UNIVERSIDAD CIENTÍFICA DEL SUR

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS EMPRESARIALES

"DISEÑO DE UNA ARQUITECTURA DE SEGURIDAD INFORMÁTICA PARA INCREMENTAR LA SEGURIDAD DE INFORMACIÓN EN LA EMPRESA BAFING S.A.C. EN 2021"

Tesis para optar el título profesional de:
INGENIERO DE SISTEMAS EMPRESARIALES

Presentado por:

Josué David Asurza Cáceres (0000-0001-7679-1716)

Asesor:

Arturo Eduardo Garro Morey (0000-0001-6014-4055)

Lima - Perú

2022

UNIVERSIDAD CIENTÍFICA DEL SUR

ACTA DE SUSTENTACIÓN DE TESIS

Lima, 28 de abril de 2022

Los integrantes del Jurado de tesis:

Presidente	**JEAN MERRY SALAS ROJAS**
Miembro 1	**JOSÉ ALBERTO RODRÍGUEZ PARRA FERIA**
Miembro 2	**LUIS RICARDO CARPIO CENTELLAS**

Se reúnen para evaluar la tesis titulada:
"DISEÑO DE UNA ARQUITECTURA DE SEGURIDAD INFORMÁTICA PARA INCREMENTAR LA SEGURIDAD DE INFORMACIÓN EN LA EMPRESA BAFING S.A.C. EN 2021"

Presentado por el(la) bachiller.
JOSUÉ DAVID ASURZA CÁCERES

Para optar al título profesional de
INGENIERO DE SISTEMAS EMPRESARIALES

Asesorado(a) por:
ARTURO EDUARDO GARRO MOREY

Luego de haber evaluado el informe final de tesis y evaluado el desempeño de(l) (los) estudiante de la Carrera de **Ingeniería de Sistemas Empresariales** en la sustentación, concluyen de manera unánime (X) por mayoría simple ( ) calificar a:

Tesista:	JOSUE DAVID ASURZA CACERES		
Nota (en letras):	16		
Aprobado ( )	Aprobado - Muy buena (X)	Aprobado - Sobresaliente ( )	Desaprobado ( )

Los miembros del jurado firman en señal de conformidad.

JEAN MERRY SALAS ROJAS
Presidente(a) del Jurado

ARTURO EDUARDO GARRO MOREY
Asesor(a)

JOSÉ ALBERTO RODRÍGUEZ PARRA FERIA
Miembro 1

LUIS RICARDO CARPIO CENTELLAS
Miembro 2

T // (511) 610 6738
informes@cientifica.edu.pe
cientifica.edu.pe

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El objetivo del proyecto es demostrar que el diseño de arquitectura de seguridad informática puede incrementar la seguridad de información de la empresa BAFING S.A.C. La investigación tiene carácter experimental porque manipula la variable independiente "Arquitectura de Seguridad Informática" para impactar en la variable dependiente "Seguridad de Información", reforzando sus efectos. La empresa tiene por rubro el desarrollo de proyectos informáticos de seguridad de información, la misma que está integrada por consultores expertos en el campo de gestión de riesgos e implementación de sistemas de administración de software informático. La arquitectura propuesta ofrece mayor alcance para la protección de información como activo importante de las empresas que trabajan con equipos informáticos. Para llevar a cabo dicho propósito se evaluaron propuestas de software de seguridad objetivo seleccionado bajo un perfil elaborado de características y se juzgó cada uno de ellos confrontando sus resultados en función al cumplimiento de la integridad, confidencialidad y disponibilidad como pilares de concepto. Lo que permitió en el nivel administrativo el planeamiento de adquisición de nuevo software o renovación del mismo en función a la información obtenida.

Las herramientas de evaluación usadas en el proyecto fueron colectadas a partir de la información de entrevistas con especialistas en el rubro de protección de información y activos informáticos y están disponibles para evaluaciones futuras de otros productos de seguridad informática.

Los resultados obtenidos mostraron mejoras en las dimensiones de seguridad de información analizadas respecto a la situación actual de la empresa auditada BAFING S.A.C.

PALABRAS CLAVES. Información, seguridad, vulnerabilidad, Antivirus, DLP.

