UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA: INGENIERÍA DE SISTEMAS

Artículo Académico previo a la obtención del título de:

INGENIERO DE SISTEMAS

TEMA:

“Modelo de red segura en un entorno distribuido para la transferencia de datos con mecanismos básicos de seguridad”

AUTOR:

Cristhian Oswaldo Sánchez Guzmán

DIRECTOR:

Joe Llerena Izquierdo, MSc.

Guayaquil, abril del 2021

DECLARATORIA DE RESPONSABILIDAD

Yo, **Cristhian Oswaldo Sánchez Guzmán**, declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del/los autor/es.

Firma del autor

Firma del tutor

Modelo de Red Segura en un Entorno Distribuido para la Transferencia de datos con mecanismos básicos de seguridad

Cristhian Sanchez Guzman[1][0000-0001-5981-594X] and Joe Llerena-Izquierdo[1][0000-0001-9907-7048]

[1]Universidad Politécnica Salesiana, Guayaquil, Ecuador
csanchezg3@est.ups.edu.ec, jllerena@ups.edu.ec

Abstract. Empresas a nivel mundial y especialmente en Latinoamérica, continuamente tienen dificultades por una implementación deficiente en sus modelos de red bajo entornos distribuidos, con un futuro posible de riesgos existentes, vulnerabilidades continuas y amenazas latentes que ponen en peligro la información de una organización, incluso llegan a afectar a los servicios existentes que estas brindan. Este artículo tiene como objetivo presentar una propuesta de modelo de red que permite mantener segura la información de una organización mediante el análisis de vulnerabilidades y riesgos de ataques más predominantes, aplicando mecanismos de seguridad para los equipos de comunicación, así como a los equipos de los usuarios. Se ha realizado la búsqueda y síntesis de técnicas utilizadas junto a los requerimientos presentados de investigaciones que presentan implementaciones en entornos u organizaciones pequeñas y grandes, para determinar políticas aplicables. En esta investigación se usó el método deductivo de investigación exploratoria para el análisis de información de fuentes existentes. El análisis de políticas y estándares de seguridad evidenció que pueden mitigarse los riesgos y amenazas en los entornos distribuidos dentro de una organización logrando desarrollar e implementar el modelo de red segura. Se concluye con la propuesta del diseño de un modelo de red segura, enfocado a las áreas de una organización, previo análisis de ciberataques que se conectan entre sí, mitigando el robo de información o ataques que se producen en situaciones inesperadas. Se evidencia la aplicabilidad de estándares y mecanismos de seguridad para la transferencia segura de información.

Keywords: Seguridad de datos, red segura, integridad de la información, técnicas de seguridad, protección de la información, estándares de seguridad.

1 Introducción

A nivel mundial especialmente en América Latina los problemas de seguridad en áreas administrativas, Intranet, correos electrónicos entre otros, se evidencian en estudios recientes sobre ataques informáticos a empresas que tienen poco tiempo de inicio, es decir microempresas, dentro de escenario difícil de evadirlo, siendo esto imperceptible en el momento en que se descubren [1–4]. De igual manera temas relacionados para considerar la seguridad informática enfocados en ciberseguridad, es una preocupación que va en aumento en estas empresas. Al ser tecnologías nuevas que se implementan de acuerdo a un análisis específico, al iniciar una empresa, no tienen estandarizados mecanismos de seguridad que son prioritarios para una organización sino al momento de implementar algún sistema a nivel de hardware como software, esto hace que muchas empresas no sean conscientes de las vulnerabilidades, los riesgos y peligros que puedan existir en la base de datos o información interna [5–7].

Todo esto se lleva a cabo al momento de implementar un diseño de red, por lo que muchos no dispondrán de una correcta organización de este en entornos distribuidos o áreas que comparten información entre sí. Esto llega a ser uno de los mayores desafíos para muchas de ellas [8]. Por esto, existen numerosos riesgos que pueden afectar a una empresa en muchos temas incluyendo la transferencia de información que, debido a la gran cantidad de ataques cibernéticos, es necesario mantener actualizada y desarrollada varias técnicas de seguridad, como son la confidencialidad, integridad y disponibilidad de datos, a nivel interno como externo. Es un riesgo transferir información, entre computadores o servidores, sin alguna encriptación de datos que ayude a mantener seguro el traspaso de información importante, al igual que la escasez de medidas seguridad cuando se tiene un diseño o redes ya implementadas. Es un problema que sigue creciendo hoy en día [9], esto se da por el crecimiento del Internet y de programas informáticos que hayan sido desarrollados en una complejidad extrema [10–13] Llega a existir una gran dificultad de detección de los diversos problemas de seguridad en una red a medida que vayan presentándose y desarrollándose [14]. Muchos diseñadores pensaron que Internet no crecería demasiado en el momento en que se pensó en un sistema o un conjunto de cables estructurados, ya que, en ese momento, los sistemas no consideraban la seguridad como prioridad, es por eso por lo que cuando se incorporan medidas de protección y seguridad se es perseverante en el nivel o etapa de diseño [15–21]. A pesar de tener todas las medidas y mecanismos de seguridad esta, no ayuda a proteger una contraseña fácil de adivinar por el intruso [22, 23]. Una red segura puede llegar a ser muy importante para prevenir y proteger contra intrusos que no están autorizados dentro de un entorno. Un prototipo de red puede llegar a centrarse en la interacción entre dispositivos a nivel interno y la conectividad que hay entre ellos [24].

Este trabajo de investigación nos lleva a una pregunta de importancia a nivel organizacional en un Sistema informático o Infraestructura de red, en el ámbito de las técnicas de seguridad en un sistema distribuido: *¿Los mecanismos de seguridad pueden evadir riesgos y vulnerabilidades en la transferencia de los archivos de forma no autorizada en un ambiente distribuido?*

Estos mecanismos ayudan a una empresa cuando los ataques lleguen a darse y se vean reducidos cuando no afecten de forma grave a la información de la empresa, así

como datos personales de los trabajadores. Llega a ser un gran problema si muchas organizaciones no disponen de las suficientes maneras o técnicas de mantener seguro un Sistema Informático en un ambiente dado. Con el pasar del tiempo estos pueden ser vulnerables a robos masivos, ataques cibernéticos, manipulación de información o datos, causando desconfianza en el personal, perjudicando a la empresa económicamente deteniendo las actividades que se realizan internamente en una organización [25].

1.1 Revisión de la literatura

En el 2015 se evidencia que los enfoques de seguridad para los sistemas no eran una prioridad alta ya que no existían suficientes amenazas ni riesgos que puedan comprometer la información interna de los trabajadores y bases de datos, por lo que se declaró que las organizaciones deben intentar captar o detectar, actividades maliciosas que traten de poner en riesgo los datos. Se implementaron sistemas de detección de intrusos que sirvan para el monitoreo y así lograr identificar cualquier amenaza o mal comportamiento que exista. Generalmente estos sistemas de monitoreo manejan el riesgo de tráfico que existe principalmente en una red, por lo que llega a ser conveniente implementar una de estas en una microempresa, ya que no disponen de tecnologías lo suficientemente seguras y avanzadas [26].

