



UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

**TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL
TÍTULO DE:**

INGENIERO DE SISTEMAS

CARRERA:

INGENIERÍA DE SISTEMAS

TEMA:

**"ESTUDIO DE LOS PATRONES DE SEGURIDAD PARA LA
ATENUACIÓN DE LAS IRREGULARIDADES, LAS
DEBILIDADES Y AMENAZAS EN EMPRESAS DE SERVICIOS
DE TELECOMUNICACIONES "**

AUTOR:

María José Chévez Morán.

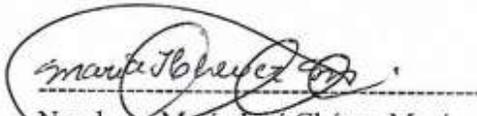
TUTOR:

Msg. Joe Frand Llerena Izquierdo.

**Abril 2021
GUAYAQUIL-ECUADOR**

DECLARATORIA DE RESPONSABILIDAD

Yo MARÍA JOSÉ CHÉVEZ MORÁN declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del/los /las autor/es/as.



Nombres: María José Chávez Morán.

CI: 0931275549

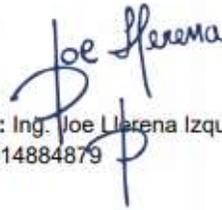
Fecha: Guayaquil, 8 de febrero del 2021.



Firma:

(Tutor): Ing. Joe Llerena Izquierdo, MSig.

C.I.: 0914884879



Estudio de los patrones de seguridad para la atenuación de las irregularidades, las debilidades y amenazas en empresas de servicios de telecomunicaciones

Abstract. Se evidencia la problemática de seguridad en el sector de telecomunicaciones ya que al ser proveedores de este tipo de servicio son blancos perfectos de ataques DoS, por lo tanto, en este artículo se estudió un modelo de tecnología de la información para la creación de un plan de mitigación de riesgos de protección en las entidades de telecomunicaciones. El objetivo principal es definir un prototipo de seguridad de la información para diferentes tipos de ataques, mejorando los protocolos de seguridad. Como herramienta fundamental, se realizó un método deductivo y exploratorio para el análisis y prueba de la información de referencia para aumentar la seguridad en estas empresas. Los modelos propuestos como resultados son una opción para lograr una protección más eficaz de los procesos y datos. Adicional se hace un énfasis en la correcta aplicación de los modelos y protocolos ya que mejorar la calidad del servicio y ayuda a las entidades tener planes de contingencia en caso de ataque con un modelo de defensa activa.

Keywords: mitigación, prototipo, ataque, deductivo, defensa activa, protocolos.

1 Introducción

Hoy en día la tecnología de la información, en la que prevalece el crecimiento de los equipos informáticos y de las redes, es necesario proteger los recursos e información. El incremento del número de ordenadores en red siempre implica un coste de actividad intrusivas. Por consiguiente, es preciso adoptar diferentes formas que aporten seguridad, fiabilidad y escalabilidad en las diferentes redes de información y comunicación, se requiere que los datos sean confidenciales, completos y auténticos.

Los ataques DoS son los asaltos informáticos más dañinos usados por los piratas cibernéticos para perjudicar a una organización. Este tipo de amenazas se producen cuando el atacante intenta hacer que el servidor o servidores no estén disponibles para los usuarios legítimos, este se realiza inundando la cola de solicitudes del servidor con peticiones falsas [1].

En esta investigación se tomará como caso de estudio las distintas empresas de telecomunicaciones que brindan sus servicios a nivel nacional en el Ecuador. El sector de las telecomunicaciones ha hecho una contribución extraordinaria al incremento de las infraestructuras de comunicaciones que vinculan a las comunidades en prácticamente todos los ámbitos de la industria y en todas las partes del mundo. Es indiscutible que la protección debe ser un proceso elaborado cuidadosamente en todas sus etapas; es esencial que la protección esté disponible en la formulación de las medidas de seguridad.

A nivel mundial la vulnerabilidad en las empresas que brindan servicios de telecomunicaciones se ha incrementado debilidad a la facilidad con la que se pueden crear

nuevos ataques, como el gran número de computadoras configuradas incorrectamente, lo que provoca fallos de seguridad, a esta lista se suma el denominado Bring Your Own Device implica que el funcionario tiene la posibilidad de hacer uso de sus dispositivos personales en la red interna de la entidad, por lo que es preciso aplicar controles de seguridad apropiados para proteger los datos de la compañía [2]. El uso de terminales privados para los negocios presenta riesgos, como la fuga de información comercial o personal de un empleado.

La llegada de BYOD a los lugares de trabajo está aumentando, adicional la amenaza a la seguridad de los datos dentro de las organizaciones que han adoptado tal tendencia [3][4]. Sin embargo, a diferencia de los dispositivos controlados por entidades, los dispositivos personales representan una amenaza para los recursos de información de la entidad debido a la flexibilización de las normas de accesibilidad que deben ser adoptadas para autorizar a los dispositivos personales a ingresar a las redes. Esto se está transformando cada vez más en un desafío para las entidades de tamaño mediano debido a sus iniciativas de disminución de gastos y a la imposibilidad de implementar soluciones de protección costosas [5]. La evaluación de la seguridad es un importante recurso de administración para lograr un funcionamiento correcto. Debemos estar informados de los peligros de seguridad de la red y adoptar medidas de protección efectivas.

