nube, para controlar la actividad de los usuarios y gestionan los datos dentro de las cuentas de la nube (Sierra, 2017).

- **Cloud Data Protection permite cifrar** para garantizar el cumplimiento de las leyes de localización de los datos y otras normas. (Sierra, 2017).

3.1.2 Control de acceso adaptativo

La identificación es permanente en todos los sistemas de seguridad. La autenticación es el proceso que asegura que la otra parte es quien dice ser, por lo que su robustez incide directamente en la fiabilidad de los sistemas de seguridad (Safelayer, 2017).

No existe un mecanismo de autenticación "ideal" que proporcione la máxima seguridad y sea, a la vez, de uso sencillo en todos los contextos. No contemplar el mecanismo de autenticación adecuado puede repercutir en un incremento de costes y actuar de freno para la mejora de la seguridad (Safelayer, 2017).

El **acceso adaptativo** se basa en la combinación de mecanismos de autenticación para proporcionar en cada caso la mejor relación entre seguridad, costes y facilidad de uso. Usa diferentes factores, en cada caso, en función de determinados parámetros del sistema, del contexto o el comportamiento del usuario.

Es una modalidad de control de acceso sensible al contexto, que actúa para equilibrar el nivel de confianza contra el riesgo. El uso de una arquitectura de gestión del riesgo adaptativo posibilita a una empresa permitir el acceso desde cualquier dispositivo y en cualquier lugar, habilitando a un sistema de identificación social acceder a una amplia de recursos de la compañía con perfiles mixtos de riesgo (Merino, 2014).

3.1.3 Sandboxing' ubicuo

Algunos ataques son, inevitablemente, pasados por altos por los mecanismos de protección tradicionales, en cuyo caso resulta clave detectar la intrusión en un período de tiempo tan breve como sea posible. Muchas plataformas de seguridad incluyen ahora funciones para 'detonar' archivos ejecutables, haciéndolos funcionar en máquinas virtuales y monitorizándolos en busca de funciones maliciosas (Merino, 2014).

3.1.4 Soluciones edr

Más allá de detener el enorme volumen de amenazas, detectar y proteger contra éstas avanzadas se ha convertido en algo esencial para mantener endpoints confiables. La seguridad de endpoint complementa las medidas de seguridad centralizada con protección adicional en el punto de entrada para muchas amenazas, así como bloquea efectivamente los intentos de acceso previos a la entrada (Techtarget, 2015).

Mercado emergente creado para satisfacer la necesidad de una protección continua contra amenazas en los 'puntos finales' (PC de escritorio, tablets, portátiles…) registrando en una base de datos centralizada eventos relativos tanto a los mismos

como a la red, para a continuación analizar la base de datos en busca de factores que afecten a la seguridad del sistema (Sierra, 2017).

3.1.5 Analítica 'big data' de seguridad

Esta tecnología podrá identificar los patrones de 'lo normal' para así detectar cuando se produzcan desviaciones significativas respecto a la misma.

3.1.6 Inteligencia de amenazas procesable

La capacidad para integrar fuentes de inteligencia externas y contexto se convertirá en un diferenciador fundamental para la próxima generación de plataformas de seguridad.

3.1.7 Contención y aislamiento

En un mundo donde las compañías son cada vez más ineficaces para detener los ataques, una estrategia alternativa es tratar a todo lo que no se conoce como no confiable y aislar a su ejecución para que no pueda causar daños permanentes en el sistema. Se prevén unos niveles de adopción cercanos al 20% para 2016.

3.1.8 Seguridad basada en software

Se trata de un modelo de seguridad en el que la detección de intrusiones, la segmentación de la red y los controles de acceso están automatizados y controlados mediante software.

3.1.9 Pruebas interactivas de seguridad de aplicaciones

Esta técnica (también conocida con IAST) combina, a su vez, tests estáticos de seguridad de aplicaciones (CET) y tests dinámicos de seguridad de aplicaciones (DAST); y hace posible confirmar o refutar la gravedad de la vulnerabilidad detectada, así como determinar su procedencia en el código de la aplicación.

3.1.10 Pasarelas y cortafuegos para el internet de las cosas

La 'tecnología operativa' es considerada el subconjunto industrial de la "Internet de las Cosas" e incluirá miles de millones de sensores interconectados, dispositivos y sistemas, muchos de los cuales se comunicarán sin intervención humana y necesitarán estar protegidos.

3.2 Importancia de los protocolos

El enrutamiento dentro de las redes de datos es de suma importancia ya que los routers son los encargados de transferir paquete de una red origen-destino, un router es conocido como enrutador o encaminador de paquetes, en donde el router desempeña la función de seleccionar la mejora ruta o la red, conmutación de paquetes y reenvió de paquetes.

Por ende, los protocolos de enrutamiento proporcionan mecanismos distintos para elaborar y

mantener las tablas de enrutamiento de los diferentes routers de la red, así como determinar la mejor ruta para llegar a cualquier host remoto. Entre ellos tenemos el protocolo de enrutamiento estático y el protocolo de enrutamiento dinámico cada uno de ellos tienes sus propias funciones, así como sus ventajas y desventajas al ser implementadas.

3.2.1 Protocolos de enrutamiento

Un protocolo de enrutamiento es un conjunto de procesos, algoritmos y mensajes que se usan para intercambiar información de enrutamiento usando las tablas de enrutamiento con la elección de los mejores caminos que realiza el protocolo para poder dirigir o enrutar los paquetes hacia diferentes redes en la tabla 10 se muestran los protocolos de enrutamiento más importante.

Tabla 10. Protocolos de enrutamiento

Características	RIPv1	RIPv2	EIGRP	IS-IS	OSPF	BGP
Vector Distancia	✓	✓	✓	x	x	✓
Estado de Enlace	x	x	x	✓	✓	x
Direccionamiento sin clase	x	✓	✓	✓	✓	✓
VLSM	x	✓	✓	✓	✓	✓
Sumarización automática	✓	✓	✓			✓
Sumarización manual	x	✓	✓	✓	✓	✓
Requiere diseño jerárquico	x	x	x	✓	✓	x
Tamaño de la red	Pequeño	Grande	Grande	Grande	Grande	Muy Grande
Métrica	Saltos	Saltos	Compuesta	Métrica	Costo	Atributos de ruta
Tiempo de convergencia	Lento	Lento	Muy rápido	Rápido	Rápido	Muy lento
Distancia administrativa(AD)	120	120	5/90/170	115	110	20/200
Número de Protocolo	x	x	88	124	89	x
Número de puerto	x	520 UDP	x	x	x	179 TCP
Entrada en la tabla de enrutamiento	R	R	D(*)	i	O(*)	B
Tipos de Paquetes	Query Update	Query Update	Hello Update Query Reply Ack	Hello Link Stare Sequence	Hello DBD LSR LSU LSAck	Open Keepalive Update Notification

3.2.1.1 El propósito de un protocolo de enrutamiento

- Descubrir redes remotas.
- Mantener la información de enrutamiento actualizada.
- Escoger el mejor camino hacia las redes de destino.
- Poder encontrar un mejor camino nuevo si la ruta actual deja de estar disponible.

Su función principal es facilitar el intercambio de información, esto permite compartir información de redes remotas y agregarla automáticamente a la tabla de enrutamiento.

3.2.3 Componentes de un protocolo de enrutamiento

Estructuras de datos

Tablas o bases de datos que se guardan en la memoria RAM.

Algoritmos

Conjunto de pasos a seguir para completar una tarea.

Mensajes de protocolo

Utilizado por los routers para intercambiar información, descubrir routers u otras tareas.

Actividades de Enrutar

Determina las trayectorias óptimas a través de una red.

- Menor retardo.
- Mayor fiabilidad.

Transportar paquetes a través de la red.

- Examina la dirección de destino del paquete.
- Decide a través de qué puerto enviar el siguiente paquete.
- Basa su decisión en la tabla de rutas.

Los enrutadores interconectados intercambian sus tablas de rutas para mantener una visión clara de la red.

En una red grande, los intercambios de tablas pueden consumir mucho ancho de banda.

- Se requiere un protocolo para actualización de rutas.

Existen protocolos de enrutamiento estático y dinámicos.

Los protocolos de enrutamiento permiten a los routers poder dirigir o enrutar los paquetes hacia diferentes redes usando tablas.

Protocolo de Enrutamiento Estático

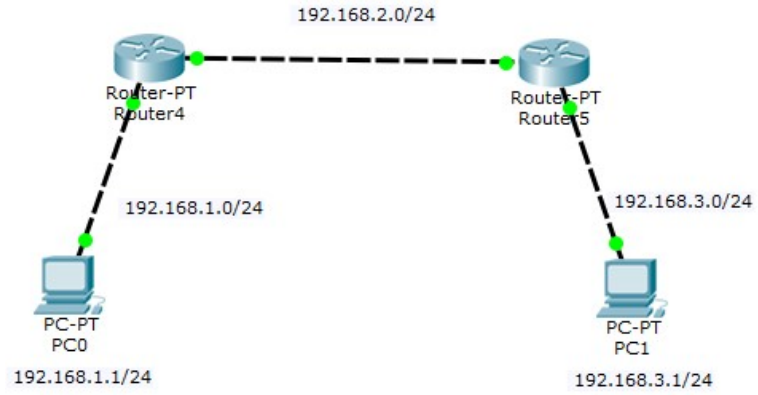
Es generado por el propio administrador, todas las rutas estáticas que se le ingresen son las que el router "conocera", por lo tanto, sabrá enrutar paquetes hacia dichas redes.

Comando iproute

Este comando se utiliza para configurar una ruta estática en los routers Cisco comando se utiliza para configurar una ruta estática en los routers Cisco, la sintaxis es la siguiente:

```
ip route prefijo máscara {dirección_ip |
tipo_de_interfaz número_de_interfaz}
[distancia] [tag etiqueta] [permanent]
```

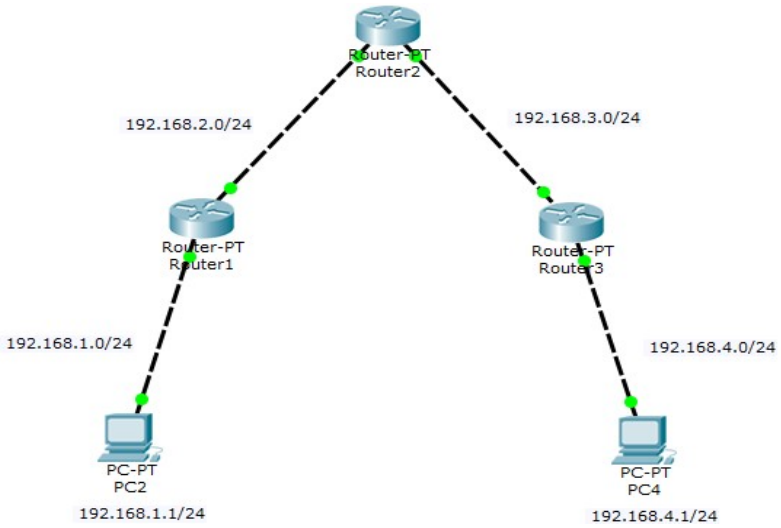
En el siguiente gráfico mostramos un ejercicio de enrutamiento estático.



Router4: ip route 192.168.3.0 255.255.255.0 192.168.2.2

Router5: ip route 192.168.1.0 255.255.255.0 192.168.2.1

A continuación, mostramos otro ejercicio de enrutamiento estático.



Router1: ip route 192.168.3.0 255.255.255.0 192.168.2.2
ip route 192.168.4.0 255.255.255.0 192.168.2.2

Router2: ip route 192.168.1.0 255.255.255.0 192.168.2.1
ip route 192.168.4.0 255.255.255.0 192.168.3.2

Router3: ip route 192.168.2.0 255.255.255.0 192.168.3.1
ip route 192.168.1.0 255.255.255.0 192.168.3.1

Protocolos de Enrutamiento Dinámico

Con un protocolo de enrutamiento dinámico, el administrador sólo se encarga de configurar el protocolo de enrutamiento mediante comandos IOS, en todos los routers de la red y estos automáticamente intercambiarán sus tablas de enrutamiento con sus routers vecinos, por lo tanto cada router conoce la red gracias a las publicaciones de las otras redes que recibe de otros routers.

Ventajas

- Comparten automáticamente la información acerca de las redes remotas.
- Determinan la mejor ruta para cada red y agregan esta información a sus tablas de enrutamiento.
- En comparación con el routing estático, los protocolos de enrutamiento dinámico requieren menos sobrecarga administrativa.
- Ayudan al administrador de red a administrar el proceso prolongado que implica configurar y mantener las rutas estáticas.

Desventajas

- Dedican parte de los recursos de los routers al funcionamiento del protocolo, incluso el tiempo de CPU y el ancho de banda del enlace de red.
- En ocasiones, el enrutamiento estático es más adecuado

Algunos protocolos de enrutamiento dinámicos

RIP

Protocolo de enrutamiento de gateway Interior por vector distancia.

IGRP

Protocolo de enrutamiento de gateway Interior por vector distancia, del cual es propietario CISCO.

EIGRP

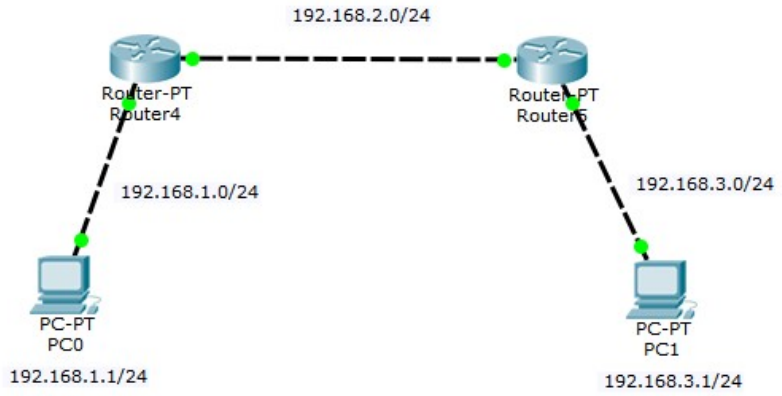
Protocolo de enrutamiento de gateway Interior por vector distancia, es una versión mejorada de IGRP.

OSPF

Protocolo de enrutamiento de gateway Interior por estado de enlace.

BGP

Protocolo de enrutamiento de gateway exterior por vector distancia.



Router4

router > enable
router # configure terminal
router (config)# router rip
router (config-router)# network 192.168.1.0
router (config-router)# network 192.168.2.0

Router5

router > enable
router # configure terminal
router (config)# router rip
router (config-router)# network 192.168.2.0
router (config-router)# network 192.168.3.0

3.3 Importancia de la calidad de la disponibilidad

La disponibilidad es una de las características de las arquitecturas empresariales que mide el grado con el que los recursos del sistema están disponibles para su uso por el usuario final a lo largo de un tiempo dado. Ésta no sólo se relaciona con la prevención de caídas del sistema (también llamadas tiempos fuera de línea, downtime u offline), sino incluso con la percepción de "caída" desde el punto de vista del usuario: cualquier circunstancia que nos impida trabajar productivamente con el sistema – desde tiempos de respuesta prolongados, escasa asistencia técnica o falta de estaciones de trabajo disponibles – es considerada como un factor de baja disponibilidad.

3.4 Calidad de servicio en una red convergente

3.4.1 Definición de una red convergente

Una red convergente no es únicamente una red capaz de transmitir datos y voz sino un entorno en el que además existen servicios avanzados que integran estas capacidades, reforzando la utilidad de los mismos. A través de la convergencia, una compañía puede

reinventar tanto sus redes de comunicaciones como toda su organización. Una red convergente apoya aplicaciones vitales para estructurar el negocio -Telefonía IP, videoconferencia en colaboración y Administración de Relaciones con el Cliente (CRM) que contribuyen a que la empresa sea más eficiente, efectiva y ágil con sus clientes.

3.4.2 Impacto en los negocios

Las empresas descubren que los beneficios de la convergencia afectan directamente los ingresos netos:

Las soluciones convergentes nos hacen más productivos, pues simplifican el usar aplicaciones y compartir información.

Tener una red para la administración significa que el ancho de banda será usado lo más eficientemente posible, a la vez que permite otras eficiencias y ahorros de costos: en personal, mantenimiento, cargos de interconexión, activaciones, mudanzas y cambios.

Los costos más bajos de la red, productividad mejorada, mejor retención de clientes, menor tiempo para llegar al mercado-son los beneficios netos que posibilitan las soluciones de redes convergentes.

Reducción de costos de personal para la administración de red y mantenimiento.

Viabilidad de las Redes Convergentes

En lo general, los directores y/o gerentes de IT presentan grandes proyectos de convergencia los cuales enfrentan el problema de su justificación.

Es recomendable, crear una visión de la red convergente de la empresa y empezar por resolver en etapa esta visión.

Las recomendaciones son:

1. Empezar por la red WAN de la empresa (si la tiene), unificar en un mismo medio voz, datos y video por un mismo medio, nos da los beneficios de:

Administrar un solo equipo (router)

Aprovechar anchos de banda desperdiciados por la demanda de cada aplicación (voz, datos, video, etc.)

Aprovechar anchos de banda por horarios, existen generalmente diferentes picos de demanda en cada aplicación (voz, datos, video, etc.)

Verifica conceptos

1. En seguridad informática una DMZ (zona desmilitarizada) es:

a) Una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
b) Cualquier ataque informático que no use la red.
c) Una red local que se encuentra entre la red interna de una organización y una red externa como internet.

2. Escriba tres razones que justifiquen la creación de Listas de control de acceso (ACL).

_____
_____
_____
_____
_____
_____

3. ¿Qué es un proxy público?

_____
_____
_____
_____
_____
_____

4. De las siguientes sentencias, identifique la o las falsas:

a) Un firewall es un dispositivo que filtra el tráfico entre redes.
b) Para que un firewall funcione debe tener al menos dos tarjetas de red.
c) En una zona desmilitarizada debe ubicarse un solo servidor que sea accesible desde internet.
d) Un proxy actúa como un relé para facilitar la conexión entre dos puertos.
e) Los firewalls no pueden ser usados en cualquier red.

5. Complete:

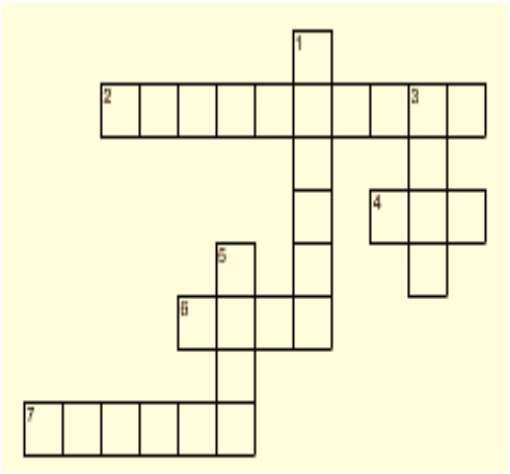
_____ es un sistema de firewall vinculado al Kernel de Linux y básicamente su función es aplicar reglas por medio de comandos. Las reglas de tipo _____ filtran los paquetes dirigidos al cortafuegos, las de tipo _____ filtran los paquetes que se originan desde el cortafuegos y las reglas _____ filtran los paquetes dirigidos a la red protegida por el cortafuegos.