La seguridad de la red en cualquier entorno es un tema que hoy va tomando más importancia ya que, así como Internet va creciendo, la cantidad de datos también crecen. Todo esto se maneja por dispositivos, ya sean móviles o computadoras personales que están conectados entre sí, esto puede llegar a hacernos vulnerables a amenazas y riesgos internos y externos, que se consideran como virus, troyanos, o incluso llegar a un hackeo masivo dependiendo de qué cantidad de información exista [27–30].

Las organizaciones existentes intentando mantener protegida la información interna implementan medidas y programas de seguridad informática continuamente, sin embargo, estas herramientas no pueden evitar las brechas, riesgos y ataques cibernéticos. En los años 80 según el grupo de control de auditoria de la información con el fin de tener conocimiento de la seguridad informática se publicaron artículos sobre la primera prueba de un gusano informático, es decir un virus, que dieron paso al origen de procesos de ciberseguridad [31].

El tema de ciberseguridad se menciona en muchos aspectos actualmente, y cada vez se vuelve un componente de la seguridad de la información. Las auditorías de TI y seguridad de la información que fueron eficientes hace veinte años, trataron de utilizar las mismas auditorías de seguridad para poder abordar las amenazas y riesgos cibernéticos. A medida que aumenta la cantidad de información en una organización, también se desarrollan estrategias para mitigar las amenazas y riesgos, sin embargo este crecimiento de ataques pueden llegar a evadir las auditorías de seguridad implementadas, poniendo en complejidad a la empresa [32].

La necesidad de implementar un modelo de seguridad, a partir de uno obsoleto dependía de evaluar y validar diferentes controles de auditoría que pueden ser preventivos, como su detección, para todas las áreas administrativas que conforma dicha organización. En esta investigación se obtuvo como resultado un modelo de auditoría para la ciberseguridad, que sirve como propuesta para realizar auditorías que mitiguen las

vulnerabilidades de las organizaciones. Este modelo evalúa y valida los controles de auditoría que se realiza para todas las áreas administrativas conectadas entre sí [33].

En el año 2017 se analizaron los diferentes ajustes y propiedades que existían en un sistema distribuido que fueron realizadas en un entorno informático a nivel global, en la que se revelaron razones de vulnerabilidad, riesgos y amenazas frente a la manipulación y exposición de programas o archivos no autorizados o de proveniencia no confiable, por lo que se describieron principios de formación programable en el espacio algorítmico y de ciberseguridad para un entorno distribuido dentro de una organización dada por computadoras en red [34–36].

1.2 Protocolo de investigación

Se usan protocolos de investigación como el mapeo sistemático de la seguridad en la transferencia de información investigado acerca del tema en áreas específicas dentro de una organización o un ambiente distribuido con el fin de obtener y realizar un estudio de toda la información existente.

Para la realización de un mapeo de la información se presentan las siguientes preguntas de investigación:

Tabla 1. Preguntas de investigación

Preguntas de Investigación	Motivación
Q1. ¿Qué propuestas existen sobre la implementación de modelos de red segura?	Mitigar los riesgos y vulnerabilidades que se da en un entorno distribuido al momento de transferir información.
Q2. ¿Qué evidencia empírica existe sobre los modelos de red segura?	Implementar una metodología correcta para poder mitigar los riesgos y vulnerabilidades mediante un modelo de red segura
Q3. ¿Qué métodos, normas, materiales se usan para implementar un modelo de red segura?	Determinar cuáles son los estándares, mecanismos, herramientas que se usan para evaluar e implementar un correcto modelo de red segura.

En la Tabla 1 se detallan las preguntas de investigación que, al momento de realizar el análisis de los artículos relacionados con el presente tema, se identifican modelos de red con carencias de estándares, técnicas y mecanismos de seguridad, y que este estudio propone optimizar estos modelos.

1.3 Alcance de revisión

En la actualidad existen muchas bibliotecas virtuales que disponen de una gran cantidad de artículos publicados relacionados con el tema, en este estudio nos hemos enfocado en el análisis de mecanismos, estándares de seguridad implementadas en organizaciones. Este estudio se enfoca al análisis de riesgos, amenazas o pérdida de información en áreas informáticas y administrativas. Para el desarrollo de este artículo se revisan artículos científicos, referencias de publicaciones indexadas, búsquedas en Google Scholar y diferentes bases científicas disponibles.

1.4 Variables de análisis de riesgos

Muchos de los artículos mencionaban diferentes amenazas que existían en diferentes activos de un ambiente distribuido u organización, estos son factores que ayudan a mantenerla segura, ya que a veces estos activos por la perdida, daño, o cualquier otra incidencia catastrófica puede llegar a poner en riesgo mucha información interna [23, 37, 38] tal como se muestra en la tabla 2.

Tabla 2. Variables en el análisis de riesgo

Activos	Amenazas	Vulnerabilidades
Antivirus	Programa maligno, archivos infectados	No existe software antivirus
Switch, router	Carencia de configuración de VLANs, daño de dispositivo	Sin mantenimiento preventivo
Cortafuegos	Carencia de actualización en las políticas de seguridad	Falta de actualizaciones
Servidores	Daño de componentes o so-brecalentamiento	Sin mantenimiento, no existe medidor de temperatura
Base de datos	Pérdida de información	Respaldo de datos no activa
Infraestructura de redes	Cableado defectuoso	Sin mantenimiento preventivo

1.5 Estrategia de búsqueda

En esta fase de realiza la lectura de artículos científicos y sus referencias, conferencias de bases abiertas entre otras. Se utiliza las bases de datos de IEEExplore, Scopus, Web of Science, Science Direct, ACM Library entre las principales, donde se introduce palabras claves relacionadas con el tema del presente artículo, en la Tabla 3 se detallan.

Tabla 3. Búsqueda de artículos con palabras claves

Concepto	Términos y sinónimos
Seguridad	Security model
Modelos de red segura	Prototype Secure Network
Ambiente distribuido	Environment distributed
Mecanismos de seguridad	Security mechanism, techniques

La búsqueda que se realiza es por el tema y palabras claves para tener mejores resultados al momento de investigar, estos estudios se consideraran desde el año 2015 hasta el año 2020. Este rango de fechas se utiliza, ya que existen modelos de red obsoletas de anteriores años por lo que no es recomendable desarrollar un modelo sobre esas investigaciones que otros autores lo determinan, se utilizan investigaciones de los cinco últimos años disminuyendo a tres años en lo posible.

1.6 Esquema de caracterizacion

Se utilizan artículos y trabajos que evidencien metodologías, técnicas, procesos de seguridad en las diferentes áreas o entornos administrativos y que se detecte la implementación de un modelo de red segura. De esa revisión se categoriza y se sintetiza la información para el diseño de una propuesta que evite riesgos de seguridad en la transferencia de información, al igual que permite responder a las preguntas de investigación que se realizan anteriormente, se muestra este proceso en la Tabla 4.

Tabla 4. Esquema de caracterización

Preguntas	Respuesta
Q1. ¿Qué propuestas existen sobre la implementación de modelos de red segura?	a) Estándares b) Métodos c) Procesos d) Evaluaciones e) Otros
Q2. ¿Qué evidencia empírica existe sobre los modelos de red segura?	a) Mapeo sistemático b) Propuesta c) Pasos d) Análisis e) Otros
Q3. ¿Qué métodos, normas, materiales se usan para implementar un modelo de red segura?	a) NSA/IAM b) SGSI c) ISO/IEC 27001 d) Mecanismos e) Requisitos f) Otros

1.7 Análisis de resultados

Se analizan los estudios que respondan a las preguntas de investigación que se realizan en el esquema de caracterización, se muestran los porcentajes de artículos que contienen las correspondientes respuestas de palabras claves.