1.1 Revisión de literatura

Los ataques de baja tasa de denegación de servicios envían ráfagas de ataques de forma intermitente a la red, lo que puede degradar gravemente la calidad de servicio del sistema víctima. La naturaleza de baja tasa de estos ataques complica la detección de estos [6].

Los últimos progresos de la tecnología y de las telecomunicaciones han contribuido a la eficacia de la transmisión de datos en los sistemas de monitoreo o control. No obstante, los sistemas de control también son vulnerables a los ataques informáticos, así mismo son una gran preocupación para el desarrollo de los sistemas de control en red, y el incremento de la resistencia a los ciberataques en un tema importante [7].

Descubrimos dos patrones de ataque DoS que tiene consecuencias diferentes. El primer patrón es que el agresor se oculta no modificando la posibilidad de una decodificación exitosa, sino incrementando el costo de la energía de transmisión; el segundo patrón es que tanto el costo del mando como el de la comunicación se incrementan por cambio en la probabilidad de una decodificación exitosa con la inyección del atacante [8].

Los cortafuegos son la principal línea defensiva contra los ataques y las amenazas que apuntan a las redes. La función principal de un cortafuegos es el filtrado del tráfico que ingresa y sale de una red. Esto se hace de conformidad con una política de filtrado predeterminada, que generalmente se elabora para que permita o impida el tránsito de un paquete [9].

Los ataques DoS son realizados por enrutadores atacantes que pueden ser programados sin un detallado conocimiento de la arquitectura de los sistemas objetivo. Por lo tanto, incluso los agresores con escasa información sobre los controles pueden crear

una violación de la seguridad a través de los ataques DoS [7]. Con el incremento de las violaciones de la seguridad en las empresas e instituciones que archivan, sostienen y colaboran con información crítica, es preciso disponer de una solución que refuerce la protección y mitigue los riesgos, que funcione sobre la marcha y sea factible de aplicar [10]. Las víctimas de este tipo de ataques son a menudo servidores de macroempresas y microempresas como lo son banca, el comercio, empresas de medios de comunicación y las microempresas que recién establecen sus protocolos de seguridad [11].

El objetivo de este estudio es cómo atenuar los riesgos, vulnerabilidades y amenazas en organizaciones que brindan servicios de telecomunicaciones, con el fin de mejorar los protocolos de seguridad, aplicándolos correctamente y a su vez estos sean respetados en todas sus fases.

1.2 Protocolo de investigación

El método deductivo se emplea para revisar y evaluar la información de referencia con el fin de reforzar la protección de las entidades de servicios de telecomunicaciones. Los productos resultantes son: un patrón que permite atenuar el riesgo dentro de las organizaciones. Se ha concluido que la ejecución de los esquemas de atenuación puede aportar a la reducción de los riesgos, pero esto dependerá de la entidad y la correcta implementación.

Table 1. Preguntas de investigación

Preguntas de Investigación	Motivación
¿Cuál es la importancia de la mitigación de riesgos?	Es de vital importancia ya que este tipo de entidades manejan información sensible de clientes a nivel nacional.
¿Qué efecto tiene el método a implementar?	Permite revisar y evaluar la información a través de las búsquedas realizadas.
¿Qué protocolos, normas, materiales se usan para implementar el modelo elegido?	Determinar protocolos y herramientas que se usan para evaluar e implementar un correcto esquema de seguridad.

En la Tabla 1 se exponen las preguntas de investigación, al momento de realizar el análisis de los artículos relacionados, se identifican esquemas, protocolos de seguridad que esta investigación propone mejorar lo antes mencionado.

1.3 Alcance de la investigación

Hoy en día los trabajos de investigación disponen de una gran cantidad de bibliotecas virtuales que disponen de variedad de artículos publicados relacionados con lo expuesto es por ello que nos hemos enfocado en el análisis de distintos protocolos de seguridad para la mitigación de amenazas y vulnerabilidades en las organizaciones de telecomunicaciones a nivel nacional en el Ecuador.

2 Materiales y métodos

Los métodos y materiales utilizados en esta investigación se fundamentan en el análisis de los artículos de referencia y en la secuencia de información general que todavía está en la fase de obtener resultados. Todas las tareas propuestas se cumplen siempre y cuando se cuente con una revisión y evaluación de los sistemas informáticos, conociendo los equipos detalladamente para desglosar el tipo de utilización y eficiencia. La función principal de los métodos antes mencionados es de detectar y analizar los incidentes que presentan las redes monitoreadas. Esto se lleva a cabo mediante una serie de indicadores de compromiso que permite tener una idea general del tipo de actividad que se está monitoreando, cuando se de algún evento el primer paso es verificar que efectivamente se trate de un incidente de seguridad y no de un falso positivo.

2.1 Medidas de prevención

Este apartado pretende aplicar diferentes niveles de seguridad en la propia infraestructura de la red, ya que es la manera de acceso a los diferentes servicios que se brindan. Cualquiera de las acciones para tener en cuenta es que, por ejemplo, en el caso de tener servicios en línea dentro de una red corporativa, debido a que podemos establecer fácilmente capas de seguridad como una lista de acceso en la base a las IP de los solicitantes o firewall.