Problemas básicos

6. En las siguientes sentencias de Iptable seleccione la que permite habilitar en un servidor web el puerto 80:

a) iptables – A INPUT –s 80.37.45.194 –p tcp –dport 80 –j ACCEPT
b) iptables –A INPUT –p tcp –dport 80 –j ACCEPT
c) iptables –A INPUT –p tcp –dport 80 –j DROP

7. En el siguiente crucigrama encuentre las acciones más comunes para las reglas IP Tables.

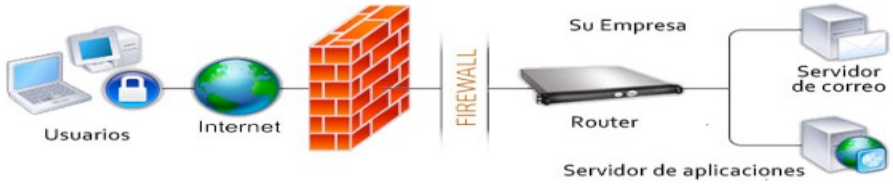


HORIZONTAL

2 .Para hacer NAT de origen.
4. La información del paquete s envía al proceso encargado de registro el log.
6. Para hacer NAT de origen cambiando la dirección IP de destino.
7.El paquete se entrega al sistema operativo para ser procesado

VERTICAL

1. El paquete es bloqueado pero en este caso se envía al origen en mensaje d error.
3.. El paquete es bloqueado.
5. Para hacer NAT en destino cambiando la dirección IP de origen.



CAPÍTULO 4

4.1 Métodos de encriptación y la importancia que tienen estos para la seguridad de los correos electronicos.
4.2 Algoritmos apropiados para ejecutar una encriptación.
4.3 Modelos de encriptación a la hora de transmitir datos.
4.4 Importancia de cifrar los datos en un canal seguro.
4.5 Actividades

UNIDAD 4

4.1 Métodos de encriptación y la importancia que tienen estos para la seguridad de los correos electrónicos

La encriptación se desarrolla mediante métodos y técnicas numéricas para codificar un mensaje a través de un algoritmo, usando una o más claves (Borghello, 2009a).

Los métodos criptográficos más importantes, y que a continuación serán detalladas, son: criptografía Simétrica y criptografía Asimétrica.

4.1.1 Criptografía simétrica

Técnica de encriptación que utiliza la misma clave para cifrar y descifrar los mensajes. Para la correcta comunicación, las dos partes deben ponerse de acuerdo previamente sobre cuál es la clave que se va a utilizar. Tras tener acceso a esa clave, el remitente cifra un mensaje usándola, lo envía a un destinatario y usando la clave acordada lo descifra (López, 2002).

Esta forma de cifrado no ofrece problema de seguridad, ya que tras el intercambio de las claves las comunicaciones son seguras. Pero no garantiza la seguridad del canal utilizado para la transmisión de las claves. En caso de un potencial ataque, sería más fácil realizarlo intentando interceptar la clave que probando las combinaciones posibles.

Como ejemplos de criptografía Simétrica se encuentran los siguientes: DES, 3DES, RC5, AES, Blowfish e IDEA.

4.1.2 Criptografía asimétrica

Esta técnica se caracteriza por la utilización de dos claves para enviar mensajes. Estas claves pertenecen a la persona a la que se le envía el mensaje. Una de ellas es pública, pudiéndose entregar a cualquier persona. Mientras, la otra es privada y debe ser guardada de forma segura, sin que nadie pueda acceder a ella (Angel, 2010).

Si el remitente utiliza la clave pública ofrecida por el destinatario para cifrar el mensaje, este mensaje sólo podrá ser descifrado por la clave privada del destinatario, ya que es el único que la conoce. De esta forma se consigue que el envío del mensaje sea confidencial.

En el caso de que el propietario del par de claves utilizara su clave privada con el fin de cifrar el mensaje, cualquiera podría descifrarlo utilizando su clave pública. De esta forma, se consigue la autentificación e identificación de quién remite, ya que sólo él puede emplear su clave privada, excepto en el caso de que alguien la hubiera robado.

Con estos sistemas de cifrado asimétricos, se elimina el problema de la seguridad durante el intercambio de claves que supone el uso de sistemas de cifrado simétricos.

4.1.3 Funciones hash

Una función Hash es una función matemática para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito generalmente menor. Estas propiedades serán esenciales en el uso de estos códigos en la firma electrónica.

Las funciones Hash criptográficas son utilizadas en multitud de contextos: identificación de ficheros, comprobación de integridad de ficheros, autenticación de usuarios o para la firma electrónica.

4.1.4 Seguridad del correo electrónico

La utilización del correo electrónico por Internet o por otras redes que no sean de confianza supone riesgos de seguridad para su sistema, aunque este esté protegido por un cortafuego.

Debe conocer estos riesgos para garantizar que su política de seguridad indique cómo minimizarlos.

El correo electrónico es similar a otras formas de comunicación. Es importante ser prudente a la hora de enviar información confidencial por correo electrónico. El correo electrónico viaja a través de numerosos sistemas antes de llegar a su destino, por lo que es posible que alguien lo intercepte y lo lea. Por lo tanto, convendrá que emplee medidas de seguridad para proteger la confidencialidad del correo electrónico.

4.1.5 Riesgos más comunes de la seguridad del correo electrónico

La Inundación

El spam se define como los mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva a muchos usuarios al mismo tiempo. La vía más utilizada es la basada en el correo electrónico pero puede presentarse por programas de mensajería instantánea o por teléfono. El término spam proviene de la contracción de Spiced Ham (carne especiada), un producto muy comercializado en Reino Unido durante la Segunda Guerra Mundial. Años más tarde, el grupo humorístico británico The Monty Python fue el responsable de otorgarle el significado que tiene hoy spam tras popularizar una broma televisiva en la que sus protagonistas repetían esta palabra en innumerables ocasiones, de la misma manera en que ahora lo hace el correo no deseado (Heras, 2000).

Correo masivo

Es otro tipo de ataque común dirigido al correo electrónico. Con el aumento del número de empresas que practican el comercio electrónico en Internet, se ha producido una invasión de mensajes comerciales de correo electrónico no deseados o no solicitados. Este es el correo basura, que se envía a una amplia lista de distribución de usuarios de correo electrónico, llenando el buzón de correo de todos los usuarios.

La Confidencialidad

Es un riesgo asociado al envío de correo electrónico a otra persona a través de Internet. El mensaje de correo electrónico pasa a través de numerosos sistemas antes de llegar al destinatario. Si el mensaje no está cifrado, cualquier pirata informático podría hacerse con él y leerlo en cualquier punto de la ruta de entrega (Álvarez & Pérez, 2004).

4.1.6 Importancia de cifrar los correos electrónicos

El software de cifrado de correo es importante ya que frustra los riesgos planteados por los espías de la red. Por defecto, el correo electrónico no está generalmente protegido por protocolos como SSL/TLS, y se transmite en texto plano a través de redes locales e Internet. Como resultado, el contenido de los mensajes de correo, así como sus adjuntos, pueden ser interceptados y leídos por un atacante en el camino entre el emisor y el receptor (por no hablar de los correos archivados almacenados en un servidor).

Esto crea problemas obvios cuando se envía datos sensibles a través del correo, aunque solo entre dos usuarios de la misma organización.

Todo lo que toma es que un host esté infectado con malware para permitir la interceptación de mensajes de correo electrónico y la ex filtración de información sensible.
En respuesta a estos riesgos, las organizaciones implementan el software de cifrado de correo para cifrar cada mensaje de correo y archivo adjunto sensibles (y en algunos casos, cada correo electrónico, punto) antes de enviarlos. El receptor es el responsable de descifrar los mensajes y archivos adjuntos.

4.1.7 Estándares para cifrar correos

Funcionamiento de PGP

PGP funciona con criptografía asimétrica (aunque por cuestiones de eficiencia también hace uso de criptografía simétrica), y su punto fuerte radica en la facilidad que ofrece a los usuarios comunes para generar las claves (algo que como antes he mencionado no es en absoluto trivial) y gestionarlas (Carlos Lamas & Escriba, 1997).

PGP proporciona lo que se denomina "anillo de claves" (llavero), que es un único fichero donde el usuario puede guardar todas sus claves, con facilidad para realizar inserción y extracción de claves de manera sencilla. Además, proporciona un mecanismo de identificación y autentificación de claves (certificación de que una clave pública es realmente de quien dice que es) para evitar los "ataques de intermediario". Estos ataques consisten en que una persona que intervenga el canal de comunicación nos proporcione una clave pública falsa del destinatario al que deseamos enviar el mensaje.

Para autentificar claves, PGP permite que los usuarios "firmen claves", por lo que podemos confiar en la autenticidad de una clave siempre que ésta venga firmada por una persona de

confianza. Así la "autoridad de certificación" de otro tipo de sistemas (entidades que aseguran la autenticidad de las claves), en PGP son los propios usuarios.

Como cualquier herramienta, PGP proporciona un nivel de seguridad muy bueno y gran rendimiento si se utiliza correctamente. Sin embargo, un uso inadecuado puede convertirlo en algo completamente inútil.

4.1.8 Servidor de Correo

Un servidor de correo es una aplicación informática que tiene como objetivo, enviar, recibir y gestionar mensajes a través de las redes de transmisión de datos existentes, con el fin de que los usuarios puedan mantenerse comunicados con una velocidad muy superior a la que ofrecen otros medios de envío de documentos.

Configuración de correo en Centos

Para comenzar con el procedimiento utilizaremos Postfix, este es un servidor de correo de software libre y código abierto, que se lo utiliza normalmente para el enrutamiento y envío de correo electrónico, fue creado con la intención para que sea una alternativa más rápida, fácil de administrar y segura ampliamente utilizado Sendmail.

Primero se debe instalar los paquetes de postfix.
yum -y install postfix*

Comprobamos si el servicio se está correctamente ejecutando a través del siguiente comando.
systemctl status postfix.service
Ahora vamos a configurar el archivo de postfix.
gedit /etc/postfix/main.cf

Dentro de archivo postfix varios de los comandos se encuentran comentado con el signo #, debemos descomentar algunos comandos entre ellos están:
myhostname= accserver.localdomain.com

En el comando “mydomain” ponemos el nombre del servidor que utilizamos, para hacer la cuenta de los usuarios de quienes van a pertenecer al servicio.
mydomain= accserver.com
myorigin= $mydomain
inet_interfaces= all
Por defecto nos trae la interfaz de manera local y comentamos tal comando:
#inet_interfaces= localhost

Por defecto nos trae la configuración de destino descomentada y la cual esta no usaremos, por lo tanto lo volvemos a comentar de esta manera:
#mydestination= $myhostname, localhost.$mydomain, localhost

y luego descomentamos al comando, que si vamos a utilizar:
mydestination= $myhostname, localhost.$mydomain, localhost, $mydomain

Procedemos a descomenta el siguiente comando:
home_mailbox= Maildir/

En “mynetworks” descomentamos y luego debemos colocar una dirección de red válida para nuestro servidor.
mynetworks= 192.168.43.0/24 127.0.0.0/8

Una vez realizado todo esto, presionamos el botón” Guardar” de la terminal y posteriormente cerramos el archivo.

Para el siguiente paso, reiniciamos el servicio de postfix, a través del comando:
systemctl restart postfix.service

Ahora con los siguientes comandos creamos los usuarios netamente en CentOS para los cuales vamos a utilizar en nuestro servicio de postfix. Ver figura 39.
useradd danny

Asignamos una contraseña.
passwd danny

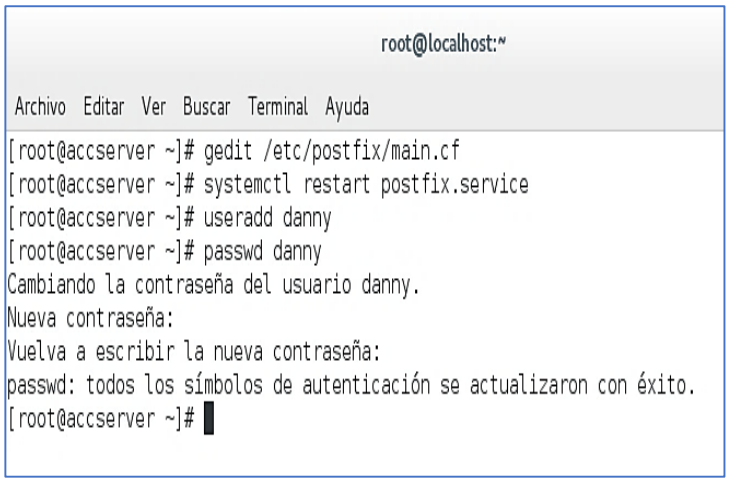


Figura 40. Creación de usuario.

Ahora hacemos un envío de mensaje de prueba, en donde utilizaremos el comando telnet y luego procedemos a escribir los siguientes parámetros. Ver figura 40.
telnet localhost smtp
Nota:

- ✓ Con el parámetro punto “.” Hacemos la terminación del texto.
- ✓ Con el parámetro “quit” damos por terminado del servicio.

```
root@localhost:~
 Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@accserver ~]# telnet localhost smtp
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 accserver.localdomain.com ESMTP Postfix
ehlo localhost
250-accserver.localdomain.com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
mail from: danny
250 2.1.0 Ok
rcpt to: alex
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
mensaje de prueba
.
250 2.0.0 Ok: queued as 8268520F323F
quit
```

Figura 41. Mensaje de prueba.

Para verificar si el mensaje ha llegado al otro usuario, digitamos el siguiente comando.
cd /home/alex/Maildir/new
ls -l
Para el siguiente paso, debemos utilizar el servicio llamado “Dovecot”, es un servidor de POP3 e IMAP de fuente abierta que funciona en Linux y sistemas basados sobre Unix™ y diseñado con la seguridad como principal objetivo. **Dovecot** puede utilizar tanto el formato **mbox** como **maildir** y es compatible con las implementaciones de los servidores UW-IMAP y Courier IMAP.

Lo instalamos con el siguiente comando.
yum -y install dovecot*

Configuramos el archive dovecot.
gedit /etc/dovecot/dovecot.conf

Procedemos a descomentar el comando relacionado con el postfix para el respectivo funcionamiento y después de ello damos click en el botón “Guardar” y cerramos la terminal del archivo. Ver figura 41.
protocols= imap pop3 lmtp

```
# Default values are shown for each setting, it's not required to uncomment
# those. These are exceptions to this though: No sections (e.g. namespace {})
# or plugin settings are added by default, they're listed only as examples.
# Paths are also just examples with the real defaults being based on configure
# options. The paths listed here are for configure --prefix=/usr
# --sysconfdir=/etc --localstatedir=/var

# Protocols we want to be serving.
protocols = imap pop3 lmtp

# A comma separated list of IPs or hosts where to listen in for connections.
# "*" listens in all IPv4 interfaces, "::" listens in all IPv6 interfaces.
# If you want to specify non-default ports or anything more complex,
# edit conf.d/master.conf.
#listen = *, ::
```

Figura 42. Configuración archivo dovecot.

Colocamos el siguiente comando para modificar algunos archivos y luego digitamos con el comando ls para observar los archivos pertenecientes. Ver figura 41.
cd /etc/dovecot/conf.d

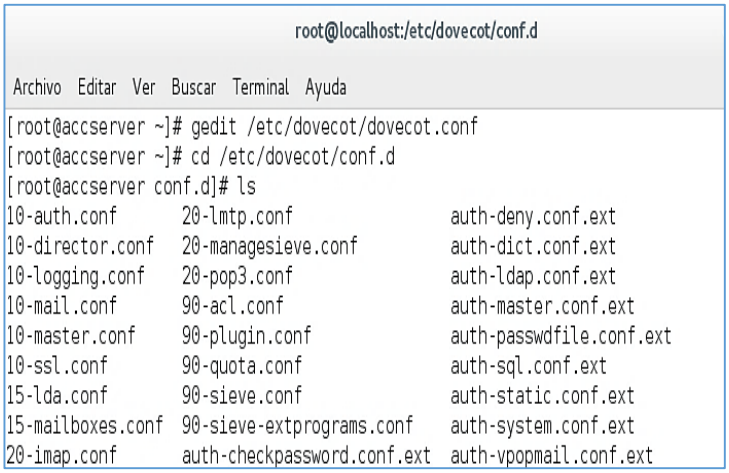


Figura 43. Acceso a dovecot/conf.d

Comenzamos a escribir los comandos de los archivos a modificar.

- ✓ Primer archivo
  gedit 10-auth.conf

Una vez que escribimos el comando, se abrirá una ventana del archivo para lo cual descomentaremos **disable_plaintext_auth= no** luego guardamos y cerramos.

- ✓ Segundo archivo.
  gedit 10-mail.conf

Se abrirá una ventana donde descomentaremos **disable_plaintext_auth= yes** seguido a esto cambiamos el valor del parámetro a un valor **no.** Por lo tanto, quedará de esta forma: **disable_plaintext_auth= no** luego guardamos los cambios y cerramos la ventana del archivo.

- ✓ Tercer archivo
  gedit 10-email.conf

Descomentaremos las siguientes opciones, y luego de eso guardaremos.
mail_location= maildir:~/Maildir
Aquí colocamos los siguientes valores:
mail_uid= vmail
mail_gid=vmail

- ✓ Cuarto archivo
  gedit 20-pop3.conf

Descomentaremos las siguientes opciones, y luego de eso guardaremos.
pop3_uidl_format = %08Xu%08Xv

Reiniciamos y comprobamos el estado el servicio de dovecot. Ver figura 43.
systemctl restart dovecot.service

systemctl start dovecot.service

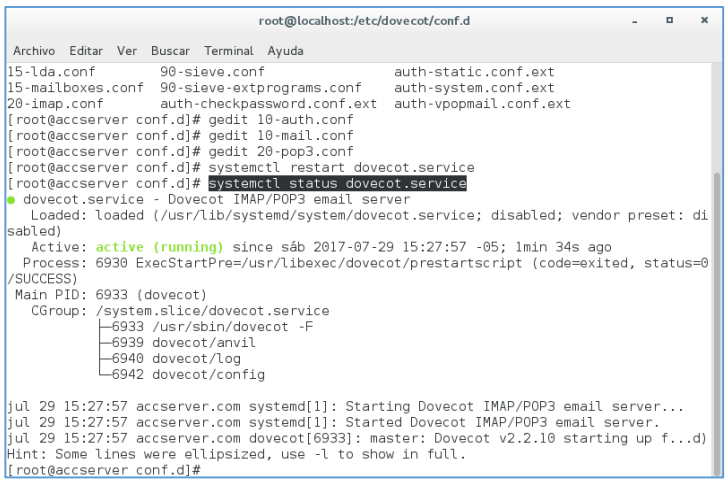


Figura 44.Comprobación del servicio dovecot

Debemos descargar Thunderbind, y lo haremos a través del siguiente enlace.

https://centos.pkgs.org/7/centos-86_64/thunderbird-45.4.0-1.el7.centos.x86_64.rpm.html

Accedemos a la carpeta descarga y comprobamos que el programa este allí. Ver figura Presionamos sobre el programa y procedemos a instalarlo. Ver figura 44 y 45.