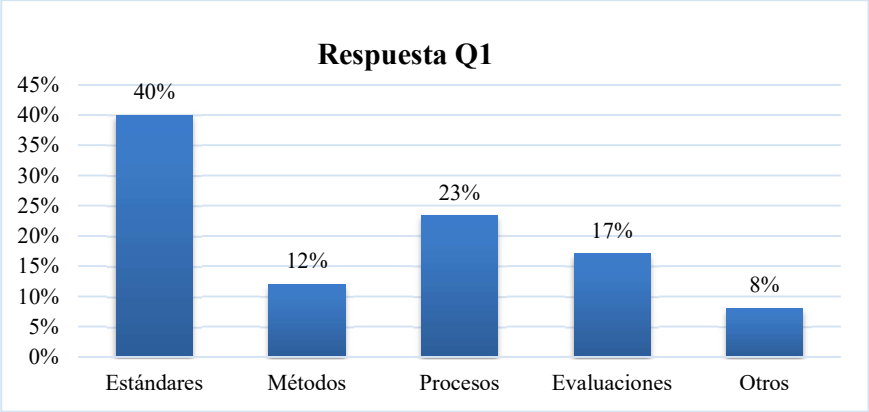

Fig. 1. Pregunta Q1: ¿Qué propuestas existen sobre la implementación de modelos de red segura?

La gráfica de la respuesta a la pregunta de investigación Q1, determina que el 40% de las propuestas existentes en la revisión de los trabajos, utilizan estándares para el diseño e implementación del modelo de red en las organizaciones, un 12% utiliza metodologías establecidas por la organización, un 23% utiliza procesos de la organización, un 17% evaluaciones y un 8% otros modelos a medida (ver Fig. 1).

La gráfica de la respuesta a la pregunta de investigación Q2, sobre la evidencia empírica existente sobre modelos de red segura, obteniendo que el 18% de los trabajos analizados evidencia una propuesta de una modelo, un 52% evidencian un mapeo sistemático de procesos que finalizan en un modelo, un 10% evidencian un conjunto de pasos definidos, un 8% evidencian solo un análisis y un 12% otras formas de propuesta empírica (ver Fig. 2).

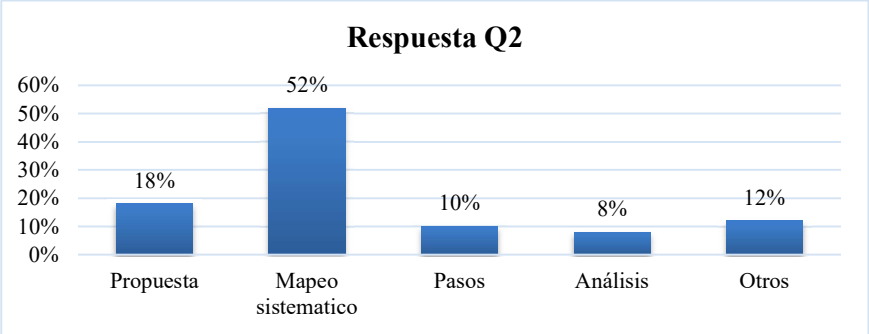

Fig. 2. Pregunta Q2: ¿Qué evidencia empírica existe sobre los modelos de red segura?

La gráfica de la respuesta a la pregunta de investigación Q3, determina que el 9% de las propuestas existentes en la revisión de los trabajos, utilizan estándares NSA/IAM para el diseño e implementación del modelo de red en las organizaciones, un 25% utiliza SGSI, un 22% utiliza ISO/IEC 27001, un 35% mecanismos de desarrollo, un 7% requerimientos específicos y un 2% otros requisitos para la implementación del modelo de red (ver Fig. 3).

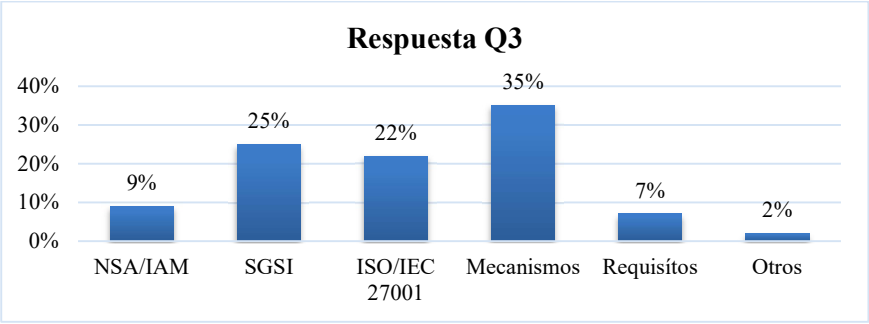

Fig. 3. Pregunta Q3: ¿Qué métodos, materiales usar para implementar un modelo de red segura?

2 Materiales y métodos

Se utiliza el método deductivo de investigación exploratoria para analizar información de artículos científicos de acuerdo con el tema de investigación, trabajos en los que se implementaron modelos de red. Para llevar a cabo una correcta gestión de seguridad al momento de implementar un modelo de red en un entorno distribuido se toma en cuenta puntos clave que sigan una secuencia de actividades, mediante una metodología.

Los materiales, técnicas, estándares, mecanismos y medios utilizados están basados en la investigación de otros trabajos relevantes que se analizaron para poder obtener resultados para la propuesta del modelo de red.

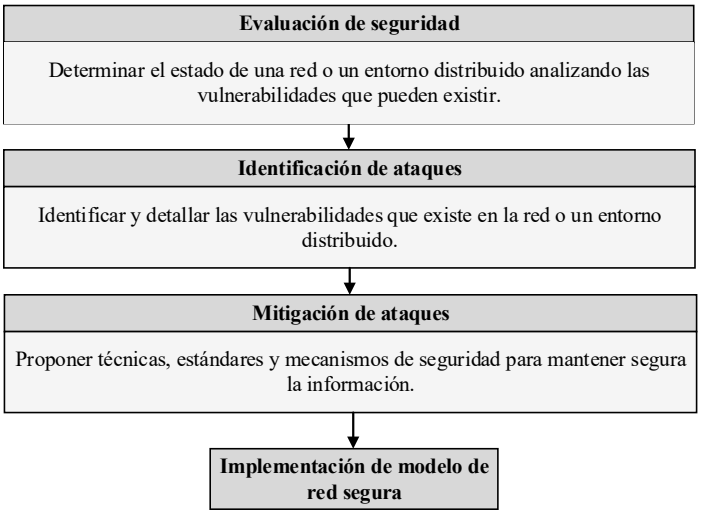

Fig. 4. Metodología propuesta para la implementación del modelo de red

La metodología propuesta describe el proceso en fases, evaluación, identificación, mitigación e implementación un modelo de red para la transferencia segura de información en ambientes distribuidos. Teniendo en cuenta que para mantener una correcta gestión de seguridad es necesario cumplir con cada una de las fases mencionadas (Fig. 4).

Evaluación de seguridad.