ABSTRACT

The objective of the project is to demonstrate that the design of computer security architecture can increase the information security of the company BAFING S.A.C. The research is experimental in nature because it manipulates the independent variable "Computer Security Architecture" to impact the variable dependent "Information Security", reinforcing its effects. The company's business is the development of information security computer projects, which is made up of expert consultants in the field of risk management and implementation of computer software management systems. The proposed architecture offers greater scope for the protection of information as an important asset of companies that work with computer equipment. To carry out this purpose, objective security software proposals selected under an elaborated profile of characteristics were evaluated and each one of them was judged comparing their results based on compliance with integrity, confidentiality and availability as pillars of the concept. This allowed, at the administrative level, the planning of the acquisition of new software or its renewal based on the information obtained.

The evaluation tools used in the project were collected from information from interviews with specialists in the field of protection of information and computer assets and are available for future evaluations of other computer security products.

The results obtained showed improvements in the information security dimensions analyzed with respect to the current situation of the audited company BAFING S.A.C.

KEYWORDS. Information, Security, Vulnerability, Antivirus, DLP.

INTRODUCCIÓN

En el presente, las empresas tratan información como un activo importante y parte crucial para el funcionamiento del negocio. De esta manera se tiene la necesidad de monitorizar y proteger la información que se trata a través de un ordenador. Con el objetivo de cubrir tal necesidad las empresas adquieren software de seguridad para aumentar los mecanismos de defensas que reducen el riesgo de que esta información pueda resultar vulnerada, alterada o no disponible temporal o permanentemente.

La diversidad de software de seguridad y sus componentes vienen presentados por cada empresa proveedora que se anuncia a sí misma como la mejor solución para cubrir dichos riesgos. En este proyecto se exponen los mecanismos de protección de cada solución de seguridad informática y se confrontan los productos objetivos a fin de comprobar que solución tiene un mayor índice de cumplimiento dimensiono en torno a disponibilidad, integridad y confidencialidad en el procesamiento de información y cumplimiento de políticas de seguridad empresarial.

CAPITULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

La innovación de la tecnología ha contribuido a que los empresarios y trabajadores transformen sus operaciones y la forma en cómo interactúan entre sí, convirtiendo los equipos informáticos en activos importantes para las organizaciones. Esto ha traído riesgos y dificultades en cuanto a la seguridad de la información y los canales por los que se trata por parte de los individuos.

En esta situación, a nivel mundial existen datos que reportan esta problemática, es así como Reclamitos (2018) publicó en Marketwatch la cantidad de incidentes de fuga de informaciones reportadas por las firmas Business, Medical, Educational, Government y Financial, entidades que fueron objeto de ataques informáticos entre los años 2005 al 2017. En la figura 1 se reporta el número de incidentes de fuga de datos detectados en las entidades desde el año 2005 (200 casos) y que progresivamente se ha ido incrementado preocupantemente las casuísticas hasta el año 2017 (1400 casos).

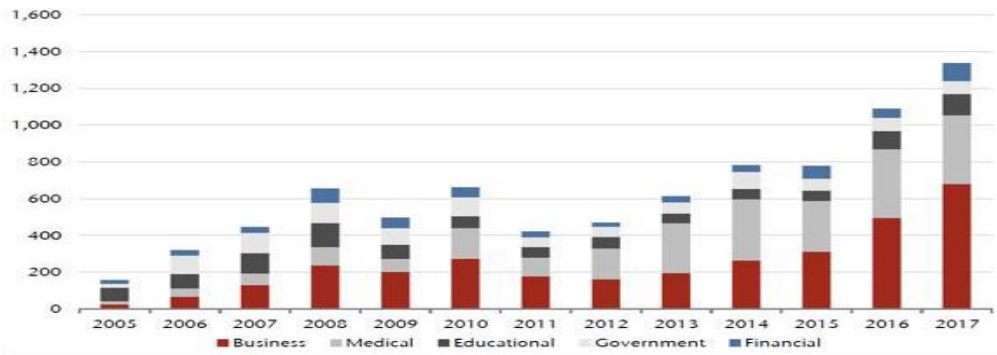

Figura 1. *Número de incidentes por fuga en datos por entidad*
Nota. De Reklaitis (2018), (https://on.mktw.net/2YiM6wI).