— *Protección de red*

La aplicación de niveles de seguridad es indispensable ya que es el primer canal de acceso a los recursos. Es estos dispositivos, como los enrutadores, se puede llevar a cabo la configuración del control de acceso, se pueden gestionar IPs válidas, etc. También es recomendable contar con un ancho de banda considerable para evitar los ataques de inundación ICMP, entre otros.

— *Configuración de equipos*

Es fundamental mantener el software correctamente actualizado para impedir algún tipo de ataque, de lo contrario este punto sería fundamentalmente el más vulnerable. También es vital comprobar la configuración de los enrutadores y el cortafuegos para detectar las IPs inválidas.

— *Tráfico*

Es recomendable limitar el impuesto de tráfico que llega desde un único host con el objetivo de advertir un ataque DoS que busquen saturar el servidor. El tráfico a menor escala tiene las particulares de la no linealidad y el caos. Aunque la proyección es relativamente compleja, la estimación del transporte de red a pequeña escala puede hacer que la representación de los diferentes estados de la red se realice en tiempo real. Cuando se produce un ataque el tráfico variará. Por ello es importante la proyección del flujo de tráfico a menor escala y la identificación de la amenaza para adoptar decisiones

eficaces y a su vez pueda aumentar en gran medida la capacidad de subsistencia de la red [12].

— *Lista de IP bloqueada*

En los últimos tiempos ha ocurrido un fuerte incremento de los ataques cibernéticos. Es por lo que, un firewall deberá comprobar todas las debilidades comunes y hacer frente a los daños en el cliente. Este firewall deberá tener un mecanismo de verificación y filtrado de entrada eficaz [13]. Esta medida de seguridad se puede implementar de forma manual o automática a través de la lista de bloqueo del firewall.

— *Redundancia y balance de carga*

Consiste en disponer de un duplicado activo en más de un servidor y el equilibrio de carga permite designar un servidor u otro en función de la capacidad de trabajo que soporta. Esta medida disminuye el riesgo de padecer uno de estos ataques, ya que al tener más de un servidor se disminuye la posibilidad de que se detenga por sobrecarga.

— *Control de acceso*

El control de acceso es de vital importancia y el requisito principal a cumplir dentro de una organización asegura que solo el personal o los dispositivos autorizados podrán acceder a los componentes de la red, la información registrada, los flujos de datos, los procedimientos y aplicaciones, lo cual nos permitirá salvaguardar los activos de información dentro de las organizaciones [14].

— *Cifrado*

Las estrategias de cifrado son cruciales para cualquier empresa que use la nube y son una excelente manera de proteger los discos duros, los datos, etc. que están en camino por buscadores o en la nube. El cifrado no debe dejarse hasta el final y debe integrarse cuidadosamente en la red y el flujo de trabajo existente para tener el mayor éxito. Se adopta este tipo de técnica para el cifrado de datos a fin de proporcionar una comunicación segura a través de la red[15].

— *Escaneo de sistemas operativos*

El análisis de las vulnerabilidades nos permite detectar fallos de seguridad en un sistema operativo y sus servicios. Si llegamos a conocer la vulnerabilidad de cualquier software a su debido tiempo, actuara como una alarma activa [16].

2.2 Herramienta de prevención

Es de vital importancia que conociendo las medidas de prevención conocer la herramienta que nos ayuda a la prevención de amenazas.

— *Seguridad DNS*

Asegurar el DNS de ataque DoS y proteger las respuestas DNS para que no sean enviadas a otros sitios ayudara a que las aplicaciones del negocio estén siempre disponibles

y visibles al mundo. Hoy en día, el uso de los servicios DNS no es solo para traducir nombres de dominio, sino que también se usa para bloquear el correo no deseado, la autenticación de correo electrónico, por lo tanto, todas las aplicaciones de Internet utilizan DNS, si este no funciona correctamente, toda la comunicación colapsará. Es por ello que las infraestructuras de DNS es uno de los requisitos fundamentales para cualquier organización en el ámbito actual de la seguridad cibernética. DNS aborda los problemas de integridad y disponibilidad al establecer una cadena de confianza utilizando datos de DNS firmados digitalmente, los protocolos de seguridad deben ser endurecidos para evitar amenazas y ataques maliciosos [17]. En la Figura 1 podemos visualizar el correcto funcionamiento de DNS aplicado en las organizaciones, lo cual garantiza la resolución óptima de las direcciones IP y nombres host.

