ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"MODELO DE PREVENCIÓN DE SEGURIDAD PARA UN SISTEMA DE TELECOMUNICACIONES"

TRABAJO DE TITULACIÓN

Previa a la obtención del Título de:

MAGÍSTER EN TELECOMUNICACIONES

EDISON GABRIEL ERIQUE JARAMILLO

GUAYAQUIL – ECUADOR

AÑO 2018

AGRADECIMIENTO

A mi madre por haberme forjado como la persona que soy en la actualidad; muchos de mis logros se los debo a ella, entre esos logros se incluye este. Me formó con reglas y actitudes, que al final de cuentas, me motivaron constantemente para alcanzar mis anhelos. A mi esposa Katherine por confiar en mí y ser mi apoyo incondicional en todo momento.

A mis compañeros y profesores de maestría por su amistad y conocimientos impartidos. A mi director de trabajo de titulación, Vladimir Sánchez, por su gran ayuda en el paso final de esta meta propuesta. Y un agradecimiento especial a la ESPOL por su acogida y por formarme como profesional.

DEDICATORIA

A mi madre con mucho amor le dedico todo mi esfuerzo y trabajo puesto para la realización del presente proyecto. Gracias mamá por hacerme siempre apuntar a lo más alto.

TRIBUNAL DE SUSTENTACIÓN

César Antonio Martín Moreno, Ph.D.
SUBDECANO DE LA FIEC

Vladimir Sánchez Padilla, M.Sc.
DIRECTOR DEL TRABAJO DE TITULACIÓN

Albert Espinal Santana, Mgtr.
MIEMBRO PRINCIPAL DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, me corresponde exclusivamente; y doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

_____

Edison Gabriel Erique Jaramillo

RESUMEN

Los riesgos de un ciberataque a las empresas son una consideración primordial hoy en día. Se vive en una sociedad dependiente de la tecnología, por lo que la información empresarial y personal es vulnerable a ataques cibernéticos, sin importar el tamaño de la red. Organizaciones que parecen ser disponer de seguridades informáticas sólidas pueden ser vulneradas. Ante esto, tener un modelo para prevención de seguridad es algo que se debe tener en cuenta para prevenir un ataque.

En realidad no existe la fórmula mágica que permita estar protegidos al cien por cien ante estos posibles ataques. Hay que tener en cuenta que incluso grandes empresas multinacionales han sufrido daños debido a vulnerabilidades desconocidas, por lo cual se debe estar preparado para reaccionar contra las amenazas lo antes posible.

Este trabajo de titulación presenta un modelo de prevención de seguridad basado en políticas y normas para evitar (o reducir) las fallas en sistemas informáticos, redes de datos, Internet y todo patrimonio informático (entiéndase hardware, software y datos) debido a potenciales ataques antes de que éstos se produzcan, a través de un proceso de establecimiento de procedimientos, registros, controles y documentación. Este modelo puede ser utilizado como base para que cualquier tipo de organización pueda realizar un uso seguro de las Tecnologías de Información y Comunicación (TIC).

ÍNDICE GENERAL

CAPÍTULO 1

SITUACIÓN ACTUAL

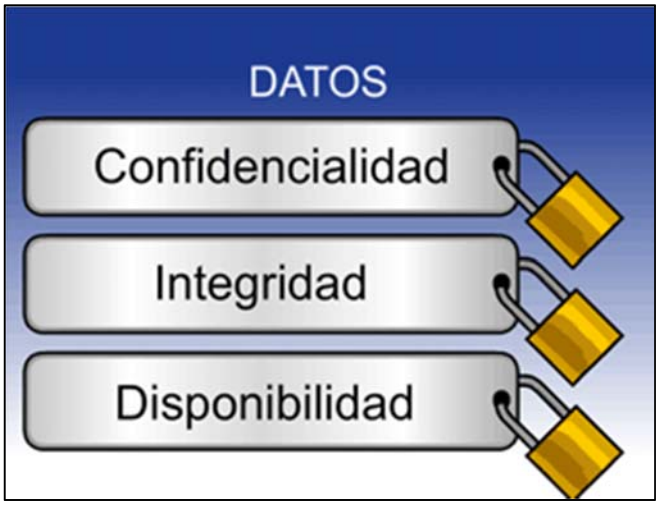
En el presente capítulo se describe una política de seguridad en donde se mencionan los aspectos básicos y los elementos que la conforman, planteando el problema de seguridad en las empresas y los factores limitantes para una política de seguridad adecuada.

1.1 Política de Seguridad del Sitio

Para una organización es vital tener una política de seguridad de red bien constituida que pueda proteger la información. La mayoría de las empresas tienen en sus redes de datos información sensible que puede comprometerse en caso de un ataque informático interno o externo. Ante ello, es importante establecer y obedecer principios relacionados a políticas de seguridad para que formen parte de la cultura organizacional.

Las políticas de seguridad que se plantean para una organización definen lo que está permitido y lo que está prohibido, así como también permiten conocer riesgos y mecanismos de salvaguardia, ello como primer paso en la defensa de la seguridad. Se recomienda tener cuidado en la confianza que se le pueda brindar al personal y a quien o quienes se otorguen privilegios, debiendo ser administrados y supervisados.

Se deben elaborar lineamientos sencillos que permitan proteger la información a través de planes de aseguramiento de la información con el objetivo de garantizar la seguridad de la información. Se define el término "Seguridad de la Información" como el conjunto de normas y medidas preventivas que se deben cumplir para reguardar y proteger la información. En la Figura 1.1 se mencionan los tres aspectos básicos, que son confidencialidad, integridad y disponibilidad, sin olvidar las medidas de seguridad física.



[1] Figura 1.1 Aspectos básicos para una política de seguridad

Confidencialidad: La información debe ser bien guardada y debe ser accesible únicamente a personal autorizado en cualquier momento y de cualquier forma prevista.

Integridad: La información debe ser completa y correcta para dar garantía a que los datos permanezcan inalterados, excepto cuando deban ser modificados por personal autorizado.

[1] Disponibilidad: La información debe ser accesible en todo momento al usuario, debiendo garantizar su propia persistencia ante cualquier eventualidad.

[2] Hay que considerar que tanto las amenazas como los mecanismos para contrarrestarla suelen afectar a estas tres características de forma conjunta. Por ende, un fallo del sistema que haga que la información no sea accesible puede llevar consigo una pérdida de integridad. Generalmente tienen que existir los tres aspectos descritos para que exista seguridad.

Cuando se decide desarrollar una Política de Seguridad se establecen bases para la gestión de la seguridad de la información, la cual será procesada en los sistemas de información o base de datos. [3] No se establecen políticas técnicas, sino más bien políticas organizativas, relacionadas con recursos humanos, o incluso con la seguridad física de las instalaciones.

La efectividad de una política de seguridad no depende del presupuesto asignado, sino de la política de gestión y la concienciación sobre los riesgos a los usuarios de una organización. Los riesgos son varios, pero se pueden mitigar si hay una buena gestión de seguridad y una política que se aplique al entorno.

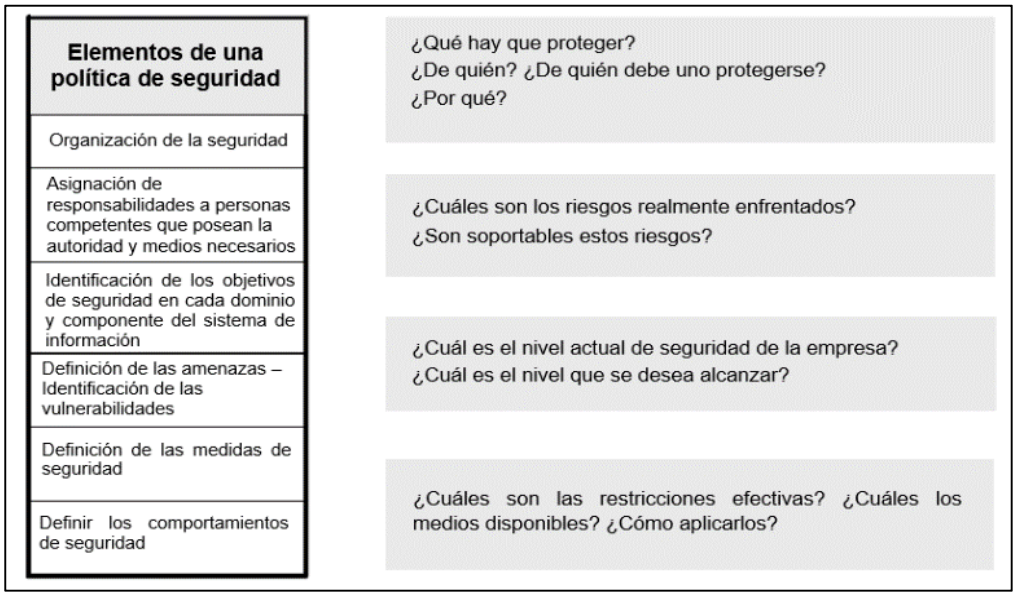


Figura 1.2 Elementos de una política de seguridad

En la Figura 1.2 se mencionan los elementos para mantener una política de seguridad, la cual es de suma importancia que todos conozcan, debido a que es su propia responsabilidad aplicarlas. Resulta difícil que una política de seguridad anticipe todas las amenazas. Sin embargo, con las políticas se puede manejar de forma responsable aspectos relacionados a la seguridad de la información.

1.2 Descripción de la Infraestructura

En la actualidad los sistemas de información, los datos, los archivos y la información son los activos más valiosos para una organización, siendo imprescindible dedicarles una protección especial apropiada frente a posibles intrusiones derivadas de las vulnerabilidades existentes en sus sistemas de seguridad. Una forma práctica de descubrir estas vulnerabilidades y amenazas es iniciando procesos diagnósticos que permitan conocer el estado actual de la

seguridad dentro de la organización, teniendo en cuenta la normatividad vigente y los procesos de análisis y evaluación de riesgos.

Tener una infraestructura de seguridad definida para una organización es de suma importancia, ya que continuamente las amenazas maliciosas representan un problema serio que merecen atención inmediata, debido a que pueden llevar a efectos catastróficos si entes ajenos a la red acceden a información delicada o confidencial de la organización. [4] Esta información delicada en manos de personas inescrupulosas puede ser usada con fines poco éticos y con el fin de causar daño al atacante, como pidiendo dinero por la misma o causando otros tipos problemas.

Una organización debe estar prevenida contra los ataques de red. Para ello se debe contar con una infraestructura de seguridad informática basada en estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la información.

Para una buena infraestructura de seguridad se deben elaborar mecanismos de seguridad que permitan la protección de los bienes y servicios informáticos. Se pueden mencionar como mecanismo de seguridad los siguientes:

- Autenticación.
- Autorización.
- Registro.
- Encriptamiento.
- Filtro de Paquetes.
- Firewalls.
- Sistema de Detección de Intrusos.

En la actualidad es difícil garantizar que la información en una red se encuentre totalmente segura mientras tenga acceso a Internet. Para proteger los sistemas se debe realizar un análisis de las amenazas potenciales, las pérdidas que podrían generar y la probabilidad de ocurrencia. [4] En base a este análisis se

diseña una política de seguridad que define responsabilidades y reglas a seguir para evitar que tales amenazas se produzcan.

Toda organización tiene la necesidad de definir bien su estructura de seguridad para dar mayor protección a la información y al mismo tiempo adaptarse a cambios tecnológicos y a la aparición de nuevas amenazas de la red.

[5] “El Centro Criptológico Nacional, dependiente del Centro Nacional de Inteligencia (CNI), ha alertado de la existencia de un nuevo ciberataque internacional de virus ransomware que, de momento, no ha afectado a ningún organismo público aunque sí a multinacionales. El nuevo ciberataque parece similar al denominado WannaCry, que en mayo pasado afecto a empresas de y a instituciones de distintos países”

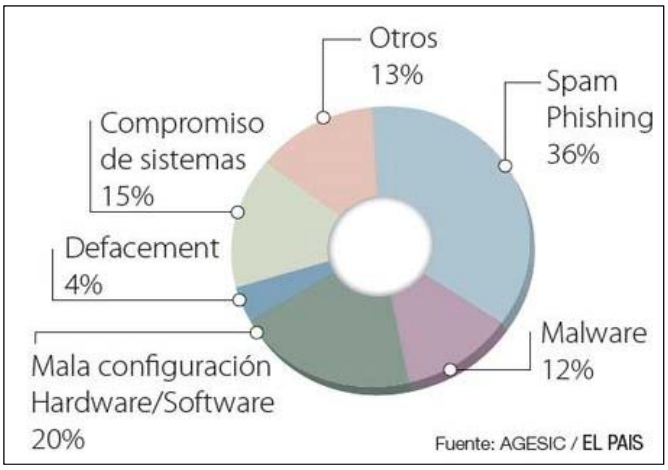


Figura 1.3 Tipos de Ataque en la Red

En la figura 1.3 se muestran los tipos de ataques en la red con sus respectivos porcentajes e incidencias el cual no da entender que muchos sistemas de información no son muy seguros. La seguridad que puede lograrse a través de medios técnicos es muy poca, debiendo apoyarse en una infraestructura de seguridad bien constituida, la cual necesita como requisito mínimo la participación del personal involucrado para hacer conciencia sobre el manejo prudente de la información.

Tener un sistema complejo de seguridad no ayudará en la protección de la información. Si el personal de una organización facilita contraseñas o información de acceso a personas ajenas, dejan abierta la posible filtración de información delicada al exterior de la organización.

1.3 Planeamiento del Problema

Las empresas en desarrollo enfrentan la necesidad de formar parte de la Sociedad de la Información (SI) gracias a las nuevas Tecnologías de Información (TI), lo cual aumenta la dependencia de las organizaciones a las redes de datos (la palabra red se empleará en este documento indistintamente para referirse a una red de datos). Esto genera un alto riesgo de primer orden que debe tomarse como un riesgo de seguridad.

En base a las amenazas de red y las distintas formas en que pueda ser vulnerada la información, se plantean hipótesis y problemas sobre lo que podrían ser puntos de falla a considerar al momento de elaborar un modelo de prevención de seguridad.

Una red debe estar bien configurada, caso contrario se vuelve una entrada a usuarios no autorizados. El dejar una red local abierta a la Internet es muy inseguro, similar a dejar en un domicilio una puerta abierta estando en un barrio peligroso; puede que con suerte no ocurra nada, pero con el tiempo alguien se dará cuenta de la vulnerabilidad para acceder, lo cual ya es un acto fuera de la ley.

Al diseñar una red se debe considerar el hardware de red, esto es, el hardware simple de ruteadores y conmutadores de capa de red (de acuerdo al modelo de referencia OSI), ya que a menudo se basa en difusión (broadcast), en donde un solo emisor envía información a múltiples nodos de manera simultánea sin necesidad de reproducir la transmisión nodo a nodo.[6] Este método comúnmente usado en un hardware simple es muy vulnerable para hacer engaños de direcciones (spoofing) al protocolo de resolución de dirección (ARP) por parte de usuarios no autorizados, siendo una vulnerabilidad muy conocida.

En muchas organizaciones, al centralizar todo en un servidor se da paso a una vulnerabilidad común, esto dada la conveniencia para reducir costos. Sin

embargo, esto introduce a la red un punto de falla muy grande, ya que si el servidor está comprometido puede dejar a la red totalmente inútil, expuesto a la manipulación o robo de información. [7] Tener una red privada virtual (VPN, por sus siglas en inglés) no configurada de forma correcta podría ser también otro punto de fallo en una red, ya que dejaría una brecha abierta hacia el servidor, lo cual podría ser utilizado para atacar y robar información.

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.

[8] Un esquema óptimo de seguridad plantea la seguridad física y lógica. La primera refiere contra robo o daño físico. La segunda y la que se desarrolla en este documento refiere a la protección de la información y la elaboración de una arquitectura de seguridad eficiente.

En conclusión, se puede decir que tener una red mal configurada es una brecha abierta a intrusos con avanzados conocimientos en informática (hackers) que tratan de robar información sensible. Por ello, se propone un modelo de prevención de seguridad que minimice todos estos puntos de falla con el fin de tener una red segura y poder estar prevenidos de los ciberataques.

1.4 Justificación del Trabajo

El mundo actual depende mucho de la tecnología, por lo que la información de una organización o personal está expuesta a ataques, de tal forma que la información pueda ser usada de forma fraudulenta. Como se indicó anteriormente, no existe una red de telecomunicaciones que sea segura en su totalidad. Sin embargo, se puede mitigar el impacto y resguardar la información importante. Por tal motivo, se propone una modelo de prevención de seguridad contra ciberataques que sirva como plantilla para las organizaciones.

[9] “Una decena de grandes empresas españolas de servicios han sufrido un ciberataque masivo a través de un virus malicioso, de tipo ransomware, que bloquea los equipos y solicita un rescate para desbloquearlos. La compañía más afectada ha sido Telefónica, ya que varios centenares de ordenadores de su sede central del Distrito C de Madrid se vieron infectados. Lo que parecía

inicialmente un ataque nacional se ha ido multiplicando con las horas, hasta exponerse como una agresión mundial, con 74 países afectados, entre ellos Portugal, Reino Unido, Rusia y Turquía. Se han registrado en total 45.000 ciberataques."