Para realizar una evaluación de seguridad dentro de un entorno distribuido, se presentan opciones como las pruebas de vulnerabilidades. Dentro de estas pruebas se incluyen el análisis de la red, mecanismos, estándares, políticas y pruebas de seguridad dando paso al escaneo y simulación de ataques, así lograr un informe de los riesgos,

vulnerabilidades y amenazas encontradas en las evaluaciones afinando las diferentes sugerencias que se permiten dar en la implementación de mecanismos de seguridad [39].

Este proceso de recolección de información en un entorno referente al descubrimiento de vulnerabilidades existentes dentro de una organización es importante para alguien que desee implementar la parte práctica a futuro, por lo que no se trata a fondo en el presente artículo. Se pueden aplicar normas, auditorias para el escaneo de vulnerabilidades o evaluación de una red tenemos:

1. NSA IAM: Este estándar trabaja para la evaluación de vulnerabilidades teniendo una perspectiva organizacional a diferencia de una técnica, esta generalmente evita los procesos documentados o actividades que no tengan nada que ver con la organización es decir trabajos informales.
2. Auditoria de seguridad: En esta parte el auditor de una organización debe realizar un proceso que consta en la revisión del funcionamiento de determinados entornos de la empresa y el análisis de vulnerabilidades [33], uno de los pasos a seguir por parte de un auditor debe ser:

- Verificar y analizar si el sistema de seguridad que se tiene implementado en la organización cumple con los estándares de protección u otras herramientas que cumplen funciones como la protección del sistema informático y la información.
- Elaborar un informe con todos los resultados encontrados en el primer paso de evaluación para que con eso se tenga a detalle de lo que se tiene implementado en la organización.
- Describir el Modelo NSA utilizado.

En la tabla 5 se describe los pasos o fases que tiene el modelo NSA para poder implementar un buen modelo de seguridad dentro de una organización, por lo que es conveniente seguir con todas las fases en orden y exactitud.

Tabla 5. Fases del modelo NSA

Fases	Descripción
Avalúo	En esta fase se recopila y se examina las diferentes políticas, mecanismos, estándares de seguridad que se tienen implementadas en la organización, también se realiza un análisis de las funciones críticas de la misma.
Evaluación	En esta parte se debe realizar test de seguridad del sistema en general, incluyendo equipos de redes como el firewall, routers, switch entre otros, realizando el escaneo de la intranet utilizando herramientas adecuadas.
Penetración	Una forma de realizar una evaluación segura es que un integrante de la organización realice la prueba de penetración en el intenta acceder de forma legal a la red con el fin de encontrar los puntos más débiles que existen.

Informes	En esta fase se detalla con informes, escritor o documentos todos los puntos que se evaluaron, es decir llevar un listado de las vulnerabilidades, problemas, errores que se encontraron a lo largo de la evaluación.
Sugerencias	Finalmente, los evaluadores recomiendan herramientas, estándares de seguridad, normas, mecanismos para poder implementarlos en la red organizacional.

Identificación de ataques.

Así como existen medidas de seguridad también se involucra los tipos de vulnerabilidades que puede existir en una organización, existen intrusos que pueden llegar a obtener información o hacer manipulación de esta, desarrollando algún software malicioso que puede llegar a ser fácil de ingresar en una organización cuando no existen usuarios con conocimientos básicos en ataques o formas de robar información [40] e incluso existen empresas que no cuentan con software de seguridad que eviten esto como es el antivirus.

- Rastreador de trafico de red: Algo esencial que ayuda a que los atacantes tengan rápido acceso a la red es mediante la captura de paquetes de datos y tramas que circulan, a partir de los resultados que obtienen estas personas pueden realizar ataques a servidores dependiendo de la seguridad que se tenga para ingresar a dichos equipos incluso al sistema o base de datos empresarial, en el momento que una atacante este dentro de la red es posible que haga lo que él quiera, pero es importante saber que es posible que logra obtener usuarios y contraseñas propias de la empresa y con dichos datos realizar el robo de información sin dejar sospecha, lo que ocasionaría que un entorno esté en peligro, dependiendo de la información que tenga.
- Ataques de denegación de servicio: Esta vulnerabilidad puede llegar a convertirse en algo esencial para los atacantes ya que su objetivo principal es detener los servicios de los servidores cancelando solicitudes de petición de otros usuarios provocando que queden totalmente inaccesible para los usuarios internos que se comunican mediante una red.
- Enmascaramiento IP: Un atacante puede hacer manipulación de paquetes TCP/IP con el fin de recibir o enviar información a otros usuarios, pero usando la autenticación e identidad de otra persona, falsificando la IP es decir tomando IP de otro usuario valido para poder tener privilegios a través de la suplantación de direcciones.
- Virus o Programa maligno: esta vulnerabilidad se da mucho hoy en día de parte de los intrusos ya que son programas que desarrollan ellos mismo para poder distribuirlo en una organización ocasionando fallos en las computadoras de los usuarios, por lo general estos virus llegan a infectar otros archivos sin que el usuario se dé cuenta dando como resultado la alteración o modificación de información con el fin de destruir información que se encuentra almacenada de forma local.

Mitigación de ataques.

Cuando se haya hecho el escaneo de vulnerabilidades, ataques, amenazas entre otros y teniendo listo el informe detallado de cada una es necesario que se implementen medidas de seguridad que mitiguen estos ataques con el fin de contrarrestarlos y que al momento de un ataque este no afecte de forma crítica la información de la empresa, si es que es posible que no existe riesgo y se bloqueen o eliminen del todo, pero ningún sistema de seguridad es 100% eficiente, ya que no solo depende se software sino que también dependen de los usuarios, ya que pesar de tener todas las medidas y mecanismos de seguridad implementadas, esta no nos ayudara a protegernos contra una contraseña fácil de adivinar por el intruso [41].

Se pueden usar software como es el antivirus organizacional, es muy importante disponer de uno ya que a diario existen programas maliciosos que puedan llegar a atacar la información, incluso poniendo en riesgo los datos. Entre otras formas de mitigar es implementando estándares de seguridad, medidas y mecanismos que se detallarán más adelante en la sección de materiales.

2.1 Requerimientos para el diseño del modelo

Se presenta en esta sección los procesos, estándares y los mecanismos que se quieren establecer en un modelo de red para la implementación, el diseño de un modelo de red debe estar estructurada con normas de seguridad e incluso disponer de dispositivos de comunicación para la seguridad de la intranet como es el firewall.

Sistema de gestión de seguridad.

Esta metodología fue utilizada ya que describió el contenido que hay en las diferentes etapas mientras se desarrolla el diseño estructural organizacional, operación e implementación de un SGSI [42], este método se apoyó por la norma ISO/IEC 27001 que también está relacionado con la implementación y revisión de un SGSI, en su desarrollo se usó definiciones ligadas al estándar ISO/IEC 27000 pero analizando en particular el estándar 27001.