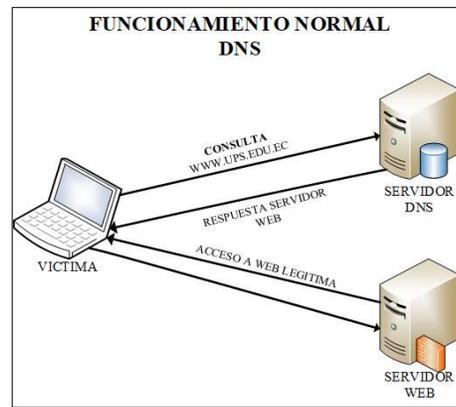


Fig. 1. Funcionamiento DNS

— *Detección de intrusos*

Consiste en detectar anomalías, insuficiencias o errores en las operaciones desde el exterior o el interior de un dispositivo o infraestructura de red. El IDS se basa en la teoría de que el comportamiento de un intruso es distinto al de un usuario auténtico, que se emplea para la identificación mediante el cálculo de las estadísticas de uso. Este modelo tiene como finalidad de determinar los patrones de comportamiento del usuario con el manejo de programas, archivos y dispositivos, tanto a corto como a medio y largo plazo, para que la detección sea efectiva; también utiliza un sistema de reglas predefinidas como “firmas” para la representación de infracciones conocidas.

En una red de comunicaciones, un IDS no solo analiza que tipo de tráfico se está utilizando, sino que también estudia su contenido y comportamiento; también detecta si está transmitiendo escaneo de puertos o paquetes de datos mal estructurados, entre otros aspectos.

Un IDS suele estar integrado con un cortafuegos, preferiblemente en un dispositivo que actúa como una puerta de enlace de red. En la compilación de cada uno de los enfoques, también se pueden descubrir ataques adicionales de falsos positivos y falsos

negativos [18]. Las herramientas estudiadas permitirán reducir el volumen de paquetes a ser procesados para el mismo sistema de control de infracciones, pues nos permitirá identificar y procesar el tráfico que no se le considera un ataque dañino (flechas verdes) o posibles amenazas (flechas rojas).

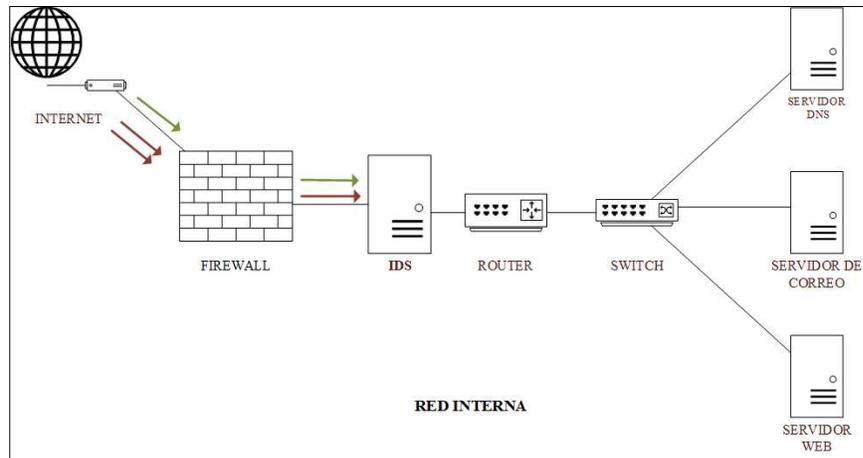


Fig. 2. Representación de defensa activa.

Con la figura 2 se logra identificar que una demanda de segundas líneas de seguridad más prometedoras después de los cortafuegos. Estos sistemas deben tener la capacidad de escanear los registros de red para la integridad, privacidad y disponibilidad de estos sistemas. La detección de intrusiones como cualquier conjunto de acciones que compromete los puntos antes mencionados [19]. Es así como implementamos IDS basado en firmas, anomalías agregar una función de enfoque de bloque (firewall) para mitigar el nodo de ataque drenando la energía del atacante.

2.3 Criterios a considerarse

Análisis de vulnerabilidades

El estudio de las vulnerabilidades se emplea para explotar cualquier punto débil de una máquina, una red o una infraestructura de comunicaciones, fijando prioridades y ocupándose de cada una con planes de protección, detección y respuesta.

Nivel de criticidad de vulnerabilidades

Con este proceso de análisis interno se demuestra hasta donde es posible acceder, a que datos se pueden capturar y el daño que se puede generar a una organización por agujeros de seguridad o fallos en la ciberseguridad. Es necesario y tener una idea clara del nivel de criticidad de vulnerabilidades:

Table 2. Niveles de vulnerabilidad

TIPOS	DESCRIPCIÓN
Baja	Vulnerabilidades en el cual no se percibe riesgo de explotación a la disponibilidad, integridad y confidencialidad de la información y servicios.
Media	Comprende vulnerabilidad con capacidad baja de explotación.
Alta	Comprende vulnerabilidad con mayor posibilidad de acceso a la información haciéndola vulnerable a cualquier tipo de ataque.
Crítica	Es capaz de poner en riesgo efectivo la explotación de los pilares fundamentales de la seguridad de la información: Disponibilidad, integridad y confidencialidad de los datos.

Con la Tabla 2 podemos tener una perspectiva clara de los niveles de vulnerabilidad a los cuales están expuestas este tipo de organizaciones, al identificar estos factores permitirá establecer un esquema eficaz al momento de implementar un sistema de defensa.

— Pruebas de intruso

El análisis de amenazas puede incluir la búsqueda de fallas en una red o un programa, o la comprobación de intrusiones, se lo considera como una alternativa viable detectar las debilidades con anticipación y elaborar un plan para resolverlas. Así mismo es una opción favorable contar con planes de contingencia.