Tener un personal muy instruido sobre los riesgos de seguridad en la red es muy importante para una organización. Lo citado sobre el ataque a Telefónica se hubiera podido evitar si su personal hubiera tenido en consideración los siguientes consejos prácticos:

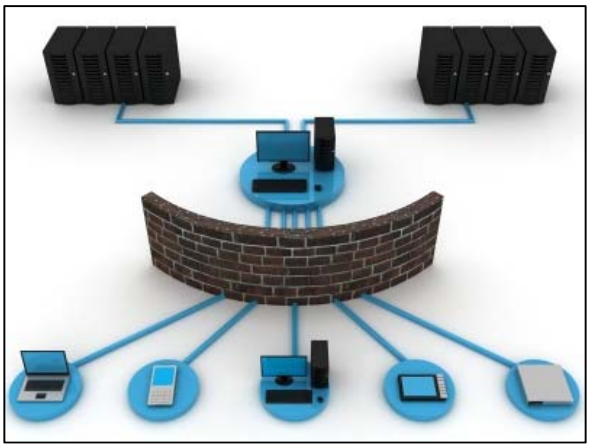
1. No abrir correos electrónicos tipo spam.
2. Evitar descarga de contenidos provenientes de páginas electrónicas de dudoso origen.
3. Tener las computadoras personales (PC) y dispositivos móviles con software de seguridad actualizado y eficaz.
4. Crear respaldos (backup) de los archivos.
5. Mantener el sistema operativo (SO) actualizado.

Es común que los ataques sean dirigidos a empresas pequeñas, debido a su vulnerabilidad y a que su infraestructura de seguridad es muy limitada. El caso de Telefónica fue un ataque perpetrado a gran escala que afecto a centenares de ordenadores. Ante esto, se propone una infraestructura de seguridad basada en estándares y en políticas para mitigar ciberataques, no necesariamente perfecto, pero sí de difícil acceso por los hackers.

1.5 Factores Limitantes

Encontrar los recursos para enfrentar todos los problemas que supone la ciberseguridad puede ser un gran desafío. Todas las organizaciones, sean grandes o pequeñas, [10] al igual que las personas, dependen de las TIC como una herramienta esencial para alcanzar objetivos y metas en un negocio, siendo importante que las organizaciones cuenten con herramientas que garanticen la seguridad de la información.

Para un modelo de prevención contra ciberataques se debe implementar una infraestructura que proteja la seguridad de red y el perímetro lógico. Un cortafuegos (firewall) y un ruteador debidamente configurados son una buena defensa que ayuda a mantener la protección de perímetro, el cual comprende cada punto donde la red interna se interconecta a los hosts y red que no son verificados por el grupo de TI, incluyendo accesos a la Internet, socios empresariales, VPN, conexiones de voz, entre otras. En la figura 1.4 podemos ver como el firewall sirve de barrera para ingresar a una red.



[10] Figura 1.4 Firewall Seguridad perimetral

Según datos de la UIT, se estima que alrededor del 90% de los virus que entran a las organizaciones lo hacen a través del correo electrónico. [11] Los correos electrónicos que se reciben de páginas electrónicas traen en cierto caso un peligro que no es reflejado a simple vista. El firewall analiza el tráfico SMTP y POP3 de los correos electrónicos, pero en el caso de los correos web viajan a través de HTML, por lo que su análisis muchas veces no puede ejecutarse.

El mayor ataque de DoS efectuado hasta la fecha ocurrió en China en el año 2010, lo cual provocó deficiencias del servicio de Internet en ese país y que, por ejemplo, fuese imposible acceder a páginas con dominio. [12] Aun así, la caída del servicio no fue total porque algunos sitios recurrieron a servidores caché y también a servidores externos. Según CloudFare, un proveedor de servicios de seguridad, el tráfico de Internet de China, que está relacionado con sus servicios, cayó en un 32% en las horas en las que se produjo el ataque.

Como se puede inferir, los ataques a las empresas no solo están relacionados con aspectos monetarios, sino en cierta forma con el daño de la imagen y al robo de información delicada para en lo posterior pedir dinero por la recuperación de la misma. Este tipo de ataque se conoce como ramsonware, debido a que solicita un rescata para restaurar la información robada o denegada.

Dentro del estudio se encontró que el 27% de las aplicaciones en nube de terceros fueron clasificadas como de alto riesgo y crearon problemas de seguridad. Las aplicaciones que funcionan en la nube y que tienen mayor riesgo de ser infectadas son las que pertenecen al sector financiero, gubernamental, educativo (universidades), manufactura, medios de comunicación y empresas de tecnología. [12] Con esto se confirma que siempre habrá alguna vulnerabilidad que haga posible el robo de información. Lo que se puede hacer es crear una infraestructura de red difícil de perpetrar para reducir las probabilidades a niveles ínfimos al acceso de los hackers.

1.6 Análisis de Factibilidad

Un elemento muy importante en una infraestructura de seguridad como se mencionó anteriormente es un firewall, elemento que ofrece una solución a los problemas de intento de acceso no autorizado a los dispositivos internos, [13] bloqueando el tráfico según sea las necesidades de una organización. Una metodología muy utilizada por los piratas informáticos es enviar paquetes de manera aleatoria en búsqueda de una máquina conectada, para hallar un hueco en la seguridad que se puede utilizar para acceder a los datos que ahí se almacenen.

Mediante un firewall se pueden crear reglas personalizadas para el control y fluidez sobre la red. Mediante el filtrado de contenidos se logra examinar los paquetes que intentan pasar a través de un firewall, comparándolas con las reglas establecidas. De esta manera, se bloquean fácilmente algunos tipos de contenido web sin tener que hacerlo manualmente con cada URL individual.

Se pueden definir tres reglas básicas para un firewall:

- Autorizar (allow)

- Bloquear (deny)
- Redireccionar (drop)

Un firewall ayuda a manejar una variedad de aspectos en el punto de acceso a la red pública manteniendo fuera a intrusos externos, mientras permite a la red interna concentrarse en ofrecer sus servicios. [14] La idea básica es permitir a los usuarios de una red protegida acceder a una red pública y a la vez hacer disponibles a la red pública los servicios y productos de la organización, garantizando una red protegida.

El control de acceso que ofrece un firewall a un sistema de red permite que los servidores puedan estar disponibles desde la red externa, mientras otros puedan ser cerrados del acceso externo no deseado. De esta forma se previene que los servicios inseguros o vulnerables sean explotados por atacantes externos. [14] Es posible el uso de estos servicios con un riesgo reducido de exposición, debido a que solo algunos protocolos seleccionados serán capaces de pasar a través del firewall.

El firewall es una herramienta poderosa en caso de ataques externos pero debemos tener en cuenta que tener un firewall no es una solución completa a la seguridad, debido a que no puede proteger a la red de ataque internos, existiendo otros niveles de seguridad unificados. [15] Un punto de falla del firewall es que no examina contenido de la capa de aplicación (de acuerdo al modelo referencial OSI), por lo cual es muy vulnerable a un ataque de DoS.

Las soluciones de seguridades actuales no son de carácter universal, ya que con frecuencia solo resuelven un problema en particular en una determinada situación. Se debe tener en claro que adquirir una solución de seguridad no es universal ni definitiva.

CAPÍTULO 2

ANÁLISIS DE RIESGO

En este capítulo se identifican los tipos de riesgos y amenazas. Se hace un resumen de los tipos de ataques comunes a la red y la posible forma de contrarrestarlos. A su vez, se evalúa la relación entre las amenazas, vulnerabilidades y riesgos. Adicionalmente, se comenta sobre la seguridad lógica.

2.1 Identificación del Riesgo

La identificación de riesgos es un procedimiento en el que se reconocen activos y vulnerabilidades, así como la probabilidad que ocurra una amenaza a la red, a fin de poder definir los mecanismos a seguir en caso que ocurran. Las TIC giran en torno a la seguridad, ya que es la parte principal de toda actividad relacionada a las telecomunicaciones, y se debe apreciar como una prestación que tiene facultad de generar valor agregado con independencia de las tecnologías. Los riesgos informáticos tienen naturaleza operacional, generando un punto de partida en el análisis de la seguridad, permitiendo definir estrategias que permiten gestionar una política de seguridad.

[16] Según un estudio hecho por la consultora española Necsia, el 15,5% de las empresas encuestadas aumentó sus presupuestos durante el año 2016 para combatir estos riesgos informáticos, mientras que el 57,1% los mantendrá sin cambios. En su elaboración han participado entidades de hasta 10.000 empleados, coincidiendo la mayoría en que las vulnerabilidades que sufren hacen referencia a aspectos relacionados con fuga de información, fraude, robo de datos, o la falta de desarrollo de un software seguro, entre otros.

Es de suma importancia que una organización tenga una herramienta que asegure la buena evaluación de riesgos. Por medio de procedimientos de control se pueda determinar el desempeño en el entorno y los posibles fallos en la red de manera que se puedan tomar medidas en caso de un evento de robo de información como muestra la figura 2.1 o de ser víctimas del hacking.

Figura 2.1 Robo de Información

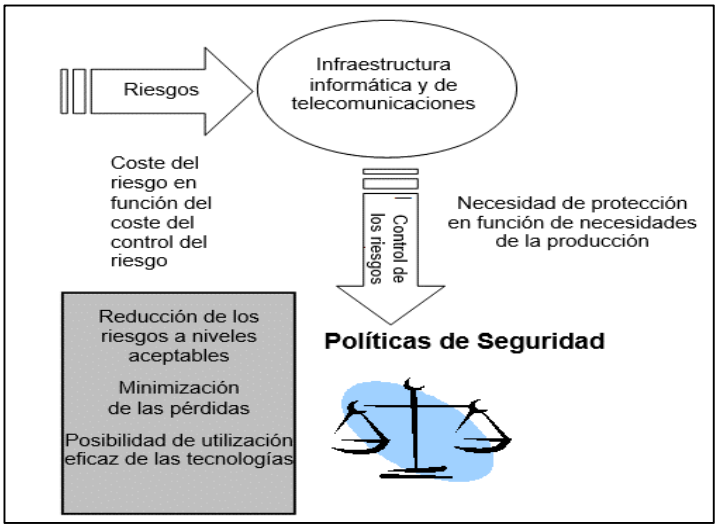
Por medio de un análisis de riesgo se puede reconocer el impacto que tiene un fallo en la seguridad y la probabilidad que ocurra. La inversión en seguridad tiene que ser proporcional al riesgo, esto es, se debe evaluar primero la información que se desea proteger para, de acuerdo a la situación, proceder a realizar la inversión en seguridad.

El análisis y evaluación de riesgos, la verificación de la existencia de controles de seguridad existentes, las pruebas con software y el monitoreo de los sistemas de información, permiten establecer el estado actual de la organización, [17] identificando posible causas de vulnerabilidades, proponiendo a la vez soluciones de control que permitan su mitigación.

Con la evolución de los SI y la forma actual de hacer negocio de las corporaciones, la información se ha convertido en uno de los activos de mayor valor para las organizaciones. Por ende, la información debe ser manejada y protegida adecuadamente de los riesgos o amenazas a la que pudiera estar expuesta.

El compromiso entre el costo del riesgo y el de su reducción permite determinar el nivel de protección y las medidas de seguridad a aplicar. [18] Es necesario identificar los valores que han de protegerse con las respectivas razones, ello en función de las limitaciones efectivas y de los medios organizativos, financieros, humanos y técnicos disponibles. Estas medidas deben ser eficaces e inscribirse

en una lógica de optimización y rentabilidad, en la figura 2.2 podemos apreciar como todo se enfoca en crear una política de seguridad en base a los riesgos.



[19] Figura 2.2 Compromisos de la identificación de Riesgos

En conclusión, para toda organización es fundamental identificar potenciales riesgos para poder aplicar una política de seguridad eficaz que permita afrontar situaciones de sumo riesgo vinculados a la informática, las telecomunicaciones y el ciberespacio.

2.2 Identificación de las amenazas

Una vez identificados los riesgos y los recursos a proteger, es hora de identificar las amenazas en la red que puedan converger en un problema de seguridad. Es importante que antes que analizar las amenazas se examinen los posibles atacantes que pueden violentar la seguridad. [20] No se debe pensar que las amenazas pueden ser siempre externas, ya que también existe la posibilidad que los ataques provengan desde adentro de la organización. Por ello se debe tener un modelo de seguridad que proteja los ataques internos como externos.

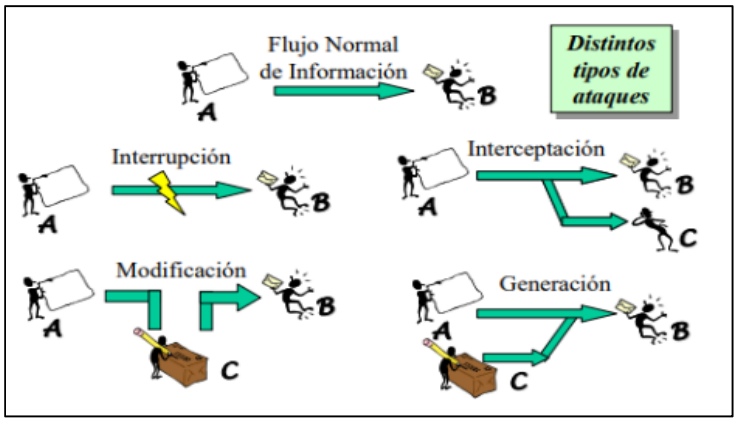
Para una organización es importante definir el nivel de seguridad que se desea tener, llevando a cabo un análisis costo/beneficio, debido a que el nivel de seguridad es proporcional a la importancia de la información, Por ejemplo, un banco maneja un nivel de seguridad muy alto por las transacciones económicas

que realiza, mientras una empresa catalogada como PYME que no realice transacciones similares puede que maneje un nivel de seguridad bajo.

Tras identificar todos los recursos a proteger, así como posibles vulnerabilidades y amenazas, más los potenciales atacantes que pueden intentar violentar la seguridad de red, se ha de estudiar cómo proteger los sistemas, sin ofrecer aún implementaciones concretas para protegerlos, pasando de ser políticas a mecanismos. [21] Esto implica cuantificar los daños que cada potencial vulnerabilidad puede provocar considerando las posibilidades de que una amenaza se pueda convertir en realidad. Este cálculo puede realizarse partiendo de hechos sucedidos con anterioridad en la organización. Por desgracia, suelen no registrarse estos eventos para evitar mala propaganda, solo por citar un ejemplo.

Antes de revisar los principales ataques a la red de una organización es importante que se clasifiquen los tipos de ataques:

- Activos: Son aquellos que producen cambios en la información (suplantación de identidad, replicación, modificación de mensajes, degradación fraudulenta del servicio).
- Pasivos: Registran el uso de los recursos y/o acceden a la información del sistema. Son difíciles de detectar, aunque es posible evitarlos mediante técnicas, como la encriptación de la información.



[21] Figura 2.3 Distintos tipos de ataque

En la figura 2.3 podemos apreciar los tipos más comunes de ataques y si bien en la actualidad aparecen cada vez más nuevos y complejos tipos de amenazas, es necesario que los usuarios y las organizaciones enfoquen su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos. Por otro lado, los incidentes de seguridad impactan en forma cada vez más directa sobre las personas. Esto hace que se requieran efectivas acciones de concienciación, capacitación y difusión de mejores prácticas. La solución inmediata en cada caso es mantenerse informado sobre todos los tipos de ataques existentes y las actualizaciones que permanentemente lanzan las empresas desarrolladoras de software, principalmente de SO.

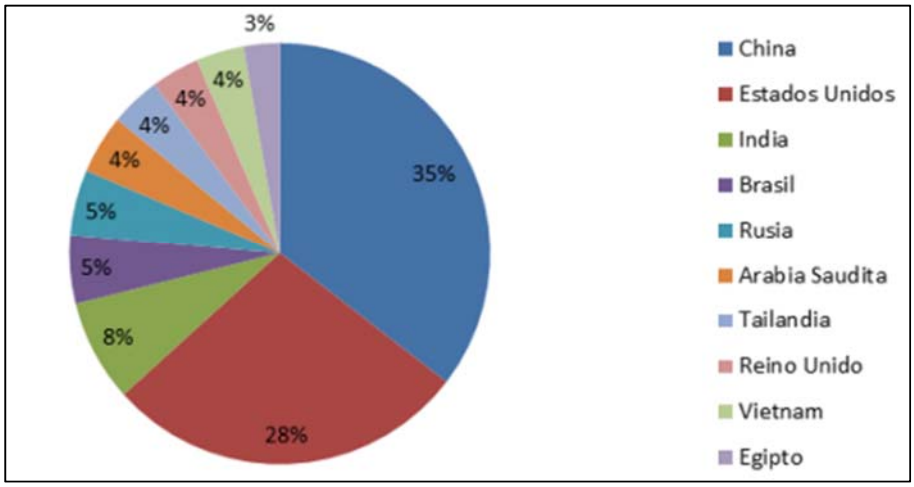
2.2.1 Ataques de Inundación

En seguridad informática, un ataque de inundación o ataque DoS se realiza mediante la saturación del destino con múltiples flujo de información, provocando la caída del servidor dado el gran número de solicitudes que no pueden ser atendidas.