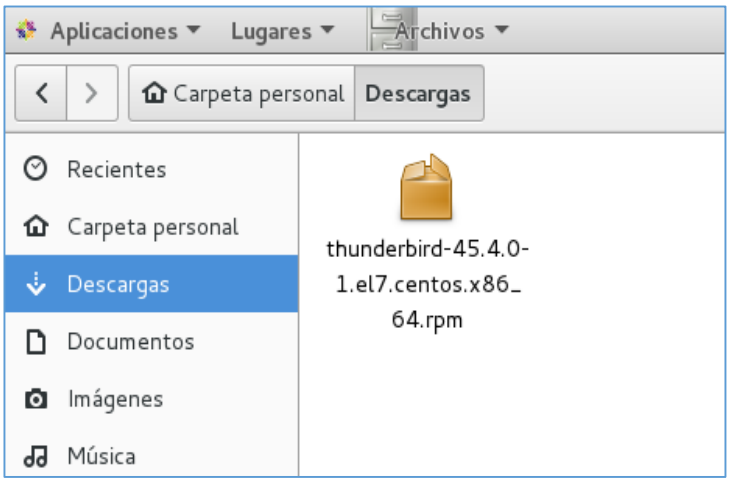


Figura 45. Programa Thunderbird

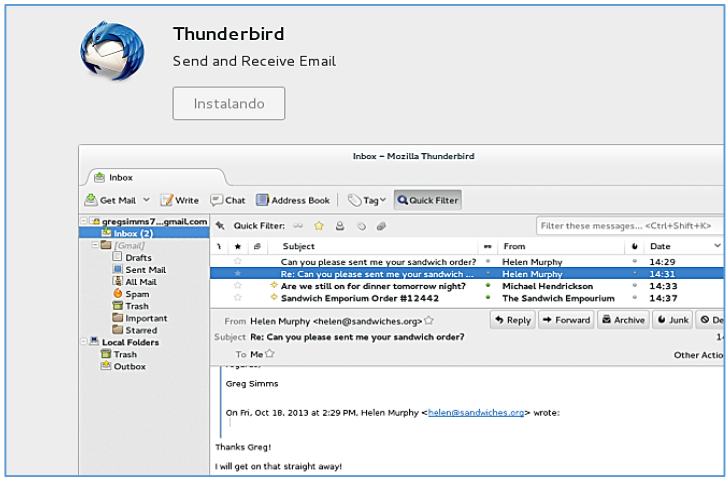


Figura 46. Instalación de Thunderbird

Para abrir el programa seguimos los siguientes pasos: **Aplicaciones>Thunderbird** Creamos las cuentas de usuario. Ver figura 46.

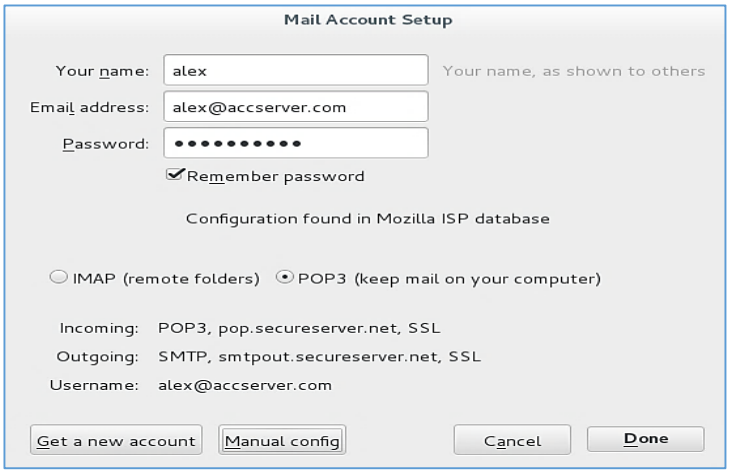


Figura 47. Creación de usuario.

Configuramos manualmente, para eso damos click en el botón **Manual Config.** Ver figura 47.

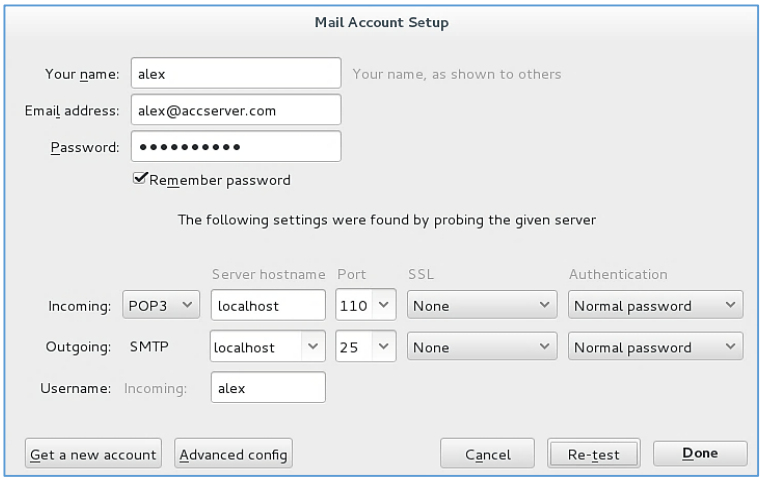


Figura 48. Configuración de cuenta usuario.

Aparecerá un aviso de peligro el cual presionamos el check **I understand the risks** damos click en Done. Ver figura 48.

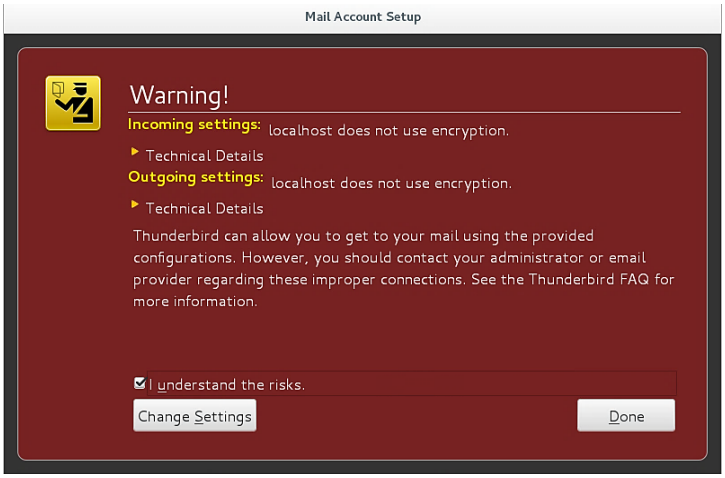


Figura 49. Ventana de alerta.

Nos fijamos que se ha creado correctamente. Ver figura 49.

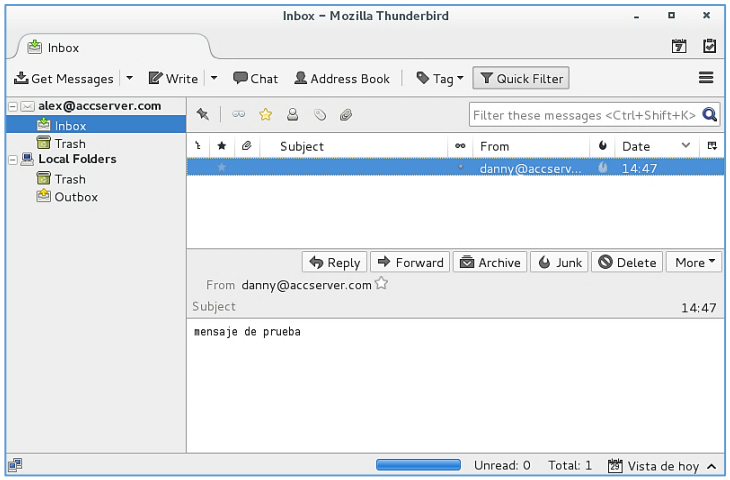


Figura 50. Verificación del usuario creado.

Creamos el usuario 2. Presionamos click en el botón **Skip this and use my existing email.** Ver figura 50.

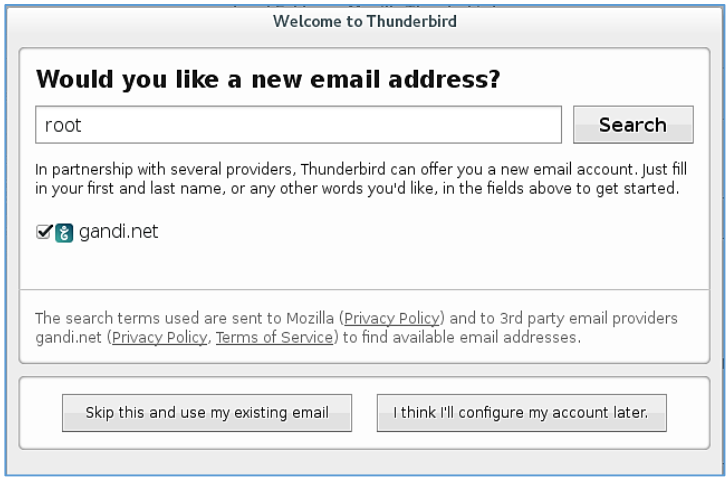


Figura 51. Creación de usuario 2.

Y seguimos los pasos anteriormente indicados. Ver figura 51, 52, 53.

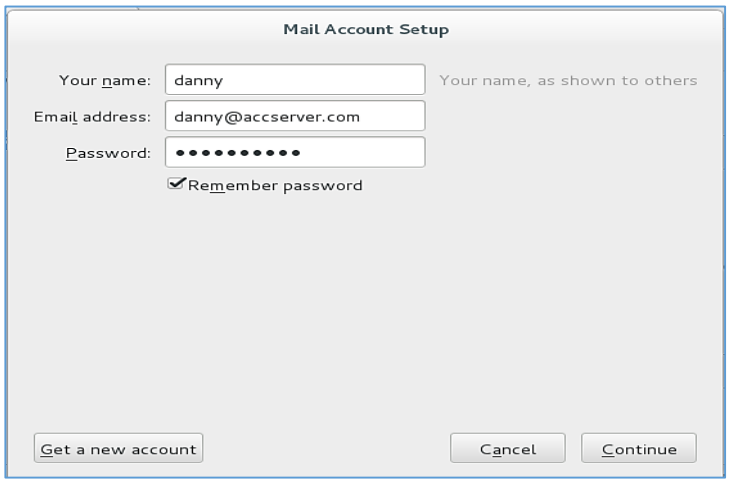


Figura 52. Creación usuario 2. Paso 1.

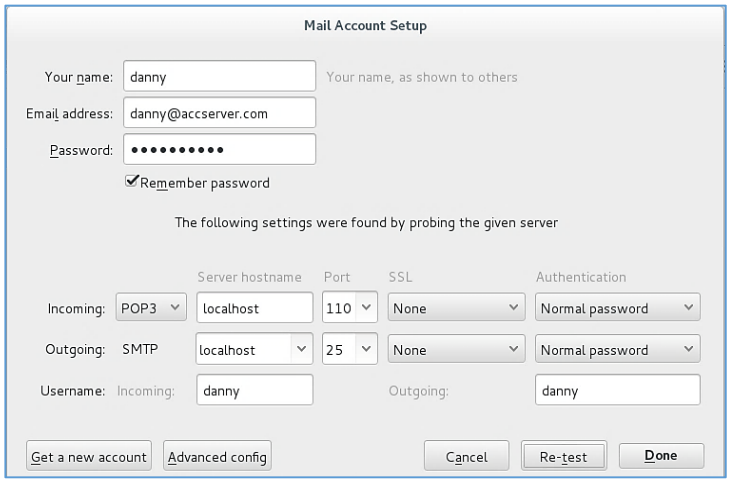


Figura 53. Creación usuario 2. Paso 2.

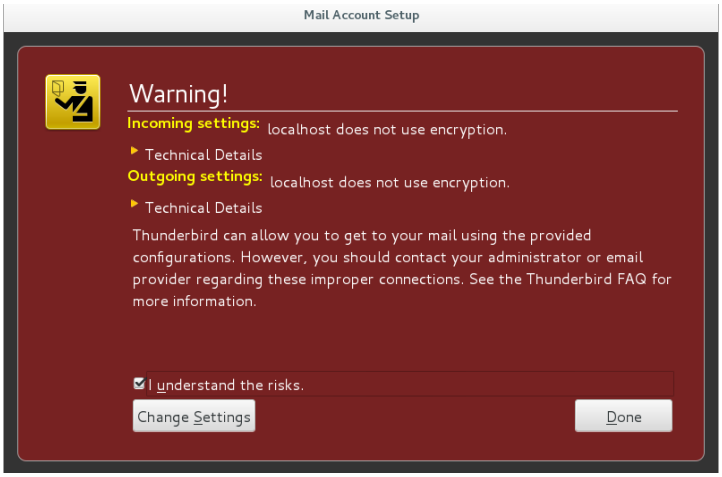


Figura 54. Creación usuario 2. Paso 3.

Una vez finalizado la creación de los dos usuarios, realizamos una prueba de envío de mensaje para comprobar su funcionamiento. Ver figura 54.

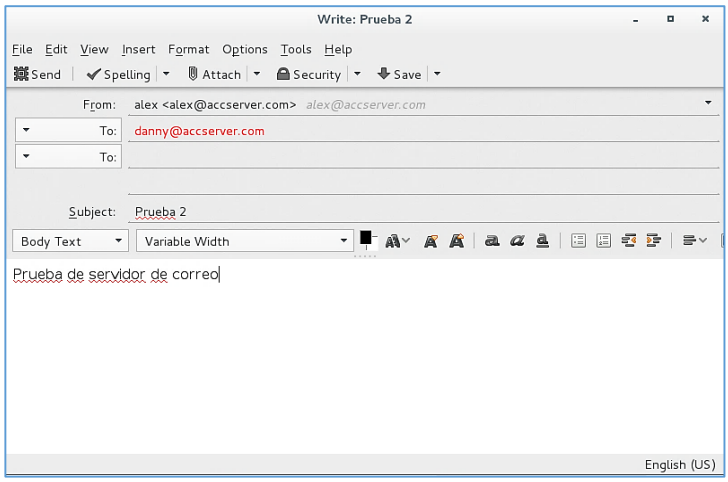


Figura 55. Prueba de mensaje

Como nos fijamos se enviado correctamente el mensaje del primer usuario **alex** hacia el segundo usuario **danny.** Ver figura 55.

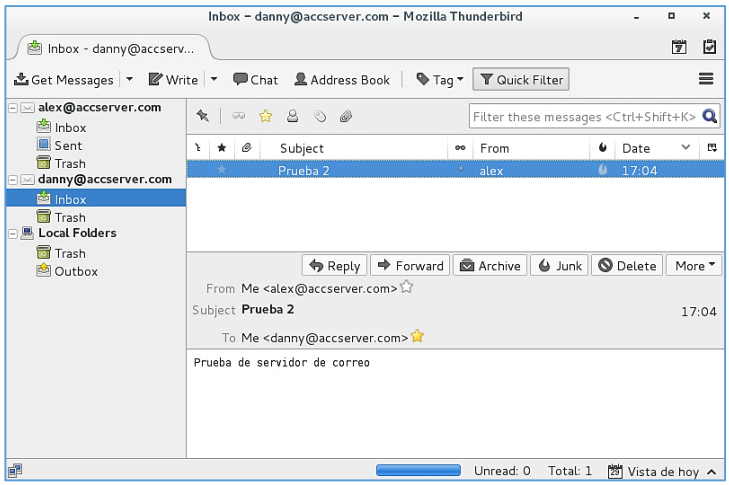


Figura 56. Comprobación de mensaje recibido.

4.2 Algoritmos apropiados para ejecutar una encriptación

AES

También conocido como Rijndael. Esquema de cifrado por bloques, que fue adoptado como estándar de cifrado por el gobierno estadounidense. Reemplaza progresivamente a su predecesor (DES y Triple DES). AES es uno de los algoritmos más utilizados en criptografía simétrica (Selent, 2010).

ARC4

El Algoritmo RC4 fue diseñado por Ron Rivest en 1987 para la compañía RSA Data Security. Su implementación es extremadamente sencilla y rápida, y está orientado a generar secuencias en unidades de un byte, además de permitir claves de diferentes longitudes. El código del algoritmo no se ha publicado nunca oficialmente, pero en 1994 alguien difundió en los grupos de noticias de Internet una descripción que, como posteriormente se ha comprobado, genera las mismas secuencias (Silvana, 2002).

DES / TripleDES

En criptografía, tipo de algoritmo que realiza un triple cifrado tipo DES, esto lo hace muchísimo más seguro que el cifrado DES simple. Triple DES fue desarrollado por IBM en el año 1998 (James Audubon, 2004).

El Triple DES, no es un cifrado múltiple, pues no son independientes todas las subclases. Esto es porque DES tiene la propiedad matemática de no ser un grupo; esto implica que si se cifra el mismo bloque dos veces, con dos llaves distintas, se aumenta el tamaño efectivo de la llave.

TDES nació por la inseguridad que traía una clave de 56 bits. Las claves de 56 bits eran posible de descifrar utilizando un ataque de fuerza bruta. El TDES agrandaba el largo de la llave, sin necesidad de cambiar de algoritmo cifrador.

El método de cifrado TDES desaparece progresivamente, siendo reemplazado por el algoritmo AES que es considerado mucho más rápido (hasta 6 veces más rápido). De todas maneras, algunas tarjetas de créditos y otros métodos de pago electrónico, todavía tienen como estándar el algoritmo Triple DES.

DSA

El algoritmo de firma digital (DSA, Digital Signature Algorithm) emplea un algoritmo de firma y cifrado distinto al del RSA, aunque ofrece el mismo nivel de seguridad. Lo propuso el **National Institute of Standards and Technology** (NIST) en 1991 y fue adoptado por los Federal Information Processing Standards (FIPS) en 1993. Desde entonces se ha revisado cuatro veces (Ssl, 2017).

Con el certificado DSA es más fácil estar al día en cuanto a normas gubernamentales, ya que lo respaldan las agencias federales (incluyendo el cambio obligatorio a las claves de 2048 bits).

Si quiere mejorar aún más la seguridad, puede ejecutar RSA y DSA de forma simultánea. Los servidores Apache, por ejemplo, pueden ejecutar los certificados RSA y DSA simultáneamente en el mismo servidor web. En una ventaja para aquellas empresas que quieran maximizar el alcance en la correspondencia corporativa de su organigrama.

ECC

Es el acrónimo del inglés Elliptic Curve Cryptography, y promete una seguridad más fuerte y mejor rendimiento con claves más cortas. Estas características lo hacen ideal para el ámbito móvil, con cada vez más dispositivos.

Solo para comparar: una clave ECC de 256 bits ofrece la misma seguridad que una clave de 3072 bits.

Como la clave es más corta, se necesita menos potencia informática para obtener conexiones más rápidas y seguras, ideales para dispositivos portátiles como smartphones y tabletas. Además, pese a su novedad, Symantec incorpora los certificados raíz ECC desde hace más de 5 años, así que el certificado ECC funcionará en todo su sistema. Cómo no, el ECC cuenta con el certificado FIPS, como el DSA, y está respaldado por la National Security Agency estadounidense.

WEP

El algoritmo WEP (Wired Equivalent Privacy) es el sistema de cifrado incluido en el estándar IEEE 802.11 (estándar que define las redes inalámbricas). WEP está basado en el algoritmo de cifrado RC4, teniendo dos variantes, una que usa clave de 64 bits (40 bits más 24 bits de vector de iniciación) y otra que usa clave de 128 bits (104 bits y 24 bits de vector de iniciación). En 2003 la Wi-Fi Alliance anunció la sustitución de WEP por WPA y en 2004 se ratificó el estándar 802.11i (WPA2) declarando WEP-40 y WEP-104 como inseguros. A pesar de ello todavía hoy en día se sigue utilizando (Alejandro Cuevas, Héctor Corrales, 2010).

4.3 Modelos de encriptación a la hora de transmitir datos

Un modelo de servicio define las propiedades que debe tener un servicio y que éste ofrece a las aplicaciones que lo usan. En general se puede hablar de dos modelos: servicios integrados (IntServ) y servicios diferenciados (DiffServ).

4.3.1 Modelo de servicios integrados

El modelo de servicios integrados intenta integrar todos los tipos de tráficos posibles en una misma red de uso general [Braden94]. Este modelo ofrece servicios cuantificables y mesurables en el sentido que son definidos para proporcionar una determinada calidad de servicio para un tipo de tráfico cuantificado. Este modelo está típicamente asociado a mecanismos de admisión y reserva de recursos en la red (Carlos, Diego, & Arturo, 2010).

El modelo de reserva describe cómo una aplicación negocia el nivel de calidad de servicio. El modelo más simple es que una aplicación pida una calidad de servicio particular y que la red se lo proporcione o lo deniegue.