Si existen fallos en el sistema operativo, errores en los valores predeterminados u otras fallas semejantes, un gestor de red con experiencia en pruebas de invasión puede ayudarle a detectar estos inconvenientes y aplicar correcciones para que sea menos propenso a sufrir un ataque. Se crea un marco de prevención de la filtración de información para la protección de los datos confidenciales e impide la revelación de datos a los terceros implementando el diseño IDS para lograr un filtrado de alarmas [20].

Las evaluaciones de ataques consisten en la aplicación de procedimientos manuales o de autoaprendizaje que interrumpirán los servicios, las aplicaciones, las redes e incluso los dispositivos de usuario final para ver la intrusión.

En la figura 3 podemos visualizar el correcto funcionamiento al momento de implantar IDS en las organizaciones, junto al firewall y una base de datos actualizada con las firmas de detección de ataques se lo considera una herramienta óptima de prevención.

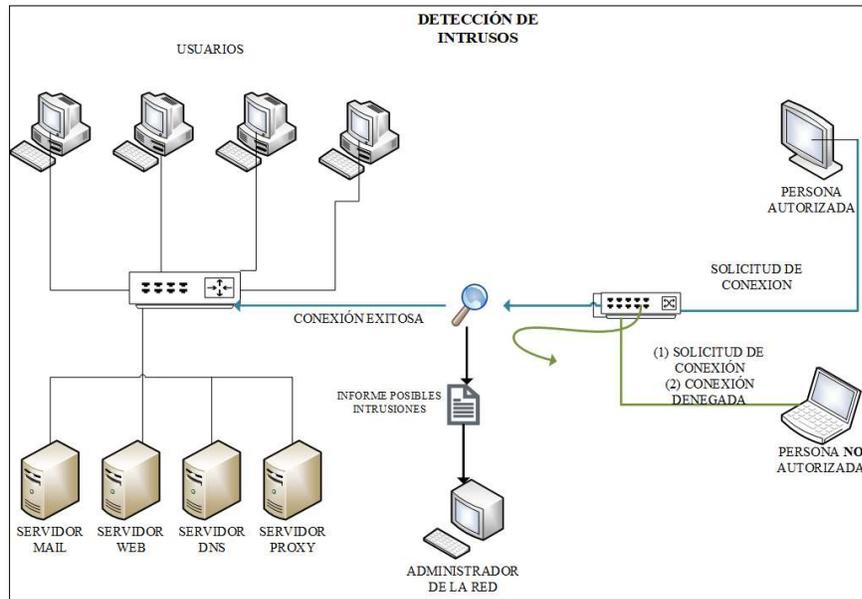


Fig. 3. Detección de intrusos

2.4 Fases de prevención

Se realizó el análisis de distintas fases, adicional se discutieron los casos de estudios de medidas implementadas en otros trabajos realizados. La Figura 4 se demuestra en un prototipo para la atenuación de las irregularidades, las debilidades y amenazas en empresas de servicios telecomunicaciones con 4 fases y 3 sub-fases.

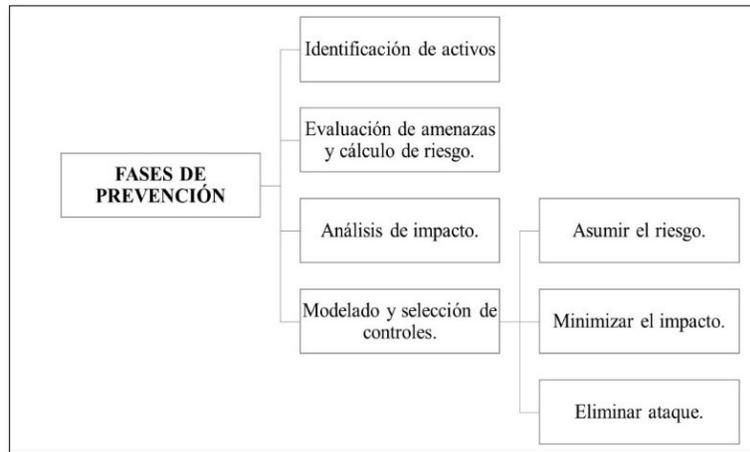


Fig. 4. Fases de prevención de amenazas.

1. Detección de amenazas

Una amenaza se puede definir como cualquier evento que pueda alterar los bienes de información y que esté relacionado sobre todo con los recursos humanos, los acontecimientos naturales o los fracasos técnicos. Una vez que se han conocido los riesgos, los activos a proteger y la manera en que su destrucción o ausencia puede afectar a la organización, es preciso determinar cada una de las amenazas y vulnerabilidades que pueden causar la pérdida de estos activos.

2. Modelo de seguridad

En la Tabla 3 obtenemos la descripción las fases de seguridad de la información ya que es de vital importancia conocer sobre los pilares fundamentales de la seguridad de la información:

Table 3. Pilares fundamentales de la seguridad de la información.

FASE	DESCRIPCIÓN
Integridad	Permite identificar al generador de la información y que se logra con los correctos accesos de usuario y con otros sistemas. La integridad hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones o alteraciones de terceros.
Confidencialidad	Es básicamente la propiedad por la que esa información solo resultara accesible con la debida y comprobada autorización.
Disponibilidad	Información a la que podemos acceder cuando la necesitamos a través de los canales adecuados siguiendo los procesos correctos.
Autenticación	Información procedente de un usuario que es quien dice ser. Se valida y se debe garantizar que el origen de los datos es correcto.