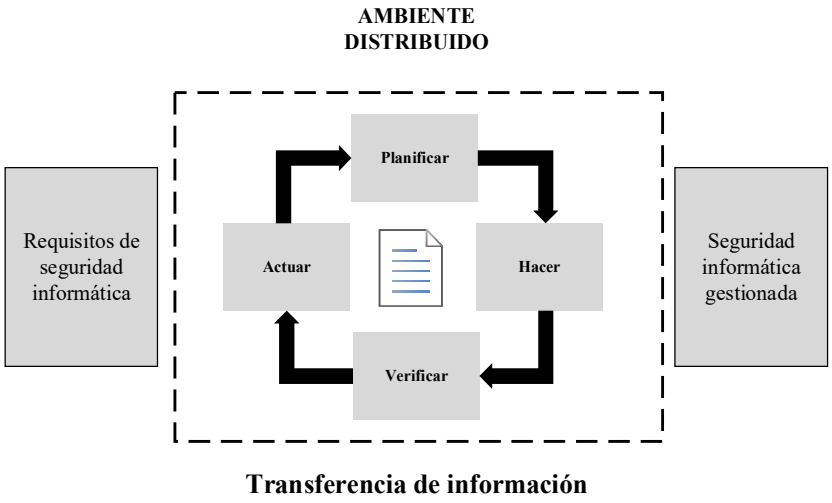

Fig. 5. Proceso de gestión de seguridad

En la figura 5 se describe las etapas PDCA (Planificar, hacer, verificar y actuar) que se deriva por las iniciales en inglés, que ayudara a tener mejoras continuas, es decir que todo esto conlleve a la disminución de riesgos, fallas, problemas, solución de errores y problemas en la seguridad. Este proceso es un ciclo por lo que cuando llegue a la última fase tendrá que volver a iniciar con la primera fase, ya que esto ayuda a que todas las actividades dentro de un ambiente distribuida sean evaluadas periódicamente logrando incorporar nuevas mejores en la seguridad. En la tabla 4 se detalla con mayor información la función y tareas que tienen cada uno de los procesos [42].

Tabla 6. Proceso de gestión de seguridad

Proceso	Definición
Planificar	Este proceso trata de buscar las actividades dispuestas a mejorar que ayudara a establecer objetivos a alcanzar, para buscar las mejoras es necesario buscar nuevas tecnologías con respecto a las que ya están implementadas, también es necesario escuchar opiniones de los demás para poder mejores en diferentes aspectos.
Hacer	Aquí se realizan los cambios que fueron planificados en la primera etapa logrando implementar la mejora propuesta, es recomendable que se realicen pruebas ya que en este proceso se desea implementar controles que se analizaron anteriormente, ya que puede tener errores.

Verificar	Cuando se implementa la mejora después de haber hecho las pruebas es necesario dejar un tiempo de prueba para que su funcionamiento sea correcto, después de ese tiempo si la mejor no es eficaz[42] o no cumple con las expectativas desde el inicio será necesario modificarla hasta que logre los objetivos esperados.
Actuar	En el proceso final del ciclo, una vez que se finalice el tiempo de prueba es decir el proceso de verificar, será necesario visualizar los resultados que se logró y comprobar con el funcionamiento de las tareas o actividades antes de haber sido implementada la mejora. Los resultados deben ser eficaces ya que en este último proceso de implementa de forma definitiva.

ISO/IEC 27001

Este estándar está destinado para aquellas empresas privadas o públicas que contengan un entorno inseguro, para que así logren utilizarla como un apoyo o ayuda para la implementación de un buen Sistema de Gestión de Información y también para la selección de controles de seguridad.

Esta norma también está diseñada para poder determinar puntos de seguridad críticos en una organización y que también toma en cuenta el ambiente si es que existe algún riesgo o peligro de seguridad de datos. Existen grandes empresas que, aunque no sean tan importantes no son seguros dentro de ISO/IEC 27001[43], si se quiere saber que sistemas de control están establecidos dentro de un sistema distribuido es necesario establecer una planificación cuidadosa, poniendo importancia a los detalles, es necesario que exista un respaldo al momento de gestionar los procedimientos adecuados.

Es importante que una empresa tenga claro lo que va a requerir en cuanto a seguridad, ya que un sistema de gestión de seguridad conserva la disponibilidad, integridad y confidencialidad en la transferencia de información, esto ayuda a generar confianza a personal interno de una organización, ya que los riesgos se gestionan correctamente. En este Estándar existen funciones y responsabilidades que deben ser tomadas en cuenta para la seguridad de la información, ya que de esto depende de que responsabilidades se le va a asignar en un puesto de trabajo o un trabajador en el ámbito de la seguridad informática, pero no solo hay que asignar funciones al personal o al puesto de trabajo políticas, tareas, funciones o roles, es necesario dar un aviso o comunicar al usuario para que tenga en consideración que funciones o roles tiene su cargo para evitar inconvenientes, confusión o pérdida de tiempo al momento de realizar su tarea según su cargo.

Requisitos de seguridad.

Para que la información tenga un gran alto de seguridad es necesario mantener mecanismos de seguridad, pero para eso deben cumplir con un conjunto de requisitos que se mencionan en la Tabla 7.

Tabla 7. Requisitos de seguridad de la información

Procesos	Definición

Confidencialidad	Este requisito trata de salvaguardar la información de personas no autorizadas que quieran acceder a datos confidenciales de otras personas o a los servidores, ya que puede haber personas que quieran ingresar y hacer mal uso o filtrar datos confidenciales [44]. Existen posibilidades negativas que pueden lograr los atacantes, como editar datos una vez tenido el acceso total a la información. Hay que tener en cuenta que la información debe ser de único acceso al personal que se le asigna la autorización
Integridad	Este requisito es de suma importancia, la información original debe permanecer ahí sin ser manipulada por cualquier persona, debe existir garantía de la autenticidad de la información y datos, es importante que esta información no sea editada o alterada de forma incorrecta [45] por personas a las que no se les haya concebido la autoridad necesaria para el manejo de archivos.
Disponibilidad	Otro elemento necesario que fue analizado es la disponibilidad, ya que es fundamental tener al alcance todo tipo de datos con acceso único para el usuario que tenga función o autorización de manipulación, es decir que exista integridad por parte del usuario, este requisito nos ayudó a garantizar que la información se mantenga segura en todo momento, ya que en el momento que exista ausencia de datos, cuando el usuario solicite acceso a estos, esto conducirá a una perdida que no podrán ser recuperables por más que se usen programas de tercero.
Confiabilidad	Este término es importante ya que se refiere a que tanto se puede creer o confiar en la información que se tiene o que brinda una organización. Es importante saber la procedencia de la información, solicitudes, datos que llegan a nuestros destinos, para ello se revisa un factor, como el origen del archivo.

Mecanismos de seguridad.

Analizado los requisitos anteriormente, es necesario contar con mecanismos de seguridad ya que van tomadas de la mano con los requisitos para la implementación de un modelo de red segura, estos pueden llegar a ser beneficiosos para la correcta implementación de un sistema seguro en la transferencia de archivos.

Autenticación.

Esto permite identificar a los usuarios con sus datos personales, para saber a quién pertenece algún rol en su función de trabajo, es decir según el puesto en el que está ubicado y así asignarle sus tareas correspondientes[46], sin autenticación todo sería un desastre, no habría un buen control, usuarios con tareas incorrectas, roles que no correspondan según el usuario entre otros factores negativos

Auditoria.

Este mecanismo verifica que todas las políticas, permisos estén en correcto funcionamiento y asignada según el usuario, ubicación, área, rol etc. Fue necesario establecer los permisos adecuados[33] para el manejo de datos de forma legal, sin cuestionar a detalle el uso indebido por parte de otras personas, evitar desconfianza y mal uso de información.

Autorización.

Esto se logra una vez superado el mecanismo de autenticación, por lo que es importante autenticarse para dar autorización al usuario a que sitio, archivo, información puede acceder con autorización, esto ayudó a controlar el acceso restringido a cierta información explícita que existe en un sistema.