Sin embargo, más que rechazar la petición, la red podría conceder un nivel de recursos menor que el pedido. Un esquema más complejo es el modelo de reserva de "doble pasada". En este esquema, se propaga la especificación del tráfico inicial desde el origen a los posibles destinos.

Cada router en las rutas guarda estos valores y quizá los ajusta para reflejar su capacidad disponible. Esta especificación ajustada a la red es devuelta al origen que decide si admite o no el canal.

4.3.2 Modelo de servicios diferenciados

Este modelo es un mecanismo de calidad de servicio de nivel 3 que ha sido utilizado durante algunos años, aunque se ha realizado poco esfuerzo para su estandarización hasta la aparición recientemente del grupo de Servicios Diferenciados de la IETF (DiffServ) (Carlos et al., 2010).

En este modelo, la red clasifica el tráfico en distintas clases y les aplica una disciplina de servicio diferenciada con el objetivo de proporcionar distintos niveles de calidad de servicio. En este caso no se reservan recursos por lo que no se puede garantizar a priori una calidad de servicio.

De este modo, se pueden tener varias clases de servicio para tiempo real, con varios niveles de retraso. También habrá niveles con servicio predictivo y otros sólo con garantía de entrega. El cliente escogerá el tipo de servicio en función del tráfico a transmitir y por supuesto, el precio que quiera pagar.

Otra de las ventajas de este modelo es su menor complejidad de implementación y su fácil integración con los protocolos IP, en el que cada paquete puede ser marcado con la clase de servicio que requiere.

Esta marca será utilizada por lo routers para diferenciar el servicio por paquete.
Tráfico agregado y por conversación

Es importante determinar cómo se va a gestionar el tráfico internamente en la red. La gestión del tráfico por conversación trata cada conversación como un flujo separado. Tradicionalmente, este tipo de gestión está asociado al modelo de servicios integrados. En este caso, la red asigna recursos independientes al resto de las conversaciones y mantiene un control de ellos.

En el núcleo de grandes redes, donde es posible soportar cientos de miles de conversaciones simultáneamente, este mecanismo no es práctico. En estos casos se utiliza el tráfico agregado. De esta forma, un conjunto del tráfico de diferentes conversaciones, se clasifica como un mismo flujo y se maneja como un tráfico

agregado. Además, esta agregación permite reducir en conjunto los recursos necesarios y permite obtener una calidad de servicio casi equivalente al modelo por conversación. Los servicios diferenciados son claros ejemplos de uso de tráfico agregado.

4.3.3 Requerimientos para compartir recursos

Normalmente la red va a ser compartida por distintos tipos de tráfico Mientras el aspecto más importante en la calidad de servicio es el retraso, aquí el interés primario es el ancho de banda de los enlaces.

Este componente del modelo de servicio, llamado compartición de enlaces, contempla como compartir el ancho de banda de un enlace entre varios flujos de acuerdo con ciertas características. Se pueden distinguir los siguientes tipos de comparticiones:

Compartición multi-entidad: Un enlace puede ser usado por varias organizaciones. Se debe asegurar que los enlaces son compartidos de forma controlada, quizás de forma proporcionar a lo que paguen.

Compartición multi-protocolo: Se debe prevenir que una familia de protocolos (DECnet, IP, IPX, OSI, SNA, etc.) sobrecargue un enlace y excluya al resto. Esto es importante porque las distintas familias de protocolos responden de forma diferente a la congestión.

Compartición multi-servicio: Un administrador de red puede limitar la fracción de ancho de banda para cada clase de servicio.

El control de admisión será necesario de nuevo para asegurar que la compartición de recursos se va a cumplir.

Para poder garantizar la integridad de los datos se usan funciones hash. Entre las más utilizadas se destacan:

4.3.4 CheckSum

La suma de verificación es una función hash computable mediante un algoritmo cuya función consiste en detectar cambios en una secuencia de datos (archivos) para proteger la integridad de estos (González, 2014).

El CheckSum es muy usado, ya que permite comprobar la integridad de los contenidos que se envían (generalmente para comprobar la originalidad del software). Por ejemplo, cuando se distribuye un contenido a través de la red, para estar seguro de que lo que le llega al usuario es lo que se está enviando, se manda un valor hash de ese contenido de manera que ese valor tiene que obtenerse al aplicar la función hash sobre el contenido enviado, lo que asegura la integridad del mismo. En ese caso, el CheckSum recibe el nombre de CheckSum criptográfico

debido a que requiere usar funciones hash para que sea imposible crear otros ficheros falsos y que coincidan en el mismo valor hash.

4.3.5 MD5

(Message Digest Algorithm 5, Algoritmo de Ordenación de Mensajes 5) es un algoritmo seguro desarrollado por RSA Data Security, Inc. MD5 es una función hash de 128 bits, que toma como entrada un mensaje de tamaño arbitrario y produce como salida un resumen del mensaje de 128 bits. El MD5 no sirve para cifrar un mensaje ya que lo destruye completamente, la información no es recuperable de ninguna manera ya que hay pérdida de información. El primer paso es dividir el mensaje en bloques de 512 bits.

El último bloque o si el mensaje completo es menor a 512 bits, se formatea para tener un tamaño de 512 bits mediante el agregado de bits 0 más la longitud del tamaño del mensaje. Además, se tiene un búfer estado de 128 bits manejado como cuatro palabras de 32 bits. La función compresión tiene cuatro rondas y en cada ronda el bloque de mensaje y el búfer son combinados en el cálculo, mediante el uso de sumas modulares, XOR's, AND's, OR's y operaciones de rotaciones sobre palabras de 32 bits (Algredo Badillo, Cumplido Parra, & Uribe, 2008) .

4.4 Importancia de cifrar los datos en un canal seguro

Cifrar los datos implica que cada vez que se quiera acceder a los mismos, se deban descifrar, lo que agrega un nivel de complejidad al acceso simple, pero reduce la velocidad del proceso. A raíz de esto, surgen ciertas preguntas: ¿por qué hay que cifrar la información importante en una empresa? ¿Cuáles son los beneficios de hacerlo?

Es muy difícil para una compañía poder revertir el daño generado luego de una intrusión significativa, por lo que es fundamental tomar las medidas necesarias para evitarlas y, si ocurren, contar con la preparación adecuada para minimizar el riesgo, por ejemplo, utilizando datos cifrados

4.4.1 Beneficios del cifrado

- ✓ **Proteger la información confidencial de una organización**

Si la información sensible de una compañía llegara a caer en las manos equivocadas, pueden producirse perjuicios económicos, pérdidas de ventaja competitiva, o incluso significar el cierre de la empresa. En este sentido, la encriptación ayuda a proteger Información delicada, como los datos financieros, de los colaboradores, procedimientos o políticas internas, entre otros.

- ✓ **Proteger la imagen y el prestigio de una organización**

Existe cierta información que si es robada, puede dañar la imagen corporativa. Un ejemplo notable, son los datos que se almacenan de los clientes; el robo de los mismos puede afectar considerablemente a la empresa, llevándola a pérdidas irrecuperables.

- ✓ **Proteger las comunicaciones de una organización**

El cifrado es comúnmente asociado con las transmisiones de datos, dado que los mensajes enviados por una empresa suelen viajar por canales o infraestructura externa, como Internet, y son susceptibles a ser interceptados. El ejemplo más significativo, es el cifrado de los mensajes enviados por correo electrónico.

- ✓ **Proteger dispositivos móviles e inalámbricos**

Todos aquellos dispositivos que salen de la empresa, como teléfonos celulares, tablets o computadoras portátiles, pueden ser extraviados y/o robados. Ante estas situaciones, es importante asegurarse de que ningún tercero esté autorizado pueda acceder a la información (Morales, 2007).

4.4.1.1 Criptografía y Métodos de Cifrado

4.4.1.1.1 Qué es la criptografía

(Corrales, 2014) Antes de zambullirnos en el mundo de la criptografía creemos necesario aclarar en qué consiste la criptografía. Según la RAE: Criptografía: Arte de escribir con clave secreta o de un modo enigmático. Aportando una visión más específica, la criptografía es la creación de técnicas para el cifrado de datos. Teniendo como objetivo conseguir la confidencialidad de los mensajes. Si la criptografía es la creación de mecanismos para cifrar datos, el criptoanálisis son los métodos para "romper" estos mecanismos y obtener la información. Una vez que nuestros datos han pasado un proceso criptográfico decimos que la información se encuentra cifrada. Cabe destacar el uso incorrecto del termino encriptar, que proviene de una mala traducción del inglés encrypt. La palabra encriptar no está reconocida por la RAE y el término correcto es cifrar. La interpretación del término encriptar sería introducir cuerpos en una cripta.

4.4.1.1.2 ¿Por qué es necesaria la criptografía?

La criptografía siempre había estado vinculada al ámbito militar. ¿Por qué se hizo necesaria para el resto de la gente? Aunque el uso de comunicaciones seguras ha sido siempre una prioridad militar, la privacidad es requerida en otros sectores. Las empresas necesitan mantener unas comunicaciones seguras para proteger su información. Por esta razón el gobierno de EEUU y la NSA se ven obligados a crear DES. Aparte de a las empresas, se hace necesario otorgar al ciudadano de privacidad y seguridad. Con el nacimiento de internet y la progresiva oferta de servicios telemáticos como acceso al banco, citas médicas y un sinfín de posibilidades se tiene que ofrecer confidencialidad y seguridad a estos servicios. Por estas razones es necesaria la criptografía. Para otorgar privacidad, confidencialidad y seguridad a nuestras transacciones telemáticas.

4.4.1.2 Método de trasposición

4.4.1.2.1 El cifrado por transposición

(Pomeyrol, 2012) Es una de las técnicas de criptografía más básicas que existen. Consiste en intercambiar la posición de las letras de una palabra o frase siguiendo siempre un esquema bien definido, que puede ser sencillo o muy complejo (y se puede hacer de muchas formas distintas; hoy explicaremos solo una y la desarrollaremos).

Un ejemplo del cifrado por transposición es tan fácil de ejecutar como escribir algo al revés: “Bienvenido a Muy Seguridad” pasaría a ser “odinevneib a dadirugesyum”. Pero dependiendo de las reglas que apliquemos, se pueden conseguir resultados mucho más intrincados. Siguiendo con el mismo ejemplo:

- 4d3n2vn23b1d1d3r5g2sy5m (eliminando los espacios e intercambiando las vocales por números según su orden, donde “a” es “1” y “u” es “5”)

En este caso utilizaremos para cifrar nuestros mensajes la llamada escritura inversa, un simple (y fácil de descifrar) método de cifrado es el de escribir una palabra al revés (de atrás hacia delante). Por tanto la cadena: "Hola mi nombre es Pepa" sería cifrada por "aloH im erbmon se apeP". Pero si a este mensaje le reemplazamos los números por las vocales quedaría de la siguiente manera- 1L4h 3m 2rbm4n s2 1p2P.

Ejemplo:

Tenemos la siguiente palabra (INGENIERIAS), ahora debemos cifrarla utilizando el método de trasposición.

I	N	G	E	N	I	E	R	I	A	S

a) Intercambiamos las vocales por números según el orden de las mismas si es A será reemplazada por el número 1 y si es E será reemplazada por el número 2 y así sucesivamente con todas las siguientes vocales**.**

I	N	G	E	N	I	E	R	I	A	S
3			2		3	2		3	1	

b) Escribimos al revés la palabra remplazando los números por las vocales, es decir comenzamos de derecha a izquierda**.**

S	1	3	R	2	3	N	2	G	N	3

c) Nuestra palabra cifrada es la siguiente

S13R23N2GN3

4.4.1.2.2 Método de las cajas

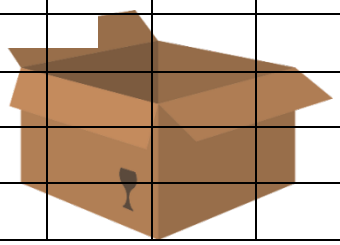
Según (Maths, 2010)Los dos métodos más importantes para cifrar un mensaje son el de transposición y el de sustitución. En el primero las letras del mensaje original permanecen intactas y lo que se cambia es el orden en el que estas aparecen. En cambio, en el método de sustitución las letras son reemplazadas por números, letras o signos cualesquiera, dejando el orden original de las letras intacto. Este último método también se conoce como codificación. Ambos métodos pueden ser utilizados en un mismo sistema de cifrado, una o varias veces, con el fin de hacer más difícil el descifrado.

En este tema vamos a aprender a utilizar un sencillo método de transposición conocido como el "método de las cajas” y que fue utilizado hasta finales de la Segunda Guerra Mundial por los servicios de inteligencia de diferentes países.

Como en todo sistema de encriptación, tanto el que envía el mensaje, como el que lo recibe, deben conocer la "clave".

En este método la clave consiste en una palabra. Vamos a describir su funcionamiento mediante un ejemplo práctico.

P	A	T	I	O



Ejemplo 1.

Supongamos que el mensaje que recibimos es

- ELDAA AILT SDAE TOACR HVOR

La palabra clave

- PATIO

Para descifrar el mensaje primero colocamos la palabra clave en la primera fila de la tabla.

A continuación debemos numerar las letras según el orden en que aparecen en el alfabeto. (Como lo muestran los números de color azul)
Si la letra aparece repetida le ponemos números consecutivos. Por ejemplo, la A es la primera letra, pero si hay dos, le ponemos a la primera uno y a la segunda un dos. La siguiente letra del alfabeto que aparece es la I, luego la O y así sucesivamente.
Finalmente escribimos los grupos de palabras siguiendo el orden de las columnas.

P	A	T	I	O
4	1	5	2	3
T	E	H	A	S
O	L	V	I	D
A	D	O	L	A
C	A	E	T	E
R	A			

Ahora ya tenemos construida la caja que nos va a servir para codificar el mensaje. Lo que debemos hacer ahora es escribir todos los grupos de letras que aparecen bajo cada número. Y hacerlo ordenadamente. Empezamos por el grupo que está debajo del 1.

1) ELDAA
2) AILT
3) SDAE
4) TOACRHVOE

Y confirmamos que nuestro mensaje está bien decodificado con el mensaje que se dio al inicio:

- ELDAA AILT SDAE TOACR HVOR

4.4.1.2.3 Cifrado de polybios

(Marquez, 2008). Es el cifrado por sustitución de carácter más antiguo que se conoce, nombrado así por el historiador griego Polybios. El sistema establece una matriz de dos dimensiones de 5x5 en la que cada entrada de la letra del alfabeto se representa por sus coordenadas dentro de la matriz esta matriz deberá ser conocida tanto por el emisor como por el receptor del mensaje.
En primer lugar, para adaptarlo al lenguaje español hay que fijarse en que hay algunas combinaciones de letras como serían “ij” y “nñ”a las que le correspondería el mismo código de cifrado, pero son lo suficientemente diferentes para poder salir de dudas sobre el carácter correcto desencriptando el mensaje.
El método, consistía en corresponder la letra que se deseaba ocultar con otras dos según la fila y la columna de la matriz a la que pertenecía. Por ejemplo, la letra “a” sería “AA”, la “s” sería “DC”.

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	IJ	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Para poner un ejemplo de mayores dimensiones trabajaremos con la frase: VAMOS A PRACTICAR.

Cuyo resultado sería el siguiente:

VAMOS = EAAACBCDDC

	A	B	C	D	E
A	A				
B					
C		M		O	
D			S		
E	V				

A = AA

	A	B	C	D	E
A	A				
B					
C					
D					
E					

PRACTICAR = CEDBAAACDDBDACDB

	A	B	C	D	E
A	A		C		
B				IJ	
C					P
D		R		T	
E					

Ejemplo 2.

1. Codifica El Siguiente Mensaje:
   "NO OLVIDES LA TAREA"

2. Decodifica El Siguiente Mensaje:
   NO = CCCD

	A	B	C	D	E
A					
B					
C			N	O	
D					
E					

OLVIDES = CDCAEABDADAEDC

	A	B	C	D	E
A				D	E
B				IJ	
C	L			O	
D			S		
E	V				

LA = CAAA

	A	B	C	D	E
A	A				
B					
C	L				
D					
E					

TAREA = ADAADBAEAA

	A	B	C	D	E
A	A				E
B					
C					
D		R		T	
E					

4.4.1.3 Código de mensajes secretos (juego del gato)

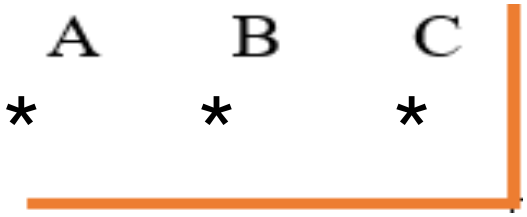
Es posible relacionar el juego del gato con un código para mensajes secretos. Era muy popular allá por los años cincuenta.

tres en línea, también conocido como Ceros y Cruces, tres en raya (en España, Ecuador y Bolivia), **juego del gato**, Tatetí (en Argentina), Triqui (en Colombia), Totito (en Guatemala), Cuadritos o Cero Mata Cero (en República Dominicana), Tic-Tac-Toe (en Estados Unidos), **Gato** (en Chile y México), Michi (en Perú), Es un juego de estrategia que con el paso del tiempo fue evolucionando y se convirtió en un juego de encriptación, usado por nuestros antepasados para dejar claves secretas.

1.1. Consiste en trazar una serie de líneas casi similares al del tres en raya pero dividiendo cada sección en 3x3 y en cada cuadricula deberá ir 3 letras, que en este caso serán del abecedario.

1.2. Se van a separar en secciones de acuerdo a sus posiciones en la gráfica de la siguiente manera, donde un asterisco(*) estará debajo de cada letra para ser representado en la criptografía:

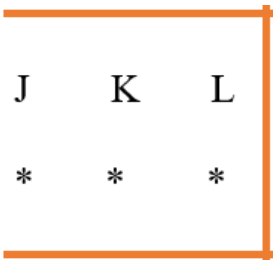
a) Primera sección queda así y cada asterisco va a representar la ubicación de cada letra.



b) La sección siguiente (en medio) de la primera fila queda de esta manera

c) La última sección de la primera fila termina así:

d) La segunda fila quedaría representado de la siguiente manera:



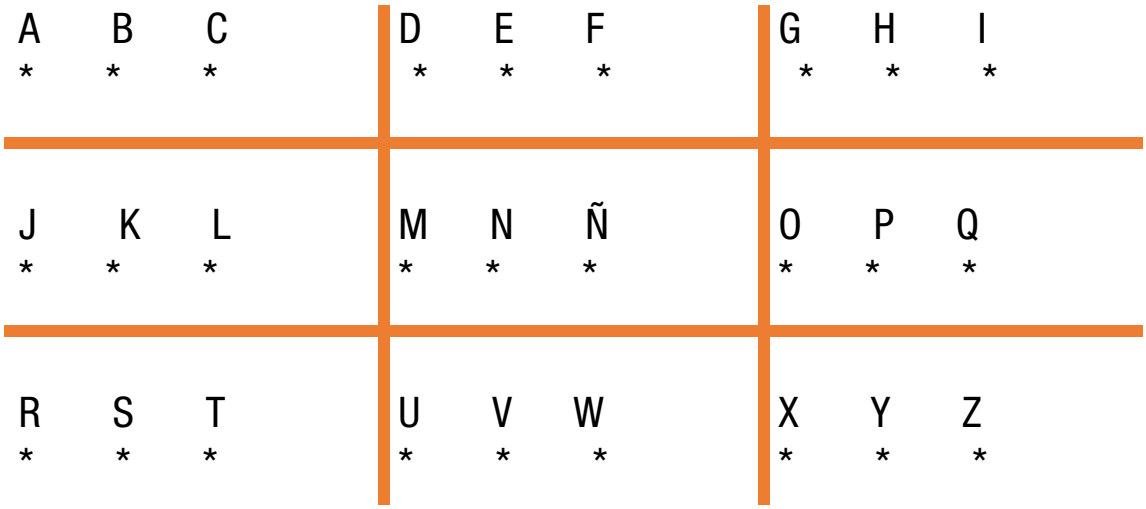
e) la última fila se la separa de esta manera.