Los ataques de inundación son muy comunes. Muchas páginas electrónicas han sufrido bajas temporales por ataques relacionados al protocolo TCP. Este ataque era hasta hace poco muy efectivo. [22] En la actualidad existen mecanismos preinstalados en los ruteadores y firewalls para filtrar direcciones IP inválidas con el fin de prevenir ataques de inundación SYN. Aunque aún se pueden encontrar sistemas vulnerables, estos ataques seguirán ocurriendo. Ante ello, es recomendable que se tenga una política de seguridad para evitarlos, así como también se deben contar con mecanismos de respuesta en caso que el ataque fuera exitoso. [20] La principal función de los ataques de inundación es la interrupción de los servicios, provocando que la red experimente retardos en las respuestas, ya que consumen el ancho de banda, generando un cuello de botella entre el atacante y la víctima.

Prolexic, empresa conocida por sus servicios de mitigación de ataques DoS, dio a conocer un informe en donde se indica que en el tercer

trimestre de 2016 los ataques distribuidos de denegación de servicios (DDoS) aumentaron un 88%. Por otro lado, la magnitud de algunos de estos aumentó considerablemente. [24] Por ejemplo, siete tuvieron una tasa de bits promedio de más de 20 Gbps. A nivel general, hubo un incremento del 230% en la cantidad de ancho de banda que consumen estos ataques en comparación con el tercer trimestre de 2015. En cuanto a los países en donde se originan los casos de DDoS, China lidera la lista, seguido de los Estados Unidos, la India y Brasil, en la figura 2.4 podemos apreciar el porcentaje de ataque de DoS según los países.



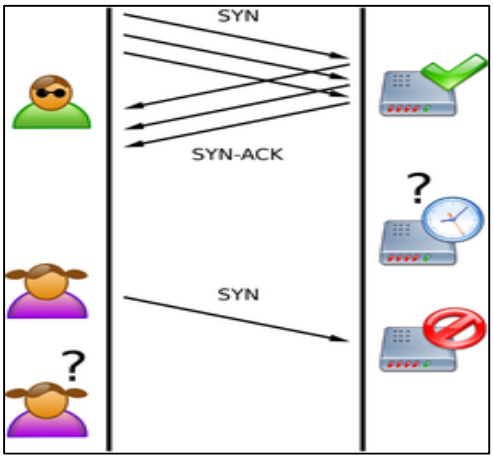
[22] Figura 2.4 Orígenes de ataques DoS

2.2.2 Principales Ataques mediante Negacion de Servicio (DoS)

Como se mencionó en el capítulo anterior, un ataque de DoS es un ataque de negación de servicio en donde se ataca al servidor desde múltiples ordenadores con la finalidad de saturarlo y detener su funcionamiento. A continuación se mencionan los principales ataques de DoS.

Ataque Smurf: Basado en el uso de varios servidores de difusión con el fin de paralizar la red. Se lleva a cabo enviando una solicitud de conectividad (ping) a uno o más servidores de difusión mientras se falsifican las IP de origen, haciendo que todas las respuestas del ping enviado se enruten hacia el destino.

Ataque de Inundación TCP – SYN: Consiste en saturar la red tomando ventaja del mecanismo de respuesta de tres vías del protocolo TCP. La inundación SYN envía un flujo de paquetes TCP/SYN a través de una dirección IP no válida al servidor tratando de establecer conexión. [24] El servidor, al tratar de responder las múltiples solicitudes de una dirección no válida y al no recibir respuesta tipo ACK, lo mantendrá en un estado de espera, generando un consumo de recursos dadas las muchas solicitudes de SYN en espera de un ACK haciendo que se limiten la cantidad de conexiones y reduciendo la capacidad del servidor para responder peticiones legítimas, en la figura 2.5 podemos ver un ejemplo de ataque de SYN.



[23] Figura 2.5 Ataque de Inundación SYN

Ataque Teardrop: También llamados ataques por fragmentación, consisten en la fragmentación de grandes paquetes del protocolo IP en paquetes más pequeños agregando en cada secuencia, vacíos o paquetes falsos que al momento del resemblado generan una sobrecarga desestabilizando el sistema.

Ataque Peer- to-peer: Producidos al aprovechar errores en los servidores peer to peer. Estas redes comparten información sin necesidad de un servidor central, esto es, actúan simultáneamente como cliente y servidor en relación a los demás nodos de la red. El atacante aprovecha la

compartición de archivos y crea nodos maliciosos introduciendo algún malware o un troyano a la red.

Ataque Nuke: Consiste en enviar paquetes ICMP inválidos a través de una alteración a la conectividad por medio del envió de datos adulterados constantemente, provocando lentitud en la navegación a la víctima.

2.3 Seguridad Lógica

La Seguridad Lógica consiste en la seguridad en el empleo de software y la aplicación de las políticas de seguridad que protejan los datos ya que solo deben tener acceso las personas autorizadas hacerlo.

[26] En un nivel básico la seguridad lógica se limita a activar las contraseñas. Se deben definir usuarios en la organización y obligar el uso de contraseñas de complejidad mínima, usar políticas de seguridad que permiten establecer permisos y ejecutar las auditorias con el fin de mejorar la seguridad lógica en los sistemas.

[27] En una organización se deben desarrollar procedimientos para asignación de privilegios e incluir una solicitud de concesión de permisos y de revocación para que quede constancia de quien y cuando se le han concedido. Se recomienda auditar de forma periódica los privilegios concedidos para comprobar que continúan siendo efectivos.

En conclusión la principal función de la seguridad lógica es implementar métodos que mitiguen los riesgos que puede haber en una red organizacional o personal con respecto al robo de información confidencial o en ataques malintencionados.

2.3.1 Vulnerabilidades, Riesgo y Seguridad

La palabra vulnerabilidad en seguridades hace referencia a una debilidad en la red o a un punto de fallo. Un sistema nunca será completamente seguro, pero la aplicación de una buena política de seguridad minimiza un posible robo de información o un ataque.

Durante los primeros meses de 2015, España vivió una época de crisis financiera, ocasionando numerosos despidos laborales. [28] La situación

produjo un aumento en los casos de robos de información confidencial por parte de los empleados despedidos, poniendo en evidencia la falta de seguridad informática. Las vulnerabilidades de un sistema son una puerta abierta para posibles ataques, de ahí que sea tan importante tenerlas en cuenta

Como ejemplo sencillo para entender lo que es una vulnerabilidad, se puede observar el caso en que en un hogar tengan una PC o laptop conectada a la Internet, donde se tienen grabadas todas las contraseñas de acceso a correo electrónico, redes sociales, cuentas bancarias, archivos compartidos, entre otros, y cuenta con protección de un antivirus ya caducado. [29] Ese dispositivo es vulnerable a nuevas versiones de virus. Si bien es cierto hay una vulnerabilidad en los dispositivos mencionados, pero no por esto se puede predecir un fallo, aprovechando este punto débil para robar información delicada.

En la figura 2.6 se propone una metodología básica para el escaneo de vulnerabilidades en la red, la cual la vamos a centrar en tres fases importantes:

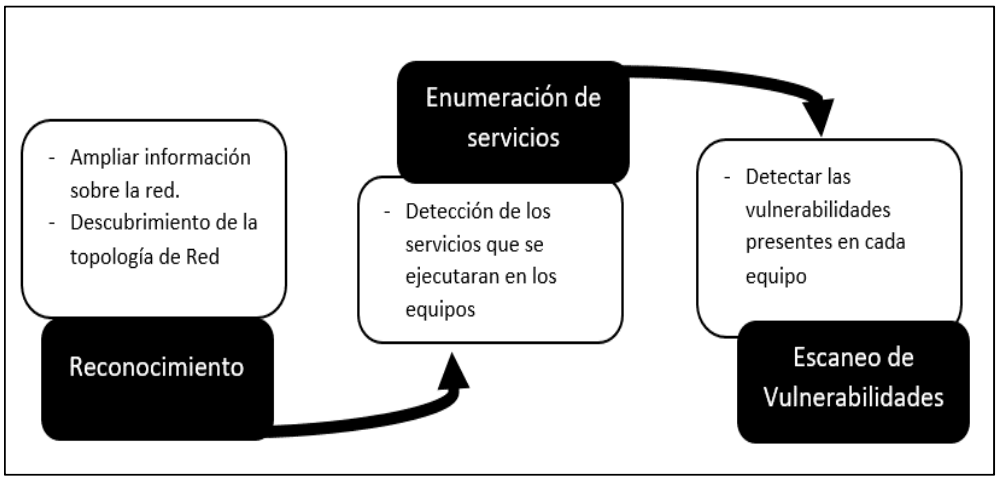


Figura 2.6 Vulnerabilidades en la Red

Estas tres fases se puntualizan acciones que deben realizarse y como deben llevarse a cabo con el uso de herramientas apropiadas. Se puede definir un riesgo como la probabilidad de que se produzca un ataque,

cualquier organización está expuesta a una serie de riesgos sean estos externo o internos, al analizar un riesgo estamos elaborando un instrumento provechoso para calificar el riesgo y examinar si este estudio es el adecuado, además de elaborar una relación costo / beneficio de un plan efectivo para la seguridad de una organización. [30] Cualquier estudio sobre el riesgo de la seguridad de una organización debe indicar:

- El nivel actual del riesgo
- Las consecuencias del riesgo
- Qué medidas tomar si el riesgo es muy alto

[28] La evaluación de riesgos identifica amenazas y riesgos de la información, sobre la plataforma tecnológica de una organización, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo criterios de confidencialidad, integridad y disponibilidad de la información.

Como evaluación y prevención de riesgos se debe:

- Obtener una valoración económica del impacto sobre los sucesos. Este valor se podrá utilizar para sacar la relación costo de la protección de la información, sobre el costo de que vuelva a ocurrir.
- Considerar la posibilidad de que sucedan cada uno de los posibles sucesos, priorizando los problemas para tomar un plan de acción adecuado que minimice el riesgo.
- Conocer con exactitud qué es lo que se desea proteger y cuanto se está invirtiendo para proteger la información. Para ello se deberá identificar los recursos con que se cuenta y los posibles riesgos a los que será expuesto.

En la Tabla 2.1 se muestra los tipos de riesgos como se los clasifica según su factor:

Tipo de Riesgo	Factor
Robo de Hardware	Alto
Robo de Información	Alto
Vandalismo	Medio
Fallas en los equipos	Medio
Virus Informáticos	Medio
Equivocaciones	Medio
Accesos no autorizados	Medio
Fraude	Bajo
Fuego	Muy Bajo
Terremoto	Muy Bajo

Tabla 2.1 Clasificación de Riesgos

2.3.2 Distinción entre Amenaza, Vulnerabilidad y Riesgo

En la actualidad, las organizaciones presentan múltiples amenazas en la seguridad de la información que van cambiando paulatinamente. Muchas de ellas son preexistentes y otras aparecen a partir de los nuevos avances. La seguridad no es algo se puede hablar en términos absolutos y tampoco se puede cuantificar. Decir que un sistema es totalmente seguro es falso. Lo que sí se puede hacer es proteger un sistema identificando las amenazas con una prueba de concepto cuantificando las vulnerabilidades y sus potenciales riesgos.

Para poner el asunto en un contexto más simple: La amenaza es el daño potencial que puede llegar a un activo (lo que está tratando de proteger). [29] El riesgo es la probabilidad de que el daño se realice. Vulnerabilidad hace referencia a la debilidad por la cual el daño puede llegar al activo.

Lo más importante al momento de diferenciar estos términos es saber quién puede provocar más incidencia en un sistema. Una forma sencilla de entender estos conceptos es atreves de la siguiente ecuación (2.1):

Amenaza + Vulnerabilidad = Riesgo Activo (*2.1*)

El riesgo de un sistema se calcula en función de las amenazas y las vulnerabilidades. Si existen amenazas y no hay vulnerabilidades, entonces existe poco riesgo. Por otra parte, si existe una vulnerabilidad y no hay amenazas se tiene ninguno o poco riesgo. Esto quiere decir que el factor más importante que debemos calcular es el riesgo.

Un aspecto muy importante que se debe considerar es la mitigación de los riesgos informáticos, que es un proceso que comprende la identificación de activos informáticos, [17] sus vulnerabilidades y amenazas a los que están expuestos, incluyendo su probabilidad de ocurrencia y el impacto de las mismas para determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

2.4 Ataques Relacionados con la capas del Protocolo de Control del Transmisión/Protocolo de Internet del protocolo (TCP/IP)

El protocolo TCP/IP apareció en los años 1960 como un sistema de comunicaciones basado en conmutación de paquetes elaborado por el gobierno estadounidense y su departamento de Defensa Nacional. [14] Con el paso del tiempo se convirtió en el estándar de comunicaciones de redes de computadores, ya que es el único protocolo de enlace y transporte de la Internet. TCP/IP fue creado en una época en donde la seguridad era algo no gravitante, por tal motivo tenía vulnerabilidades en su infraestructura.

Con el paso de los años se han ido desarrollando nuevos ataques cada vez más sofisticados para explotar vulnerabilidades, tanto en el diseño de las redes TCP/IP como en la configuración, operación y mantenimiento de los sistemas informáticos que conforman las redes conectadas a la Internet. [30] Estos nuevos métodos de ataque se han ido automatizando, por lo que en muchos casos solo se necesita un conocimiento técnico básico para realizarlos. Cualquier usuario con una conexión a la Internet tiene acceso hoy en día a

numerosas aplicaciones para realizar estos ataques y las instrucciones necesarias para ejecutarlos se encuentran fácilmente en tutoriales disponibles en la web.

[22] Cada capa del protocolo TCP/IP tiene una función independiente, pero a su vez es dependiente de la capa anterior, esto es, cada capa recibe servicios de su capa inferior y cada capa proporciona ciertos servicios a la capa superior.

El protocolo TCP/IP se divide en cuatro capas. Cada una tiene sus vulnerabilidades las cuales se presentan a continuación:

1. Capa de Red. Con vulnerabilidades ligadas a cómo se realiza la conexión. Esta capa tiene problemas en el control de acceso y la confidencialidad.
2. Capa de Internet. En esta capa se puede realizar cualquier ataque a través de la IP de la víctima, como sniffing, modificación de datos, pérdida de paquetes. En esta capa la autenticación se realiza a través de la dirección IP. Si un sistema suplanta una dirección IP errónea, el receptor no detecta esta suplantación o si a su vez se manipulan los paquetes el receptor tampoco sería capaz de detectarlo.
3. Capa de Transporte. En esta capa se envía información TCP/UDP sobre el protocolo IP. Esta capa es muy vulnerable, debido a que presenta problema de autenticación, confidencialidad. Un tipo de ataque conocido en esta capa es el DoS, o si un usuario con malas intenciones puede ponerse a capturar paquetes e interceptar una conexión en marcha con el fin de poder secuestrar una sesión.

   En cuanto a los mecanismos de seguridad incorporados en el diseño del protocolo de TCP (como las negociaciones involucradas en el establecimiento de una sesión TCP), existe una serie de ataques que aprovechan ciertas deficiencias en su diseño. [23] Una de las vulnerabilidades más graves contra estos mecanismos de control puede comportar la posibilidad de interceptación de sesiones TCP establecidas, con el objetivo de secuestrarlas y dirigirlas a otros equipos con fines deshonestos.

4. Capa de Aplicación. Esta capa presenta vulnerabilidades y deficiencia en la seguridad asociada a sus protocolos. En esta capa se maneja un gran número de protocolos. Una vulnerabilidad en esta capa se presenta al realizar una solicitud de una dirección IP de una página web al servidor DNS. [30] Ésta es una base de datos accesible desde la Internet, lo cual puede ser aprovechado por un atacante al modificar la información que suministra el servidor DNS y acceder a información almacenada en la base de datos como la topología de la red, las direcciones IP de cada una de las maquinas.

CAPÍTULO 3

PROPUESTA PARA UNA INFRAESTRUCTURA DE SEGURIDAD

Este capítulo plantearemos una propuesta para una infraestructura de seguridad junto con su arquitectura y diagnóstico, adicional se evaluara los planes del gobierno para prevenir los ciberataques y la ciberseguridad.

3.1 Política de Seguridad Informática (PSI)

En la época actual no es probable decir que un sistema es totalmente seguro a nivel informático, debido a que los costos para establecer seguridad total son demasiado altos. Es imposible determinar cómo y cuánto un hacker quiere invertir recursos en equipos y logística para tratar de descifrar una encriptación. El tratar de evitarlo podría gastar demandar muchos aspectos, de índole financiero. La solución a medias seria acotar todo el espectro de seguridad en lo que respecta a plataformas, procedimientos y estrategias de esta manera se puede controlar un conjunto de vulnerabilidades, aunque esto puede en cierta instancia que no se logre la seguridad total.

La Política de Seguridad Informática (PSI) puede definirse como las leyes, reglas y normativas que regulan de manera directa los recursos de una organización, definiendo lo que está prohibido y lo que está permitido.

Las PSI son parte de una táctica en la que se fijan reglas, consejos, estándares y leyes que una organización utiliza para la implementación de medidas de seguridad informática para asegurar los diferentes bienes de la organización. [31] Este esfuerzo se orienta a implementar un nivel apropiado de seguridad informática, de tal manera que cualquier tipo de información sea empleada de manera conveniente.