Firewalls.

Este mecanismo es muy importante cuando existen servidores que se publican o tiene salida a internet, estos pueden ser servidores Web, SMTP entre otros, por lo que es conveniente mantener seguro la red local con firewall, implementando políticas de seguridad en redes, evitando la conexión mediante autenticación con claves o permisos. Los firewalls funcionan como un dispositivo de seguridad que monitorea la red entrante y saliente, como se indicó anteriormente, este decide si permite o no deniega la entrada de tráfico mediante reglas definidas que son configuradas dentro de este, este dispositivo ayuda a establecer una barrera entre la intranet y la red externa [47].

Existe también las VPN que ayuda a que un empleado se pueda conectar a la intranet de una organización utilizando internet, para esto se establece dos mecanismos importantes como es la autenticación y autorización que se mencionaron anteriormente, se detalla a continuación de cómo trabaja un firewall en un trabajo remoto en la figura 6.

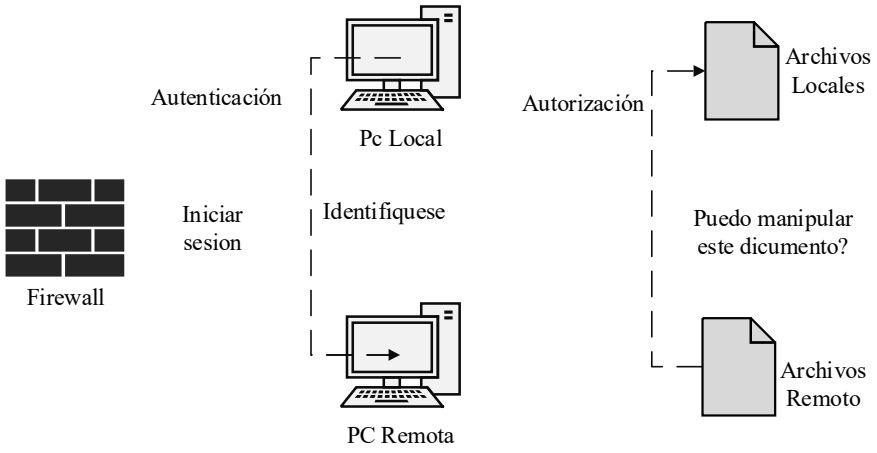

Fig. 6. Restricciones de seguridad para trabajos remotos

En la figura 6 se muestran tres mecanismos para restringir el acceso a los equipos o sistemas de forma remota, que es el firewall, autenticación y autorización

En la primera parte donde se ubica el firewall se establecen las reglas de permiso o bloqueo que ayuda a restringir las operaciones remotas que se realicen con sistemas que están fuera del firewall.

En la segunda parte donde se ubica los equipos, los equipos remotos utilización el mecanismo de autenticación en donde ayudara a restringir el acceso solo para usuarios restringido, es decir que tengan un usuario y contraseña.

Por último, tenemos la gestión de archivos en donde se aplica el mecanismo de autorización que ayuda a impedir que los usuarios que fueron autenticados realicen operaciones o trabajos en sus sistemas de archivos.

Encriptación.

A pesar de que se implementen otros mecanismos importante, la encriptación no puede faltar en ningún momento, esto ayudará a que la información este mas segura contra usuarios que tengan acceso a la red, la función de este mecanismo es mantener la información oculta que se transmite creando un cifrado entre el receptor y emisor de la comunicación, evitando que otras personas se intercepten en dicha comunicación, en caso que no existiese encriptación cualquier atacante puede ingresar y alterar o robar la información.

Respaldos.

Es necesario que existan respaldos de información y más cuando se tiene una base de datos extensa, que esto ayudara a que la información este siempre disponible para toda la organización, y en caso de que exista alguna falla de la base de datos esta se pueda restaurar sin ningún problema, puede llegar a ser una catástrofe por el un daño de hardware y enseguida se necesite cambio de hardware y no tener un respaldo puede ser un riesgo grande.

Antivirus.

Este mecanismo puede llegar a ser indispensable en un ambiente en la que existen personas que cargan y descargan información, existen muchas áreas, la más vulnerable puede llegar a ser áreas donde no tengan mucho conocimiento de informática, por lo que son las vulnerables a que los atacantes ingresen mediante los equipos de dicha área, aunque la área de Tecnología puede llegar a ser más vulnerable que el resto, ya que dicha área está en constante descarga de programas sea cual sea su procedencia, para ello es necesario contar con un servidor de antivirus para la organización o ambiente distribuido, esta evitara que les notifique cuando descarguen algo de procedencia no segura, evitando que su equipo local se infecte a perjudique a la organización.

3 Resultados y discusión

3.1 Resultados

El análisis de estándares de seguridad, técnicas, mecanismos entre otros factores extraídos de artículos de relevancia permite lograr un modelo de una red segura para la transferencia de información manteniendo siempre el orden de procesos, fases, técnicas

mostradas en otras etapas de este artículo, luego de realizar estudios de otras fuentes se diseñó un modelo de red para las organización teniendo en cuenta alternativas de seguridad, mejorando y actualizando varias característica que tiene una red, tanto en equipos informáticos locales, equipos de comunicación de seguridad como la implementación de firewalls con sus respectivas reglas.

A pesar de que internet se actualiza y surgen nuevas técnicas de atacar a la información será necesario actualizar las medidas de seguridad, ya que así como avanza la tecnología también se van quedando obsoleta lo que en su día se implementó, por eso es necesario no siempre limitarse a un modelo de red sino también ver alternativas que sean mejores, y no solo se trata de modificar características en el ambiente de redes sino que los usuarios internos también deban actualizarse con cursos, documentos, lectura, ya que gran responsabilidad también lo tiene el usuario

En la figura 7 se propone un prototipo de modelo de red segura para un entorno distribuido en la que existe mucho tráfico de archivos entre usuarios y servidores. Para esto aplicamos algunos mecanismos, objetivos que se establecieron anteriormente dentro de los materiales y métodos, la ventaja de implementar VLANs que viene dentro del mecanismo de disponibilidad, es que ofrece mayor seguridad en la comunicación entre usuarios que se encuentren en otras redes, esto refuerza la confidencialidad y otros factores.

Se determinó una zona desmilitarizada manteniendo los servidores que se publican en internet por separado para que exista menos ataques a los servidores de la intranet.

Para mantener la disponibilidad en todo momento en un entorno distribuido fue necesario implementar switch de respaldo que ayuda a que la comunicación no se pierda, es decir en caso de que exista alguna falla en un switch principal entra en funcionamiento el switch de respaldo evitando así las interrupciones.

Así también se determinó firewalls que disponen de reglas de seguridad para quienes tengan único acceso a la red, esto varía dependiendo de las políticas que se implementen.