Solución: Transformar el mensaje

La solución consiste en transformar el mensaje de una manera en la cual no pueda ser descifrado por cualquier persona, solo por aquellas que conozcan del método de transformación.

Esto implica que el emisor debe enviar el mensaje en un sentido y el receptor lo invierte para así poder leer dicho texto.

- Cada letra del abecedario estará representada por un asterisco todas por igual
- La base aquí del juego será la posición de cada letra y la forma del recuadro en el que se encuentra
- Si nos fijamos atentamente en la tabla, está ya se encuentra con sus cifrados



Ejemplo del ejercicio:

G	R	A	C	I	A	S
*	*	*	*	*	*	*

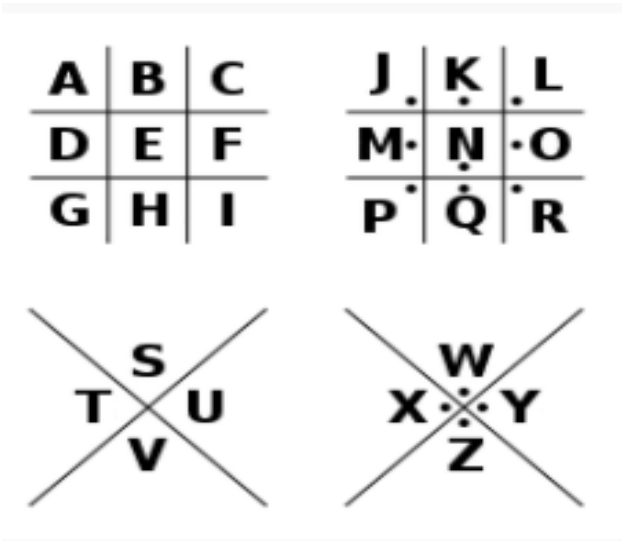
Se lo trasforma o encripta de la siguiente manera:

4.4.1.4 Métodos de cambiar

4.4.1.4.1 Cifrado francmasón (la cifra pig pen).

(Gómez, 2012) Es un cifrado por sustitución simple que cambia las letras por símbolos. Sin embargo, el uso de símbolos no impide el criptoanálisis, y el criptoanálisis es idéntico al de otros métodos de cifrado por substitución simple.

Llamado también "cifra Pig Pen" este método de cifrado fue utilizado por los masones en el siglo XVIII para preservar la privacidad de sus archivos. Se basa en la sustitución de cada letra por un símbolo de acuerdo al siguiente modelo:



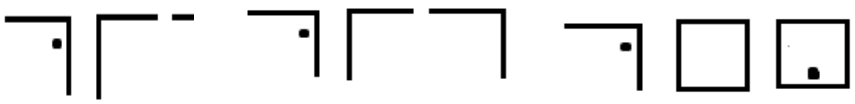
Empleado por los Masones desde el 1700 hasta nuestros días, la cifra denominada PigPen es una sustitución monoalfabética. En este caso, se sustituye una letra del alfabeto por un símbolo en función de un patrón pre-establecido que se muestra abajo y que consiste en dos tic-tac-toe y dos líneas cruzadas. Se coloca un punto en las últimas dos figuras, su utilidad se verá unos párrafos más abajo. Una de las traducciones posibles de PigPen es pocilga. Ta vez, su nombre se debe a como están desparramadas las letras del alfabeto sobre las grillas.

Ejemplo:

- Te dan el siguiente mensaje para que lo codifiques

  PIG PEN

- Utilizando la tabla que nos dan al inicio buscamos la ubicación y forma de cada letra y codificamos.



4.4.1.4.2 La cifra de cesar

a). El cifrado César es uno de los primeros métodos de cifrado conocidos históricamente. Julio César lo usó para enviar órdenes a sus generales en los campos de batalla. Consistía en escribir el mensaje con un alfabeto que estaba formado por las letras del alfabeto latino normal desplazadas tres posiciones a la derecha. Con nuestro alfabeto el sistema quedaría así:

Alfabeto claro	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Alfabeto cifrado	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**

EJEMPLOS:

Texto claro	Texto cifrado
SEGURIDAD INFORMATICA	**PBDROFAXA FKCMOJXQFZX**

MENSAJES	**JBKPXGBP**
SECRETOS	**PBZOBQMP**

b). La transformación se puede representar alineando dos alfabetos; el alfabeto cifrado es un alfabeto normal que está desplazado un número determinado de posiciones hacia la izquierda o la derecha. Por ejemplo, aquí el cifrado César está usando un desplazamiento de seis espacios hacia la derecha:

TEXTO ORIGINAL	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
TEXTO CODIFICADO	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**

Para codificar un mensaje, simplemente se debe buscar cada letra de la línea del texto original y escribir la letra correspondiente en la línea codificada. Para decodificarlo se debe hacer lo contrario. **EJEMPLO:**

TEXTO ORIGINAL	TEXTO CODIFICADO
ENCICLOPEDIA LIBRE	KSIÑIQUVKJÑG QÑHXK

4.4.1.4.3 Cifrado de Vigenere

Según (Fiuricci, 2011)El cifrado Vigenère es un cifrado basado en diferentes series de caracteres o letras del cifrado César formando estos caracteres una tabla, llamada tabla de Vigenère, que se usa como clave. El cifrado de Vigenère es un cifrado polialfabético y de sustitución. El cifrado Vigenère se ha reinventado muchas veces. El método original fue descrito por Giovan Batista Belaso en su libro de 1553 La cifra del Sig. Giovan Batista Belaso. Sin embargo, fue correctamente atribuido más tarde a Blaise de Vigenère, concretamente en el siglo XIX, y por ello aún se le conoce como el "cifrado Vigenère". Este cifrado es conocido porque es fácil de entender e implementar, además parece irresoluble; esto le hizo valedor del apodo el código indescifrable (le chiffre indéchiffrable, en francés).

El cifrado Vigenère es lo suficientemente simple si se usa con discos de cifrado. Los Estados confederados de América, por ejemplo, utilizaron un disco de cifrado para implementar el cifrado Vigenère durante la Guerra Civil Americana. Los mensajes confederados fueron poco secretos, ya que los miembros de la Unión solían descifrar los mensajes. Gilbert Vernam trató de arreglar el cifrado (creando el cifrado Vernam-Vigenère en 1918), pero no importa lo que hiciera, el cifrado sigue siendo vulnerable al criptoanálisis. (No confundir con el cifrado de Vernam)

Tabla 11. Vigenere

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

EJERCICIOS:

1. Construye un alfabeto de cesar con desplazamiento de cada letra por la que se encontraba 3 lugares más a la derecha.
2. Según la tabla del tema 1 decodifica el siguiente mensaje;
   Wuhv wulvwhv wljuhv froldq wuljr hq xq wuljdñ
3. Inventa un mensaje con cifrado de cesar, la clave es opcional.

H	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Ñ	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ

P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y

El cifrado Vigenère ganó una gran reputación por ser excepcionalmente robusto. Incluso el escritor y matemático Charles Lutwidge Dodgson (Lewis Carroll) dijo que el cifrado Vigenère era irrompible en el artículo "The Alphabet Cipher" para una revista de niños. En 1917, "Scientific American" describió el cifrado Vigenère como imposible de romper. Esta reputación fue mantenida hasta que el método Kasiski (1863) resolvió el cifrado y algunos criptoanalistas habilidosos pudieron romper ocasionalmente el cifrado en el siglo XVI.

El cifrado Vigenère es lo suficientemente simple si se usa con discos de cifrado. Los Estados confederados de América, por ejemplo, utilizaron un disco de cifrado para implementar el cifrado Vigenère durante la Guerra Civil Americana. Los mensajes confederados fueron poco secretos, ya que los miembros de la Unión solían descifrar los mensajes.

Ejemplo:

a) mensaje: AVANZAR A LA DERECHA
b) clave: CONTROL

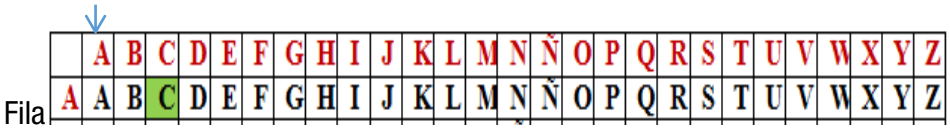
1) Ubicamos el mensaje en la tabla separando un espacio cada palabra.

A	V	A	N	Z	A	R		P	O	R		L	A		D	E	R	E	C	H	A

2) Comenzamos a poner la palabra clave de la siguiente manera.

1ER	A	V	A	N	Z	A	R		P	O	R		L	A		D	E	R	E	C	H	A
2DO	C	O	N	T	R	O	L		C	O	N		T	R		O	L	C	O	N	T	R

3) El primer mensaje hará referencia a las filas de la tabla de Vigenere y el segundo mensaje que de la palabra clave referenciará a las columnas.
Ejemplo, entre la fila de la A y la columna de la C, la letra clave seria C.
Columna



- Así continuaríamos con cada par de letras hasta tener nuestro mensaje cifrado. Entonces el mensaje cifrado quedaría de la siguiente manera:

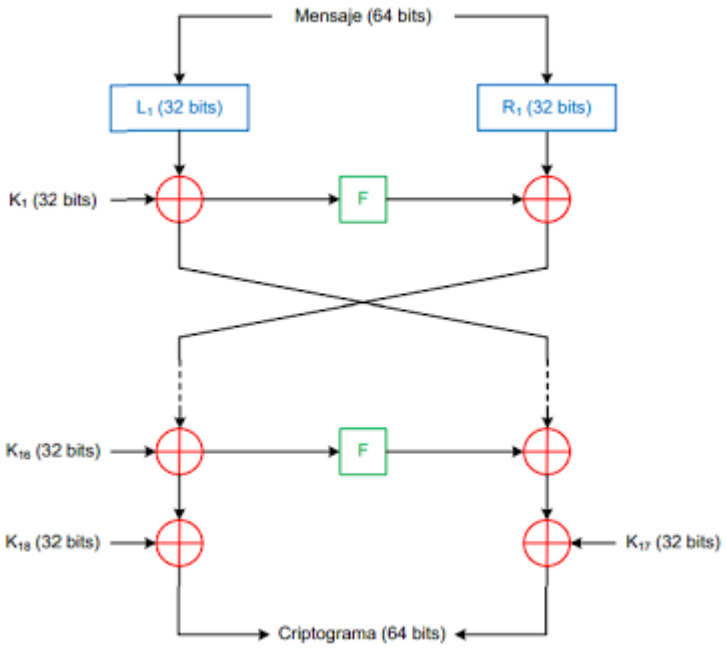
CKNGQOC RDE ER ROTSOAR

4.4.1.5 Cifrado por Bloque

4.4.1.5.1 Cifrados por Bloque – Blowfish

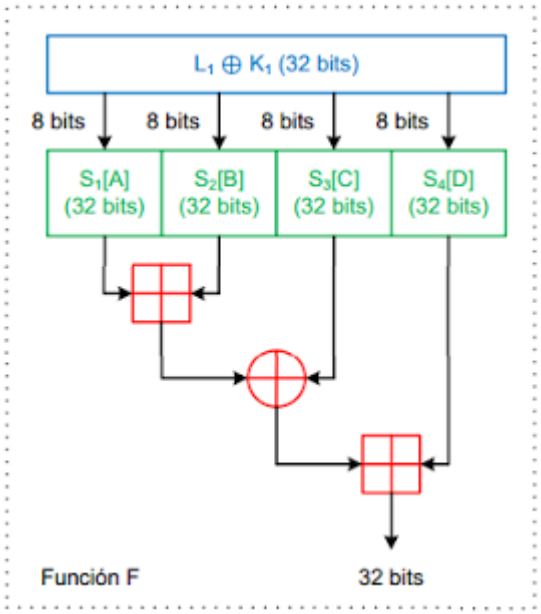
(Jimenez, 2013)Blowfish es un algoritmo de cifrado por bloques simétrico libre de patente creado por Bruce Schneier en 1993 como una alternativa para reemplazar a DES como estándar de cifrado. Este algoritmo está compuesto por 18 semiclaves (K) y 4 cajas (subtitution boxes S). Es un proceso relativamente simple y altamente seguro ya que a la fecha no se conoce ningún tipo de criptoanálisis efectivo contra este algoritmo de cifrado.

Algoritmo de cifrado



Para poder entender el algoritmo primero tendremos que describir la función F, la cual se encarga de sustituir los valores resultantes de las operaciones XOR utilizando las cajas de sustitución (subtitution boxes).

La función F divide el grupo de 32bits en 4 grupos de 8bits el bloque a y bloque b se buscan en las cajas sustitución(representadas con la letra "S" en el diagrama), el valor representado por el primer octeto de la primer caja se suma al valor representado del segundo octeto de la segunda caja y al resultado se saca el módulo de 2^{32}, posteriormente a este resultado se aplica una operación XOR con el valor representado por el tercer bloque en la tercer caja y al resultado de esto se le suma el valor representado por el cuarto octeto en la cuarta caja y al final se vuelve a aplicar el módulo 2^{32}.



Scheier describe la función F como:
f(Li⊕Ki)=((((S1[A]+S2[B])mod232)⊕S3[C])+S4[D])mod232

Una vez entendido que es la función F del Blowfish paso a describir el algoritmo de cifrado:
Un bloque de 64bits se divide en dos bloques de 32bits (L y R)

Se realiza una operación XOR a los primeros 32bits (L) con la primera subclave (K) y se realiza la función F con el resultado de la operación.

Se realiza una operación XOR con la segunda parte de los 32 bits(R) con el resultado de la función F (L).

Se intercambian posiciones (R pasa a ser L y L pasa a ser R) y se repite el proceso anterior por 16 iteraciones.

Al terminar la última iteración no se realizara el intercambio.

Se realiza la operación XOR entre el valor alojado en L y la subclave 18.

Se realiza la operación XOR entre el valor alojado en R y la subclave 17.

Se unen los dos fragmentos del bloque para generar nuevamente un bloque de 64bits ya cifrado.

Las subclaves y las cajas de substitución no corresponden a valores arbitrarios, estos valores son el resultado de un proceso previo a la encriptación o desencriptacion con Blowfish.

Planificación de claves

La planificación es la inicialización del arreglo de las subclaves haciéndolas dependiente de la clave de usuario. Estos valores serán las subclaves para el proceso de encriptación y desencriptacion con Blowfish por lo tanto deben calcularse antes de comenzar a cifrar o descifrar mensajes propios.

Proceso:

Se define un arreglo de 18 secciones las cuales deben de poder almacenar 32bits cada una ya que estas alojaran las subclaves, además se generan 4 arreglos de 256 posiciones también de 32bits cada una, estas últimas son las cajas de substitución.

Cada sección de los arreglos (subclaves y cajas) son inicializados con una cadena fija, esta cadena son los dígitos en hexadecimal de π a excepción de su parte entera. El orden de inicialización es P1, P2, P3,…, P18, S1, S2, S3, S4

A cada una de las subclaves se le aplica un XOR con 32bits de la clave de usuario.

Una vez inicializadas las cajas y las subclaves, se cifra un mensaje nulo (lleno de ceros)

El paso anterior tiene 2 funciones, primero sustituye las primeras dos subclaves y segundo entra a Blowfish para ser cifrada (con las subclaves sustituidas).

Se repite el paso anterior pero esta vez se sustituyen las siguientes dos subclaves. Este paso se repite hasta que las 18 subclaves y el contenido de las 4 cajas hayan sido sustituidas por las salidas correspondientes del cifrado de la palabra nula.

En total se realizaran 521 iteraciones para obtener los valores que se utilizaran en el cifrado de información.

Librerías para cifrado Blowfish

- Python - Crypto
- Java - Crypto (Propia de java)

4.4.1.5.2 Cifrado de playfair

(Contreras M. Daniel, 2011). Este algoritmo surge alrededor de 1850 y es desarrollado por Wheatstone quien lo implementa en el disco desarrollado por él y nombrado así Disco de Wheatstone, son embargo, al procedimiento empleado le llama Playfair en honor a su amigo Lord Playfair.
Se trata de un algoritmo que busca aumentar la seguridad del cifrado evitando que se haga un análisis de frecuencia, para lo cual hace uso de poligramas, esto es, realiza el proceso de cifrado por bloques de caracteres, en este caso diagramas, utilizando para ello una matriz de 5 x 5 la cual contiene las 26 letras del alfabeto inglés y comenzando la matriz con la secuencia correspondiente a la palabra clave, de manera que si la palabra clave es DESTINO, la matriz de cifrado correspondiente es la que se muestra a continuación:

D	E	S	T	I
N	O	A	B	C
F	G	H	K	L
M	P	Q	R	U
V	W	X	Y	Z

Adicionalmente se deben de considerar las siguientes reglas de cifrado:

Regla	Si m1 y m2	Entonces c1 y c2
1	S encuentra en la misma fila o renglón	Corresponden al siguiente elemento a la derecha (desplazamiento circular)
2	Están ubicadas en la misma columna	Son los caracteres que están justo debajo de ellas (desplazamiento circular)
3	Ambas están en diferente columna y renglón	Son las letras que están en su misma fila pero en el eje de simetría correspondiente ya sea a m1 o a m2
4	Son iguales	Se obtienen aplicando las reglas 1 a 3 pero habiendo insertado previamente un carácter entre m1 y m2 para evitar la repetición (se sugiere X)
5	Son impares en el último diagrama	Se obtienen después de agregar una X como elemento m2 y seguir las reglas previas

Proceso de cifrado: para llevar a cabo el proceso de cifrado considérese el texto en claro:
ATAQUE A LAS CERO HORAS

Ahora bien, lo primero a realizar es la formación de diagramas:
AT AQ UE AL AS CE RO HO RA SX

Y como se puede apreciar, el último diagrama era impar por lo que fue necesario agregar una "X" al final, a continuación y siguiendo las reglas indicadas, se obtiene el criptograma:
Cripto = BS HX PI CH HA OI PB GA QB AS
Proceso de descifrado: considérese ahora que la palabra clave es MARTE y el criptograma a descifrar es:
Cripto = TN AM HS MQ HV
Lo primero a realizar es la matriz de descifrado, la cual queda como sigue:

M	A	R	T	E
B	C	D	F	G
H	I/J	K	L	N
O	P	Q	S	U
V	W	X	Y	Z

Y damos inicio al proceso de descifrado, que para el primer diagrama se observa que las letras del criptograma corresponden a la regla 3 al igual que el tercero y cuarto diagramas, en tanto, que el segundo diagrama obedece a la regla 1 y que el quinto a la regla2, de manera que el mensaje en claro es:
EL ME LO RO BO
Ejemplo 2:
Codifica El Siguiente Mensaje: "LENGUAJE"

LE	NG	UA	JE

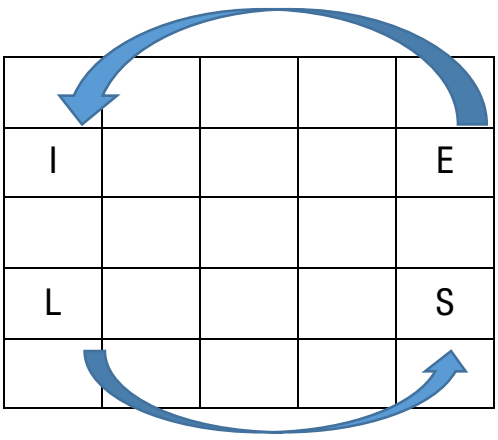
Decodifica El Siguiente Mensaje: "SIOKMBKB"

SI	OK	MB	KB

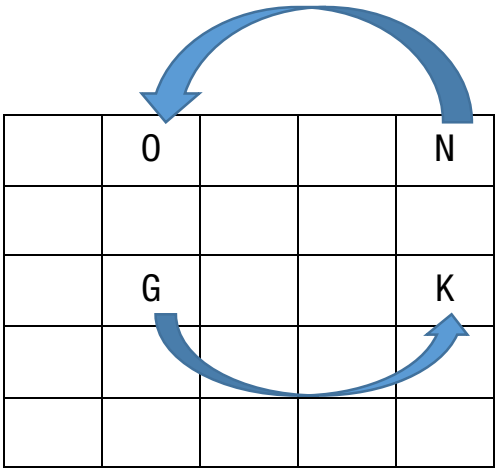
Clave: COMUNIDAD

C	O	M	U	N
I	D	A	B	E
F	G	H	J	K
L	P	Q	R	S
T	V	X	Y	Z

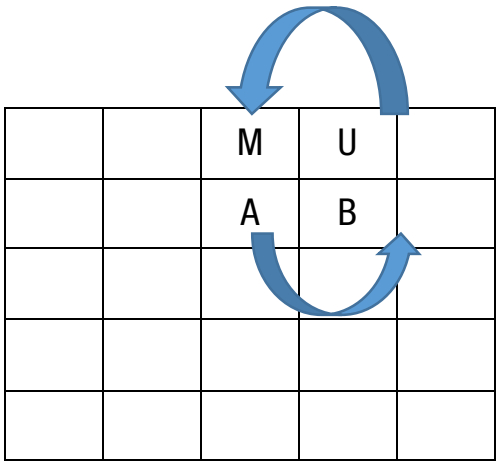
L	**E**
S	**I**



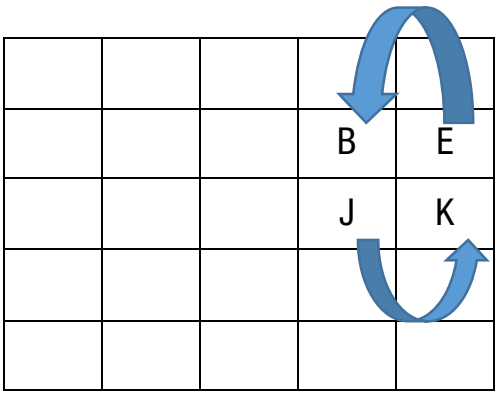
N	G
O	K



U	A
M	B



J	E
K	B



4.4.1.6 Método de desordenar

4.4.16.1 La escitala espartana

Los espartanos eran muy originales y aplicaban la astucia en la batalla. Usaban un ingenioso sistema de comunicación: la escítala. Una escítala es un sistema de criptografía utilizado para enviar mensajes en clave y secretos.