Entre los muchos beneficios que se generan al implementar de manera adecuada las PSI son:

1. Ejecución de medidas para la protección y mejor funcionamiento de la organización.
2. Capacitación y concienciación del personal acerca de las PSI.
3. Previsión de la pérdida de información.
4. Uso apropiado y eficiente de los recursos informáticos.
5. Permitir el disponer de procedimientos para posibles conflictos en la organización.
6. Permitir auditorías y dominio de la información.
7. Mejor gestión y asignación de equipos al personal según sus necesidades.

3.2 Arquitectura de Seguridad

Uno de los principales requisitos que debe tener una organización o Pymes en la actualidad es la gestión de la seguridad de los sistemas de información. Para observar todas estas necesidades se han desarrollado estándares y políticas que facilitan una buena práctica de gestión de la seguridad.

Para elaborar una arquitectura de seguridad en una organización, se debe primero evaluar los siguientes aspectos en la seguridad de la información:

Ataques a la seguridad: Referente a las maniobras que se deben hacer en caso de comprometer la seguridad de la información que pertenece a una organización.

Mecanismos de seguridad: Referente a las acciones a elaborar para detectar, prevenir, mitigar un ataque a la seguridad de la información de la organización.

Servicios de seguridad: Referente a los servicios a ofrecer al usuario respecto al intercambio de información en una red de datos.

Desde otra perspectiva, se pueden definir una serie de pasos a la hora de implementar una arquitectura de seguridad en redes de datos:

1. En primer lugar hay que definir una serie de objetivos o requisitos de seguridad que se desea que cumpla la información que se distribuye en redes de datos en función de los posibles o potenciales ataques a la seguridad, esto

es, hay que definir una política de seguridad. [31] Estos objetivos o requisitos de seguridad se van a articular en forma de servicios de seguridad que se van a ofrecer al usuario.

2. Una vez especificados los requisitos de seguridad para la información, habría que implementar los mecanismos necesarios para garantizar esos requisitos. La implementación de estos mecanismos puede ser algo complejo, dependiendo de la tecnología de la red a considerar. [32] Hay que considerar los mecanismos de seguridad que se van a implementar utilizando el protocolo de comunicaciones propio de la red de datos, lo que implica que deben haber ciertas garantías respecto a este protocolo (por ejemplo, respecto a temporizaciones, retransmisiones). Al momento de implementar un mecanismo de seguridad es importante considerar también las posibles contrapartidas o costos que puede conllevar en las comunicaciones.
3. Una vez decididos los mecanismos de seguridad a implementar se deben determinar donde situarlos. [32] Este aspecto tiene dos implicaciones: por un lado hay que determinar en qué lugar físico de la red se deben localizar estos mecanismos; y por otro lado, en qué lugar de la arquitectura de comunicaciones situar estos mecanismos.

3.3 Evaluación y diagnóstico de seguridad

La mayoría de las organizaciones se enfrentan a distintas amenazas que muchas veces exploran sus vulnerabilidades. El riesgo de ser vulnerado un sistema está siempre latente, dado estos precedentes las organizaciones si desean seguir operando deben tener un modelo de prevención de seguridad que permita tener identificados sus activos vitales de información, resguardados en caso de ser vulnerados.

Para una evaluación y diagnóstico de seguridad no se debe tratar de ver en qué casos se aplica o no un método de seguridad, sino tratar de diferenciar los espacios en que se realizan. Es necesario que para una evaluación de seguridad se establezca un *checklist*. Esto no se debe tomar como un sustituto en el análisis de riesgo, sino como un punto de inicio en la revisión antes de tomar medidas correctivas contra la amenaza.

El proceso de auditoría se debe realizar periódicamente, llevándose a cabo después que se ha realizado un análisis de riesgos, con el fin de verificar si se están cumpliendo los controles y políticas de seguridad previstos anteriormente.

Si el sistema a evaluar y diagnosticar es muy complejo, es mejor para el analista de seguridad elaborar una evaluación por subsistemas. Esto facilitará la presentación y comprensión de informes por parte de la gerencia. Los siguientes ítems corresponden la parte preliminar de la Evaluación y Diagnostico de la Seguridad:

a) *La dirección del análisis*: con el objeto de influenciar el estilo de análisis y la información de salida del proceso de valoración del riesgo. [33] Se identifica el proceso de valoración del riesgo, tipo de salida requerida y necesidades críticas.

b) *El alcance*: para determinar cuáles recursos el sistema requiere o no con respecto al análisis de riesgos, o cuáles agentes de amenazas no serán considerados, entre otros.

c) Los límites: se define en términos de límites físicos y lógicos. El límite físico indica donde termina y donde comienza el sistema. [33] Establece características de todas las interfaces con otros sistemas. El límite lógico en cambio define la amplitud y profundidad del análisis.

d) Descripción del sistema: requerimientos (o misión) del sistema, concepto de operación e identificación de la naturaleza de los recursos del sistema. Está descripción provee las bases para posteriores análisis y es prerrequisito para iniciar la valoración de riesgos.

e) Objeto del riesgo y certeza requerida: el objeto ayudará a determinar si el riesgo está en los límites aceptables. [34] La certeza define el nivel de acierto para la valoración del riesgo. Este factor determina el nivel de esfuerzo en el análisis.

3.4 Ecuador en el ciberespacio

Aunque Internet no es sinónimo de ciberespacio, es un buen indicador para posicionar al país dentro del quinto dominio. Sin embargo, la real medida de la

presencia de un Estado en el ciberespacio está directamente relacionada con su desempeño, a través de tres indicadores:

a. Conectividad
b. Desarrollo de TCP/IP
c. Manejo del DNS

3.4.1 Conectividad

La República del Ecuador traslada el 90% de su tráfico internacional mediante dos cables de fibra óptica: el submarino Panamericano o Pan-Am y el submarino Emergia o Sam-1. En ambos casos, Ecuador solicitó la entrega de una determinada capacidad internacional con acceso Internet, para uso de desarrollo social y educativo en la estación terminal de cable submarino a ser administrada por el FODETEL. [34] Esta capacidad correspondió al 1% y 2%, respectivamente. En marzo de 2015 debió entrar en operaciones un tercer cable, el Pacific Caribbean Cable Systems, que le permitiría al país tener un ancho de banda de hasta 100 Gbps.

[35] En el territorio continental existen 20000 km de fibra óptica troncal (red central de distribución) y 15000 km adicionales en última milla (conexión directa con el cliente). Este recurso llega al 67% del territorio nacional. El número de hogares conectados a Internet de banda ancha en el 2014 fue de 891000 habitantes (7.7%) y el porcentaje conectado a Internet de alta velocidad fue de 0.89%.

Estas cifras, aunque magras en el contexto internacional, indican a todas luces la agresiva expansión del país para cerrar la brecha digital con los países desarrollados y por ende mejorar su interconexión con el ciberespacio.

3.4.2 Desarrollo del Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP)

El TCP/IP es el protocolo de aceptación universal para la transmisión de datos en Internet que proporciona una transmisión fiable de paquetes de

datos sobre internet. Esta base sirve para enlazar computadoras con diferentes sistemas operativos.

A pesar de que muchos proveedores de servicios de Internet (ISP, por sus siglas en inglés) locales ya están preparados o preparándose para desplegar IPv6 y de que varias instituciones gubernamentales y académicas ya funcionan con ambos protocolos, la mayoría de usuarios aún se conectan a Internet dentro de sub-redes administradas por los proveedores de servicio, mediante soluciones tipo parche como los mecanismos NAT y CIDR. Para proveer de una solución definitiva a este problema se creó la versión seis del protocolo de Internet (IPv6), que cuenta con un número virtualmente infinito de identificadores, lo que permitiría contar una vez más con una red simétrica que restablece el principio de extremo a extremo. Sin embargo, este nuevo protocolo no es compatible con el antiguo, lo que ocasiona que ambos protocolos deban coexistir hasta que se elimine por completo el IPv4.

El avance de la migración a IPv6 comprende aspectos de política pública, economía, operativos y, aún más importante, personal de ingeniería que requieren del compromiso y cooperación de todos los sectores involucrados, entre ellos las instituciones de gobierno, industria y academia.[36] Frente a esto, el MINTEL, impulsó la incorporación de IPv6 como requisito en compras públicas de productos y servicios de TIC y estableció lineamientos generales para la implementación y creación del Plan Maestro de Transición de IPv4 a IPv6.

3.4.3 El avance del Sistema de Nombres de Dominio (DNS)

[37] El sistema para nombres de dominio es el responsable del enrutamiento de una página web desde una dirección conocida fácilmente legible hacia una dirección IP. El sistema utiliza servidores raíz dominios de primer nivel y servidores DNS.

Este sistema está estandarizado a nivel internacional. Una clase específica de dominio es el de nivel superior geográfico (ccTLD por sus siglas en inglés), el cual es utilizado y reservado para un país específicamente.

[37]En el caso de Ecuador el ccTLD asignado es ".ec" cuya administración fue concedida por la Autoridad de Asignación de Números de Internet (IANA por sus siglas en inglés) a inicios de la década de 1990 a Intercom-Ecuanex, el primer ISP del Ecuador, ahora desaparecido. Sin embargo, por su limitada capacidad técnica y porque no disponía de un enlace dedicado a Internet, esa administración fue asumida de facto por EcuaNet-Corporación Ecuatoriana de Información, en ese entonces del Banco del Pacífico. Luego de la crisis bancaria de finales de los años 1990, el ".ec" pasó a manos del Estado y desde entonces es el administrador.

Es posible que exista la intención de nacionalizar el manejo del sistema de dominios, considerando que la Constitución del 2008 designa a las telecomunicaciones como sector estratégico. Este no se trataría de un caso aislado, dado que ya se han producido casos de disputa similares en otros países. El análisis establece que el país está avanzando a configurar las condiciones para facilitar el acceso del Ecuador al ciberespacio.

3.4.4 Causas del incremento de la participación de Ecuador en el ciberespacio.

El crecimiento del país en el ciberespacio se debe a una decidida intención del Gobierno Nacional en impulsar la tecnología digital, encauzada en tres pilares fundamentales:

a. Plan Nacional de Banda Ancha: Infraestructura y conectividad.
b. Plan Nacional de Alistamiento Digital: Capacitación y entrenamiento.
c. Plan Nacional de Gobierno Electrónico: El más importante para el caso de estudio, ya que organiza las TIC de la manera más conveniente para mejorar la forma de relacionarse de los cuatro actores principales (Gobierno, ciudadanos y ciudadanas,[38] el sector productivo y los servidores públicos), eliminando de esta forma las barreras de comunicación y fortaleciendo las relaciones y alianzas con los actores de una sociedad cada vez más interconectada y globalizada

3.5 Plan Nacional de Gobierno Electrónico

La Organización de las Naciones Unidas, ONU, define al Gobierno electrónico como:

[38] “El uso de las Tecnologías de Información y Comunicación (TIC) por parte de las instituciones de gobierno para: mejorar cualitativamente los servicios e información que se ofrecen a las ciudadanas y ciudadanos, aumentar la eficiencia y eficacia de la gestión pública, así como para incrementar sustantivamente la transparencia del sector público y la participación ciudadana”

El Gobierno Electrónico en un sentido más amplio busca:

- El uso y despliegue de las TIC siguiendo determinadas pautas, normas, experiencias y buenas prácticas.
- Proveer la oportunidad de plantear una nueva forma de hacer gobierno.
- Orquestar y gestionar de forma coherente personas, tecnologías, normas, servicios, sistemas y procesos propios del campo de dominio del Gobierno Electrónico, como de otros campos que sea necesario considerar.

Estas ideas sitúan a las TIC como un elemento de apoyo para el desarrollo de un buen gobierno, ya que a través de su uso adecuado se busca alcanzar mayores niveles de eficiencia y eficacia en el quehacer gubernamental, mejorando los procesos y procedimientos del gobierno, aumentando la calidad de los servicios públicos, incorporando más y mejor información en los procesos decisorios y facilitando la coordinación entre las diferentes instancias de gobierno.

El Gobierno Electrónico no es un fin en sí mismo. Tiene un carácter instrumental que requiere la revisión, rediseño y optimización de los procesos como paso previo a la introducción de cualquier cambio en la tecnología o en las funciones de producción de las organizaciones públicas.

3.5.1 Modelos de relacionamiento de actores en el Gobierno Electrónico

El Plan de Gobierno Electrónico tiene el siguiente modelo de relacionamiento:

G2C: Gobierno para el Ciudadano.

Son iniciativas de Gobierno Electrónico encaminadas a brindar servicios públicos e información a los ciudadanos a través de las TIC, con el fin de que puedan interactuar con el Gobierno a través de cualquier medio que le provea acceso, en cualquier lugar y a toda hora.

Los beneficios que busca este modelo son principalmente ahorros de tiempo y dinero, ya que se deja de lado la necesidad de desplazarse a las oficinas públicas, donde generalmente debe esperar un tiempo considerable, para recibir un servicio público o recibir información.

G2G: Gobierno para el Gobierno.

Son las interacciones complementarias e interdependientes entre las distintas instituciones del sector público para fomentar eficiencia en la gestión. [37] Entre los principales beneficios está el evitar la duplicidad de procedimientos y agilitar los trámites entre instituciones públicas. Asimismo implica el relacionamiento con otros gobiernos para desarrollar estrategias comunes que apalanquen la madurez de Gobierno Electrónico.

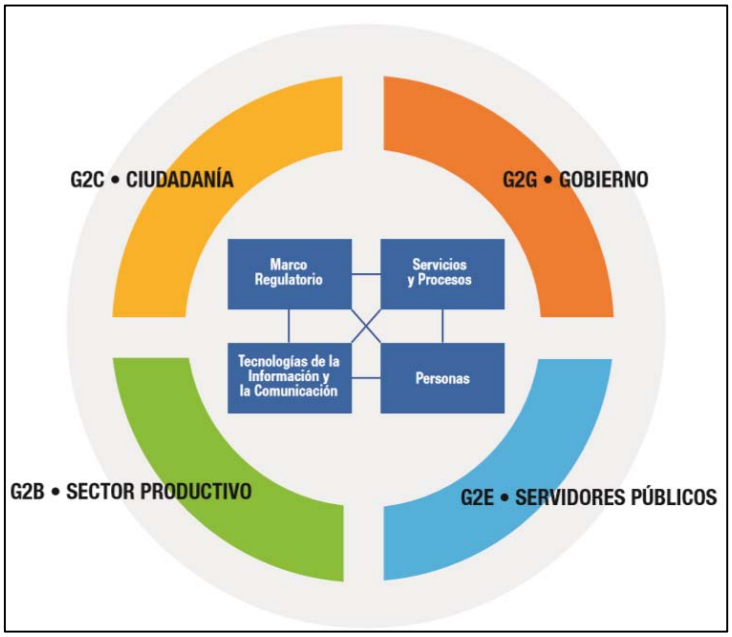
G2B: Gobierno para el Sector Productivo (Business).

Este modelo es el medio de interacción entre el gobierno y el sector productivo, con la finalidad de facilitar a este último el acceso a incentivos, productos y servicios públicos. El principal beneficio es la reducción de costos de producción, incremento de la competitividad y la consolidación de un entorno más seguro, ágil y eficiente para la actividad productiva. Adicionalmente el gobierno se beneficia de una mejor gestión tributaria.

G2E: Gobierno a Servidor Público (Empleado).

Es la gestión que desarrolla un gobierno para brindar servicios de desarrollo profesional y atención a las demandas de su talento humano. [39] El principal beneficio de este modelo de relación es que se cuenta con herramientas y mecanismos que permiten fortalecer las competencias de las servidoras y servidores públicos. En la figura 3.1 se muestra el despliegue del modelo de relacionamiento. La interrelación de las

Tecnologías de la Información y la Comunicación se relaciona con los cuatro sectores de interés del Gobierno Electrónico.



[40] Figura 3.1 Modelos de Relacionamiento del Plan Gobierno Electrónico

3.5.2 Evolución del Gobierno Electrónico

El Gobierno electrónico persigue metas en función de su grado de madurez, alcanzándolas en base a una interacción y sinergia que se basa en las tecnologías de la información y comunicaciones, en la figura 3.2 se muestras las etapas y su importancia.

Etapa emergente

En este nivel o etapa existe información básica del gobierno en línea, sobre política pública, gobernanza, legislación, reglamentación, documentación pertinente de trámites y servicios gubernamentales, así como enlaces a sitios web de otros ministerios, departamentos u otros poderes del Estado, con la finalidad de que los ciudadanos puedan obtener información en tiempo real de forma fácil.