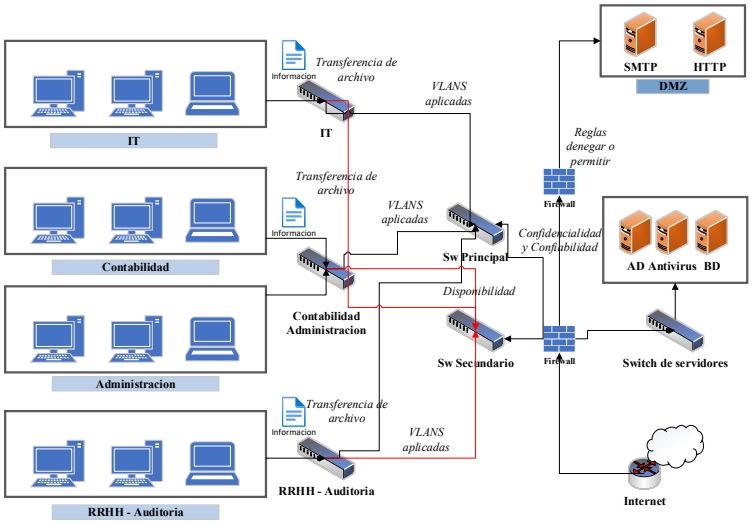

Fig. 7. Modelo de red segura para la transferencia de información.

3.2 Discusión

Las vulnerabilidades, riesgos y amenazas que existan dentro de un ambiente distribuido u organización siempre van a estar presente y en aumento, ya que no se los pueden eliminar completamente pero si reducir los ataques críticos a una base de datos o información interna de usuarios, aunque se lograron proponer medidas de seguridad no siempre serán eficaces, ya que se vuelven vulnerables con el pasar del tiempo, por lo que es conveniente actualizar muchos factores de seguridad, también los usuarios deberán entrenarse para hacer uso de algún sistema de forma correcta.

4 Conclusiones

Se concluye que mantener seguro un ambiente distribuido mediante un modelo de red debe basarse en estudios correspondientes de seguridad que son:

Se demuestra en este trabajo cómo afectan los ciberataques a los entornos distribuidos que no tienen implementado mecanismos de seguridad para la transferencia de información

Se define un modelo de red para evitar el riesgo del manejo no autorizado de la información en un sistema de comunicación distribuido.

Se compara los diferentes modelos de red de seguridad en los ambientes distribuidos y determinando cuales tienen un alto grado de efectividad, esto nos ayudó a actualizar el modelo del presente artículo con los estándares de seguridad y otros mecanismos.

Se diseña un modelo de red segura para un entorno distribuido para la protección de transferencia de datos utilizando estrategias básicas de seguridad.

Referencias

1. Martínez Rodríguez, W.H., others: Análisis de la evolución del aseguramiento informático en entidades del sector gobierno colombiano. (2020).
2. Estela Campos, M.A.: Implementación de un security information and event management (SIEM) para detectar vulnerabilidades y amenazas expuestas en las plataformas informáticas y redes de una entidad financiera. (2020).
3. Bravo Indacochea, G.E., Barrera Landires, F.A.: Auditoría de seguridad informática en la red de datos de una empresa utilizando como mecanismo de hacking ético el sistema operativo kali linux previo a la propuesta de implementación del firewall PFSENSE y correlacionador de eventos SIEM., (2020).
4. Rosales Reyes, J.D.: Plan de respuesta a incidencias de seguridad informática (IRP) para la Dirección de Tecnologías de la información de la UPSE, (2020).
5. Banga, G.: Why Is Cybersecurity Not a Human-Scale Problem Anymore? Commun. ACM. 63, 30–34 (2020). https://doi.org/10.1145/3347144.
6. AlGhamdi, S., Win, K.T., Vlahu-Gjorgievska, E.: Information security

governance challenges and critical success factors: Systematic review. Comput. Secur. 99, 102030 (2020). https://doi.org/10.1016/j.cose.2020.102030.
7. López, C., Parra, A.: Análisis técnico de los recursos disponibles de la UEFS Santa María Mazzarello de Guayaquil para el diseño e implementación de un escenario de arquitectura, http://dspace.ups.edu.ec/handle/123456789/10286.
8. Llerena, J., Mendez, A., Sanchez, F.: Analysis of the Factors that Condition the Implementation of a Backhaul Transport Network in a Wireless ISP in an Unlicensed 5 GHz Band, in the Los Tubos Sector of the Durán Canton. In: 2019 International Conference on Information Systems and Computer Science (INCISCOS). pp. 15–22. IEEE (2019). https://doi.org/10.1109/INCISCOS49368.2019.00012.
9. Rostami, E., Karlsson, F., Gao, S.: Requirements for computerized tools to design information security policies. Comput. Secur. 99, 102063 (2020). https://doi.org/10.1016/j.cose.2020.102063.
10. Urquiza, D., Vallejo, J.: Desarrollo de una aplicación web para la gestión de roles de pago y control de asistencia del personal de la empresa Andrés Arturo Coka Cía. Ltda., http://dspace.ups.edu.ec/handle/123456789/16409.
11. Carcamo, L., Pazmiño, S.: Desarrollo de aplicación web para la gestión de nómina del local máquinas Hidalgo., http://dspace.ups.edu.ec/handle/123456789/16768.
12. López-Chila, R., Llerena-Izquierdo, J., Sumba-Nacipucha, N.: Collaborative Work in the Development of Assessments on a Moodle Learning Platform with ExamView. Adv. Intell. Syst. Comput. 1277, 131–141 (2021). https://doi.org/10.1007/978-3-030-60467-7_11.
13. Llerena-Izquierdo, J., Procel-Jupiter, F., Cunalema-Arana, A.: Mobile Application with Cloud-Based Computer Vision Capability for University Students' Library Services. Adv. Intell. Syst. Comput. 1277, 3–15 (2021). https://doi.org/10.1007/978-3-030-60467-7_1.
14. Brunner, M., Sauerwein, C., Felderer, M., Breu, R.: Risk management practices in information security: Exploring the status quo in the DACH region. Comput. Secur. 92, 101776 (2020). https://doi.org/10.1016/j.cose.2020.101776.
15. Guo, J., Wang, L.: Learning to upgrade internet information security and protection strategy in big data era. Comput. Commun. 160, 150–157 (2020). https://doi.org/10.1016/j.comcom.2020.05.043.
16. Salazar, L.: Implementación de sistema de matriculación y carnetización en la unidad educativa Pablo Picasso., http://dspace.ups.edu.ec/handle/123456789/16844.
17. Loor García, Y.Y.: Desarrollo de aplicación web para la gestión de consultas y agendamiento de citas de mascota de la clínica veterinaria burgos., https://dspace.ups.edu.ec/handle/123456789/16991.
18. Montenegro Cruz, A.: Diseño e implementación de un software educativo para niños discapacitados de SERLI en la ciudad de Guayaquil, http://dspace.ups.edu.ec/handle/123456789/3185.
19. Montalvo E., A., Morán V., P.: Propuesta de un Sistema de Gestión del conocimiento para el Departamento de Tecnología de la Información y la

