



**UNIVERSIDAD TÉCNICA DE BABAHOYO**

**FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA**

**PROCESO DE TITULACIÓN**

**DICIEMBRE 2021 - ABRIL 2022**

**EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA  
PRÁCTICA**

**SISTEMAS DE INFORMACIÓN**

**PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS DE  
INFORMACIÓN**

**TEMA:**

Análisis de los problemas de seguridad y redes en la empresa de internet Netline.

**EGRESADA:**

Zamora Candelario Helen Damaris

**TUTOR:**

Ing. Wellington Isaac Maliza Cruz

**AÑO 2022**

## **CONTENIDO**

Planteamiento del problema .....	156
Justificación.....	158
Objetivos del estudio .....	160
Objetivo general .....	160
Objetivos específicos.....	160
Línea de Investigación.....	161
Marco conceptual .....	162
Marco metodológico.....	174
Resultados.....	175
Discusión de resultados .....	177
Conclusiones.....	179
Recomendaciones .....	180
Referencias .....	181

## **PLANTEAMIENTO DEL PROBLEMA**

La seguridad de la red es una de las consideraciones más importantes en el campo de la seguridad de la información hoy en día con la expansión de las dependencias de los sistemas comerciales en las infraestructuras basadas en TI. La falta de medidas de seguridad en la infraestructura de TI puede causar daños irreparables a las organizaciones y empresas que no son deseables para los procesos comerciales y de marketing.

El propósito de la seguridad de la red es principalmente evitar daños por el mal uso de los datos. Hay una serie de problemas potenciales que pueden ocurrir si la seguridad de la red no se implementa correctamente. Todas las empresas deberán mantener cierta información crítica y clasificada fuera del acceso de sus competidores.

La pérdida de datos puede disminuir el valor agregado en el proceso de producción y comercialización de piezas. Además, la verdadera forma de moverse en el negocio y la comercialización de productos puede perderse debido a la manipulación de datos como consecuencia de la falta de medidas de seguridad en la información financiera. Como resultado, la falta de medidas de seguridad en la web de datos puede causar la violación de la confidencialidad en los diferentes negocios y comercialización de productos.

Por lo tanto, es fundamental que cualquier administrador de red utilice políticas estrictas para evitar posibles pérdidas, independientemente del tamaño y tipo de red. Es un conjunto de políticas, regulaciones y arreglos desarrollados por un administrador o administradores de red para prevenir y monitorear el acceso no autorizado, el uso indebido, la corrección, la prevención de cambios o la restricción del acceso a redes informáticas y recursos accesibles a la red.

La empresa Netline, se encuentra ubicada en el Cantón Urdaneta, en la parroquia Ricaurte. Su dirección es Av. Emiliano Pinoargote y Bartolomé Bastidas, junto a la comercializadora de productos agrícolas a Fertisa. Su representante legal es el señor Benjamín

Franklin Pérez Ponce identificado con el número de RUC es 1204729535001, cuyo giro de negocio está relacionado con las actividades de reventa de servicios de telecomunicaciones (suministro de servicios telefónicos y de internet en instalaciones abiertas al público: cabinas telefónicas y cibercafés.), información que fue obtenida del portal del Servicio de Rentas Internas.

En la mayoría de las empresas de telecomunicaciones a pesar de que se trata de proteger la información de la mejor manera posible, todavía se evidencia que las seguridades se implementan con carácter reactivo y no preventivo, es decir, se corrige el problema cuando éste ocurre y no se mantiene un proceso de gestión que se encargue de salvaguardar la seguridad de los sistemas.

Para ello, en el presente caso de estudio se plantea realizar el Análisis de los problemas de seguridad y redes en la empresa de internet Netline, considerando como un factor crítico incrementar la seguridad para proteger la información importante de la empresa, debido a que una red empresarial no solo se necesita tener conectados a los usuarios sino también salvaguardar la información que se gestiona en ella.

En el presente trabajo de investigación, se categorizan diferentes temas de trabajos de investigación en las amenazas de red y medidas de seguridad para proporcionar un estudio de caso en el campo de interés. Como resultado, se obtienen nuevas ideas para los sistemas de seguridad de redes y lagunas en la literatura existente y también se sugieren futuros trabajos de investigación para impulsar este interesante campo de investigación.

## JUSTIFICACIÓN

Hoy en día la información es uno de los activos más importantes para toda organización, sin embargo, es uno de los recursos más expuestos a vulnerabilidades, teniendo la necesidad de proteger este valioso activo de amenazas internas y externas. Actualmente las empresas necesitan que la información que manejan esté siempre en alta disponibilidad, íntegra sin alteraciones en sus datos y sea confiable en su procesamiento.

Es necesario e importante tener un vasto conocimiento acerca de las redes de datos, incluyendo todos sus componentes, y desde luego se tiene que tener implementado las condiciones necesarias para poder controlar los accesos desde redes externas a la red privada de la empresa, llevando a cabo un análisis de los problemas de seguridad para poder tomar las decisiones pertinentes, por luego elaborar un esquema de seguridad bien estructurado para así evitar que la empresa se encuentre expuesta a vulnerabilidades logrando tener la red segura y eficiente para las operaciones normales de la organización.

Tener un buen sistema de seguridad de información, brinda la calidad de seguridad de información de una forma normalizada, que pretende ayudar a optimizar el control y gestión de la seguridad de la red, minimizando riesgos de daño o pérdida de información y además permitiendo cumplir los tres objetivos principales de la seguridad de la información; los cuales son la integridad, confidencialidad y disponibilidad de la misma.

Para Netline, una empresa que brinda servicios internet para hogares que gestiona información sensible y confidencial, es necesario realizar un análisis de los problemas seguridad en la red que garantice el rendimiento, disponibilidad y escalabilidad de la misma.

El desarrollo del análisis de los problemas seguridad en la red informática permitirá conocer las vulnerabilidades existentes en el manejo de la información física, así como la que está contenida en los sistemas de procesamiento de información, de tal forma que se puedan

tomar acciones preventivas y correctivas dentro de la organización, para evitar que se lleguen a comprometer datos confidenciales.