Etapa avanzada

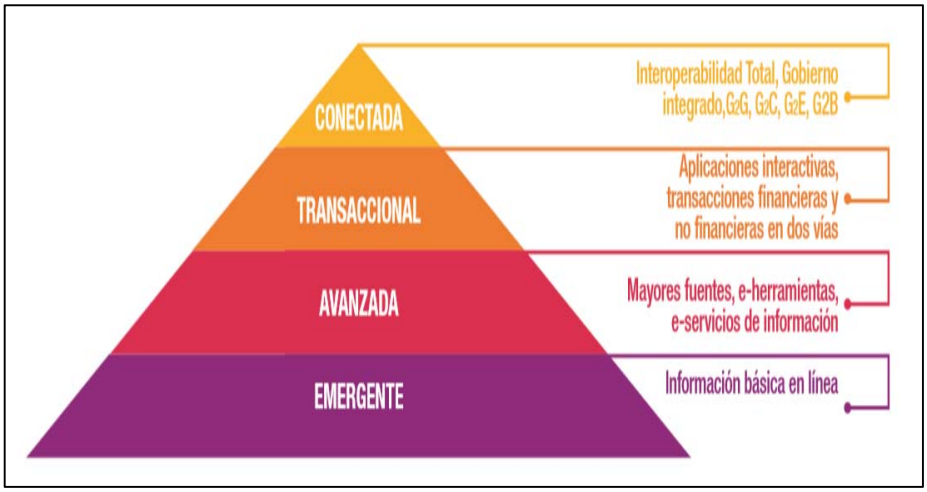
En esta etapa se incorporan mejoras a los servicios de información, facilitando la comunicación unidireccional o bidireccional simple entre el gobierno y el ciudadano, permitiendo la descarga de formularios para acceder a un servicio público; adicionalmente los sitios web presentan funciones multimedia, a la vez que son multilingües.

Etapa transaccional

En esta etapa existen servicios transaccionales en los sitios web gubernamentales, es decir, existe una comunicación bidireccional entre el ciudadano y el gobierno, abriendo un espacio de interacción para la construcción de políticas, programas, reglamentación gubernamental, etc. Para poder realizar esta interacción es necesario contar con la autenticación de la identidad del ciudadano. Se ha integrado la votación electrónica, descarga y carga de formularios, presentación de declaraciones de impuestos en línea, trámites en línea para solicitar certificados, licencias y permisos otorgados por las instituciones públicas o mejorar los sistemas financieros transaccionales del gobierno.

Etapa Conectada

En esta etapa existe la compra de servicios integrados a través de los sitios web gubernamentales. La interacción ciudadano-gobierno es más intensiva a través de distintos medios que tienen conectividad. Adicionalmente, los servicios y soluciones electrónicas traspasan los departamentos y ministerios de manera uniforme, permitiendo que los datos y el conocimiento se transfieran de los organismos gubernamentales a las demás instituciones de una manera integrada.



[40] Figura 3.2 Evolución del Plan Gobierno Electrónico

Las instituciones del Ecuador tienen un nivel heterogéneo de madurez. [39] Este Plan persigue alcanzar un desarrollo homogéneo llevándolas a un nivel conectado.

3.5.3 Análisis FODA: Identificando las potenciales amenazas

La visión del Plan de Gobierno Electrónico indica que: [40] “Para el año 2017 ser un referente regional de Gobierno Electrónico con las bases consolidadas de la etapa más alta de madurez: nivel conectado”.

Esta ambiciosa visión implica el uso de la tecnología como un medio para facilitar la interacción entre el gobierno, la ciudadanía, el sector productivo y los funcionarios públicos. Esta interacción generará nuevos espacios de participación y colaboración; incrementando los niveles de calidad, excelencia y transparencia en los servicios públicos. Sin embargo, esto también implica que el nivel de riesgo de que el país sufra de ataques cibernéticos sea extremadamente alto, tal como se observa en el análisis FODA que se presenta en Tabla 2.

El ambicioso Plan establecido por el Gobierno, identifica como amenaza a las potenciales vulnerabilidades cibernéticas que crecerán en forma exponencial en camino a llegar a un nivel de Gobierno Conectado.

Partiendo de este análisis se puede resaltar la importancia de entender que el Gobierno Electrónico constituye la gestión innovadora y dinámica en permanente construcción, que recopila la experiencia propia de cada país para perfeccionar su gestión dentro de su ámbito de acción, afirmando durante su desarrollo los objetivos iniciales e incorporando nuevos esquemas de servicio e innovación.

Cuanto más se extienda la dependencia a las Infraestructuras y tecnologías informáticas de un Estado, el nivel de vulnerabilidad se incrementará. [37] Un ciberataque a un país o nación en el nivel de Gobierno Conectado podría paralizarlo, lo cual puede producir cuantiosas pérdidas económicas y afectación a su soberanía.

3.5.4 Participación del Ministerio de Telecomunicaciones en Ciberseguridad

Tomando en cuenta que el Estado debe mantener las capacidades para minimizar el nivel de riesgo al que están expuestos sus ciudadanos ante amenazas o incidentes de naturaleza cibernética, es decir, proveer ciberseguridad, el MINTEL a través de la Agencia de Regulación y Control de las Telecomunicaciones crea el Centro de Respuestas a Incidentes Informáticos del Ecuador (EcuCERT), cuya misión es [41] “brindar a su comunidad objetivo el apoyo en la prevención y resolución de incidentes de seguridad informática, a través de la coordinación, capacitación y soporte técnico”.

MATRIZ FODA DIAGNÓSTICO Plan de Gobierno Electrónico		
	FORTALEZAS	**DEBILIDADES**
	Ampliación de coberturas de Internet y tendencia de uso creativo de las TIC. Diseño de normativas legales que respalden la gestión del Gobierno Electrónico.	Limitada oferta tecnológica de servicios en línea. Reglamentación escasa para la implementación de proyectos tecnológicos.
OPORTUNIDADES	**ESTRATEGIAS**	**ESTRATEGIAS**
Mayor acceso a los servicios públicos automatizados. Rápido desarrollo productivo e innovación tecnológica	Liderar los procesos de generación de nuevos espacios para las alianzas estratégicas público-privadas.	Efectuar proyectos para el desarrollo de sistemas y plataformas tecnológicas con la participación de las Universidades e Institutos de Investigación.
AMENAZAS	**ESTRATEGIAS**	**ESTRATEGIAS**
Costo elevado en la implementación de herramientas tecnológicas que faciliten el acceso a la información. Ataques cibernéticos a la Infraestructura Crítica del Estado	*Establecimiento de un sistema de Ciberseguridad y Ciberdefensa en la que participen de manera coordinada los sectores público y privado, con estructuras y financiamiento que permitan su continuo fortalecimiento en el tiempo.*	Actualización y adaptación del marco legal que permita la adecuada implementación del Sistema Nacional de Ciberseguridad y Ciberdefensa.

TABLA 3.1 Análisis FODA del Plan de Gobierno Electrónico

En la tabla 3.1 se muestra un análisis FODA del plan de gobierno electrónico, a continuación se listarán los propósitos del EcuCERT, los cuales son de interés para la organización de la ciberseguridad y ciberdefensa en el país:

a. Promocionar, difundir y asesorar en el cumplimiento de la Normativa de Seguridad de la Información de aplicación vigente en el Ecuador.
b. Promover la creación y adopción de Políticas de Seguridad de la información en las Instituciones del Estado Ecuatoriano y el sector de las telecomunicaciones.
c. Liderar actividades de capacitación, entrenamiento y sensibilización en la prevención de incidentes informáticos y en el buen uso de las tecnologías de la información y comunicación a las Instituciones del Estado Ecuatoriano, empresas del sector de las telecomunicaciones y ciudadanía en general.
d. Apoyar técnicamente a su Comunidad Objetivo en la rápida detección, identificación y gestión y recuperación de datos frente a incidentes de seguridad informática.
e. Proporcionar información técnica, especializada y confiable a las autoridades respectivas durante los procesos investigativos relacionados con incidentes de seguridad informática, de acuerdo a las políticas y procedimientos establecidos.
f. Mantener un laboratorio de análisis técnico enfocado a la identificación de actividades maliciosas, análisis forense, recuperación de datos y elaboración de informes técnicos. Liderar la creación y gestión de una red de sensores para la detección temprana de amenazas informáticas.
g. Apoyar a los organismos de seguridad e investigación del estado para la prevención e investigación de delitos que involucren tecnologías de la información y comunicación.
h. Establecer y mantener un vínculo fluido y una relación colaborativa con sus equivalentes en otros países, así como con organismos internacionales involucrados en ciberseguridad.

i. Ser el punto de contacto entre el Estado Ecuatoriano y otros equipos de respuesta internacionales en lo que se refiere a la gestión de incidentes de seguridad informática.
j. Promover la creación de equipos de respuesta a incidentes de seguridad informática (CSIRT, Computer Security Incident Response) sectoriales para la gestión de los incidentes de seguridad informática en las Infraestructuras Críticas nacionales, el sector privado y la sociedad civil.
k. Coordinar y asesorar a los CSIRT y entidades tanto del nivel público, como privado y de la sociedad civil para responder antes incidentes de seguridad informática.
l. Establecer una red de confianza nacional entre las organizaciones que formen parte de la Comunidad Objetivo, a través de lazos que fomenten una cultura de seguridad de la información.
m. Impulsar la conformación de un Comité de Ciberseguridad dentro del cual se desarrollará y promoverá guías de buenas prácticas y recomendaciones en seguridad de la información.

Los objetivos “k”, ”l” y “m” concurren a la consolidación de un CSIRT con la participación del sector público, privado y académico (ciberseguridad) y el sector defensa (ciberdefensa). Un ciberespacio seguro es esencial para la seguridad de la Nación.

CAPÍTULO 4

MODELO DE PREVENCIÓN

En este capítulo se elabora un modelo de seguridad orientado a PYMES para prevenir ciberataques. Se realizan pruebas de seguridad y test de penetración, enfocados a evaluar la factibilidad de un modelo para ciberseguridad costo/ beneficio.

4.1 Elaboración de un modelo empresarial para prevenir los ciberataques

La ciberseguridad es un asunto muy importante aún sin resolver para todas las empresas que manejan gran cantidad de información. Una muestra de esto ha sido el reciente ataque *ransomware* (WannaCry), por el cual sus creadores pudieron "secuestrar" alrededor de 360,000 equipos en 180 países, pidiendo posteriormente un rescate por ellos. La mayoría de organizaciones no están preparadas para prevenir un ciberataque. Uno de los principales motivos es la falta de una cultura de seguridad en las empresas. Afirmar que un sistema es 100% seguro es falso. Lo que si se puede hacer es poner el camino difícil para los atacantes.

De acuerdo con la telemetría de la empresa de seguridad Kaspersky Lab, durante el año 2016 más de 1.445.000 usuarios (incluidas empresas) de todo el mundo fueron víctimas de este tipo de malware. [42] De las 62 nuevas familias de ransomware descubiertas el pasado año, al menos 47 fueron desarrolladas por cibercriminales de habla rusa. Para entender mejor la naturaleza de estos ataques, los analistas han examinado el mercado sumergido de cibercriminales rusos parlantes. En la figura 4.1 se muestra un ejemplo de ataque ransomware en donde la PC estaba completamente bloqueada. La intensión de los hackers era pedir dinero por el desbloqueo.

[42] Figura 4.1 Ataque Ransomware

Los ataques pueden responder a causas ideológicas, económicas, personales, de competencia o de pura venganza, pero el motivo es casi lo de menos: lo importante es que, de un modo u otro, las empresas están amenazadas. [43] Además, según el informe de la revista “ESG Proyect 2016”, un solo ciberataque a una gran empresa puede generar un coste económico de hasta 3,79 millones de dólares. Esta cifra no solo supone un aumento del 23% respecto al coste del año anterior, sino que también se puede saber hasta qué punto puede influir un ‘hackeo’ en una gran compañía.

En base a las amenazas existentes y las vulnerabilidades que tiene una empresa proponemos un modelo empresarial para prevenir ciberataques:

1. **Proteger la red con un Firewall**. Es importante que la organización cuente con un firewall para monitorear el tráfico entrante y saliente de la red, creando reglas que permitan bloquear o autorizar el tráfico específico.
2. **Proteger los Ordenadores**. Se debe tomar en cuenta que para prevenir un ataque, todas las computadoras o servidores cuenten con un antivirus

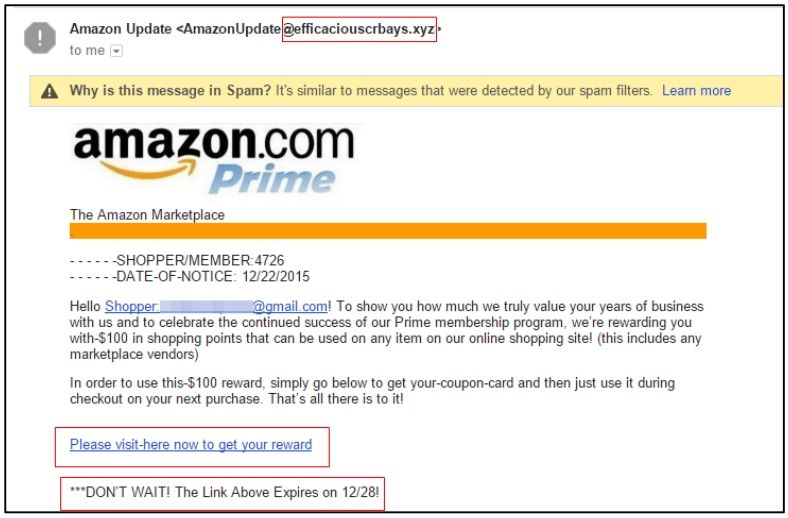
actualizado. En caso de un ataque es recomendable la creación de copias de seguridad, además de contar con un protocolo de recuperación de datos.

3. **Segmentar la Red**. Es importante aislar todo el tráfico de la organización por segmentos para proteger de forma dinámica la infraestructura y lo servicios de red.

4. **Mantener al mínimo los privilegios de los usuarios.** Se debe crear privilegios y controles en la navegación y descarga de archivos, la segmentación de red nos ayudara en esto creando VLAN para invitados, VLAN para usuarios y VLAN para súper usuarios estas se pueden autenticar en la red atreves de la MAC.

5. **Usar Protocolos de Seguridad.** Para toda transferencia de archivos a un servidor se deben usar protocolos de seguridad (SFTP, FTPS, NFS). Además, es recomendable revisar las políticas de seguridad de los productos y monitorear frecuentemente las alertas y logs de incidencias.

6. **Autenticidad de Enlaces.** Se deben comprobar siempre los enlaces para no ser víctima del phishing, educando al personal para que filtren adecuadamente los correos electrónicos, tratando con precaución cualquier mensaje sospechoso, sin abrir enlaces que provengan de fuentes no confiables. En la figura 4.2 se visualiza un correo electrónico que parece ser originado desde Amazon, pero que fue enviado desde un dominio diferente, ajeno a Amazon.



[44] Figura 4.2 Ataque Phishing

7. **Realizar auditorías rutinarias y test de penetración.** Es recomendable cada cierto tiempo realizar auditorías a la seguridad de la red y un test de penetración con la intensión de encontrar debilidades de seguridad verificando si el sistema es vulnerable a los ataques.

8. **Elegir prevención antes que detención**. Con el fin de detectar y mitigar los daños causados a la brevedad, invirtiendo en tecnología y productos que pongan la prevención antes que la detección.

9. **Cubrir todo los vectores de ataque**. Los hackers usan todo tipo de truco para introducirse a la red de correo, búsquedas por la web, aplicaciones. Se debe encontrar una solución que puede cubrir todos los elementos y que ofrezca una protección en todos las superficie de ataque.

10. **Crear una arquitectura de seguridad unificada**. En muchas organizaciones se puede verificar que la arquitectura de seguridad está hecha con una variedad de productos de muchos proveedores, muchas ocasiones entre tecnologías que no colaboran entre sí, dando lugar a agujeros en la seguridad.

En conclusión, el modelo descrito puede ayudar a evitar un ciberataque, pero se debe tomar en cuenta que no existe la bala de plata tecnológica que pueda

proteger a una organización ante todas las amenazas de cualquier tipo. Hoy en día se cuenta con tecnologías excelentes que pueden ser muy efectivas frente a los ataques, pero no es la solución definitiva.

Hay que estar preparados para cualquier tipo de ataque desde el más reciente hasta el que recién se acaba de inventar. El modelo propuesto permitirá a una organización tener una primera línea de respuesta para prevenir, detectar y bloquear estos ataques.

4.2 Implementación de un portal cautivo para la gestión de acceso a la red

Una buena práctica de seguridad en la organización es la implementación de un portal cautivo en donde los usuarios que se conecten a una red inalámbrica se autentiquen en el portal para que puedan ejecutar políticas en la navegación, como por ejemplo, controlar el ancho de banda, limitar el tiempo de conexión, permitir solo la conexión a ciertas páginas electrónicas, entre otras.

En el aspecto comercial se puede usar el portal cautivo para llevar a cabo un marketing, ya que facilita la captación del cliente, haciendo que los usuarios llenen encuestas, visualicen publicidad patrocina o presentar cualquier promoción activa en ese momento.

Un portal cautivo se puede implementar a través de software con Linux, Windows, o por hardware, esto es, usar el portal nativo que viene instalado por defecto en los equipos sean estos Cisco, Ruckus, Fortinet, entre otros.

En la figura 4.3 se presenta de forma general la implementación de un portal cautivo por software enfocado a redes Wi-Fi de corto alcance empleando autenticación local. Para ello, existen muchas aplicaciones de software libre de muy fácil instalación.