incidencia Económica para el Grupo MAVESA, https://dspace.ups.edu.ec/handle/123456789/3653.
20. Murillo, K.: Desarrollo de aplicación web para la gestión y control académico de la escuela particular Lidia Dean de Henríquez., http://dspace.ups.edu.ec/handle/123456789/17146.
21. Sanunga Totoy, J.E., Pérez Palma, K.N.: Implementación del sistema para el control de historia clinica de pacientes en centro odontologico dental group., https://dspace.ups.edu.ec/handle/123456789/16767.
22. Abbass, W., Baina, A., Bellafkih, M.: Survey on information system security risk management alignment. In: 2016 International Conference on Information Technology for Organizations Development, IT4OD 2016. Institute of Electrical and Electronics Engineers Inc. (2016). https://doi.org/10.1109/IT4OD.2016.7479260.
23. Semin, V.G., Khakimullin, E.R., Kabanov, A.S., Los, A.B.: Problems of information security technology the "Internet of Things." In: Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2017. pp. 110–113. Institute of Electrical and Electronics Engineers Inc. (2017). https://doi.org/10.1109/ITMQIS.2017.8085775.
24. Song, H.H.: Testing and evaluation system for cloud computing information security products. In: Procedia Computer Science. pp. 84–87. Elsevier B.V. (2020). https://doi.org/10.1016/j.procs.2020.02.023.
25. Sauerwein, C., Pekaric, I., Felderer, M., Breu, R.: An analysis and classification of public information security data sources used in research and practice. Comput. Secur. 82, 140–155 (2019). https://doi.org/10.1016/j.cose.2018.12.011.
26. Zonouz, S.A., Berthier, R., Khurana, H., Sanders, W.H., Yardley, T.: Seclius: An information flow-based, consequence-centric security metric. IEEE Trans. Parallel Distrib. Syst. 26, 562–573 (2015). https://doi.org/10.1109/TPDS.2013.162.
27. Iyer, S.R., Simkins, B.J., Wang, H.: Cyberattacks and impact on bond valuation. Financ. Res. Lett. 33, 101215 (2020). https://doi.org/10.1016/j.frl.2019.06.013.
28. Llerena-Izquierdo, J., Barberan-Vizueta, M., Chela-Criollo, J.: Novus spem, 3D printing of upper limb prosthesis and geolocation mobile application. RISTI - Rev. Iber. Sist. e Tecnol. Inf. 2020, 127–140 (2020).
29. Llerena-Izquierdo, J., Merino-Lazo, M.: Aplicación móvil de control nutricional para prevención de la anemia ferropénica en la mujer gestante. Rev. InGenio. 4, 17–26 (2021). https://doi.org/10.18779/ingenio.v4i1.364.
30. Izquierdo, J.L., Alfonso, M.R., Zambrano, M.A., Segovia, J.G.: Aplicación móvil para fortalecer el aprendizaje de ajedrez en estudiantes de escuela utilizando realidad aumentada y m-learning. Rev. Ibérica Sist. e Tecnol. Informação. 120–133 (2019).
31. Bland, J.A., Petty, M.D., Whitaker, T.S., Maxwell, K.P., Cantrell, W.A.: Machine Learning Cyberattack and Defense Strategies. Comput. Secur. 92,

101738 (2020). https://doi.org/10.1016/j.cose.2020.101738.
32. Ali, O., Shrestha, A., Chatfield, A., Murray, P.: Assessing information security risks in the cloud: A case study of Australian local government authorities. Gov. Inf. Q. 37, 101419 (2020). https://doi.org/10.1016/j.giq.2019.101419.
33. Sabillon, R., Serra-Ruiz, J., Cavaller, V., Cano, J.: A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In: Proceedings - 2017 International Conference on Information Systems and Computer Science, INCISCOS 2017. pp. 253–259. Institute of Electrical and Electronics Engineers Inc. (2018). https://doi.org/10.1109/INCISCOS.2017.20.
34. Zatuliveter, Y.S., Fishchenko, E.A.: Cybersecurity in the mathematically uniform algorithmic space of the distributed computing. In: Proceedings of 2017 10th International Conference Management of Large-Scale System Development, MLSD 2017. Institute of Electrical and Electronics Engineers Inc. (2017). https://doi.org/10.1109/MLSD.2017.8109713.
35. Arief, R., Khakzad, N., Pieters, W.: Mitigating cyberattack related domino effects in process plants via ICS segmentation. J. Inf. Secur. Appl. 51, 102450 (2020). https://doi.org/10.1016/j.jisa.2020.102450.
36. Bagay, D.: Information security of Internet things. In: Procedia Computer Science. pp. 179–182. Elsevier B.V. (2020). https://doi.org/10.1016/j.procs.2020.02.132.
37. Szczepaniuk, E.K., Szczepaniuk, H., Rokicki, T., Klepacki, B.: Information security assessment in public administration. Comput. Secur. 90, 101709 (2020). https://doi.org/10.1016/j.cose.2019.101709.
38. Toapanta, S.M.T., Cobeña, J.D.L., Gallegos, L.E.M.: Analysis of cyberattacks in public organizations in Latin America. Adv. Sci. Technol. Eng. Syst. 5, 116–125 (2020). https://doi.org/10.25046/aj050215.
39. Jeong, C.Y., Lee, S.Y.T., Lim, J.H.: Information security breaches and IT security investments: Impacts on competitors. Inf. Manag. 56, 681–695 (2019). https://doi.org/10.1016/j.im.2018.11.003.
40. Angraini, Alias, R.A., Okfalisa: Information security policy compliance: Systematic literature review. In: Procedia Computer Science. pp. 1216–1224. Elsevier B.V. (2019). https://doi.org/10.1016/j.procs.2019.11.235.
41. Zeng, W., Koutny, M.: Modelling and analysis of corporate efficiency and productivity loss associated with enterprise information security technologies. J. Inf. Secur. Appl. 49, 102385 (2019). https://doi.org/10.1016/j.jisa.2019.102385.
42. Macias, M., Barria, C., Acuna, A., Cubillos, C.: Apoyo al SGSI por Medio de la Clasificación de Malware Empleando Análisis de Patrones. In: 2016 IEEE International Conference on Automatica, ICA-ACCA 2016. Institute of Electrical and Electronics Engineers Inc. (2016). https://doi.org/10.1109/ICA-ACCA.2016.7778516.
43. Longras, A., Pereira, T., Cameiro, P., Pinto, P.: On the Track of ISO/IEC 27001:2013 Implementation Difficulties in Portuguese Organizations. In: 9th International Conference on Intelligent Systems 2018: Theory, Research and

Innovation in Applications, IS 2018 - Proceedings. pp. 886–890. Institute of Electrical and Electronics Engineers Inc. (2018). https://doi.org/10.1109/IS.2018.8710558.

44. Al-Far, A., Qusef, A., Almajali, S.: Measuring Impact Score on Confidentiality, Integrity, and Availability Using Code Metrics. In: ACIT 2018 - 19th International Arab Conference on Information Technology. Institute of Electrical and Electronics Engineers Inc. (2019). https://doi.org/10.1109/ACIT.2018.8672678.
45. Alkhudhayr, F., Alfarraj, S., Aljameeli, B., Elkhdiri, S.: Information Security:A Review of Information Security Issues and Techniques. In: 2nd International Conference on Computer Applications and Information Security, ICCAIS 2019. Institute of Electrical and Electronics Engineers Inc. (2019). https://doi.org/10.1109/CAIS.2019.8769504.
46. Hoffmann, R., Napiórkowski, J., Protasowicki, T., Stanik, J.: Measurement Models of Information Security Based on the Principles and Practices for Risk-Based Approach. In: Procedia Manufacturing. pp. 647–654. Elsevier B.V. (2020). https://doi.org/10.1016/j.promfg.2020.02.244.
47. Cheng, Y., Wang, W., Wang, J., Wang, H.: FPC: A new approach to firewall policies compression. Tsinghua Sci. Technol. 24, 65–76 (2019). https://doi.org/10.26599/TST.2018.9010003.