En síntesis de lo antes mencionado, la empresa Netline, tiene la necesidad de implementar un departamento de riesgos y seguridad de la información los cuales vieron que el enfoque tradicional que consistía en implementar únicamente firewalls y soluciones de virus ya no es suficiente, adquiriendo la necesidad de realizar un Análisis de los problemas de seguridad y redes, para resguardar su información y evitar actuales y futuros ataques, de ahí nace la importancia y la justificación del presente caso de estudio.

Mediante el análisis de los problemas de seguridad y redes, la empresa Netline podrá conocer estos problemas y poder aplicar los controles de seguridad pertinentes para salvaguardar la información que se maneja en ya mencionada empresa, para asegurarse que éste siendo utilizada adecuadamente y solo tenga acceso personas autorizadas.

## **OBJETIVOS DEL ESTUDIO**

### **Objetivo general**

Analizar de los problemas de seguridad y redes en la empresa de internet Netline.

### **Objetivos específicos**

- Conocer sobre el funcionamiento de las tecnologías seguridad y redes en la empresa de internet Netline.
- Examinar el riesgo actual y problemas de la seguridad y redes en la empresa de internet Netline.
- Proveer lineamientos de seguridad para garantizar la confidencialidad, disponibilidad e integridad de la información en la empresa de internet Netline.

## LÍNEA DE INVESTIGACIÓN

El presente caso de estudio se encuentra relacionado con la línea de investigación sistemas de información y comunicación, emprendimiento e innovación; además relacionada mutuamente con la sublínea de redes y tecnologías inteligentes de software y hardware, gestionadas por la coordinación de titulación de la facultad.

En el campo de los sistemas de información de gestión se supervisa el flujo y el comportamiento de la información digital de una empresa. Son responsables de asegurarse de que el uso compartido, el almacenamiento y la accesibilidad de los datos corporativos funcionen a niveles óptimos, sin fuerzas internas o externas que ralenticen estos y otros procesos.

Cuando se relaciona los sistemas de información y comunicación con la seguridad informática, es fácil encontrar algún cruce en las habilidades y responsabilidades. Por ejemplo, en ambas temáticas los profesionales deben asegurarse de que los sistemas de TI funcionen correctamente y tengan información actualizada sobre el estado de la red. Ambos puestos también requieren sólidas competencias analíticas para detectar las deficiencias del sistema. Las habilidades de pensamiento crítico y resolución de problemas son imprescindibles en ambos roles para evitar que las debilidades de seguridad causen problemas mayores.

Un administrador de sistemas de información se enfoca en la eficiencia de la red de una empresa, asegurándose de que los sistemas computarizados y los recursos en línea funcionen correctamente. Un especialista en ciberseguridad, por otro lado, busca principalmente debilidades y vulnerabilidades dentro del sistema de seguridad de una red.



## MARCO CONCEPTUAL

La seguridad de la RED es una de las consideraciones más importantes en el campo de la seguridad de la información hoy en día con la expansión de las dependencias de los sistemas comerciales en las infraestructuras basadas en TI. La falta de medidas de seguridad en la infraestructura de TI puede causar daños irreparables a las organizaciones y empresas que no son deseables para los procesos comerciales y de marketing.(Estrada et al., 2016)

El propósito de la seguridad de la red es principalmente evitar daños por el mal uso de los datos. Hay una serie de problemas potenciales que pueden ocurrir si la seguridad de la red no se implementa correctamente. Todas las empresas deberán mantener cierta información crítica y clasificada fuera del acceso de sus competidores. La pérdida de datos puede disminuir el valor agregado en el proceso de producción y comercialización de piezas. Además, la verdadera forma de moverse en el negocio y la comercialización de productos puede perderse debido a la manipulación de datos como consecuencia de la falta de medidas de seguridad en la información financiera.(Arellano Martínez, 2017)

Como resultado, la falta de medidas de seguridad en la web de datos puede causar la violación de la confidencialidad en los diferentes negocios y comercialización de productos. Por lo tanto, es vital que cualquier administrador de red utilice políticas estrictas para evitar posibles pérdidas, independientemente del tamaño y tipo de red. Es un conjunto de políticas, regulaciones y arreglos desarrollados por un administrador o administradores de red para prevenir y controlar el acceso no autorizado, el uso indebido, la corrección, la prevención de cambios o la restricción del acceso a las redes informáticas y los recursos accesibles de la red.

Para proporcionar las medidas de seguridad en la red de datos, los ataques deben estar claramente definidos. Un ataque es un intento peligroso o no peligroso de modificar o utilizar un recurso accesible a través de la red de una forma no prevista. Los ataques a la red se pueden clasificar en tres categorías generales:

- 1- Acceso no autorizado a recursos e información a través de la red.
- 2- Manipulación no autorizada de información en una red.
- 3- Ataques que conducen a la interrupción de la prestación del servicio y se denominan Denegación de servicios.

La palabra clave en las dos primeras categorías es realizar acciones ilegalmente. Definir una acción autorizada o no autorizada es responsabilidad de la política de seguridad de la red, que puede definirse como un intento de un usuario de ver o modificar información que no está permitida. El acceso no autorizado puede ser uno de los ataques más comunes en cualquier red. De esta forma, el atacante intenta acceder al área restringida de información ya la red. Romper contraseñas, crear subrutinas, crear identidades falsas o usar malware son las principales formas de llevar a cabo estos ataques.(Álvarez Roldán & Montoya Vargas, 2020)

La destrucción de información es una de las redes de ataque más destructivas. De esta forma, el atacante intenta destruir cierta información ejecutando comandos en la base de datos. Esta puede ser limitada o muy extensa. Dependiendo del tipo de atacante, la red puede perder toda su información en cuestión de segundos. Los ataques que conducen a la interrupción de la prestación del servicio son otra forma de acceso no autorizado. En este método, la persona ingresa al área de usuario o de administración para ejecutar el comando o un conjunto de comandos que normalmente están prohibidos. De esta forma, el atacante puede escribir, modificar, enviar correos electrónicos, copiar información o eliminar cierta información para encontrar una forma de acceder a los datos restringidos. El alcance del ataque depende de las capacidades del atacante.