En esos tiempos era vital que el enemigo no captara ningún tipo de información, por eso, al igual que en épocas modernas, era necesario preservar los datos en forma segura.

Inventaron un procedimiento más que simple, pero al mismo tiempo era muy complicado de descifrar. Era un sencillo bastón. La escítala está formada por dos varas de grosor variable pero iguales en ambos casos. Eso se complementaba con una tira de cuero o papiro, donde se ubicaban letras que a simple vista parecían dispuestas al azar. Todos los jefes de tropa tenían el mismo bastón.

Para ver en la práctica cómo funcionaba la escítala imaginemos que tras enrollar la tira escribimos un mensaje formado por 3 filas de 9 caracteres de longitud. Al desenrollarla obtenemos una tira con 27 letras. La primera letra de la tira es la primera letra de la primera línea, la segunda letra de la tira es la primera letra de la segunda línea. Así hasta la tercera letra. La letra 4 de la tira es la segunda de la primera fila y continuamos hasta el final. En general la j-ésima letra de la i-ésima fila ocupará el lugar

$$\mathbf{3}(\boldsymbol{j}-\mathbf{1})+\boldsymbol{i}$$

Veamos ahora un ejemplo de criptograma creado utilizando una escítala como la comentada anteriormente. Como es costumbre en criptografía, el texto al que no se le ha aplicado la criptografía se llama *texto claro* (otros autores lo llaman *texto plano* puesto que en inglés es *plaintext*) y se escribe en minúsculas. El texto cifrado lo escribiremos en mayúsculas. También es costumbre en criptografía no escribir los espacios en blanco, ni los signos de puntuación ni de acentuación.

Texto llano: ejemplodelmetododelescitalo
Texto cifrado: **ELLJMEEESMTCPOILDTOOADDLEEO**

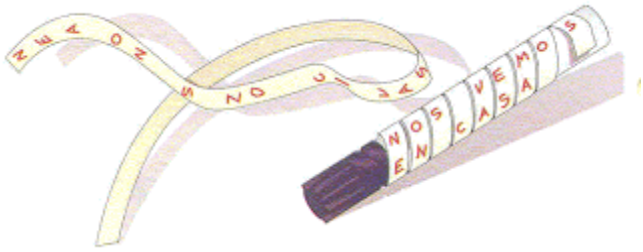
Para cifrar utilizando este método, si no poseemos la madera en cuestión, podemos seguir los siguientes pasos:

- Se dibuja una cuadrícula rectangular.
- Se escribe el texto en horizontal, empezando por la izquierda.
- El texto cifrado se obtiene leyendo en vertical lo que hemos escrito.

El mensaje cifrado depende de las dimensiones de la cuadrícula.

En términos modernos decimos que este cifrado es de *transposición*, pues a cada letra del texto cifrado le corresponde la misma letra del texto claro. Lo único que hemos hecho es "desordenarlas" siguiendo un patrón matemático que previamente mencionamos.

El criptoanálisis de este método es muy simple. Partimos de la primera letra y vamos tomando letras dando saltos de dos letras. Si obtenemos un mensaje con sentido, resultará que la escítala tenía únicamente dos líneas. Si dando saltos de dos letras no conseguimos nada, pasamos a dar saltos de tres letras. Y continuaríamos hasta averiguar cuantas líneas tenía el mensaje. Luego continuamos con la letra número 2 y finalmente desencriptamos el mensaje.



e	j	e	m	p	L	o	d	e
l	m	e	t	o	D	o	d	e
l	e	s	c	i	T	a	l	o

EJERCICIOS:

1. **Utilizando el método del escitalo codificar lo siguiente:**
   - eljuegodelosmensajessecretosdelescitalo
   - leerbuenoslibrosescomoconversarconlasmejoresmentesdelpasado

Otro punto importante que se debe tener en cuenta es el diseño de redes jerárquicas.

4.4.2 Modelo jerárquico

Un diseño jerárquico tradicional de una red LAN tiene 3 capas, entre las ventajas que tenemos de separar las redes en 3 niveles tenemos que es más fácil diseñar, implementar, mantener y escalar la red, además de que la hace más confiable, con una mejor relación costo/beneficio. Cada capa tiene funciones específicas asignadas y no se refiere necesariamente a una separación física, sino lógica; así que podemos tener distintos dispositivos en una sola capa o un dispositivo haciendo las funciones de más de una de las capas, a continuación, detallaremos cada capa.

4.4.3 Capa de núcleo (core layer)

Esta capa es el backbone de alta velocidad de la red, la cual es crucial para comunicaciones corporativas. Debe tener las siguientes características: transporte rápido, alta confiabilidad, redundancia, tolerancia a fallos, rápida adaptación a fallos, baja latencia. Su única función es conmutar tráfico tan rápido como sea posible. Se debe diseñar el core para una alta confiabilidad (high reliability), por ejemplo, con tecnologías de capa dos que faciliten redundancia y velocidad, como FDDI, Gigabit Ethernet (con enlaces redundantes), ATM, y seleccionamos todo el diseño con la velocidad en mente, procurando la latencia más baja, y considerando protocolos con tiempo de convergencia más bajos (Morales, 2007).

4.4.4 Capa de distribución (distribution layer)

Esta capa es el medio de comunicación entre la capa de acceso y el núcleo. Las funciones de esta capa son proveer ruteo, filtrado, acceso a la red WAN y determinar qué paquetes deben llegar al core. Aquí se implementan las políticas de red, por ejemplo: ruteo, access-list, filtrado de paquetes, colas de espera, se implementan la seguridad y las políticas de red (traducciones NAT y firewalls), la redistribución entre protocolos de ruteo, ruteo entre VLANs, se definen dominios de broadcast y multicast.

4.4.5 Capa de acceso (access layer)

Esta capa proporciona a los usuarios acceso a segmentos locales de la red, controla a los usuarios y el acceso de grupos de trabajo o los recursos de la red. Entre las funciones más importantes están la continuación de control de tráfico y políticas, creación de dominios de colisión separados (segmentación), alta disponibilidad, seguridad en puertos, limite en tasas de transferencia, inspección del protocolo ARP. En esta capa se lleva a cabo la segmentación Ethernet, DDR y ruteo estático.

4.4.6 Configuración del router

Configuración de la fastethernet 0/0

```
switch> enable
switch# configure terminal
switch(config)# interface fastethernet 0/0
switch(config)# ip address 192.168.1.10 255.255.255.0
```

Configuración de la fastethernet 0/1

```
switch> enable
switch# configure terminal
switch(config)# interface fastethernet 0/1
switch(config)# ip address 192.168.2.10 255.255.255.0
```

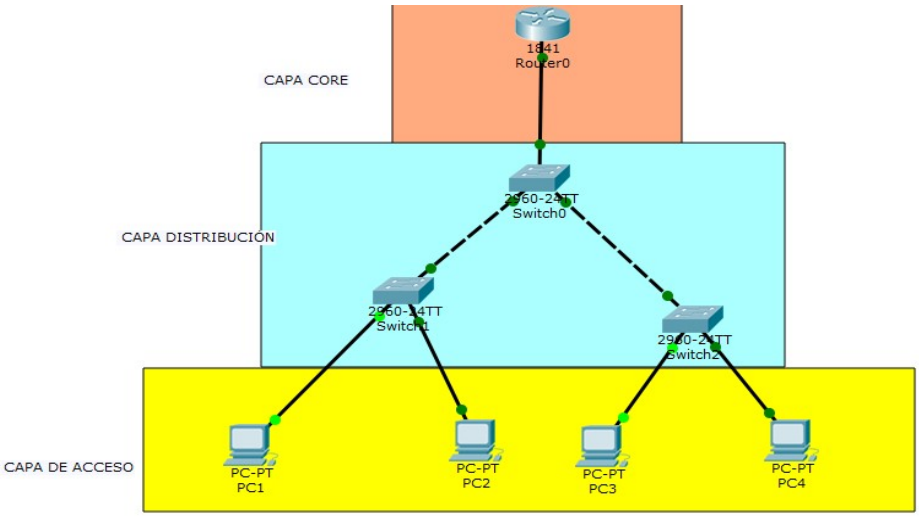


Figura. 57 Diseño Jerárquico

4.4.7 Direccionamiento lógico de cada componente

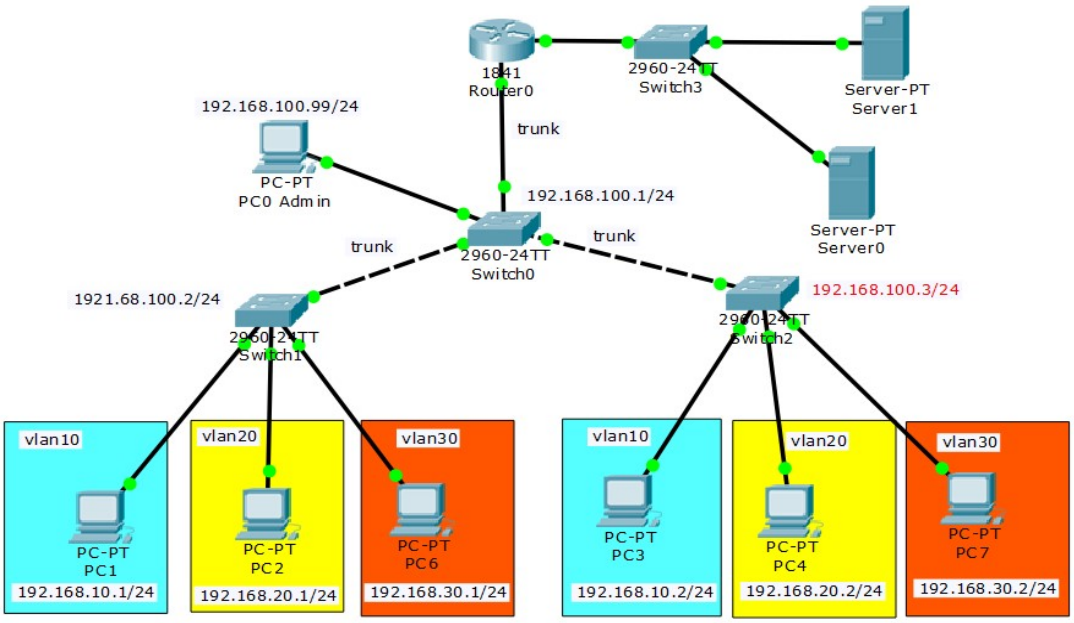
En la siguiente estructura de red establecemos configuraciones de seguridad tanto en el router como switches facilitando el control y monitoreo de los mismos, partimos por la capa de acceso asignando las respectivas IP, máscara de red, Gateway, DNS a cada Workstation.

En la capa de distribución, a los switches se le implementa seguridad en la parte de consola y modo privilegiado enable, continuando con la creación de las vlan's que nos ayudará a segmentar una red principal en subredes (para la práctica vlan10, vlan20 y la interfaz administrativa de la vlan99), en el swicth0 con su respectiva seguridad se crea la subred administrativa vlan99 y su interfaz para que interactúe con el administrador y la capa de acceso.

En la capa core, establecemos seguridad en el router y las respectivas configuraciones para que su interfaz reconozca las diferentes vlan's permitiendo el flujo de datos para llevar a cabo la comunicación con el server web y de correo a través del swicth3.

Para el siguiente ejemplo tenemos los siguientes componentes.

4 Switch Cisco 2960
7 PC's
1 Router CISCO 1841
2 Servidores



IP asignadas a cada componente

Componente	IP	Área
VLAN 10	192.168.10.0/24	Administración
VLAN 20	192.168.20.0/24	Sistemas
VLAN 30	192.168.30.0/24	Ventas
PC0	192.168.100.99/24	Admin - switch
VLAN 99	172.16.10.0/16	
Router	192.168.50.0/24	

CONFIGURACION MEDIANTE CLI (Command Line Interface)

Mediante el CLI podemos incorporar seguridad ya que se pueden realizar acciones más explicitas, también se pueden hacer estas configuraciones mediante interfaz gráfica. Pero en este ejemplo lo realizaremos mediante CLI.

4.4.8 Configuración de básica del router.

Contraseña de acceso a consola

```
router> enable
router # configure terminal
router (config)# line console 0
router (config-line)# password cisco
router (config-line)# login
```

Contraseña terminal virtual (telnet) y contraseña de acceso a modo privilegiado

```
router > enable
router # configure terminal
router (config)# line vty 0 4
router (config-line)# password cisco
```

```
router (config-line)# enable password class2
```

Contraseña encriptada de acceso a consola

```
router > enable
router # configure terminal
router (config)# service password-encryption
```

Contraseña encriptada de acceso a consola

```
router > enable
router # configure terminal
router (config)# enable secret class2
```

Configuración de banner

```
router > enable
router # configure terminal
router (config)# banner motd #ACCESO SOLO A PERSONAL AUTORIZADO#
```

```
ACCESO SOLO A PERSONAL AUTORIZADO

User Access Verification

Password:
```

Configuración de la fastethernet 0/1

```
router > enable
router # configure terminal
router (config)# interface fastethernet 0/1
router (config)# ip address 192.168.50.10 255.255.255.0
```

4.4.9 Configuración de contraseñas de los switch

Contraseña de acceso a consola

```
Switch> enable
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# password cisco
Switch(config-line)# login
```

Contraseña terminal virtual (Telnet) y contraseña de acceso a modo privilegiado

```
Switch> enable
Switch# configure terminal
Switch(config)# line vty 0 15
Switch(config-line)# password cisco
Switch(config-line)# enable password class2
```

Contraseña encriptada de acceso a consola

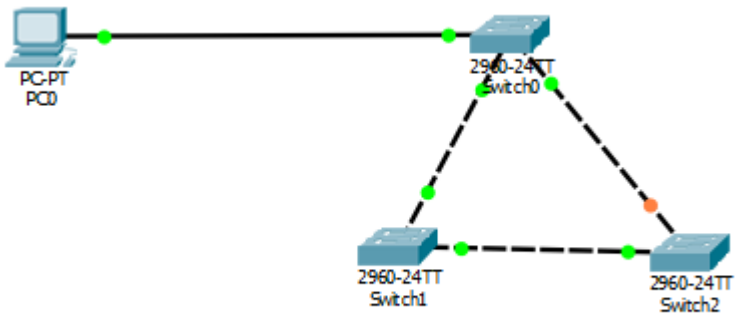
```
switch> enable
```

```
switch# configure terminal
switch(config)# service password-encryption
```

Contraseña encriptada de acceso a consola

```
switch> enable
switch# configure terminal
switch(config)# enable secret class2
```

4.4.10 Creación de vlan



La VLAN 99 la cual es para que acceda únicamente el administrador de los switches.

```
switch> enable
switch# configure terminal
switch(config)# vlan99
switch(config)# name administracion
```

Configuración de la interfaz de la vlan99 para sw0

```
switch> enable
switch# configure terminal
switch(config)# interface vlan99
switch(config)# ip address 192.168.100.1 255.255.255.0
```

Configuración de fastethernet 0/24 como puerto acceso a la vlan99

```
switch> enable
switch# configure terminal
switch(config)# interface fastethernet 0/24
switch(config)# switch port mode access
(config)# switch port access vlan99
```

Crear Vlan10 tanto para sw1, sw2

```
switch> enable
switch# configure terminal
switch(config)# vlan10
switch(config)# name sistema
```

Configuración de la interfaz de la vlan99 para sw1

```
switch> enable
switch# configure terminal
switch(config)# interface vlan99
switch(config)# ip address 192.168.100.2 255.255.255.0
```

Configuración de la interfaz de la vlan99 para sw2

```
switch> enable
switch# configure terminal
switch(config)# interface vlan99
switch(config)# ip address 192.168.100.3 255.255.255.0
```

Configuración de gigabitethernet 0/1 como puerto trunk

En caso de que su uso sea de manera troncal asignamos el modo trunk; este enlace troncal es el que lleva la información de VLAN entre dispositivos de capa 2 preparados para la VLAN.

```
switch> enable
switch# configure terminal
switch(config)# interface gigabitethernet 0/1
switch(config)# switchport mode trunk
switch(config)# switchport trunk encapsulation dot1q 99
```

Cerrar interfaces no utilizadas en los switches

Con el fin de hacer más difícil el acceso a la red y volverla más robusta se cierra las interfaces. En este ejemplo lo hacemos una por una.

```
switch(config)#interface fastethernet 0/1
switch(config-if)#shutdown
```

También se puede cerrar por rango de interfaces.

```
switch(config)#interface range fastethernet 0/5-16
switch(config-if-range)#sh
switch(config-if-range)#shutdown
```

Configuración de la interfaz de acceso del router

- **Configuración de fastethernet 0/1 como puerto trunk para vlan10 y vlan20**

```
router> enable
router# configure terminal
router(config)# interface fastethernet 0/0.10
router(config)# encapsulation dot1q 10
router(config)# ip address 192.168.10.10 255.255.255.0
router(config)# interface fastethernet 0/0.20
router(config)# encapsulation dot1q 20
router(config)# ip address 192.168.20.10 255.255.255.0
```

Configuración de la interfaz de acceso del router

- **Configuración de fastethernet 0/1 como puerto trunk para vlan10, vlan20, vlan30**

```
router> enable
router# configure terminal
router(config)# interface fastethernet 0/0.10
router(config)# encapsulation dot1q 10
router(config)# ip address 192.168.10.10 255.255.255.0
router(config)# interface fastethernet 0/0.20
router(config)# encapsulation dot1q 20
router(config)# ip address 192.168.20.10 255.255.255.0
router(config)# interface fastethernet 0/0.30
router(config)# encapsulation dot1q 30
router(config)# ip address 192.168.30.10 255.255.255.0
```

Configuración de contraseñas de los switch.