La tabla nos ayuda identificar las fases del modelo de seguridad lo que nos ayudara elegir un esquema factible de información, adicional en este módulo debemos evaluar 3 fases del IDS: detección de ataques, recopilación de información y por último bloqueo de ataque, IDS basados en firmas y anomalías se lo conoce como un diseño híbrido propuesto que pretende mejorar los sistemas de detección y prevención de intrusos [21].

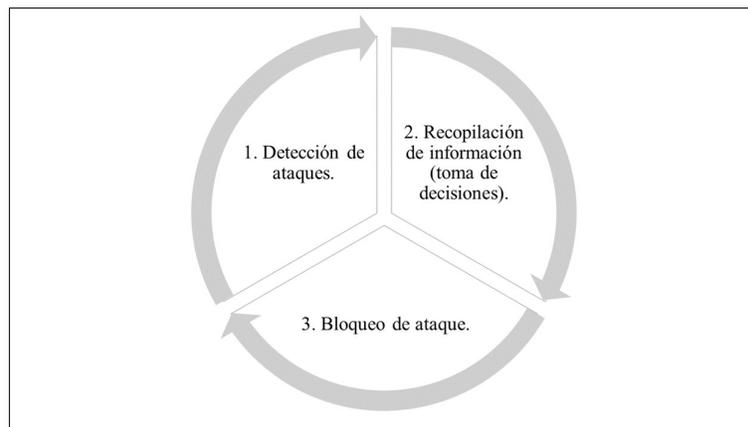


Fig. 5. Fases de herramientas IDS

En la Figura 5 se indican las etapas que se han de aplicar y que deberían ser desarrolladas por ciclos, ya que la siguiente fase dependerá de la precedente, creándose así un círculo de análisis continuo, con las fases previamente establecidas nos permite identificar el tipo de ataque, nos ayuda con la toma de decisiones al momento de implementar protocolos de seguridad eligiendo una opción viable para prevenir ataques o reaccionar al momento de recibirlos con la estrategia de firmas actualizadas constantemente implementando IDS basado en firmas y anomalías lo cual junto al firewall realizara el bloqueo del ataque.

3 Resultados

En esta búsqueda, se planteó un esquema de defensa activa. Este esquema hace la detección y protección en base a las grandes diferencias de datos y de tiempo entre ellos y el esquema de exploración de los consumidores estándar.

Proponen algoritmos para reconocer ataques ocultos, posibles y latentes. Además, identifican los ataques de manera conjunta, ofreciendo sus propias estadísticas de detección. Con el fin de reducir los potenciales riesgos en una entidad, es preciso establecer unas políticas de defensa en sus distintos niveles, así como establecer un área estratégica de TIC.

Administración de recursos

Según la ISO 27001 son los recursos del sistema de seguridad de la información, los mismos que son necesarios para que las entidades funcionen correctamente y esta a su vez logre los objetivos propuestos. La gestión de la seguridad de la información se ha convertido en una de las esferas clave en el sistema de gestión de la seguridad de la información se ha convertido en una gran preocupación de las empresas para mejorar el nivel de gestión estratégica. Las normas ISO 27001 son un sistema de prueba del sistema funcional de protección de la información [22].

Monitoreo de amenazas

El control del tráfico de la red se hace a través de mecanismos y protocolos, así como un riguroso seguimiento del análisis de los registros a través de las aplicaciones. Por otra parte, una vez determinados los parámetros y puntos vulnerables descubiertos en la red, se adoptarán disposiciones de protección. Los indicadores que se han analizado en las pruebas son la alteración y la falta de paquetes.

Ya que son los parámetros que influyen en la calidad del servicio. Por último, el indicador más destacado es el tiempo de suspensión, que permitió conocer el tiempo exacto en el que el servicio no estaba operativo lo que a su vez a la nueva calidad de servicio capaz de vigilar y detectar amenazas internas [23].

Normativa ISO 27001

Se puede construir una directiva de seguridad de la información global como una extensión de la política de seguridad local de las distintas entidades, evitando comenzar de nuevo. Numerosas empresas padecen importantes pérdidas a causa de la materialización de riesgos vinculados a la política “Bring Your Own Device”, por falta de mejores prácticas y estándares de protección de la información aplicados y conservados. Con el fin de tratar de mejor manera las vulnerabilidades de seguridad causadas con la implementación de nuevos servicios y normas como la política BYOD, es preciso medir el nivel de madurez en el manejo seguro del mismo [24]. Las normas ISO 27001 son un esquema de valoración del sistema operativo de seguridad de la información. Este prototipo se fundamenta en la normativa ISO/IEC 27001 con el propósito de reducir los posibles riesgos para la protección de la información. Para la valoración de la aplicación correcta de los procedimientos es preciso seguir los siguientes procesos:

Table 4. Cumplimientos de procesos de seguridad

PROCESO	TAREA
DIRECCIÓN DE ESTRATEGIAS	Aplicación de normas de forma regular.
	Optimización de procesos.
	Aplicación correcta de procesos.
SEGURIDAD TI	Cumplimientos de actividades de organizaciones políticas.
	Cumplimiento de procesos.
	Verificación de recursos