Las amenazas a la seguridad de la red se dividen en una o dos categorías generales como Ataques lógicos o Ataques de recursos. Los ataques racionales, como su nombre lo indica, son una estrategia con fines de lucro utilizada para eliminar cualquier debilidad en el sistema. Las debilidades pueden incluir vulnerabilidades de software como puertas traseras y errores de

seguridad en el código. El propósito del ataque es ingresar al sistema para corromper u obtener acceso no autorizado al sistema. Los ataques de recursos tienen como objetivo destruir los recursos de las redes. (Carrasquero & Pérez, 2016)

El truco se hizo más popular en la década de 1990, pero su popularidad disminuyó gradualmente. En este método, el sistema de red se ve obligado a ser destruido, por lo que es vulnerable. Estos ataques se realizan de diferentes formas con el fin de aplicar fuerzas a la web de datos. La forma más rápida es que el servidor enfrente una gran avalancha de solicitudes de servicio que están fuera de su control. Además, algunos ataques de recursos implican la instalación de malware en la red, lo que la hará vulnerable.

También existe otra clasificación para los diferentes ataques a las redes seguras como,

*Ataques pasivos:* Los ataques pasivos son contra la seguridad de la red de la organización, con el fin de identificar la red; el intruso monitorea la red de la organización. Como en este ataque el intruso no realiza ninguna actividad maliciosa para detectar este tipo de ataque, es muy difícil, por ejemplo, un tipo de ataque pasivo es que el atacante captura los paquetes de la red interna de la organización, la esperanza es que este El tipo de ataque se puede prevenir fácilmente con el cifrado adecuado en la infraestructura de la red.(Gil Vera & Gil Vera, 2017)

*Ataques activos:* En este tipo de ataque, el atacante ataca directamente a los servidores de la organización. Los ataques son visibles para los sistemas de seguridad de la red con el fin de ser monitoreados. Las estrategias para combatir estos ataques incluyen la instalación de firewalls (software y hardware), así como sistemas IPS.

*Ataques internos:* (Close-in) en este tipo de ataque, los intrusos acceden físicamente a los sistemas. Desafortunadamente, con acceso físico a los sistemas, casi cualquier intruso puede hacer mucho trabajo y causar daños irreparables a la organización. Una forma adecuada y

lógica de hacer frente a este tipo de ataques es velar por la seguridad física de los sistemas y servidores.(Rodríguez Prieto, 2016)

*Ataques desde adentro:* este tipo de ataques a la red suelen ser realizados por usuarios internos de organizaciones que tienen acceso a sistemas e información. Según el nivel de conocimiento y conciencia de los atacantes a las redes informáticas, pueden penetrar en los sistemas de red. La solución de los ataques es prevenir este tipo de ataques a la seguridad en la Capa 2 y centrarse en la autenticación, mientras que la seguridad física debe estar totalmente asegurada.(Roba Iviricu et al., 2016)

Para proporcionar conocimientos básicos sobre las medidas de seguridad en la web de datos, en esta sección se presentan algunos conceptos sobre seguridad en redes. En una red moderna hay muchos recursos para la protección. La siguiente es una lista de recursos de red que deben protegerse contra todo tipo de ataques:

- 1- Firewalls, enrutadores y conmutadores como equipos de red,
- 2- Información de operación de red, como tablas de enrutamiento y configuraciones de listas de acceso almacenadas en el enrutador.
- 3- Recursos de red intangibles como ancho de banda y velocidad.
- 4- Información y recursos de información conectados a la red, tales como bases de datos y servidores de información.
- 5- Terminales que se conectan a la red para utilizar diferentes fuentes.
- 6- Información intercambiada en la red en cualquier momento del tiempo.
- 7- Mantener la privacidad de las operaciones de los usuarios y el uso de sus recursos de red para evitar la identificación del usuario.

En las computadoras en red, como la base de datos y los servidores web, la información se intercambia a través de la red y la información sobre los componentes de la red para realizar

tareas como las tablas de enrutamiento del enrutador. Los recursos de red también pueden ser equipos terminales como enrutadores y cortafuegos o mecanismos de conexión para evitar que los piratas informáticos accedan a los datos protegidos.

Principios de diseño de seguridad de red: para implementar un sistema de seguridad avanzado en la web de datos, se debe aplicar un método y principios de diseño adecuados a las medidas de seguridad de las redes. Las protecciones de seguridad de la red son la primera línea de defensa de los recursos del sistema de tecnología de la información (TI) contra las amenazas (como intrusos o códigos maliciosos) que surgen de los flujos fuera de la red.

Las medidas de protección clave para la seguridad de la red incluyen cortafuegos, detección de intrusos y cortafuegos de aplicaciones web, sistema de detección de intrusos (IDS) y sistema de prevención de intrusos (IPS), protecciones de red privada virtual (VPN) y sistemas de revisión de contenido como antivirus, antimalware, anti - Filtrado de spam y ubicación uniforme de recursos (URL). (Amaro López & Rodríguez Rodríguez, 2017)

Estas soluciones de hardware y software soportan y complementan los mecanismos de seguridad para sistemas operativos, bases de datos y aplicaciones. Para proporcionar un sistema de seguridad eficiente en los datos protegidos de las redes, se aplican métodos avanzados de diseño de diagramas de flujo con respecto a los niveles de amenazas.

Política seguridad: La política de seguridad de la red debe definirse de tal manera que se minimice el riesgo y la cantidad de daño después del análisis de riesgo en la web de datos. La política de seguridad debe ser general y en el campo de la visión general y no entrar en detalles. Los detalles pueden cambiar en poco tiempo, pero los principios generales de seguridad de una red que conforman sus políticas siguen siendo los mismos.