- **Crear Vlan30 tanto para sw1, sw2**

```
switch> enable
switch# configure terminal
switch(config)# vlan30
switch(config)# name finanzas
```

Configuración de la interfaz de la vlan99 para sw0

```
switch> enable
switch# configure terminal
switch(config)# interface vlan99
switch(config)# ip address 172.16.10.1 255.255.0.0
```

Configuración de la interfaz de la vlan99 para sw1

```
switch> enable
switch# configure terminal
switch(config)# interface vlan99
switch(config)# ip address 172.16.10.2 255.255.0.0
```

Configuración de la interfaz de la vlan99 para sw2

```
switch> enable
switch# configure terminal
switch(config)# interface vlan99
switch(config)# ip address 172.16.10.3 255.255.0.0
```

4.5 Actividades

EJERCICIOS PARA RESOLVER

Cifrado por trasposición

Según el método de trasposición realice el siguiente ejercicio:

1. **Cifrar las palabras; SEMESTRES, COMPUTACION, SOFTWARE, HARDWARE y ACTIVIDADES.**

A.

Palabra	S	E	M	E	S	T	R	E	S
N°									
Palabra cifrada									

B.

Palabra	C	O	M	P	U	T	A	C	I	O	N
N°											
Palabra cifrada											

C.

Palabra	S	O	F	T	W	A	R	E
N°								
Palabra cifrada								

D.

Palabra	H	A	T	D	W	A	R	E
N°								
Palabra cifrada								

E.

Palabra	A	C	T	I	V	I	D	A	D	E	S
N°											
Palabra cifrada											

Verifica conceptos

1. Encuentre los Protocolos TCP/IP:

SMTP-TELNET-HTTP-SNMP-FTP

O	E	V	U	U	J	Y	S	O	P	Y	M	Y	F
Y	O	A	F	E	W	Y	E	Y	U	G	V	A	E
E	E	E	Y	S	H	V	L	C	K	Q	V	M	A
L	D	G	X	A	C	U	E	X	H	R	E	Y	A
Y	Y	U	U	Z	Y	C	A	D	Q	S	R	G	Q
Z	U	A	F	X	Z	R	K	P	W	I	Y	C	P
T	E	L	N	E	T	N	I	S	X	H	T	T	P
Q	L	R	I	E	E	J	A	J	W	O	J	R	Y
C	B	Q	P	E	U	O	S	M	T	P	J	Y	I
E	P	H	Y	U	U	F	K	Z	V	Q	U	F	O
B	C	G	F	C	S	N	M	P	R	K	A	J	E
L	A	T	B	T	T	G	A	Q	O	P	P	N	I
F	T	P	M	B	I	Y	M	J	A	A	Q	U	E
W	U	I	E	L	A	H	K	J	V	U	U	V	O

2. ¿Qué es un router?

_____
_____
_____
_____
_____
_____

3. Escribas los comandos que permitan configurar el nombre de un routing.

_____
_____
_____
_____
_____
_____

4. Escriba los comandos que permitan configurar las contraseñas para las líneas de terminales virtuales y para la línea de consola.

_____
_____
_____
_____
_____
_____

5. Complete:

El _____ es el proceso usado por el router para enviar paquetes a la red de destino. Cuando los routers usan _____, esta información se obtiene de otros routers y cuando se usa_____, el administrador de la red configura manualmente la información acerca de las redes remotas.

6. ¿Qué es la encriptación?

_____
_____
_____
_____
_____
_____

2. **Por el método de trasposición descifrar el siguiente mensaje:**

S4L2D4G25JL2

Palabra cifrada	S	4	L	2	D	4	G	2	5	J	L	2
Transformación de los números a vocales												

Recordar, que encontraras el mensaje oculto jugando a la inversa.

Mensaje descifrado												

- **Siguiendo el mismo procedimiento del ejercicio anterior descifrar el siguiente mensaje.**

S4T2RC2SS2J1SN2M

Palabra cifrada	S	4	T	2	R	C	2	S	S	2	J	1	S	N	2	M
Transformación de los números a vocales																
Mensaje descifrado																

3. **Utilizando los mensajes cifrados de los ejercicios uno y dos ordene la oración oculta.**

S4L2D4G25JL2

+

S4T2RC2SS2J1SN2M

Solo te daremos unas pequeñas pistas la letra inicial y la final, el mensaje esta sin espacios.

E																									S

Método de las caias

4. Según el método de cajas descifrar el siguiente mensaje

5) LDAAUION	**6)** EOLJMCCE
7) MOSSYLMD	8) **EDCEFDPR**
9)	**10)**
11) TEASAERR	**La palabra clave** • CICLO

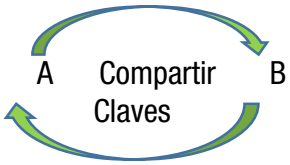
Recordar que en esta fila se ubicaran los números dependiendo del orden del alfabeto

C	I	C	L	O

5. Cifrar el siguiente mensaje utilizando el método de las cajas, la clave a utilizar será la del ejercicio anterior.

- **SISTEMAS DE INFORMACION GERENCIAL**

6. Cifrar un mensaje referente a la materia con la clave que usted elija, luego intercambiar hojas con su compañero de al lado y descifrar sus información.



Cifrado De Polvbios

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	IJ	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

1. **Cifrar la siguiente frase: todo está bien**

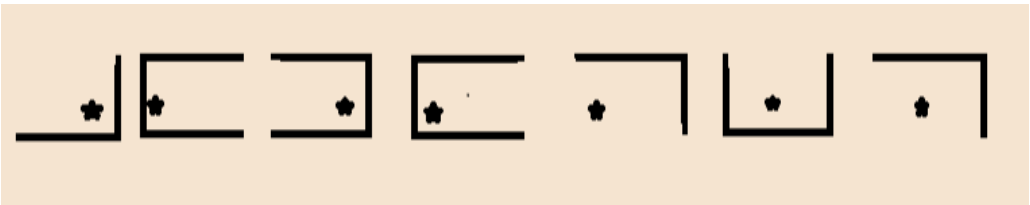
Resultado:

2. **Descifrar:** AECA AEDCBAAEDBCD AAEEDECE

Resultado:

Juego del gato

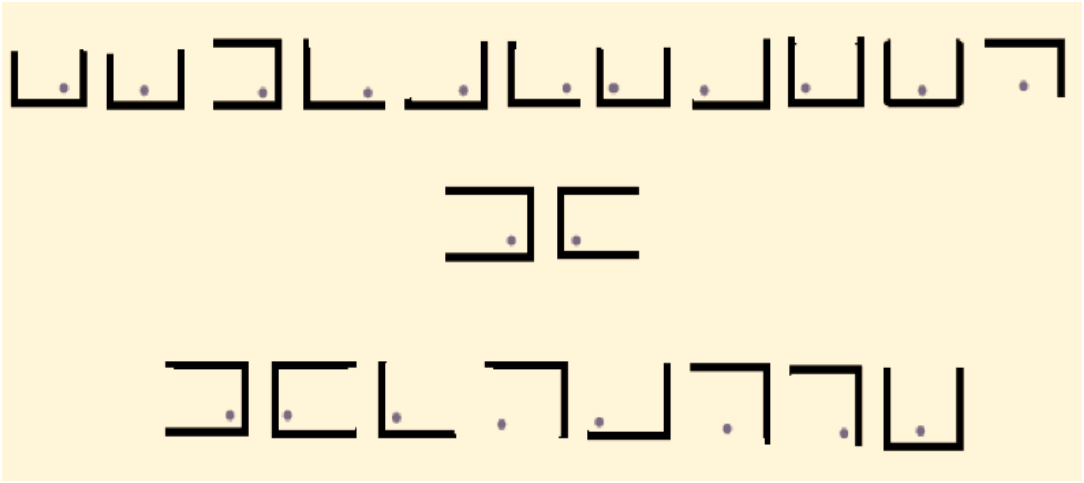
3. **Utilizando el método del gato descifrar el siguiente mensaje.**



4. **Cifrar la siguiente información:**

- **SEGURIDAD INFORMATICA**
- **SISTEMAS DE ARCHIVOS**
- **SIMULACION PROMODEL**

5. **Observa cuidadosamente y descifra el mensaje oculto para ti.**



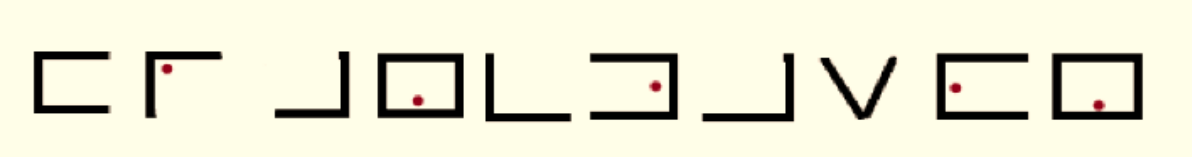
Escribe el mensaje aquí:

Cifrado francmasón (la cifra

1. **Según la tabla PIG PEN cifre el párrafo a continuación:**

Escribir un mensaje en clave mediante un sistema de signos formado por números, letras, símbolos, etc.

2. **Descifrar.**



Resultado:

3. **Reúnete en grupos de 4 personas y elaboren un mensaje con PIG PEN, luego intercambien cuadernos para que el otro grupo descifre su información.**

La cifra de cesar

6. Con la tabla a continuación cifrar las siguientes palabras.

Alfabeto claro	**A**	**B**	**C**	**D**		**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Alfabeto cifrado	**X**	**Y**	**Z**	**A**		**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**

TEXTO ORIGINAL	TEXTO CODIFICADO
• **Enciclopedia** • **Libre** • **Juego** • **Mensajes** • **secretos**	

7. Practicar lo aprendido elaborando una tabla con cifrado CESAR con desplazamiento cuatro como se explica a continuación.

a) Construye un alfabeto de cesar con desplazamiento de cuatro lugares hacia la derecha.

b) Según la tabla elaboraba en el primer punto codifica el siguiente mensaje;

Tres tristes tigres comían trigo en un trigal

8. Tomando en cuenta la tablas del Cifrado de Cesar con 6 espacios hacia la derecha del final, descifrar lo siguiente:

TEXTO ORIGINAL	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
TEXTO CODIFICADO	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**

DESCIFRAR → **ÑSZKXSKZ**

Cifrado de Vigenere

9. Utiliza la tabla de Vigenere y oculta la siguiente palabra.

D	O	C	U	M	E	N	T	A	C	I	O	N

- **clave** → **inicio**

Resultado de palabra cifrada

10. Cifrar con clave: INSERTAR

MENSAJE	A	V	A	N	Z	A	R		P	O	R		L	A		D	E	R	E	C	H	A
CLAVE	I	N	S	E	R	T	A		R	I	N		S	E		R	T	A	R	I	N	S

Resultado:

11. Con los siguientes datos y la tabla de Vigenere codifica.

Mensaje: EJERCICIOS DE PRACTICA
Clave: REVISAR

Cifrados por Bloque – Blowfish

12. Toma como ejemplo el siguiente código y elabora tu algoritmo de cifrado en Pycrypto.

```
1. from Crypto.Cipher import Blowfish
2. from Crypto import Random
3. from struct import pack
4. from sys import argv
5. def encriptar(key, plaintext):
6.     bs = Blowfish.block_size
7.     iv = Random.new().read(bs)
8.     bf = Blowfish.new(key, Blowfish.MODE_CBC, iv)
9.     plen = bs - (len(plaintext) % bs)
10.    padding = [plen]*plen
11.    padding = pack('b'*plen, *padding)
12.    msg = iv + bf.encrypt(plaintext + padding)
13.    return msg
14. def recuperar(key, ciphertext):
15.    bs = Blowfish.block_size
16.    v = Random.new().read(bs)
17.    uncipher = Blowfish.new(key,Blowfish.MODE_CBC, v)
18.    m = uncipher.decrypt(ciphertext)
19.    return m[8:]
20. if __name__ == '__main__':
21.    msg = ''
22.    for i in xrange(1,len(argv)):
23.        if argv[i].lower() == '-p':
24.            key = argv[i+1]
25.        elif argv[i].lower() == '-m':
26.            msg = argv[i+1]
27.        elif argv[i].lower() == '--test':
28.            print msg
29.            ct = encriptar(key,msg)
30.            pt = recuperar(key, ct)
31.            print 'Texto Cifrado:\t %s' % ct
32.            print 'Texto Original:\t %s' % pt
```

Cifrado De Playfair

1. **Codifica El Siguiente Mensaje:** “ARENA MOVEDIZA”

Clave: LUNES

L	U	N	E	S
A	B	C	D	F
G	H	IJ	K	M
O	P	Q	R	T
V	W	X	Z	Y

Resultado:

2. **Decodifica El Siguiente Mensaje:** “LFOTIASE”

Clave: AVION

A	V	IJ	O	N
B	C	D	E	F
G	H	K	L	M
P	Q	R	S	T
U	W	X	Y	Z

Resultado:

La escitala espartana

3. **Escitala uno de los métodos más antiguos, hazle honor y resuelve el siguiente mensaje oculto.**
    - Recuerda que se van formando por 3 filas así podrás revelar el mensaje.

MATALOÑPDAAANRLAQAIUFREAESMMAIOMLSAIANAJEUUSNGCIAODRNA

4. **Utilizando el método del escitalo codificar lo siguiente:**

- eljuegodelosmensajessecretosdelescitalo
- leerbuenoslibrosescomoconversarconlasmejoresmentesdelpasado

5. **Arma tu propio mensaje siguiendo las reglas del escitalo y codifícalo.**

QUIZ

1. **La siguiente definición "ambos extremos deben tener la misma clave para cumplir el proceso" corresponde a:**

   a) Encriptación
   b) Desencriptar
   c) Llave Simétrica
   d) Llave Asimétrica

2. **¿Cuál es la función del algoritmo?**

   a) Mantener la Clave
   b) Codificar la información de modo que sea indescifrable
   c) Transformar caracteres incoherentes
   d) Ninguna de la Anteriores

3. **A Marca la alternativa que NO corresponde a Encriptación**

   a) Autenticidad de los usuarios
   b) Confidencialidad
   c) Fácil de descifrar
   d) Integridad

4. **La llave asimétrica:**
   a) Puede desencriptar lo que la otra ha encriptado
   b) Tiene características matemáticas especiales
   c) Es difundida
   d) Todas las Anteriores

5. **El término de criptoanalista corresponde a:**

   a) La persona que sin tener la llave secreta, trata de descifrar un texto encriptado
   b) La persona que tiene la llave secreta, no descifra el texto encriptado
   c) La persona que sin tener la llave secreta, no trata de descifrar un texto encriptado
   d) La persona posee la llave secreta, descifra un texto encriptado

Solución

1. C) Llave Simétrica
2. B) Codificar la información de modo que sea indescifrable
3. C) Fácil de descifrar
4. D) Todas las Anteriores
5. A) La persona que sin tener la llave secreta, trata de descifrar un texto encriptado

ANEXO A

Leyes y regulaciones sobre los delitos informáticos en el ecuador

Tabla 1. Leyes y regulaciones sobre los delitos informáticos en el Ecuador.

DELITOS INFORMÁTICOS	REPRENSIÓN	MULTA
DELITOS CONTRA LA SEGURIDAD DE LOS ACTIVOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN		
Revelación Ilegal De Base De Datos. (Art. 229.) La persona que revele información contenida de ficheros, archivos, base de datos, o semejantes, a través de un sistema electrónico, informático, telemático, o telecomunicaciones. Violando la intimidad y privacidad de la persona. Si es un servidor público.	3 a 5 años	
Interceptación Ilegal De Datos. (Art. 230) • La persona que sin orden judicial intercepte, escuche, desvíe, grabe u observe un dato informático en su origen, destino o en el interior de un sistema informático, una señal o transmisión de datos con la finalidad de obtener información. • Persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad, páginas electrónicas, enlaces, ventanas emergentes, o modifique el sistema de resolución de nombres de dominio de un servicio financiero, de tal manera que induzca a una persona a ingresar a un sitio diferente al que quiere acceder. • Persona que por cualquier medio copie, clone o comercialice información contenida en bandas magnéticas, chips, o dispositivo electrónico soportado en tarjetas de crédito, débito, pago o similares. • Persona que fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito.	3 a 5 años	
Transferencia Electrónica De Activo Patrimonial. (Art. 231) • Persona que con ánimo de lucro altere, modifique o manipule el funcionamiento de	3 a 5 años	

un programa sistema informático, telemático o mensaje de datos, para transferencia o apropiación no consentida de un activo patrimonial de otra persona. • Persona que facilite datos de su cuenta con la intención de obtener de forma ilegítima un activo patrimonial a través de una trasferencia electrónica producto de este delito.	3 a 5 años	
Ataque A La Integridad De Sistemas Informáticos. (Art. 232) • Persona que dañe, altere, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones. • Diseñe, desarrolle, programe, adquiera, envié, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar 1os efectos señalados en el primer inciso de este artículo. • Destruya o altere sin la autorización de su titular, 1a infraestructura tecnol6gica necesaria para la transmisi6n, recepci6n o procesamiento de información en general. • Si 1a infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana	3 a 5 años 3 a 5 años 3 a 5 años 5 a 7 años	
Delitos contra la información pública reservada legalmente. (Art. 233) • el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información. • Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado.	3 a 5 años 7 a 10 años	
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. (Art. 234) • La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la	3 a 5 años	

voluntad de quien tenga el legítimo derecho.		
Delitos Contra La Información Protegida: Violación De Claves O Sistemas De Seguridad (CPP Art. 202) **Título II: DE LOS DELITOS CONTRA LAS GARANTIAS CONSTITUCIONALES Y LA IGUALDAD RACIAL.** Cap. V. De los Delitos Contra la inviolabilidad del secreto. • Empleo de cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad. • Acceder u obtener información protegida contenida en sistemas de información. • Vulnerar el secreto, confidencialidad y reserva o simplemente vulnerar la seguridad. • Agravantes dependiendo de la información y del sujeto activo • Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales. **Obtención y utilización no autorizada de Información** • La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares. • La divulgación o utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales. • Si la divulgación o la utilización fraudulenta se realizan por parte de la persona o personas encargadas de la custodia o utilización legítima de la información	Prisión 6 Meses A Un Año 1 a 3 años de prisión Prisión de 2 meses a 2 años Pena de reclusión menor ordinaria de 3 a 6 años Pena de reclusión menor de 6 a 9 años	Multa $500 A $1000 Multa $1000 A $1500 Multa $1000 A $2000 Multa $1000 A $10000 Multa $1000 A $10000
Delitos Contra La Información Protegida: Destrucción O Supresión De Documentos, Programas. (CCP Art. 262) **Titulo III. DE LOS DELITOS CONTRA LA ADMINISTRACION PÚBLICA.** Cap. V. De la Violación de los deberes de Funcionarios Públicos, de la Usurpación de Atribuciones y de los Abusos de Autoridad. • Todo empleado público y toda persona		

encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo.	3 a seis años de reclusión menor	
Falsificación Electrónica (CPP Art. 353) **Título IV. DE LOS DELITOS CONTRA LA FE PUBLICA.** Cap. III. De las Falsificaciones de Documentos en General • La persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático.	3 a 6 años	
Daños Informáticos (CPP Art. 415) **Titulo V. DE LOS DELITOS CONTRA LA SEGURIDAD PÚBLICA.** Cap. VII: Del incendio y otras Destrucciones, de los deterioros y Daños. • El que, dolosamente utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica. • Cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional. • Un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos	6 meses a 3 años 3 a 5 años 8 meses a 4 años	Multa de $60 a $150 $200 a $600 $200 a $600
Fraude Informático (CPP Art. 553)		