El volumen de los procedimientos de cada entidad variará en función de sus objetivos estratégicos. Para atenuar los riesgos potenciales para la integridad de una entidad, es indispensable establecer normas de protección a nivel estratégico, táctico y operacional, y definir el departamento estratégico de TIC a nivel de la dirección. Las directrices de seguridad y las recomendaciones son necesarias para crear la herramienta de evaluación de la implementación de seguridad [25]. Los resultados obtenidos de esta investigación dan una orientación para establecer una modalidad para el diseño en una organización, teniendo en consideración sus requerimientos encontrados en las revisiones de trabajos previos. Ayuda a considerar una estrategia clara y concreta sobre los tipos de amenazas y los niveles de seguridad que deben ser rigurosamente implementados para prevenir este tipo de daños dentro de la organización. Se ofrece una alternativa que ayuda a atenuar los riesgos en la seguridad de la información.

4 Conclusiones

Con el estudio de los puntos antes mencionados logramos los objetivos previamente establecidos, ya que la investigación nos permite identificar las fases de cada proceso de seguridad a su vez nos ayuda a tener ideas claras de lo que necesitan este tipo de organizaciones e identificar las distintas amenazas a las que pueden estar expuestas diariamente. Comprendiendo que las distintas fases deben ser respetadas para evitar ataques dentro de la organización.

Así mismo como es de vital importancia conocer las fases de seguridad es recomendable conocer los tipos de ataques a los que las empresas de telecomunicaciones están sometidas diariamente ya que ayudara a definir prototipos de seguridad de información mejorando los protocolos de seguridad, que al aplicarse correctamente nos ayudara a reducir o evitar los ataques.

Las empresas de telecomunicaciones cuentan con protocolos de seguridad para prevenir amenazas o ataques, es por ello que analizando la información referenciada nos permitió en esta investigación tener una idea clara sobre los tipos de ataques, los niveles de seguridad y las distintas herramientas que podemos implementar para evitar este tipo de actos que buscan perjudicar a las organizaciones que prestan este tipo de servicios.

Al finalizar esta investigación podemos concluir los distintos escenarios a los cuales están expuestas este tipo de organizaciones y la vital importancia de un modelo de seguridad en el cual se apliquen las políticas necesarias para correcta protección de la información acompañado de un modelo de defensa activa el cual nos ayudara mediante filtros estar preparados a las distintas anomalías presentadas y así garantizar los pilares fundamentales de la seguridad de la información.

Referencias

1. Mary, D.S.N., Begum, A.T.: An algorithm for moderating DoS attack in web based application. Proc. - 2017 Int. Conf. Tech. Adv. Comput. Commun. ICTACC 2017. 2017-Octob, 26–31 (2017).

- <https://doi.org/10.1109/ICTACC.2017.17>.
2. Ratchford, M.M., Wang, Y.: Byod-insure: A security assessment model for enterprise byod. 2019 5th Int. Conf. Mob. Secur. Serv. MOBISECSERV 2019. 1–10 (2019). <https://doi.org/10.1109/MOBISECSERV.2019.8686551>.
 3. Tanimoto, S., Yamada, S., Iwashita, M., Kobayashi, T., Sato, H., Kanai, A.: Risk assessment of BYOD: Bring your own device. 2016 IEEE 5th Glob. Conf. Consum. Electron. GCCE 2016. 16–19 (2016). <https://doi.org/10.1109/GCCE.2016.7800494>.
 4. Morolong, M., Gamundani, A., Bhunu Shava, F.: Review of Sensitive Data Leakage through Android Applications in a Bring Your Own Device (BYOD) Workplace. 2019 IST-Africa Week Conf. IST-Africa 2019. 1–8 (2019). <https://doi.org/10.23919/ISTAFRICA.2019.8764833>.
 5. Seneviratne, B.L.D., Senaratne, S.A.: Integrated Corporate Network Service Architecture for Bring Your Own Device (BYOD) Policy. 2018 3rd Int. Conf. Inf. Technol. Res. ICITR 2018. (2018). <https://doi.org/10.1109/ICITR.2018.8736155>.
 6. Tang, D., Dai, R., Tang, L., Li, X.: Low-rate DoS attack detection based on two-step cluster analysis and UTR analysis. *Human-centric Comput. Inf. Sci.* 10, (2020). <https://doi.org/10.1186/s13673-020-0210-9>.
 7. Wakaiki, M., Cetinkaya, A., Ishii, H.: Stabilization of networked control systems under DoS attacks and output quantization. *arXiv.* 65, 3560–3575 (2017).
 8. Zhang, Y., Chen, C., He, J.: DoS Attack on Networked Control System: From the Viewpoint on Communication-Control Cost. *Proc. - 2019 Chinese Autom. Congr. CAC 2019.* 5695–5700 (2019). <https://doi.org/10.1109/CAC48633.2019.8997270>.
 9. Trabelsi, Z., Zeidan, S.: Resilience of network stateful firewalls against emerging DoS attacks: A case study of the blacknurse attack. *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. AICCSA. 2019-Novem,* 0–7 (2019). <https://doi.org/10.1109/AICCSA47632.2019.9035323>.
 10. Shrivanya, G., Swati, N.H., Rustagi, R.P., Sharma, O.: Securing Distributed SDN Controller Network from Induced DoS Attacks. *Proc. - 2019 8th IEEE Int. Conf. Cloud Comput. Emerg. Mark. CCEM 2019.* 9–16 (2019). <https://doi.org/10.1109/CCEM48484.2019.000-4>.
 11. Liang, L., Zheng, K., Sheng, Q., Wang, W., Fu, R., Huang, X.: A denial of service attack method for iot system in photovoltaic energy system. *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics).* 10394 LNCS, 613–622 (2017). https://doi.org/10.1007/978-3-319-64701-2_48.
 12. Su, Y., Meng, X., Meng, Q., Han, X.: DDoS Attack Detection Algorithm Based on Hybrid Traffic Prediction Model. 2018 IEEE Int. Conf. Signal Process. Commun. Comput. ICSPCC 2018. 1–5 (2018). <https://doi.org/10.1109/ICSPCC.2018.8567771>.
 13. Nagendran, K., Balaji, S., Raj, B.A., Chanthrika, P., Amirthaa, R.G.: Web Application Firewall Evasion Techniques. 2020 6th Int. Conf. Adv. Comput.