Los elementos que intervienen en la política de seguridad son:

- 1- Qué y por qué se deben proteger los datos.

- 2- Quién es el responsable de la protección de datos.
- 3- Crear un contexto que resuelva los posibles conflictos.

Las políticas de seguridad se pueden dividir a grandes rasgos en dos categorías:

- 1- Permisivas: Se permite todo lo que no esté específicamente prohibido.
- 2- Restrictiva: Se prohíbe todo lo que no esté explícitamente permitido.

Por lo general, la idea de utilizar políticas de seguridad restrictivas es un método mejor y más apropiado en términos de mejora de la seguridad de los sistemas de red. Esta selección se debe a problemas de seguridad de las políticas autorizadas para brindar restricción al acceso de datos protegidos.(Astorga-Aguilar & Schmidt-Fonseca, 2019)

Implementación de seguridad de red: el mejor enfoque para implementar una buena seguridad de red es tener nuestra red completamente preparada para amenazas. Aquí hay 4 consejos para el proceso de implementación de la seguridad de la red:

1- Seguridad: asegúrese de que todos los componentes tengan la licencia adecuada y tengan políticas de autenticación y protección.

2- Revisión: Seguimiento de las actividades de la red y continuidad de las actividades de protección.

3- Testeo: Evaluar las vulnerabilidades de las políticas de seguridad destinadas a la red simulando un ataque por parte de una persona de confianza. Si es posible eludir las prohibiciones, será necesario implementar técnicas más sofisticadas.

4- Mejorar la situación: Basándose en todos los pasos anteriores, recopile datos y utilícelos para crear mejores medidas.

Todos los administradores de red deben tener en cuenta que una buena estrategia de seguridad para la red involucra monitoreo y mantenimiento constante. Ciertamente, no es

suficiente que las políticas de seguridad se creen y abandonen para hacer su trabajo. Los atacantes se actualizan constantemente para encontrar una forma de acceder a los datos protegidos. Por lo tanto, los administradores de red deben mantenerse al día con estas mejoras.

Eliminación del peligro: después de determinar los activos de la red y sus factores amenazantes, se deben evaluar varios riesgos. En el mejor de los casos, la red debería ser capaz de proteger contra todo tipo de errores, pero no se logra una seguridad barata. Por tanto, es necesario realizar una adecuada valoración de los tipos de riesgos con el fin de identificar los más importantes y, por otro lado, identificar las fuentes que deben protegerse frente a estos riesgos. Los dos factores principales en el análisis de riesgo son:

- 1- La posibilidad de realizar un ataque y
- 2- Daño a la red en caso de un ataque exitoso.

Capas de red: los niveles de seguridad son una clasificación de las actividades de la red para que cada actividad de la red se pueda proteger por separado y las políticas de seguridad de un nivel no afecten los parámetros de seguridad del otro nivel. Por ejemplo, si ocurre un ataque de DOS en el campo de la seguridad de la red en la capa de seguridad del lado del usuario, no buscamos enfrentar este ataque en la capa de administración.(Pacheco Amigo et al., 2018)

Los niveles de seguridad de la red permiten examinar la seguridad de cada actividad por separado al categorizar las actividades de la red y ubicarlas en diferentes niveles. Dado que cada actividad se considera por separado, las medidas de seguridad en cada nivel se pueden administrar con precisión. El servicio de VoIP en la capa de seguridad del servicio, la seguridad de la gestión del servicio (como la seguridad del usuario), la seguridad del control del servicio independiente (como el protocolo SIP) y la seguridad de los datos del lado del usuario (como la voz del usuario) son algunos ejemplos de la aplicación del nivel de seguridad de la red en las medidas de seguridad de las redes.(Figuroa Uribe & Hernández Ramírez, 2021)

Para aumentar el nivel de seguridad de la infraestructura de TI integral, se utilizarán soluciones de seguridad relacionadas en todos los niveles y capas de la arquitectura de TI de la empresa. Para establecer la seguridad de extremo a extremo, es necesario aplicar componentes de seguridad relacionados con diferentes equipos y grupos.

La tarea de las capas de seguridad, como las capas de red, es brindar servicio y activar la capa superior. Por lo tanto, la necesidad de capas de red se siente en la red de datos. Se consideran tres capas de seguridad y, al definir diferentes capas de seguridad, se propone una solución jerárquica para la seguridad de la red. La estratificación se realiza de tal manera que cada capa tiene sus propias vulnerabilidades, lo que se realiza con el objetivo de facilitar el manejo de las amenazas.(Zuñiga Paredes et al., 2021)

La "capa de seguridad de la infraestructura" habilita la "capa de seguridad del servicio" y esta capa también habilita la "capa de seguridad de la aplicación" para proporcionar una seguridad de red avanzada mediante capas de red. Las siguientes capas se explican como:

Capa de seguridad de infraestructura: La capa de infraestructura cubre la seguridad de las instalaciones de la red de transmisión, así como las herramientas de red individuales. Esta capa proporciona una descripción de la implementación de la red principal, los servicios y las aplicaciones de cada uno.

Capa de seguridad del servicio: La seguridad de los servicios que los proveedores de servicios brindan a los clientes en esta capa. Esta gama de servicios incluye servicios básicos (por ejemplo, servicios de comunicación por Internet como servidor de Contabilidad de autorización de autenticación (AAA), servicio de Sistema de nombres de dominio (DNS), etc.) hasta servicios especiales como Protocolo de voz sobre Internet (VOIP), VPN, etc. La tarea de esta capa es proteger a los proveedores de servicios y sus clientes de posibles amenazas a la seguridad.(Aguilar, 2019)



Capa de seguridad de la aplicación: esta capa se enfoca en las aplicaciones que están disponibles para los usuarios en la web. Las aplicaciones de red pueden ser proporcionadas por los proveedores de servicios de aplicaciones (ASP) como un proveedor externo, el propio proveedor de servicios como ASP o sus empresas anfitrionas que tienen un centro de datos independiente. En consecuencia, en esta capa, cuatro objetivos pueden considerarse como una amenaza:

- 1- usuarios de la aplicación,
- 2- proveedor de la aplicación,
- 3- subproveedor
- 4- Proveedor de servicios

Controlar el nivel de seguridad: La función de esta capa es soportar actividades que se encargan de transmitir información sobre servicios o aplicaciones de red. Este nivel generalmente incluye la comunicación entre máquinas en la red, que generalmente incluye mensajes de control.