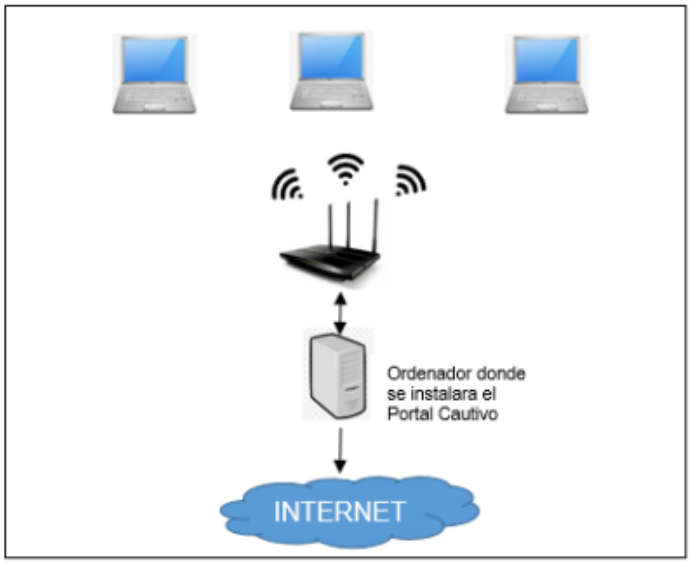


Figura 4.3 Diagrama esquemático de conexión del Portal Cautivo

Para el montaje del portal cautivo en una red Wifi pequeña lo mínimo que se necesita es:

- Un servidor (Ordenador) con 2 tarjetas de red donde se instalara el Portal Cautivo.
- Un ruteador (Punto de Acceso Wi-Fi)
- Acceso a Internet

[45] El proceso de instalación y configuración de un portal cautivo puede ser distinto existen muchos programas que ofrecen herramientas básicas y avanzadas según sea la necesidad de la compañía. A continuación se describe un ejemplo genérico para la habilitación de una porta cautivo:

- Habilitar un portal cautivo para su red. Normalmente se encuentra esta opción bajo el encabezado «portal cautivo» en el menú de configuración del punto de acceso, o bajo «configuración global». Si el punto de acceso no es compatible con la función de portal cautivo necesitará adquirir un modelo nuevo.

- [45] Personalizar los ajustes de configuración en un submenú, como por ejemplo «Perfiles del portal» o «Configuración de portal». Usualmente ahí podrá: a) darle un nombre a su portal; b) habilitar una contraseña de seguridad bajo alguna opción de «Autenticación Local» o similar; y c) optar por redireccionar el portal a un sitio web ya existente, si es que no desea crear una página personalizada.

- Bajo el menú «Pantalla de bienvenida», «Personalización de la web» o alguna opción similar, podrá elegir determinar con exactitud lo que sus clientes pueden ver o no cuando intentar acceder al hotspot Wi-Fi. Esta parte del proceso es vital para dar una buena impresión y por norma general tendrá que rellenar distintos formularios para concretar aspectos como: a) Logotipos personalizados; b) fondo, letra y colores; c) instrucciones de inicio de sesión para el usuario; d) etiquetas de nombre de usuario y contraseña: e) una detallada política de términos de uso y f) mensajes de confirmación de inicio de sesión con éxito.

- [45] Seleccione «Asociación», «Asociación de perfil» o la opción equivalente del menú del portal cautivo para asociar su portal con una banda de radio inalámbrica y SSID (Service Set Identifier). Si elige otras bandas de radio se restringirá el acceso al ancho de banda del usuario en una banda específica de un punto de acceso de doble o triple banda (como una banda de 2,4 GHz o de 5 GHz). Si selecciona un perfil SSID autorizará a los usuarios visitar su hotspot como invitados (seleccione la opción «Ninguno» del menú desplegable para permitir usuarios invitados). Consejo: si se adquiere un punto de acceso de doble o triple banda, esto ayudará a prevenir las interferencias de red, lo que agilita y facilita la experiencia online para todos los usuarios.

- Emplear un dispositivo portátil, smartphone, tablet o cualquier otro dispositivo habilitado con Wi-Fi para conectarse al hotspot y dar un vistazo al nuevo portal cautivo, introduciendo el nombre de usuario y contraseña que especificó durante el proceso de instalación y aceptando los términos de uso. Tras un componente de publicidad de calidad debería poder moverse sin

ataduras por su Wi-Fi, con la misma facilidad que sus clientes (a los que además les ha podido comunicar los mensajes de marca que desee).

Mediante la configuración de un portal cautivo se puede obtener un mejor control sobre el uso de la red, lo cual es de vital importancia, ya que puede mejorar la calidad de los servicios, asignar ancho de banda, restringir paginar, etc. En la figura 4.4 se muestran los principales software para la implementación de Portal Cautivo, unos propietarios y otros libres, dependiendo de las necesidades de la organización, si es conveniente comprar una licencia para portal cautivo o simplemente usar los software libre que hay hoy en día, como WifiDog, Easy Hotspot pfSense, etc.

Figura 4.4 Herramientas de Portal Cautivo

4.3 Monitoreo de la red a través de software de gestión

Para un nivel más avanzado de control de seguridad es recomendable el monitoreo de la red con software de gestión. [46]Esto es responsabilidad del personal a cargo de TI para tener asegurada la red, estando habilitado todo el tiempo, por medio de una software de gestión de red se puede rastrear todos los dispositivos conectados, ver el consumo de ancho de banda, monitorear transferencias de datos, entre otros. Tener la red siempre monitoreada tiene sus ventajas, tales como:

- Minimiza el tiempo de caída de la red.

- Detectar fallas antes que ocurran.
- Con la ayuda de alertas se pueda brindar soluciones al momento que ocurra una caída del sistema.
- Elaborar un registro donde se pueda saber tiempo de conexión y desconexión de los dispositivos.
- Llevar un registro de las páginas más visitadas el tiempo y el ancho de banda que se consume.

La gestión de redes no es solamente rastrear una dirección IP, asegurar que siempre haya conexión a la red o que el ancho de banda sea suficiente para transferencia de información. Se puede incluir el monitoreo del funcionamiento de ruteadores y conmutadores, incluso el mantenimiento de los servidores. Existen muchos gestores para el monitoreo de la red, al momento de escoger se debe validar primero cuales son las necesidades básicas de la empresa. A continuación se describen puntos importantes al momento de elegir un software para monitoreo de la red:

1) Principales componentes del software. Es importante que al momento de seleccionar el software disponga de distintas características, ya que tiene que monitorear ancho de banda, tener alertas en caso de fallas y limites en niveles de capacidad. Es importante que se pueda rastrear las direcciones IP de los dispositivos conectados. Estas características son básicas al momento de escoger el software de gestión de redes, la misma debe ser mostrada de manera clara y precisa para poder tomar decisiones.
2) Integración a la red. En toda empresa es importante que el software de gestión se integre a los dispositivos de redes ya establecidos. Si es difícil integrar el software a la estructura ya existente se tornaría aún más complicado notar los beneficios del programa en su totalidad. Un buen software de gestión debe ser de sencilla instalación y fluidez al momento de configurar las características necesarias para poder vigilar los equipos.
3) Sensores y alertas. Un buen gestor de red debe vigilar todos los elementos que la componen y saber cuándo hay problemas. Mediante el uso de

sensores y alertas es posible que se configure el software de gestión para que hayan notificaciones cuando haya algún inconveniente en la red.

En conclusión, es de vital importancia en las empresas monitorear la red, ya que da un control a los departamentos de TI. Con respecto al monitoreo de red, este debe ser continuo y no considerarse como una fase en la etapa de la implementación de la seguridad para evitar un ataque. Se debe recordar que la red de una organización debe tener un monitoreo permanente a cada uno de los componentes de la red. Sin un monitoreo de red, la caída de los servicios va a generar un malestar a los usuarios, provocando pérdida de productividad y creando una mala imagen a la empresa. En la actualidad existen varios software libres para el monitoreo de red como se muestra en la figura 4.5 (Nagios, Munin, Zabbix).

Figura 4.5 Herramientas de software de gestión

4.4 Políticas de seguridad en el servidor para la navegación

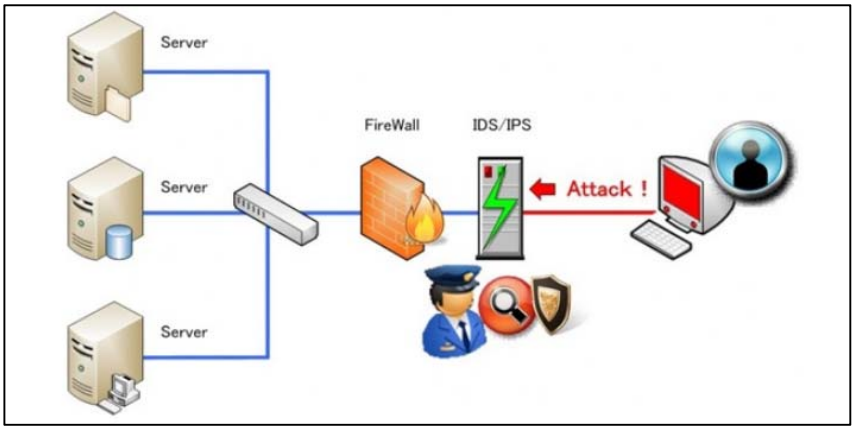
Es importante para toda empresa tener una política de seguridad en servidor de navegación, ya que en el servidor se aloja la página de la organización. [47] En ella se muestra identidad, infraestructura, imagen desde la página electrónica más sencilla sin mucho contenido, hasta la más compleja que cuenta con capacidad de realizar operaciones como pagos, compras, transacciones. Con esto, los servidores donde se encuentran las páginas de las empresas son un blanco fácil y muy atractivo para cualquier atacante por tal motivo debe estar bien protegido.

Los ataques a los servidores de las empresas son muy llamativos, debido a que es muy fácil divulgar el ataque en cuestión de segundos, haciendo que la mayor cantidad de usuarios se dé cuenta que se ha modificado algo en el servidor de la compañía. Hoy en día los servidores deben estar protegidos frente a cualquier amenaza, son el punto de entrada a la compañía por tal motivo tienen que estar bien resguardados.

[48] La gran mayoría de ataques a los servidores son la consecuencia de una muy mala configuración o un mal diseño en la infraestructura de red así como un fallo en la programación web. Las grandes corporaciones tienen sistemas más complejos y, por lo tanto, más difíciles de administrar. Las pequeñas empresas tienen servidores simples y con una configuración paupérrima, lo que hace que, en su gran mayoría, estos servidores sean susceptibles a ser atacados.

Definir una política de seguridad en el servidor es importantísimo con el fin de evitar un ciberataque. Estas políticas se basan en la seguridad del servidor no de cliente.

1. Autenticación.- Es importante que se usen contraseñas para acceder al servidor y estas se las cambien con frecuencia.
2. Usuario y Grupos.- Eliminando usuarios y grupos que ya no estén en uso, manteniendo la lista actualizada, creando cuentas de usuario, cada una de ella con privilegios.
3. Servicios.- Aplicar en el servidor las mejores prácticas de seguridad de proveedores reconocidos como SQL Server, Apache, Plesk, entre otros.
4. Firewall.- Asegurar el servidor con un firewall, a través hardware o de software. Es recomendable usar un sistema de detención de intrusos (IDS) y un sistema de prevención de intrusos (IPS) como el que se muestra en la figura 4.6, El firewall protege de los intrusos que traten de ingresar a la red desde ubicaciones externas a ella.



[49] Figura 4.6 Firewall Servidor

5. Auditorias y Análisis.- Es de suma importancia realizar periódicamente auditorias. Esto ayuda a asegurarse que se están cumpliendo los requisitos de seguridad mínimos, también ayuda a identificar los problemas de seguridad, realizando análisis periódicos para identificar vulnerabilidades, recordando que los potenciales intrusos están siempre explorando la web en busca de servidores vulnerables.

6. Sistema Operativo.- Tener el sistema operativo actualizado es muy importante ya que evita problema de seguridad provocado por el uso de versiones antiguas. Se debe actualizar el software siempre de fuentes confiables, ya que de no ser así generan un gran riesgo al servidor a ser vulnerado.

La mayoría de la empresa no tiene una política de seguridad en el servidor. Estas son esenciales orientaciones en la detención de ciberataques. Las políticas varían considerablemente según el tipo de compañía.

4.5 Prueba de Negación de Servicio (DoS)

El ataque tipo DoS se produce cuando se satura al servidor de peticiones TCP o UDP. Comúnmente se satura el puerto 80 que es el que se emplea para servicios web. [50] Dependiendo de cuales sean las intenciones del atacante, las peticiones son realizadas al servidor desde cientos, miles de máquinas infectadas de manera coordinada al mismo tiempo, lo que se hace que se

consuma el ancho de banda el uso de memoria y el procesamiento. Ningún servidor soportaría responder tantas peticiones, razón por la cual colapsa.

Este tipo de ataque puede utilizarse tanto como para dejar sin servicio a una página web, hacer caer servidores o fastidiar a los usuarios que estén conectados a la misma red. Este ataque es también una herramienta muy útil empleada por administradores red para medir la capacidad del tráfico real que puede soportar un servidor o un computador antes de quedar sin servicio.

[50] La clave para el éxito de un ataque de DoS es tener la mayor cantidad de máquinas "zombies" las cuales serán gobernadas a través de "Botnets". Un Botnet tiene 3000 máquinas zombies preparadas para atacar cada máquina tiene una conexión aproximada de 5 MB/s.

$$3000 \text{ host} \times 5 \text{ MB/s.} = 15000 \text{ MB/s.} = 15 \text{ GB/s} \qquad (4.1)$$

Del resultado obtenido de la ecuación (4.1) se puede visualizar que se está generando un tráfico de 15 GB/s de ancho de banda, lo cual es suficiente para colapsar cualquier servidor (aun estando protegido). El éxito de un ataque de DoS es el producto de una mala configuración en el servidor.

En la actualidad existen herramientas legales para probar si el servidor está protegido contra ataques de DoS una de ellos es DoSHTTP, la cual usa múltiples sockets asíncronos para efectuar el ataque. Esta herramienta funciona bajo plataforma Windows. Se inicia el uso de la herramienta ingresando el nombre del dominio del sitio web que se desea atacar. Luego se selecciona la cantidad de sockets que se desea enviar; con 500 es más que suficiente se seleccionar la opción de "start flood" tal como se muestra en la figura 4.7.

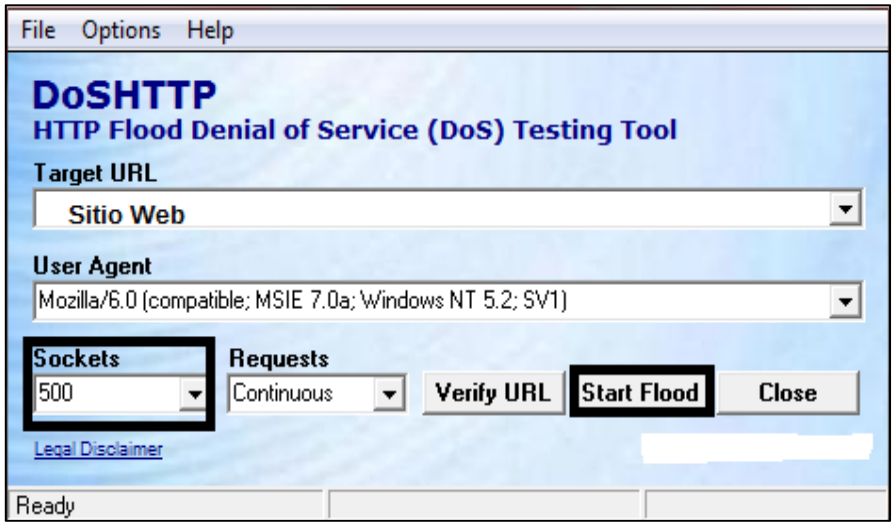


Figura 4.7 Prueba de DoS

Si el ataque es exitoso, en pocos minutos no se podrá acceder al sitio web. Caso contrario, si el sitio web está protegido, se observará un resultado como el indicado en la Figura 4.8.

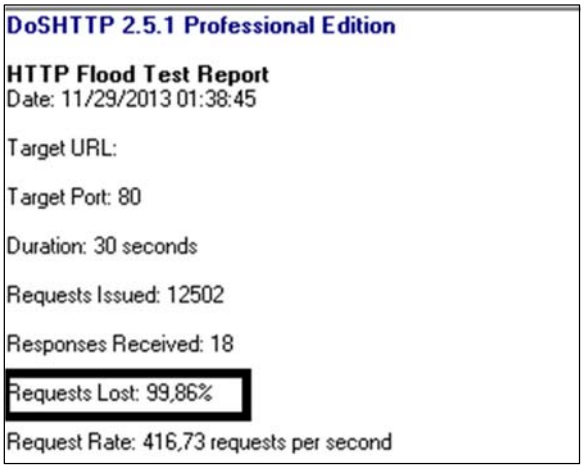


Figura 4.8 Resultados Prueba DoS

El resultado indica que las peticiones “Request Lost” con un 99.86% fueron rechazadas o descartadas por el servidor. Existen muchas formas de protegerse de un DoS. Si bien es cierto, ya vienen preinstalados módulos en los ruteadores capaces de rechazar múltiples peticiones, o en los firewalls a través de software en los servidores como “Netfilter” o “Iptables”.

4.5.1 Resultados de la Prueba

[51] La mayoría de los problemas de seguridad en las organizaciones están relacionadas con el desconociendo del personal en la seguridad de la información. Tener el personal capacitado es fundamental para manejar un esquema de seguridad. Definir políticas de seguridad en una organización es primordial, debido a que se crean normas y criterios a seguir en caso de sufrir un ataque o como prevenirlo.