- Commun. Syst. ICACCS 2020. 194–199 (2020). <https://doi.org/10.1109/ICACCS48705.2020.9074217>.
14. Uddin, M., Islam, S., Al-Nemrat, A.: A Dynamic Access Control Model Using Authorising Workflow and Task-Role-Based Access Control. *IEEE Access*. 7, 166676–166689 (2019). <https://doi.org/10.1109/ACCESS.2019.2947377>.
 15. Base, D.N.A.: Sequence. (2017).
 16. Majumder, R., Som, S., Gupta, R.: Vulnerability prediction through self-learning model. *2017 Int. Conf. Infocom Technol. Unmanned Syst. Trends Futur. Dir. ICTUS 2017. 2018-Janua*, 400–402 (2018). <https://doi.org/10.1109/ICTUS.2017.8286040>.
 17. Jalalzai, M.H., Shahid, W.B., Iqbal, M.M.W.: DNS security challenges and best practices to deploy secure DNS with digital signatures. *Proc. 2015 12th Int. Bhurban Conf. Appl. Sci. Technol. IBCAST 2015*. 280–285 (2015). <https://doi.org/10.1109/IBCAST.2015.7058517>.
 18. Khan, S., Motwani, D.: Implementation of IDS for web application attack using evolutionary algorithm. *Proc. 2017 Int. Conf. Intell. Comput. Control. I2C2 2017. 2018-Janua*, 1–5 (2018). <https://doi.org/10.1109/I2C2.2017.8321956>.
 19. Bello, F.L., Ravulakollu, K., Amrita: Analysis and evaluation of hybrid intrusion detection system models. *Proc. - 2015 Int. Conf. Comput. Commun. Syst. ICCCS 2015. 93–97* (2016). <https://doi.org/10.1109/CCOMS.2015.7562879>.
 20. Bouzar-Benlabiod, L., Meziani, L., Chebieb, A., Rim, N.E., Mellal, Z.: Experts' knowledge merging to reduce IDS alerts number. *Proc. - 2016 Int. Conf. Collab. Technol. Syst. CTS 2016. 418–423* (2016). <https://doi.org/10.1109/CTS.2016.78>.
 21. Shurman, M.M., Khrais, R.M., Yateem, A.A.: IoT denial-of-service attack detection and prevention using hybrid IDS. *Proc. - 2019 Int. Arab Conf. Inf. Technol. ACIT 2019. 252–254* (2019). <https://doi.org/10.1109/ACIT47987.2019.8991097>.
 22. Wang, C., Guo, E., Chen, S., Zhu, S., Wu, J.: Appraisal of mask manufacture information security based on ISO27001 and common criteria. *IEEE Int. Conf. Ind. Eng. Eng. Manag. 2017-Decem*, 2317–2320 (2018). <https://doi.org/10.1109/IEEM.2017.8290305>.
 23. Sarma, M.S., Srinivas, Y., Abhiram, M., Ullala, L., Prasanthi, M.S., Rao, J.R.: Insider threat detection with face recognition and KNN user classification. *Proc. - 2017 IEEE Int. Conf. Cloud Comput. Emerg. Mark. CCEM 2017. 2018-Janua*, 39–44 (2018). <https://doi.org/10.1109/CCEM.2017.16>.
 24. Hajdarevic, K., Allen, P., Spremic, M.: Proactive security metrics for Bring Your Own Device (BYOD) in ISO 27001 supported environments. *24th Telecommun. Forum, TELFOR 2016. 3–6* (2017). <https://doi.org/10.1109/TELFOR.2016.7818717>.
 25. Podzins, O., Romanovs, A.: Designing a evaluation tool for IT security solution implementation for IT enterprises. *2016 IEEE 4th Work. Adv. Information, Electron. Electr. Eng. AIEEE 2016 - Proc.* (2017). <https://doi.org/10.1109/AIEEE.2016.7821828>.