Nivel de seguridad del lado del usuario: este nivel incluye asegurar el acceso y el uso de los servicios proporcionados por el proveedor del lado del usuario. Los usuarios finales pueden usar la propia red del proveedor de servicios, o servicios de extensión como VPN, o en redes basadas en aplicaciones.

Segmentación de la información: los recursos del sistema de TI con diferentes niveles de sensibilidad, incluida la tolerancia al riesgo y la vulnerabilidad a diversos grados de amenaza, deben incluirse en diferentes áreas de seguridad. El principio de "ocultar información" se considera como uno de los casos extendidos de esta regla, de modo que los sistemas de TI solo proporcionen los datos que son necesarios para realizar las tareas del sistema de TI. El sistema

se puede proporcionar como servidores para proveedores de servicios de Internet que están registrados solo en DNS públicos.

El principio de puntos mínimos Las personas conectadas al sistema de TI (como usuarios y administradores del sistema) deben tener los privilegios mínimos necesarios para un desempeño óptimo en la organización. Esto también se aplica a los datos y servicios que se ponen a disposición de usuarios externos. Una de las extensiones de esta regla es el principio de "necesidad de saber", según el cual los usuarios y administradores de los sistemas de TI tienen acceso únicamente a la información relacionada con sus roles y tareas.

El nivel de seguridad del sistema de TI depende del factor que tiene la menor seguridad. Una de las extensiones de esta regla es el principio de Punto único de fallo (SPOF), que está relacionado con la disponibilidad de los servicios de red, según el cual todos los enlaces, equipos (red y seguridad), así como servidores en la red, enrutan entre usuarios y recursos importantes El rendimiento del sistema de TI debe implementarse en configuraciones redundantes. Al diseñar un sistema de seguridad de red, se deben considerar los principios de seguridad organizacional, incluidas las reglas de "segregación de funciones" y "flujo de trabajo".

El propósito de estos principios es limitar la capacidad de los empleados de ignorar y violar las políticas de seguridad del sistema de TI. La separación de deberes significa que las tareas y funciones importantes deben ser realizadas por dos o más empleados. Además, se debe considerar la rotación de puestos de trabajo importantes en términos de medidas de seguridad de las redes. Los recursos de los sistemas de TI con diferentes niveles de sensibilidad deben ubicarse en diferentes áreas de seguridad. Los equipos de cómputo y los proveedores de servicios para redes externas (como las empresas proveedoras de Internet) deben estar ubicados en diferentes áreas (como Zona Desmilitarizada), a diferencia de los sistemas de cómputo y equipos de redes internas.

Los recursos estratégicos del sistema de TI deben estar ubicados en áreas de seguridad específicas para estar protegidos. Los equipos y sistemas informáticos de baja confiabilidad, como servidores de acceso remoto y puntos de acceso a redes inalámbricas, también deben incluirse en áreas específicas de seguridad. Los diferentes tipos de recursos del sistema de TI deben colocarse en áreas de seguridad separadas. Las estaciones de trabajo de los usuarios deben estar ubicadas en diferentes áreas de seguridad, a diferencia de los servidores. Los sistemas de gestión de seguridad y red deben estar ubicados en áreas de seguridad específicas. Los sistemas en fase de desarrollo deben estar ubicados en un sector diferente, a diferencia de los sistemas relacionados con la fase de producción.

Los cortafuegos en los sistemas de software o hardware actúan como un muro de seguridad entre los usuarios de las redes y el mundo exterior. Los cortafuegos suelen estar situados en la frontera entre nuestra red e Internet. Los firewalls de hardware pueden monitorear el contenido y las rutas de comunicación de nuestra red. Los cortafuegos definen las reglas sobre cómo entra y sale la información de nuestra red e Internet. De hecho, utilizamos cortafuegos para determinar qué datos tienen derecho a entrar y salir y cuáles no. Los cortafuegos de software son herramientas rentables en los sistemas de cortafuegos y pueden examinar patrones y contenido y pueden proporcionar una pequeña supervisión de las amenazas. Además, los firewalls de hardware son muy poderosos y, por lo tanto, se pueden usar más que sus modos de software.

A discreción del usuario, el firewall es la herramienta principal para mantener o restringir el flujo de tráfico de la red en diversas situaciones, como equipos de firewall dedicados, función de firewall en equipos IPS y lista de control de acceso en conmutadores y enrutadores de red. Con una implementación y configuración adecuadas, los firewalls pueden ayudar a construir arquitecturas seguras, dividir la infraestructura de la red de TI en dominios de seguridad y controlar la comunicación entre ellos.

Para aumentar el ciberataque a los datos protegidos, se desarrolla un IDS avanzado. En este artículo, se presenta un modelo avanzado de ciberataque para evitar el acceso de piratas informáticos a los datos protegidos en las redes. Los virus, gusanos y troyanos intentan propagarse por la red y pueden permanecer en dispositivos infectados asintomáticos durante días o semanas. Nuestro trabajo es hacer un esfuerzo de seguridad para evitar la penetración de este tipo de malware, así como el malware que les abre el camino.