Es de suma importancia retroalimentar el proceso de análisis de riesgos y definir una política de seguridad informática en la empresa. Definir cuáles son los puntos críticos y cuales se verían afectados en caso de un ataque, pudiendo definirse los siguientes:

a.- Cuáles son los bienes informáticos más importantes para la empresa y por lo tanto requieren de una atención especial y protección, considerando de importancia crítica por el pero que tienen dentro de un sistema.

b.- Qué amenazas pudieran tener gran impacto en caso de efectuarse un ataque.

c.- Cuáles son las áreas con mayor riesgo y a qué amenazas pueden perpetrarse.

Un ejemplo de los bienes informáticos que deben protegerse en una empresa:

- La red interna de la empresa
- El servidor de aplicaciones
- La base de datos del sistema
- La base de datos de la Intranet
- El servicio de correo electrónico
- Los sistemas contables

Las amenazas más importantes a considerar de acuerdo al impacto que pueden tener en la empresa son:

- El acceso no autorizado a la red, que puede ser un ataque externo como interno.
- Perdida de disponibilidad.
- Sustracción, alteración o pérdida de datos.
- Fuga de información.
- Introducción de programas malignos.

En medida en que los análisis de riesgos y las políticas de seguridad aplicadas a la empresa sean más precisas, se logrará una visión más acertada en la protección contra ciberataques. Se debe dirigir los todos los esfuerzos de seguridad y los recursos disponibles para ello, logrando que los mismos sean más rentables en términos de prevención.

En Ecuador, las empresas no cuentan con registros acerca de los ataques a la seguridad informática, lo cual dificulta el hecho que se pueda determinar el impacto del ataque en términos económicos. Es de vital importancia llevar un registro sobre los ataques informáticos, con el fin de tener un registro y poder realizar un cálculo del impacto que causó y los posibles formas de contrarrestarlo.

4.5.2 Análisis Costo – Beneficio de la prueba

Establecer un valor a los datos de una empresa es algo relativo, pues los datos, archivos, información de la empresa constituyen un recurso que en muchos casos no se da el valor que se merece, el desafío de responder la pregunta: ¿Qué valor tiene la información? Ha sido muy complicado y más aún hacer los costos de la seguridad justificables.

Para la evaluación de los costos se debe cuantificar los daños que podría causar el hecho de que se vulnere la seguridad. Se debe plantear una política antes de realizar la inversión y analizar lo siguiente.

- ¿Qué recursos se deben proteger?
- ¿Qué tan importante es la información de la empresa?

- ¿De quién se debe proteger la información?
- ¿Qué medidas se deben aplicar para proteger la información?

Con estas preguntas sencillas se deben conocer cuáles son los recursos de la empresa a proteger y comprender cuales son más importantes que otros. Con estas premisas se puede proceder a realizar un análisis Costo / Beneficio, el cual se puede resolver en estos 6 pasos:

1. Realizar un levantamiento de información, sobre la topología de red de la empresa.
2. Determinar el costo en relación a las cantidad de equipos información que deseo proteger.
3. Sumas todos los costos involucrados en la decisión.
4. Determinar los beneficios que obtendré al implantar la decisión.
5. Poner en dólares los costos y los beneficios totales en la relación Beneficios/Costos.
6. Comparar las relaciones beneficios a costos para las diferentes decisiones propuestas. La mejor solución, en términos financieros es aquella con la relación más alta beneficios a costos.

Los riesgos que se corren en una organización son varios al no estar protegidos por una solución efectiva y garantizada de seguridad informática. Entre ellos podemos mencionar los siguientes tres puntos importantes:

1. **La navegación no auditada a empleados**. [52] El acceso a redes sociales, chats, prensa y otros de tipo entretenimiento o informativos, reduce significativamente el tiempo productividad del personal. Un estudio realizado por Secura ha arrojado que, de media, cada persona pierde 48 minutos al día en navegación personal.
2. **Fuga de información**. [52] La mayoría de los robos y fugas de información provienen de los mismos empleados. Hay dos formas

básicas para sacar información fuera de la empresa: una es Internet, ya que cualquiera puede enviarse un correo con información confidencial a una cuenta privada o incluso subir un adjunto a su correo web personal. La otra son dispositivos de almacenamiento por USB. Ambos métodos se consiguen controlar con los sistemas DLP (Data Loss Prevention) que identifican la información confidencial, evitan su envío por Internet y prohíben el uso de memorias o módems USB ajenos a la compañía tal como se muestra en la figura 4.9.

Figura 4.9 Robo de información en la Empresas

3. **Ataques de hackers**. [53] Se afirma que las pérdidas por robos informáticos ya superan a las sufridas de los robos físicos. Se tiende a pensar que es difícil ser objeto de un ataque, pero toda empresa está en el punto de mira. De hecho, las mafias organizadas usan a hackers para robar fácilmente pequeñas cantidades a miles de pequeñas y medianas empresas, en lugar de robar miles de millones a las grandes multinacionales que invierten mucho en seguridad y están bien protegidos.

En conclusión, se puede indicar que la inversión en seguridad debería hacerse de manera progresiva aunque obligada para reducir así los riesgos tecnológicos a los que estamos expuestos y potenciar al máximo nuestra productividad y seguridad.

4.6 Métodos de encriptación y protección de la información

La encriptación es un método de ocultar la información de forma que no se pueda interpretar, esto se lo hace por medio de una llave que es el método de encriptación; la información una vez se haya encriptado solo puede leerse desencriptándola de esta forma se asegura que la información sea auténtica, segura y confiable. En la figura 4.10 se muestra un ejemplo de esquema de encriptación.

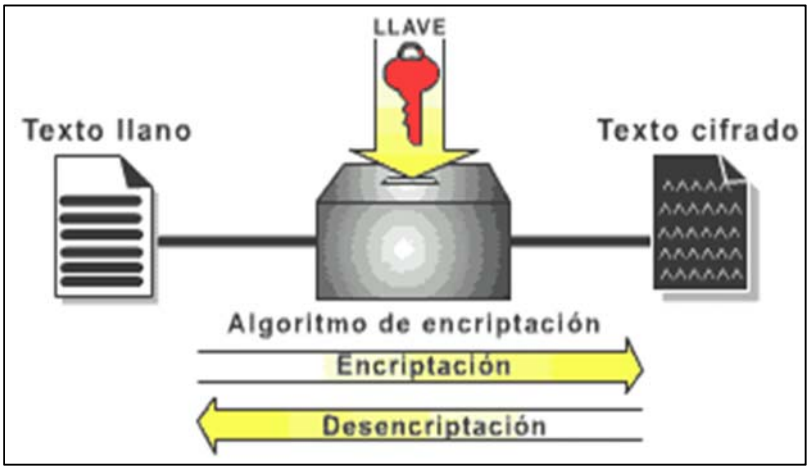


Figura 4.10 Método de Encriptación y Desencriptación

Un esquema básico de encriptación implica la utilización de una llave o clave para encriptar el mensaje de tal forma que solo puedan desencriptar aquellos que conocen la llave o la clave.

[54] El manejo de datos sensibles de los usuarios por parte de las aplicaciones y las webs, requiere que estas tengan técnicas y sistemas de seguridad para proteger dichos datos, ya que pueden ser muy relevantes y, por ello, es primordial el uso de técnicas de cifrado de datos. Hay varios métodos de encriptación, listando los siguientes:

1. Algoritmo de HASH.- Este algoritmo se basa en el cálculo matemático sobre los datos del archivo el cual da como resultado un único número llamado MAC. Un mismo archivo siempre dará un mismo MAC.

2. Criptografía de Clave secreta o Simétrica: Este método utiliza una llave o clave en la cual se encripta y se desencripta el archivo. Es importante mencionar que la llave viaja por los datos lo que hace que esta operación sea arriesgada, difícil de usar en sistemas full dúplex. Los sistemas de criptografía por clave secreta no son muy robustos, ya que la clave del cifrado y del descifrado es la misma. Sus principales funciones son:

   - Fácil y rápidos de Implementar
   - Cifrado y descifrado usan la misma clave
   - Usuarios compartes la misma clave secreta
   - Una comunicación full dúplex requieren muchas claves secretas

[54] En la actualidad existen dos métodos de cifrado para criptografía de clave secreta, el cifrado de flujo y el cifrado en bloques.

- Cifrado de flujo.- El emisor, con una clave secreta y un algoritmo, genera una secuencia binaria cuyos elementos se suman módulo 2 con los correspondientes bits de texto, dando lugar a los bits de texto cifrado, Esta secuencia es la que se envía a través del canal. En recepción, con la misma clave y el mismo algoritmo, genera la misma secuencia para desencriptar, que se suma módulo 2 con la secuencia cifrada, dando lugar a los bits de texto claro. Los tamaños de las claves oscilan entre 120 y 250 bits.
- Cifrado en bloque.- Los cifrados en bloque se componen de cuatro elementos:

  a. Transformación inicial por permutación
  b. Transformación final para que las operaciones de encriptación y desencriptación sean simétricas
  c. Uso de un algoritmo de expansión de claves que tiene como objeto convertir la clave de usuario, normalmente de longitud limitada entre

32 y 256 bits, en un conjunto de subclaves que puedan estar constituidas por varios cientos de bits en total.

3. Algoritmos Asimétricos (RSA): [54] Se Requieren dos claves, una privada (propia y única, solo conocida por su dueño) y la otra llamada pública, ambas vinculadas por una fórmula matemática compleja imposible de descifrar. El usuario, ingresando su PIN genera la clave pública y privada necesaria. La clave Pública podrá ser distribuida sin ningún inconveniente entre todos los interlocutores. La Privada deberá ser celosamente guardada.
4. Message-Digest Algorith, MD5: [55] Este algoritmo, ha sido en los últimos años el algoritmo Hash más usado, procesa mensajes de una longitud en bloques de 512 bits generando un resumen de 128 bits. Debido a su gran capacidad de procesamiento actual esos 128 bits son insuficientes para asegurar la integridad del algoritmo, además de que una serie de ataques criptoanalíticos han puesto en manifiesto algunas vulnerabilidades del algoritmo.
5. Advanced Encryption Standard, (AES): En criptografía, Advanced Encryption Standard (AES), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. [55] Se espera que sea usado en el mundo entero y analizado exhaustivamente, el AES fue anunciado por el Instituto Nacional de Estándares y Tecnologia11 (NIST) el 26 de Noviembre de 2001 después de un proceso de estandarización que duró 5 años. Se transformó en un estándar efectivo el 26 de Mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica

4.7 Implementación de algoritmo de encriptación

Existen muchas formas para la encriptación de datos en el cual se transformara la información (texto en clave) en otra información (texto cifrado) que será difícil de descifrar si no se conoce la llave. De manera que no se podrá ver la información original si no se conoce la llave.

Matemáticamente el funcionamiento de un algoritmo de cifrado está dada por una función. Supongamos que tenemos un mensaje m, al cual se le agrega el algoritmo que será llamado a, el resultado de esta operación se le conocerá como h, es decir, h es el cifrado de m y se representa matemáticamente así:

a (m)=h

[55] Esta función debe ser sencilla para un procesador pero imposible realizar la función inversa ya que esto sería una vulnerabilidad que se podría explotar (1) otra recomendación al realizar un algoritmo es que la longitud del mensaje de entrada, m puedan hacer una misma salida h. Es decir puede existir un mensaje n tal que (2):

(1) $a^{-1}(h)=m$

(2) a(n) = h

Como caso de estudio escogeremos al algoritmo AES el cual funciona a través de bucles que se repiten de 10 ciclos para claves que sin de 128 bits, 12 para 192 bit y 14 para 256.

Consideremos que tenemos 2 matrices a y k

$a00\ a01\ a02\ a03$	$k00\ k01\ k02\ k03$
$a10\ a11\ a12\ a13$	$k10\ k11\ k12\ k13$
$a20\ a21\ a22\ a23$	$k20\ k21\ k22\ k23$
$a30\ a31\ a32\ a33$	$k30\ k31\ k32\ k33$

[56] En la matriz a se tienen los datos y en matriz k se tiene el algoritmo para el cifrado y descifrado. Se usa una función ronda compuesta de cuatro trasformaciones orientadas a bytes

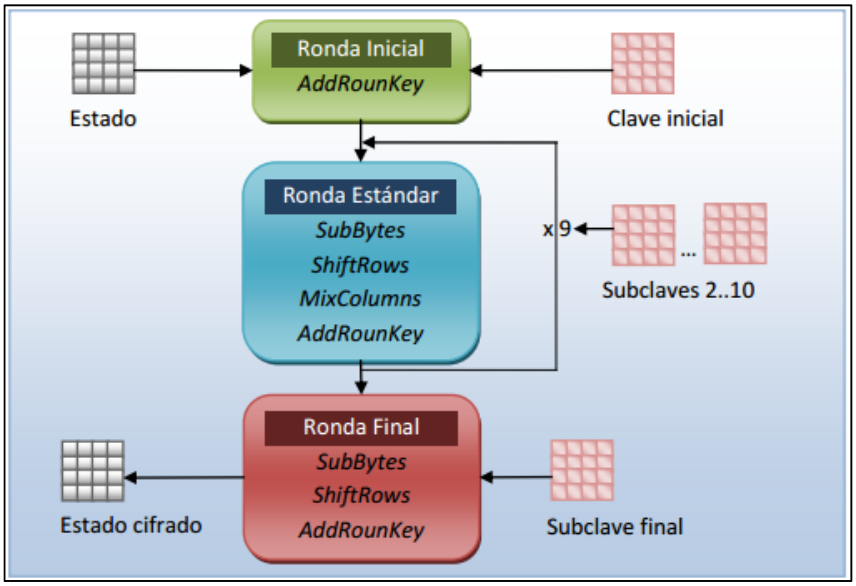
1) SubBytes: Se aplica la sustitución de bytes usando una tabla de sustitución (S-Box).

2) ShiftRows: Se aplica el cambio de filas de la matriz de estado por distintas configuraciones.

3) MixColumns: se hace una mezcla de datos entre las columnas del vector de estado.

4) AddRoundKey: Se aplica la operación XOR entre la matriz de estado y la clave de ronda.

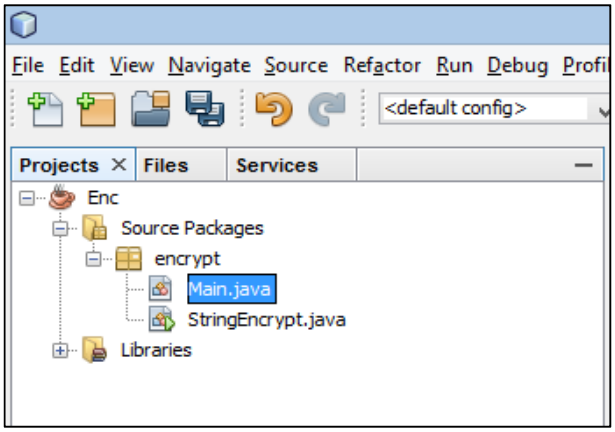
[58] El proceso de cifrado consiste en aplicar de forma reiterativa estas cuatro operaciones invertibles sobre la matriz de estado de 128 bits. Estas funciones deben aplicarse dentro del proceso de acuerdo con la secuencia descrita en la figura 4.11



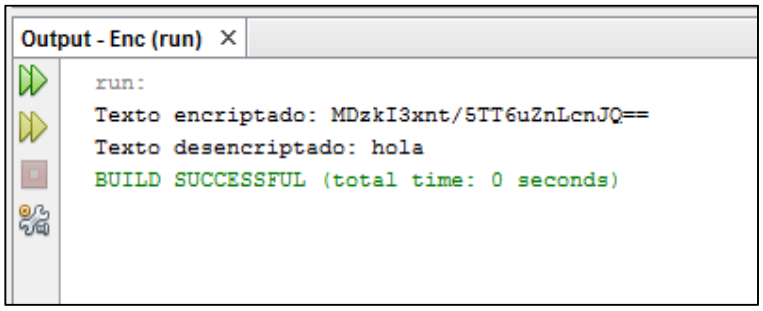
[59] Figura 4.11 Proceso de Cifrado de AES

[57]Las transformaciones de cifrado pueden ser invertidas y luego implementadas en orden reverso para producir un descifrador del algoritmo AES. En efecto, las funciones que allí se utilizan son: InvSubBytes, InvShiftRows, InvMixColumns e InvRoundKey, las cuales realizan operaciones muy similares a las del proceso de cifrado, pero con elementos diferentes y mediantes rondas en sentido contrario

En la imagen 4.12 y 4.13 se muestra la implementación del algoritmo AES en JAVA, (ver programación en Anexo 3).



[59] Figura 4.11 Proceso de Cifrado de AES



[59] Figura 4.11 Proceso de Cifrado de AES

Como conclusión, se puede decir que el cifrado AES es uno de los más seguros cifrados modernos y es de acceso público el cual permite un nivel de seguridad muy alto en comparación con los cifrados con clave de 128 bits o de 256 bits, la seguridad de AES se basa en la longitud de la clave, cuanto mayor es el tamaño de clave mayor es el número de rondas que debe realizar el cifrado y por tanto mayor número de operaciones.