Titulo X. DE LOS DELITOS CONTRA LA PROPIEDAD. Cap. II. Del Robo. Cap. V De las Estafas y otras defraudaciones. Los que utilizaren fraudulentamente sistemas de información o redes electrónicas: • Para facilitar la apropiación de un bien ajeno. • La transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de esta o de un tercero, en beneficio suyo o de otra persona • Alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.	6 meses a 5 Años	MULTA $500 A $1000
Y SI EMPLEA LOS SIGUIENTES MEDIOS: • Inutilización de sistemas de alarma o • guarda • Descubrimiento o descifrado de claves • secretas o encriptadas • Utilización de tarjetas magnéticas o • perforadas • Utilización de controles o instrumentos • de apertura a distancia, y, • Violación de seguridades electrónicas	Prisión 1 a 5 años	MULTA $1000 A $2000
Artículo 64.- Será sancionado con el máximo de la pena prevista en el inciso anterior el que cometiere el delito utilizando medios electrónicos o telemáticos.	Máximo de la pena prevista en el inciso anterior	MULTA $500 A $1000
Violaciones al Derecho a la Intimidad (Contravención) (Art. 606) **LIBRO III. CODIGO PENAL TITULO I. CAP. III. DE LAS CONTRAVENCIONES DE TERCERA CLASE.** Violación al derecho a la Intimidad: Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.	1 a 3 años	
Pornografía Infantil (Art. 528) **Título VIII, Capítulo III.1, DE LOS DELITOS DE EXPLOTACIÓN SEXUAL.** • Producción, publicación comercialización de imágenes pornográficas, materiales visuales, audiovisuales, informáticos, electrónicos o de		

cualquier otro soporte físico o formato u organizare espectáculos en vivo, con escenas pornográficas en que participen los mayores de catorce y menores de dieciocho años. • Quien distribuyere imágenes pornográficas cuyas características externas hiciere manifiesto que en ellas se ha grabado o fotografiado la exhibición de mayores de doce y menores de dieciocho años al momento de la creación de la imagen. • Quien facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico en cuyas imágenes participen menores de edad	6 a 9 años de reclusión menor ordinaria Inhabilidad para el empleo profesión u oficio.	
Cuando en estas infracciones, la víctima sea un menor de doce años o discapacitado, o persona que adolece enfermedad grave incurable,	Reclusión mayor extraordinaria de 12 a 16 años. Inhabilidad del empleo, profesión u oficio En caso de reincidencia: 25 años de reclusión mayor especial.	
Cuando el infractor de estos delitos sea el padre, madre, parientes hasta el cuarto grado de consanguinidad y segundo de afinidad, tutores, representantes legales, curadores o cualquier persona del contorno íntimo de la familia, ministro de culto, maestros y profesores y, cualquier otra persona por su profesión u oficio hayan abusado de la víctima.	pena de 16 o 25 años de reclusión mayor extraordinaria.	
Si la víctima fuere menor de doce años.	Se aplicará el máximo de la pena.	

4 Tabla 2. Algunos Delitos Informáticos en Perú y Colombia

DELITOS INFORMÁTICOS	REPRENSIÓN	MULTA
Algunos Delitos Informáticos en Perú		
Acceso ilícito a todo o parte de un sistema informático.	Hasta 4 años	
A los que atenten contra la integridad de los datos informáticos, borrándolos o deteriorándolos	Hasta 6 años de prisión	
A los que afectan la integridad de un sistema informático inutilizándolo o impidiendo su acceso	Hasta 6 años de prisión	
A la persona que crea, ingresa o usa ilegalmente una base de datos para comercializar, traficar o vender esa información	Hasta 5 años de prisión	
A los que practican la interceptación de datos informáticos, cuando se trate de información clasificada como secreta o confidencial. Cuando se compromete la defensa o la seguridad nacional.	Se regula un castigo mayor de hasta 8 años. Esa pena sube hasta 10 años	
Algunos Delitos Informáticos en Colombia		
A quienes, "con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes". El que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP (Protocolo de Internet) diferente, en la creencia de que acceda a su banco o a otro sitio personal o de confianza.	Desde los 48 a los 96 meses.	$100 a $1.000 Salarios mínimos legales mensuales vigentes.

Tabla 2. Algunos Delitos Informáticos en Perú y Colombia

DELITOS INFORMÁTICOS	REPRENSIÓN	MULTA
Algunos Delitos Informáticos en Perú		
Acceso ilícito a todo o parte de un sistema informático.	Hasta 4 años	
A los que atenten contra la integridad de los datos informáticos, borrándolos o deteriorándolos	Hasta 6 años de prisión	
A los que afectan la integridad de un sistema informático inutilizándolo o impidiendo su acceso	Hasta 6 años de prisión	
A la persona que crea, ingresa o usa ilegalmente una	Hasta 5 años de	

base de datos para comercializar, traficar o vender esa información	prisión	
A los que practican la interceptación de datos informáticos, cuando se trate de información clasificada como secreta o confidencial. Cuando se compromete la defensa o la seguridad nacional.	Se regula un castigo mayor de hasta 8 años. Esa pena sube hasta 10 años	
Algunos Delitos Informáticos en Colombia		
A quienes, "con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes". El que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP (Protocolo de Internet) diferente, en la creencia de que acceda a su banco o a otro sitio personal o de confianza.	Desde los 48 a los 96 meses.	$100 a $1.000 Salarios mínimos legales mensuales vigentes.

ABREVIATURAS

HSM.- Hardware Security Module (Módulo de seguridad de hardware).

KVM.- Keyboard Video Monitor (Teclado Video Monitor).

NAT.- Network Address Translation (Traducción de Direcciones de Red).

VLAN.- Red de área local virtual (Local Area Network Virtual)

PPTP.- Point to Point Tunneling Protocol (Protocolo de túnel punto a punto).

MPPE.- Microsoft Point-to-Point Encryption (Cifrado punto a punto de Microsoft).

L2TP.- Layer 2 Tunneling Protocol (Protocolo de túnel de capa 2).

RMS: Rights Management Services (Servicios de gestión de derechos).

VPN.- virtual private network (red privada virtual).

NTFS New Technology File System (Sistema de archivos de nueva tecnología).

SMS .- Systems Management Server

HTML.- HyperText Markup Language (Lenguaje de marcado de hipertexto).

EFS.- Encrypting File System (Sistema de cifrado de archivos).

PIN.- Personal Identification Number (Número de identificación personal).

TCP.- Transmission Control Protocol (Protocolo de Control de Transmisión).

UDP.- User Datagram Protoco l(Protocolo de datagramas de usuario).

ICMP.- Internet Control Message Protocol (Protocolo de mensajes de control de Internet).

FTP.- File Transfer Protocol (Protocolo de transferencia de archivos).

HTTP.- Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto).

MAC.- Media Access Control (El control de acceso a medios).

AES.- Agencia Estatal de Seguridad

ACL.- Access Control List (Lista de control de acceso).

SSL.- Secure Socket Layer (Capa de conexión segura).

TLS.- Transport Layer Security (Seguridad en la Capa de Transporte).

NNTP.- Network News Transport Protocol (Protocolo de transporte de noticias de red).

TGT.- Ticket de otorgamiento de tickets.

KDC.- Centro de distribución de claves.

SSH.- Secure Shell(Cubierta segura).

RAID.-redundant array of independent disks (Matriz redundante de discos independientes).

PGP.- Pretty Good Privacy (privacidad bastante buena)

FAT.- File Allocation Table (Tabla de asignación de archivos).

IIS.- Internet Information Services (Servicios de Información de Internet).

DMZ.- demilitarized zone (zona desmilitarizada).

LAN.- Red de area local

SPAM.- Stupid Pointless Annoying Messages (Mensajes molestos estúpidos e inútiles).

NMAP.- Network Mapper (mapeador de redes).

EDR.- Enterprise Data Replicator(replicador de datos empresariales).

DAST .-tests dinámicos de seguridad de aplicaciones.

CET .- tests estáticos de seguridad de aplicaciones.

CRM.- Administración de Relaciones con el Cliente (Customer Relationship Management).

WAN.- Wide Area Network (Red de Área Amplia).

WPA.- Wi-Fi Protected Access (Acceso Wi-Fi protegido).

WEP .- Wired Equivalent Privacy(Privacidad equivalente por cable).

OSI.- Open System Interconnection(Interconexión del sistema abierto).

IPX.- Internetwork Packet Exchange (Intercambio de Paquetes Interred).

SPX.- Sequenced Packet Exchange (Intercambio de paquetes secuenciados).

FDDI.- Fiber Distributed Data Interface (Interfaz de Datos Distribuida por Fibra)

DNS.- sistema de nombres de dominio/Domain Name System.

CLI.- Command line interface/interfaz de línea de comandos

REFERENCIAS

Adastra. (2012). Seguridad en Sistemas y técnicas de Hacking. Retrieved from www.thehackerway.com

Alberto, C., & Quispe, F. (2009). Tipos de hackers, 1.

Alegsa, L. (2008). Diccionario de informática y tecnología. Retrieved from www.alegsa.com.ar

Alejandro Cuevas, Héctor Corrales, C. C. (2010). Criptografía y Métodos de Cifrado Índice :

Algredo Badillo, I., Cumplido Parra, R. A., & Uribe, F. (2008). Desarrollo de un Módulo MD5 para un Sistema Criptográfico Reconfigurable en un FPGA.

Álvarez, G., & Pérez, P. P. (2004). *Seguridad informática pra empresas y particulares*. (C. S. Gonzáles, Ed.) (McGRAW-HIL). Madrid.

Angel, A. (2010). Criptografía Para Principiantes, 1–59.

Ardita, J. (2001). Adelantándose a los Hackers: Herramientas y técnicas de testing de vulnerabilidades. *Cybsec S.A.*, 1–29.

Ares, E. (2009). Mundo Cisco: Qué es un Sniffer.

Astudillo, K. (2013). *Hacking Ético 101*.

Benchimol, D. (2011). *Hacking desde 0* (Fox Andina). Buenos Aires.

Benitez, C. (2016). ¿Qué son los Hackers Black Hat y Hackers White Hat?

Bonnet, N. (2012). *Certificaciones: Wi ndows Server 2012 R2 Instalación y Configuración*.

Borghello, C. (2009a). Segu -Info: Amenazas Humanas.

Borghello, C. (2009b). Sistema de detección de Intrusos. Retrieved from http://www.segu-info.com.ar

Callejas, A. (2015). Seguridad y Hardening en Servidores Linux.

Carlos, V. L., Diego, A. G., & Arturo, G. S. (2010). Eumed.net: Algoritmos de Encriptación. Retrieved from http://www.eumed.net/libros-gratis/2008a/348/Modelos de servicios de encriptacion de datos.htm

Carlos Lamas, A. Q. y V. M. Á., & Escriba. (1997). PGP for Personal Privacy.

Carvajal, A. (2007). Introducción a las técnicas de ataque e investigación forense, un enfoque pragmático. *Tecnologías Globales Para La Seguridad de La Información*.

Cedeño, E. Y. (2015). Análisis de las herramientas para el proceso de auditoría de seguridad informática utilizando.

Centeno, F. J. U. (2015). CIBERATAQUES, LA MAYOR AMENAZA ACTUAL, 1–18.

Coronel, C. (2014). SliderPlayer. Retrieved from http://slideplayer.es/slide/122739/

CSCU. (2017). CSCU: Certificado de Dispositivo de Software (CDP). Retrieved from http://www.csuc.cat/es/e-administracion/certificacion-digital/certificado-de-dispositivo/certificado-de-dispositivo-de-1

Doevan, J. (2016). Los Virus: Carding y como eliminarlo.

Duarte, E. (2012). Capacity: Information Techonoly Academy. Retrieved from http://blog.capacityacademy.com

Ecured. (2015). Ecured: Qué es un hackers. Retrieved from

https://www.ecured.cu/Hacker
emred. (2015). Emred.com: ¿QUÉ HACE QUE ALGUIEN SEA SPAMMER? Retrieved from http://www.emred.com/alguien-sea-spammer-02-la-tasa-denuncia/
Ferić, I. (2006). Vatrozid. Zagreb.
Franco, D. A., & Perea, J. L. (2012). Metodología para la Detección de Vulnerabilidades en Redes de Datos Methodology for Detecting Vulnerabilities in Data Networks, *23*, 113–120. http://doi.org/10.4067/S0718-07642012000300014
González, E. S. M. (2014). *Salvaguarda y seguridad de los datos*. (I. Editorial, Ed.) (1eral ed.).
Hacking Ético. (2008). Retrieved from www.cursodehackers.com
Heras, J. S. de las. (2000). Ataques de spam con direcciones falsificadas, 1–6.
Hernández, J. A. G. (2015). Introducción al Hacking Ético de sistemas y redes Índice, 1–39.
IBM. (2010). IBM Knowledge Center: : Técnicas para proteger el sistema los sistemas operativos. Retrieved from www.ibm.com
IBM. (2017). IBM Knowledge Center: Protocolos IPSec (IP Security). Retrieved from https://www.ibm.com/support/knowledgecenter/es/ssw_i5_54/rzaja/rzajaipsec.htm
IBM Knowledge Center. (2016). In *Técnicas para proteger el sistema operativo*. Retrieved from https://www.ibm.com/support/knowledgecenter/es/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.crn_arch.10.2.1.doc/c_securing_the_operating_system.html
Informática Hoy: Craker. (2010).
Inteco. (2010). Botnets, 1–14.
J. Steiner, J. Neuman, J. S. (1988). *Kerberos: An Authentication Service for Open Network System UNESIX*.
James Audubon, J. (2004). Triple Data Encryption Standard (Triple-DES). *VOCAL Technologies*.
Klein, D. V. F. (1999). *A Survey of, and Improvement to, Password Security*.
Llaquet, F. P. (2011). Hardening básico de Linux Permisos y Configuraciones.
López, M. J. L. (2002). Criptografía y Seguridad en Computadores, *Tercera Ed*.
Lucena López, M. J. (1999). Criptografía y Seguridad en Computadores. Retrieved from http://www.kriptopolis.org
MARKUP. (2017). MarketWare: Certificados Digitales de Servidor. Retrieved from https://www.marketware.eu/index.php/es/certificados-de-servidor
Martinez, I. (2014). BlogPrezi.
Merino, M. (2014). Las 10 principales tecnologías de seguridad. Retrieved from http://www.ticbeat.com/seguridad/10-principales-tecnologias-seguridad-2014/
Microsoft. (2012). TechNet.
Microsoft. (2015). Administrar la configuración de directiva de seguridad. Retrieved from www.msdn.microsoft.com
Mifsud, E. (2007). Gestor de arranque GNU GRUB. Retrieved from http://recursostic.educacion.es/observatorio/web/es/software/software-general/534-el-gestor-de-arranque-gnu-grub
Morales, J. (2007). Encriptación de la Información.
Osi. (2012). Oficina de Seguridad de internauta: Cómo aceptar certificados en el navegador (I). Retrieved from https://www.osi.es/es/actualidad/blog/2014/04/24/como-aceptar-certificados-

en-el-navegador-i-internet-explorer
Oviedo, U. de. (2005). Seguridad en las comunicaciones.
Paloma, J. (2007). Microsoft TechNet: Artículo MVP del mes sobre Seguridad. Retrieved from https://www.microsoft.com/latam/technet/articulos/articulos_seguridad/2007/diciembre/sv1207.mspx
Pardo, D. (2013). BBC Mundo: Diferencia entre geek y nerd. Retrieved from http://www.bbc.com/mundo/noticias/2013/06/130624_tecnologia_geek_nerd_definicion_diferencia_dp
Pello Altadill, X. (2003). *IPTABLES Manual práctico*.
Quintero, B. (2011). Malware : Definición y tipos.
Ramos, D. A. (2012). El futuro de los ataques por desbordamiento de pila, 1.
Reis, D. (2013). *Seguridad para la nube y la virtualización* (Trend Micr). New Jersey.
S.Kent, V. V. y. (1983). *Security Mechanisms in High – Level Network Protocols* (ACM Comput).
Safelayer. (2017). Soluciones Autenticación adaptativa. Retrieved from https://www.safelayer.com/es/soluciones/adaptive-authentication
Sánchez, R. (2004). Cortafuegos y Linux.
Sarba, J. (2013). Políticas de seguridad para ReHat Linux ES y WS. Retrieved from www.github.com
seguinfo. (2013). Seguridad Informática: Noticias de Seguridad. Retrieved from https://seguinfo.wordpress.com/2013/10/17/que-es-cyberpunk/
Seguridad Informática. (2009). Seguridad Informática: Departamento de SI. Retrieved from http://www.seguridadinformatica.unlu.edu.ar/?q=taxonomy/term/23
Selent, D. (2010). Advanced encryption standard. *RIVIER ACADEMIC*, *6*(2), 1–14.
Semanat, A. S. (2008). Estrategia de seguridad contra ataques internos en redes locales, 1–9.
Setfree, L. (2015). Vix: Qué es un hackers. Retrieved from http://www.vix.com/es/btg/tech/13182/que-es-un-hacker
Sierra, J. (2017). Smart and Secure Information Management. Retrieved from http://www.davinci-ti.es/agente-de-seguridad-de-acceso-a-la-nube-bluecoat-symantec-casb/
Silvana, H. (2002). Estudio comparativo de los algoritmos de cifrado de flujo RC4, A5 y SEAL.
Ssl. (2017). SSL 247: The web Security Consultants. Retrieved from https://www.ssl247.es/certificats-ssl/rsa-dsa-ecc
Tanenbaum, A. S. (2009). *Sistemas Operativos Modernos*. (L. M. C. Castillo, Ed.) (Pearson Ed). México.
Tanenbaun, A. S., & M. Van Steen. (2008). *Sistemas Distribuidos Principios y Paradigmasa*. (L. M. Cruz Castillo & B. Gutierrez Hernández, Eds.) (Pearson Ed). México.
Techtarget, U. N. W. D. E. (2015). La Defensa Contra Amenazas no Sólo es Acerca de Detección : Es Cómo Responde Usted. Retrieved from http://www.mcafee.com/us/products/active-response.aspx.%0A2821
tugurium. (1997). GTI: Glosario Terminología Informática. Retrieved from http://www.tugurium.com/gti/termino.php?Tr=sneaker
Valencia, U. (2016). Viu: Tipos de seguridad. Retrieved from http://www.viu.es/tres-tipos-seguridad-informatica-debes-conocer

Vázquez, J. M. M. (2005). Introducción al CLI en Routers y Switches CISCO, 1–23.
Velasco, R. (2016). Herramientas Populares para Crakear contraseñas. Retrieved from https://www.redeszone.net/2016/08/06/top-10-las-herramientas-mas-populares-crackear-contrasenas/
Yrigoyen, A. e. (2008). Poder Judicial: Políticas de Seguridad de los Recursos Informáticos. Retrieved from http://www.jussantiago.gov.ar

ISBN: 978-9942-814-11-1