Esta es una estrategia de defensa contra los atacantes. Si hay un denominador común entre los expertos en seguridad, es peligroso confiar en la primera línea de defensa. Porque cualquier herramienta de defensa puede ser derrotada por el enemigo. La red no es una línea o un punto que sea realmente un territorio. Como resultado, si un atacante ha atacado parte de los datos protegidos, es posible salvar los recursos de datos y rescatarlos si el sistema de seguridad está debidamente organizado para las técnicas de defensa. Las soluciones de seguridad de red se pueden presentar como,

- 1- Evaluar riesgos y vulnerabilidades y analizar la selección de controladores adecuados.
- 2- Optimización de servidores, clientes, sitios web y el entorno de red de la organización.
- 3- Optimización de caché, traducción de direcciones de red (NAT), proxy, dirección de protocolo de Internet (IP) y redes de enrutamiento.
- 4- Asesoramiento en la elección de los estándares de seguridad adecuados.
- 5- Asesoramiento en la definición y aplicación de lineamientos e instrucciones ejecutivas para la seguridad de la información.
- 6- Capacitación presencial o periódica a varios niveles.
- 7- Probar la solidez de los sistemas de seguridad intentando romperlos.

## MARCO METODOLÓGICO

El presente caso de estudio se basa en las siguientes modalidades de investigación:

**De campo:** Se utilizará la investigación de campo pues se necesitó recurrir al lugar donde se desarrollan los hechos, obteniendo información veraz de lo ocurrido, de tal forma que el análisis realizado este acorde a los objetivos de la investigación.

Este tipo de investigación se apoya en la información levantada, obtenida mediante observaciones en el lugar donde se desarrolla cada proceso, reuniones con los Gerentes y Supervisores de cada área.

**Bibliográfica:** Debido al estudio de seguridad que se realizara, nos enmarcamos en torno al direccionamiento a la seguridad informática, que cubre criterios de buenas prácticas y gestión referente a la información. Este tipo de investigación detalla las actividades que se llevan a cabo en los procesos manejados en el objeto de estudio, a través de producción científica, permitiendo conocer en forma sistemática las falencias que se presentan en los mismos.

Como herramienta de investigación se utilizó una entrevista dirigida al jefe de sistemas de la empresa Netline. Se aplicó como instrumento un cuestionario de preguntas cerradas las cuales tienen opciones a la escala de Likert, con el objetivo de encontrar los niveles de seguridad informática aplicados por la empresa Netline.

## **RESULTADOS**

Los resultados obtenidos en la evaluación del análisis de Seguridad de la Información y Seguridad Informática ayudarán a Netline en la implementación de buenas prácticas que mitiguen las vulnerabilidades y amenazas identificadas. El proceso central analizado fue el del área de Sistemas, por ser considerado un soporte fundamental para el procesamiento y almacenamiento de datos. Asimismo, el grado de sensibilización en seguridad de la información y gestión de la información en áreas críticas como: Cartera, Crédito y Cobranzas y áreas de apoyo, Administrativo, Recursos Humanos, Control de Calidad, Contabilidad, Caja y Servicios Generales.

Con el fin de obtener resultados reales de la situación de la empresa en temas de seguridad de la información, se elaboró un cronograma de entrevistas con el personal directivo de las áreas consideradas críticas (Sistemas, Portafolio y Cobranzas), así como una entrevista con el jefe de sistemas. De acuerdo a las respuestas obtenidas en las diferentes entrevistas y encuestas realizadas al personal de Netline; así como el uso de técnicas como la observación, consulta y revisión de documentación, se logró identificar el estado actual de la empresa, en cuanto a temas de seguridad de la información y seguridad informática.

Netline no cuenta con un manual de políticas de seguridad de la información, pero ha implementado y documentado algunos controles de seguridad que permiten limitar el acceso no autorizado a la información, los cuales no han sido actualizados desde su fecha de elaboración. Existen inventarios de equipos de cómputo y dispositivos de almacenamiento, los cuales son actualizados por el área de Sistemas cada vez que se adquiere un nuevo equipo o dispositivo. Además, cuentan con un documento en el que se detallan las licencias que utilizan para cada servidor que poseen. Ninguna persona del área de Sistemas pudo identificar exactamente cuántos sistemas operativos se están utilizando en la empresa

No existe una política que determine los requisitos de seguridad que se deben exigir para el desarrollo o adquisición de software. Todo está enfocado a que el sistema funcione de acuerdo a lo que se necesita. No existe una política formal que detalle los controles a implementar para evitar la fuga de información, lo que se ha implementado como medida de seguridad es la desactivación de todos los medios removibles de almacenamiento.

## **DISCUSIÓN DE RESULTADOS**

La empresa objeto de estudio a pesar de contar con normatividad y mecanismos que les permitan prevenir la ocurrencia de un incidente que afecte los activos de información, se encuentra en un alto índice de riesgos de seguridad debido a las vulnerabilidades presentes en las actividades diarias que realizan los funcionarios. La aplicación de mecanismos y controles basados en buenas prácticas de seguridad les ayudará a dirigir de manera adecuada la gestión de la seguridad de la información, permitiéndoles así reducir el nivel de riesgo al que están expuestas la información y los sistemas de procesamiento de información. información

Una de las principales buenas prácticas de seguridad es establecer y designar al menos una persona que se encargue de la gestión de la seguridad de la información dentro de la empresa, de tal forma que se analicen y planifiquen los tiempos de implementación. de controles de seguridad que mitigarán los riesgos existentes. Actualmente, la falta de un encargado de seguridad informática y seguridad de la información no les permite monitorear constantemente todo lo que involucra temas de seguridad de la información, ni dar seguimiento a los incidentes ocurridos.

Uno de los principales objetivos debe ser empezar a mejorar la cultura organizacional en temas de seguridad, según la entrevista realizada al jefe de sistemas de la empresa se encontró que la implementación de charlas en temas de seguridad les ayudará a mantener informados a los empleados y funcionarios sobre la importancia del uso adecuado de los activos de información, de tal manera que se cumplan tanto las políticas de la empresa como los controles de seguridad actualmente implementados.

A través de la elaboración del manual de Políticas de Seguridad de la Información, la empresa podrá detallar responsabilidades de acuerdo a las actividades que realizan las diferentes áreas, de tal forma que se logre un trabajo integral en equipo, involucrando a todo el personal de la empresa, ya que, en actualmente, de acuerdo a la información obtenida como



resultado del estudio, no existen responsabilidades definidas en materia de seguridad de la información.