[59] Según un grupo de investigadores de Microsoft y de la Universidad de Cambrige, existe un defecto en AES que permite “romper” el algoritmo. Sin embargo, en el mismo estudio aseguran que incluso con este defecto un billón de ordenadores que pudieran cada uno probar mil millones de claves por segundo, tardarían más de 2.000 millones de años en dar con una clave del sistema AES-128, y hay que tener en cuenta que las maquinas actuales solo pueden probar 10 millones de claves por segundo.

CONCLUSIONES Y RECOMENDACIONES

En la mayoría de los ambientes corporativos no existe una cultura de seguridad de la información, se recomienda llevar a cabo un control de seguridad informática donde se implementen políticas de seguridad idóneas y actualizadas para que protejan las redes de datos y sistemas informáticos ante eventuales amenazas que puedan presentarse.

Todas las organizaciones están expuestas a una enorme cantidad de riesgos, los cuales deben ser tratados de manera conjunta entre diferentes sectores de la organización, con el fin de garantizar que las mejoras se complementen y que con el paso del tiempo se puedan alcanzar niveles aceptables de riesgo. La seguridad de la información puede verse afectada de muchas formas, por ende no basta con solucionar un problema ahora, sino que el tratamiento del riesgo y la mejora de los factores debe ser una actividad constante en toda organización.

Los ciberataques van a seguir creciendo a un ritmo cada vez mayor, tanto en número, como en sofisticación e impacto, las organizaciones deben responder a las posibles amenazas implementado soluciones específicas para proteger todos los entornos de TI, se debe centrar la solución en prevención más que en la detección y mitigación.

En la actualidad, Ecuador ha incrementado su presencia en el ciberespacio debido a una decidida intención del Gobierno Nacional en impulsar la tecnología digital, basada en tres pilares fundamentales: el Plan Nacional de Banda Ancha, el Plan Nacional de Alistamiento Digital y el Plan Nacional de Gobierno Electrónico, con la aspiración de llevar al país a un nivel conectado en el 2017, similar a índices de conectividad que han alcanzado otras naciones, lo cual a su vez puede conllevar a ser vulnerable a ciberataques. Realizar auditorías periódicas con el fin de asegurar la red es primordial, siendo importante establecer un continuo cambio en las configuraciones, actualizar los sistemas operativos e implementar software y hardware orientado a reforzar la seguridad de la red, más aun dado que los virus informáticos y sus variantes evolucionan día a día. La auditoría permite conocer la situación actual de los activos de información, en cuento a protección, control y medidas de seguridad.

BIBLIOGRAFÍA

[1] ISMS.(20 de 06 de 2017). P*olítica de seguridad en la empresa*. Obtenido de http://www.protegetuinformacion.com/perfil_tema.php?id_perfil=7&id_tema=63

[2] 20minutos. (28 de 07 de 2017). *Las autoridades afirman que el ataque de 'ransomware' tiene efectos limitados en España*. Obtenido de http://www.20minutos.es/noticia/3076580/0/ransomware-ataque-espana-sedes-multinacionales-organismos-publicos-cni/

[3] ICRATIAS. (30 de 01 de 2018). *INFRAESTRUCTURA DE SEGURIDAD INFORMATICA*. Obtenido de https://www.icraitas.com/infraestructura/

[4] Castro, R. (15 de 01 de 2018). *Costo / Beneficio Seguridad*. Obtenido de http://slideplayer.es/slide/4648733/

[5] Provincias, L. (10 de 07 de 2017). *Los 10 principales riesgos informáticos*. Obtenido de http://www.lasprovincias.es/economia/empresas/201409/30/principales-riesgos-informaticos-20140930162144.html

[6] ASTINAVE. (2014). *Sistema KRYPTO-AEP.* Guayaquil: Astilleros Navales Ecuatorianos.

[7] BARAHONA. (23 de 01 de 2018). *LADRONES VIRTUALES! Ataques "phishing"*. Obtenido de http://diariodigitalbarahona.blogspot.com/2014/02/ladrones-virtuales-ataques-phishing.html

[8] HUFFPOST. (1 de 07 de 2017). *Ocho consejos esenciales para evitar un ciberataque en tu ordenador*. Obtenido de http://www.huffingtonpost.es/2017/05/12/consejos-para-evitar-un-ciberataque_a_22083669/

[9] BETECH. (04 de 01 de 2018). *ROBO DE INFORMACION*. Obtenido de https://as.com/betech/2017/05/12/portada/1494593313_342164.html

[10] Carmen. (08 de 08 de 2017). *Seguridad Informatica*. Obtenido de https://carrmen.jimdo.com/riesgo-informatico/

[11] TANGIENT. (30 de 01 de 2018). *SEGURIDAD INFORMÁTICA*. Obtenido de https://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA

[12] Ciudadano, E. (18 de 09 de 2017). *Ecuador cuenta con 45.000 km de fibra óptica* . Obtenido de http://www.elciudadano.gob.ec/ecuador-cuenta-con-45-000-km-de-fibra-optica/

[13] Clarke, R., & Robert, K. (2011). *Guerra en la red, los nuevos campos de batalla.* Barcelona: Planeta.

[14] Digital, E. (6 de 07 de 2017). *Los Diez mayores ataques informaticos*. Obtenido de http://www.economiadigital.es/tecnologia-y-tendencias/los-diez-mayores-ataques-informaticos-de-2016_188964_102.html

[16] ITNOW. (5 de 07 de 2017). *Más allá del firewall y la seguridad perimetral*. Obtenido de https://revistaitnow.com/mas-alla-del-firewall-y-la-seguridad-perimetral/

[17] AEPROVI. (18 de 09 de 2017). *SENATEL, Aviso al público REGLAMENTO DEL FONDO DE DESARROLLO DE LAS TELECOMUNICACIONES, FODETEL*. Obtenido de http://www.aeprovi.org.ec/es/recursos/noticias-del-sector/55-noticias-octubre-2008/240-senatel-aviso-al-publico3

[18] DRAGONJAR. (11 de 01 de 2018). *DDoS Análisis de Ataques Coordinados*. Obtenido de https://www.dragonjar.org/ddos-analisis-de-ataques-coordinados.xhtml

[19] Edisa. (11 de 07 de 2017). *TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMATICAS*. Obtenido de http://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

[20] FAQ. (28 de 09 de 2017). *Políticas de Seguridad en Cómputo de la Facultad de Ingeniería (PSC-FI)*. Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/politicas/faq.html#faq

[21] Freire, B. (2015). *Creación del Comando de Ciberdefensa en Ecuador.* Quito: Comando Conjunto de las Fuerzas Armadas.

[22] MENTOR. (30 de 01 de 2018). *Vulnerabilidades de un sistema informático*. Obtenido de http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html

[23] Confidencial, E. (27 de 10 de 2017). *LA RECETA ANTIHACKERS*. Obtenido de https://brands.elconfidencial.com/tecnologia/2017-02-17/accenture-ciberseguridad-ataques-seguridad_1332673/

[24] Gonzales, R. (19 de 07 de 2017). *Ataque DoS: Inundación SYN*. Obtenido de http://ramon-gzz.blogspot.com/2013/02/ataque-dos-inundacion-syn.html

[25] Morales. (04 de 09 de 2017). *AMENAZA, RIESGO Y VULNERABILIDAD. ¿EXISTE DIFERENCIA ENTRE ELLOS?* Obtenido de http://www.stratcont.com/diferencia-amenaza-riesgo-vulnerabilidad/

[26] Gretel. (17 de 01 de 2018). *Encriptación de Datos*. Obtenido de http://encripdedatos.blogspot.com/

[27] Ibiblio. (11 de 07 de 2017). *Medidas de protección*. Obtenido de http://www.ibiblio.org/pub/Linux/docs/LuCaS/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node337.html

[28] Uzal, R. (2015). Taller de Defensa Cibernética. *Revista ESPE* (págs. 23-35). Quito: Escuela Politécnica del Ejército.

[29] INFOSEGUR. (1 de 08 de 2017). *Amenazas y fraudes en los sistemas de la información*. Obtenido de https://infosegur.wordpress.com/tag/vulnerabilidades/

[30] MINUTOS, 2. (24 de 01 de 2018). *Ciberataque mundial: ¿Qué es un ataque tipo 'ransomware'?* Obtenido de https://www.20minutos.es/noticia/3035545/0/que-es-ransomware-ciberataque-mundial/

[32] IWEB. (09 de 01 de 2018). *Las mejores prácticas para proteger los servidores y la infraestructura de TI (28 recomendaciones)*. Obtenido de https://kb.iweb.com/hc/es/articles/230267608-Las-mejores-pr%C3%A1cticas-para-proteger-los-servidores-y-la-infraestructura-de-TI-28-recomendaciones-

[33] KYOCERA. (17 de 01 de 2018). *Técnicas para encriptar datos web*. Obtenido de https://smarterworkspaces.kyocera.es/blog/tecnicas-encriptar-datos-web/

[34] LINKSYS. (03 de 01 de 2018). *¿Qué es un portal cautivo?* Obtenido de https://www.linksys.com/es/r/resource-center/business-solutions/portal-cautivo/

[36] Tornil, X. P. (12 de 09 de 2017). *Seguridad en Redes TCP/IP.* Obtenido de http://www.elmundodelastics.net/2010/04/seguridad-en-redes-tcpip_03.html#.WbiMBMjyjIU

[37] MENGUAL. (4 de 10 de 2017). *ARQUITECTURA DE SEGURIDAD*. Obtenido de http://www.personal.fi.upm.es/~lmengual/ARQ_REDES/Arquitecturas_Seguridad.pdf

[38] MINTEL. (2016). *MINTEL.* QUITO: EDINSA.

[40] OnaSystem. (5 de 07 de 2017). *Estadisticas ciberataques empresas*. Obtenido de http://www.onasystems.net/estadisticas-ciberataques-empresas/

[41] PAIS, E. (28 de 06 de 2017). *Uruguay víctima de más ataques informáticos: 378 en seis meses*. Obtenido de http://www.elpais.com.uy/informacion/uruguay-victima-mas-ataques-informaticos.html

[42] QW:NEWS. (4 de 10 de 2017). *Evaluación de la seguridad de los Sistemas Informáticos: políticas, estándares y análisis de riesgos"*. Obtenido de https://qanewsblog.com/2013/04/16/evaluacion-de-la-seguridad-de-los-sistemas-informaticos-politicas-estandares-y-analisis-de-riesgos/

[43] Zemáneck. (30 de 01 de 2018). *Tutorial de Seguridad Informática*. Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap4.html

[44] REDSEGURIDAD. (09 de 01 de 2018). *ÁLVARO ROLDÁN*. Obtenido de http://www.redseguridad.com/especialidades-tic/virtualizacion/seguridad-en-servidores-web-la-importancia-de-tener-un-sistema-seguro

[45] Secretaría Nacional de la Administración Pública. (2014). *Plan Nacional de Gobierno Electrónico.* Quito: SNAP.

[46] SecurityIQ. (09 de 01 de 2018). *¿Quién es vulnerable al phishing?* Obtenido de http://resources.infosecinstitute.com/web-server-security-2/#gref

[47] SEGURIDAD. (12 de 01 de 2018). *ANALISIS DE RIESGO DE SEGURIDAD*. Obtenido de http://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

[48] SOLUTIONS, E. (14 de 01 de 2018). *Protección Perimetral & Firewalls*. Obtenido de http://www.etic-solutions.net/etic/enterprise/proteccion-perimetral-y-firewalls

[49] SOROTECH. (27 de 01 de 2018). *INFRAESTRUCTURA*. Obtenido de http://www.sorotech.com/infraestructura

[50] TRESW. (24 de 06 de 2017). *Firewalls o Cortafuegos. ¿Qué son y para qué sirven?* Obtenido de http://blog.tresw.com/seguridadinformatica/firewalls-o-cortafuegos-%C2%BFque-son-y-para-que-sirven/

[51] UCAV. (30 de 01 de 2018). *CIBERSEGURIDAD: QUÉ ES Y PARA QUÉ SIRVE*. Obtenido de https://www.ucavila.es/blog/2015/07/03/ciberseguridad-que-es-y-para-que-sirve/

[52] UIT. (2014). Tecnicas para prevenir ataques en la red. *SERIE X: REDES DE DATOS, COMUNICACIONES*, 34.

[53] TECNURA. (9 de 04 de 2018). *Implementación del algoritmo criptográfico AES para un controlador de tráfico vehicular*. Obtenido de https://revistas.udistrital.edu.co/ojs/index.php/Tecnura/article/view/7236/8892

[54] Welivesecurity. (27 de 07 de 2017). *Brasil: 4to país que más genera ataques DDoS según estudios*. Obtenido de https://www.welivesecurity.com/la-es/2012/10/24/brasil-4to-pais-mas-genera-ataques-ddos-segun-estudios/

[55] WordPress. (30 de 01 de 2018). *Gestión de Riesgo en la Seguridad Informática*. Obtenido de https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

[56] Cimetrico, A. d. (9 de 4 de 2018). *OREJUELA*. Obtenido de http://bibliotecadigital.usb.edu.co/bitstream/10819/2951/1/algoritmo_cifrado_simetrico_orjuela_2008.pdf

[57] TECNURA. (9 de 04 de 2018). *Implementación del algoritmo criptográfico AES para un controlador de tráfico vehicular*. Obtenido de https://revistas.udistrital.edu.co/ojs/index.php/Tecnura/article/view/7236/8892

[58]TARINGA. (9 de 4 de 2018). *Seguridad Informatica...Criptografia*. Obtenido de https://www.taringa.net/posts/info/4030740/Seguridad-Informatica-Criptografia.html

[59]UDISTRITALL. (10 de 09 de 2017). *Implementación del algoritmo criptográfico AES para un controlador de tráfico vehicular*. Obtenido de https://revistas.udistrital.edu.co/ojs/index.php/Tecnura/article/view/7236/8892

ANEXOS

ANEXO 1: Abreviaturas

ACK: Acknowledgement – Acuse de Recibo

ARP: Address Resolution Protocol

CIDR: Enrutamiento entre dominios sin clase

CSIRT: Equipos de Respuesta a Incidentes de Seguridad Informática

DLP: Data Loss Prevention

DNS: Domain Name System

DoS: Denegation of Service

DDoS: Distributed Denegation of Service

EcuCERT: Centro de respuesta a incidentes Informáticos del Ecuador

FODETEL: Fondo de Desarrollo de las Telecomunicaciones

FTPS: File Transfer Protocol Secure

HTML: Hypertext Markup Language

ICMP: Internet Control Message Protocol

IoT: Internet of Things

MINTEL: Ministerio de Telecomunicaciones y de la Sociedad de la Información

NAT: Network Address Traslation

NFS: Network File System

POP3: Protocolo de Oficina Postal

PYMES: Pequeña y mediana empresa

SI*:* Sociedad de la Información

SFTP: Simple File Transfer Protocol

SMTP: Simple Mail Transfer Protocol

SO: Sistema Operativo

SYN: Bit de control dentro de un segmento TCP

TCP: Transmission Control Protocol

TCP/IP: Transmission Center Protocol/Internet Protocol

TI: Tecnología de Información

TLD: Servidor de Raíz de Dominio

UDP: User Datagram Protocol

UIT: Unión Internacional de Telecomunicaciones

URL: Uniform Resourse Locator

VPN: Virtual Private Network

ANEXO 2: Glosario

Ciberseguridad: Conjunto de políticas que se usan para proteger la información de una organización.

Firewall: Dispositivo que monitorea el tráfico de o hacia tu red. Permite o bloquea tráfico basado en reglas de seguridad.

Ransomware: Es un tipo de programa dañino que restringe el acceso a determinados aplicaciones, y pide un rescate a cambio de quitar esta restricción.

Ruteadores: Es el dispositivo encargado de interconectar una red de ordenadores.

ANEXO 3: PROGRAMA EN JAVA, ENCRIPTACION AES

```
package encrypt;
import javax.crypto.Cipher;
import javax.crypto.spec.IvParameterSpec;
```

```
import javax.crypto.spec.SecretKeySpec;
import static org.apache.commons.codec.binary.Base64.decodeBase64;
import static org.apache.commons.codec.binary.Base64.encodeBase64;

public class StringEncrypt {
    // Definición del tipo de algoritmo a utilizar (AES)
    private final static String alg = "AES";
    // Definición del modo de cifrado a utilizar
    private final static String cI = "AES/CBC/PKCS5Padding"
    public static String encrypt(String key, String iv, String cleartext) throws Exception {
            Cipher cipher = Cipher.getInstance(cI);
            SecretKeySpec skeySpec = new SecretKeySpec(key.getBytes(), alg);
            IvParameterSpec ivParameterSpec = new IvParameterSpec(iv.getBytes());
            cipher.init(Cipher.ENCRYPT_MODE, skeySpec, ivParameterSpec);
            byte[] encrypted = cipher.doFinal(cleartext.getBytes());
            return new String(encodeBase64(encrypted));
    }
    public static String decrypt(String key, String iv, String encrypted) throws Exception
{
            Cipher cipher = Cipher.getInstance(cI);
            SecretKeySpec skeySpec = new SecretKeySpec(key.getBytes(), alg);
            IvParameterSpec ivParameterSpec = new IvParameterSpec(iv.getBytes());
            byte[] enc = decodeBase64(encrypted);
            cipher.init(Cipher.DECRYPT_MODE, skeySpec, ivParameterSpec);
            byte[] decrypted = cipher.doFinal(enc);
            return new String(decrypted);
    }
}
```