Mediante la implementación de mecanismos de seguridad que permitan monitorear el funcionamiento y uso de los sistemas tecnológicos instalados en la empresa, se puede controlar la integridad de la información que almacenan o comunican a través de los medios y la disponibilidad de los activos de información. ya que actualmente consideramos según los resultados que la gestión de seguridad que se lleva a cabo sobre estos activos no se está realizando adecuadamente.

Reforzar los controles de seguridad en los sistemas de procesamiento de información, permite obtener datos claros y precisos de los sistemas, según lo requiera la empresa y los clientes, minimizando incidentes de seguridad como daños a aplicaciones, equipos tecnológicos, incluso robo o alteración. de información, que puede costarle mucho dinero a la empresa; En base al análisis realizado, se ha podido detectar que la ocurrencia de eventos esporádicos ha afectado la integridad de la información almacenada en los repositorios de datos, provocando cierto retraso en la consulta de la información requerida.

En los últimos años la empresa ha tenido un crecimiento considerable, por lo que aplicar la seguridad permite mejorar significativamente las operaciones en la empresa, organizando los esfuerzos realizados en el cumplimiento de los objetivos. El conjunto de todos los controles de seguridad permite a los altos directivos garantizar la correcta y adecuada confidencialidad, integridad y disponibilidad de datos e información de valor tanto para la empresa como para sus clientes, aumentando la credibilidad y confianza de los clientes externos a la empresa.

## CONCLUSIONES

En conclusión, el análisis realizado muestra que los activos de información de las áreas consideradas críticas y la situación actual de la empresa con respecto a la seguridad de la información, refleja índices de riesgo potencial, que exponen la información a daños, robos o modificaciones que pueden causar un impacto negativo. impacto dentro de las actividades comerciales.

A través de las recomendaciones indicadas, se pretende que la empresa tome acciones que le permitan prevenir y detectar oportunamente las vulnerabilidades a las que están expuestos los sistemas de procesamiento de información, así como la información que es manejada y generada por los funcionarios. La implementación de controles de seguridad les permite mejorar tres importantes características: confidencialidad, integridad y disponibilidad de la información.

La elaboración de un manual de políticas de seguridad de la información donde se detallan los controles de seguridad de acuerdo a la realidad y necesidades actuales de la empresa, la constante concienciación de los funcionarios, así como el seguimiento continuo, encamina a la empresa a la correcta gestión de la seguridad de la información. La seguridad total no existe, pero gestionar los controles de seguridad en el proceso y manejo de la información se convierte en un complemento imprescindible, ya que permite resguardar información valiosa no solo de la empresa sino también de los clientes.

## **RECOMENDACIONES**

Para empezar a tratar los temas de seguridad de la información y seguridad informática, es importante que se esté consciente de que el trabajo de implementación y cumplimiento de controles de seguridad es en equipo, e involucra a todos los funcionarios de la empresa. La concientización en los funcionarios y el compromiso de los altos directivos, permite que todos empiecen a conocer la importancia que tiene garantizar que la información de la empresa está siendo manejada y procesada adecuadamente.

Por lo tanto, la empresa se debe presentar una nueva solución con respecto a las amenazas desarrolladas para aumentar los niveles de seguridad en las redes. El hardware de los sistemas de seguridad de la red se puede modificar para proporcionar medidas de seguridad avanzadas en la web de datos.

Se deben aplicar un software de firewall, para mitigar riesgos con respecto a los métodos desarrollados por los piratas informáticos se puede presentar para proporcionar una herramienta clave en los sistemas de protección de datos. Se puede implementar un modelo avanzado de procesador de hardware y sistema de comunicación de software para detectar y prevenir los ataques a la red en términos del proceso de mejora de la seguridad de la red. Como resultado, se puede presentar un sistema de seguridad de red avanzado para disminuir los niveles de acceso a los datos por parte de los piratas informáticos.

## REFERENCIAS

- Aguilar, J. A. M. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. *URVIO Revista Latinoamericana de Estudios de Seguridad*, 24–40.
- Álvarez Roldán, M. Á., & Montoya Vargas, H. F. (2020). Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos. *Ingeniería y Desarrollo*, 38(2), 279–297. <https://www.redalyc.org/articulo.oa?id=85269294001>
- Amaro López, J. A., & Rodríguez Rodríguez, C. R. (2017). Seguridad en internet. *PAAKAT: Revista de Tecnología y Sociedad*, 6.
- Arellano Martínez, I. (2017). La cultura sobre seguridad informática en las redes sociales: el caso de los estudiantes de la Preparatoria de San Diego Cuentla, México. *RICSH Revista Iberoamericana de las Ciencias Sociales y Humanísticas*, 6(11). <https://www.redalyc.org/articulo.oa?id=503954319002>
- Astorga-Aguilar, C., & Schmidt-Fonseca, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. *Revista Electrónica Educare*, 23, 339–362.
- Carrasquero, E., & Pérez, L. (2016). SISTEMA DE GESTIÓN DE SEGURIDAD EN REDES LAN. *Télématique*, 15(2), 133–143. <https://www.redalyc.org/articulo.oa?id=78457627003>
- Estrada, J., Calva, M., Rodríguez, A., & Tipantuña, C. (2016). Seguridad de la Telefonía IP en Ecuador: Análisis en Internet. *Enfoque UTE*, 7(2), 25–40. <https://www.redalyc.org/articulo.oa?id=572261569003>
- Figueroa Uribe, A. F., & Hernández Ramírez, J. (2021). Seguridad hospitalaria, una visión de seguridad multidimensional. *Revista de La Facultad de Medicina Humana*, 21, 169–178.
- Gil Vera, V. D., & Gil Vera, J. C. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica*, 22(2), 193–197. <https://www.redalyc.org/articulo.oa?id=84953103011>
- Pacheco Amigo, B. M., Lozano Gutiérrez, J. L., & González Ríos, N. (2018). Diagnóstico de utilización de Redes sociales: factor de riesgo para el adolescente. *RIDE. Revista Iberoamericana Para La Investigación y El Desarrollo Educativo*, 8, 53–72.

- Roba Iviricu, L. R., Vento Alvarez, J. R., & García Concepción, L. E. (2016). Metodología para la Detección de Vulnerabilidades en las Redes de Datos utilizando Kali-Linux. *Avances*, 18(4), 334–344. <https://www.redalyc.org/articulo.oa?id=637867033003>
- Rodríguez Prieto, R. (2016). ¿Qué seguridad? Riesgos y Amenazas de Internet en la Seguridad Humana. *Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades*, 18(36), 391–415. <https://www.redalyc.org/articulo.oa?id=28248171018>
- Zuñiga Paredes, A. R., Jalón Arias, E. J., Andrade Olmedo, M. E., & Giler Chango, J. L. (2021). Análisis de seguridad informática en entornos virtuales de la Universidad regional autónoma de los Andes extensión Quevedo en tiempos de covid-19. *Revista Universidad y Sociedad*, 13, 454–459.

## ANEXOS

### Encuesta acerca de Seguridad Informática dirigida al área de Sistemas de Netline

**Nota:** Marcar con una **X** sus respuestas

**1. ¿Existe un área o persona responsable de seguridad informática y seguridad de la información en la empresa?**

Sí   No     

**2. ¿Qué tipo de herramientas de seguridad tiene implementado en la empresa? (se puede seleccionar varias alternativas)**

- Software
- Hardware
- No tiene
- Otros, indique cuáles

**3. ¿Tiene instalado antivirus en los equipos de computación?**

°Sí    No continuar con la pregunta 5)

**4. ¿Qué software utiliza en la empresa para controlar software malicioso? (se puede seleccionar varias alternativas)**

- Antivirus    Anti-Spam
- Antispyware    Cortafuegos/firewall
- Otros, indique cuáles  \_\_\_\_\_

**5. ¿Cuáles de los siguientes mecanismos de autenticación utiliza en la empresa? (se puede seleccionar varias alternativas)**

- Firma electrónica digital    Clave de Acceso    No tiene
- Otros, indique cuáles  \_\_\_\_\_

**6. ¿Se realiza un mantenimiento periódico en los sistemas de procesamiento de información y equipos informáticos?**

Sí  No (continuar con la pregunta 8)

**7. ¿Cada cuánto tiempo realizan mantenimientos en los sistemas de procesamiento de información? (se puede seleccionar varias alternativas)**

Trimestral  Semestral  Mensual   
Otros, Indique el período  \_\_\_\_\_

**8. ¿De cuántos computadores dispone su empresa?**

20 – 40  40 – 60  60 o más

**9. ¿Disponen de servidores centrales de datos en la empresa?**

Sí  No

**10. Si su empresa tiene conexión WIFI, ¿existen restricciones de seguridad para el acceso de dichas conexiones?**

Sí  No

**11. ¿Se realizan respaldo de la información de la empresa?**

Sí  No (continuar en 13)

**12. ¿En caso de que se realice respaldo de información, con qué frecuencia lo realizan? (se puede seleccionar varias alternativas)**

Diaria  Semanal   
Mensual   
Otros, indique el período  \_\_\_\_\_

**13. ¿Se utilizan mecanismos de bloqueo automático de las estaciones de trabajo para cuando se encuentran desatendidos?**

Sí  No

**14. ¿Existen equipos que provean de energía ininterrumpida a los servidores y computadores de los funcionarios?**

Sí  No

**15. ¿Qué servicios y sistemas considera más críticos en términos de disponibilidad? (se puede seleccionar varias alternativas)**

De almacenamiento de datos  Servicios de comunicación  Sistemas de procesamiento de datos

Otros, indique cuáles  \_\_\_\_\_

**16. ¿Dónde se encuentran almacenados los medios de respaldos? (se puede seleccionar varias alternativas)**

Dentro del área de sistemas  Dentro de la empresa, pero fuera del área de sistemas  Fuera de la empresa  No se realizan almacenamientos.  Otros, indique cuáles \_\_\_

**17. ¿Durante el último año tuvieron algún incidente de seguridad grave de la información?**

Sí  No  Desconoce

**18. ¿Se mantiene un registro de fallas cuando ocurre algún evento en los sistemas de procesamiento de información (servidores, computadores, redes, etc.)?**

Sí  No

**19. ¿El acceso a internet en la empresa es limitado por? (se puede seleccionar varias alternativas)**

Cargo

Usuario

Indique el mecanismo  \_\_\_\_\_

Ninguna

**20. ¿Posee un plan de contingencia vigente en caso de desastres naturales?**

Sí  No  Desconoce





Lcdo. Eduardo Gáneas Guijarro, MAE  
**DECANO DE LA FACULTAD DE  
ADMINISTRACIÓN, FINANZAS E INFORMÁTICA**


Martes 22 de Marzo del 2022


De mis consideraciones:


Por medio de la presente autorizo que la Srta. **ZAMORA CANDELARIO HELEN DAMARIS** con CC. **1206688662**, estudiante de la carrera de **INGENIERIA EN SISTEMAS DE INFORMACIÓN** realice el estudio de caso en la empresa de internet **NETLINE** ubicada en Ricaurte, previa a la obtención del título universitario de tercer nivel como **INGENIERA EN SISTEMAS DE INFORMACIÓN**. El estudio de caso es: **ANÁLISIS DE LOS PROBLEMAS DE SEGURIDAD Y REDES EN LA EMPRESA DE INTERNET NETLINE**.

Atentamente,

  
**BENJAMIN FRANKLIN PEREZ PONCE**  
Gerente Propietario

 [www.netline.ec](http://www.netline.ec)

 EC: 0967714947

 Av. Emiliano Pinoargote y Bartolome Bastidas, junto a Fertisa.  
Ricaurte - Urdaneta