Kaspersky (2017) publica una investigación donde determinó los principales vectores de ataque para el hurto de información en las empresas. De la lista publicada que se puede observar en la Figura 2 se obtuvo que el 38% de los vectores de ataque tenían su origen en el factor humano y el 62% era un vector de amenaza de origen lógico a través de software.

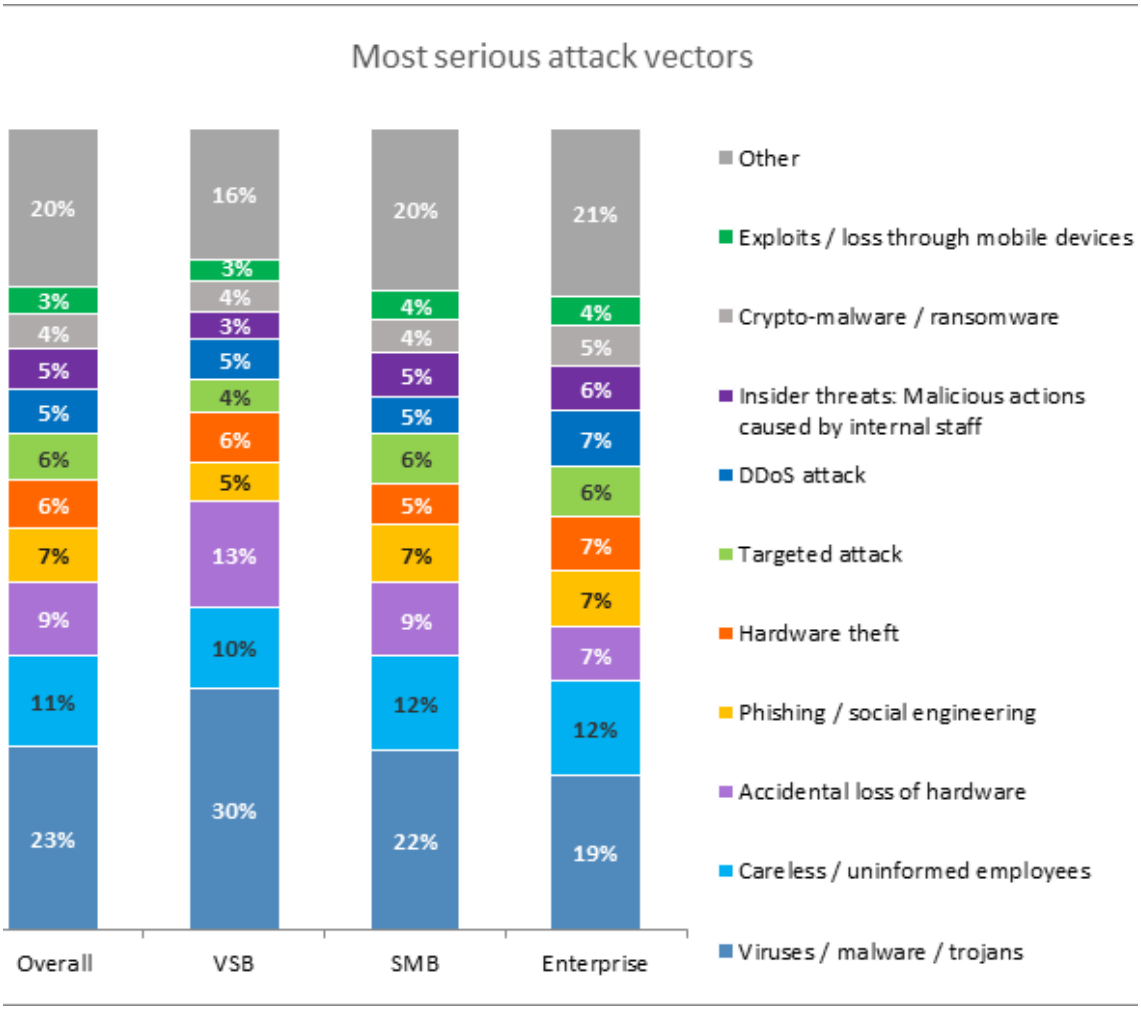

Figura 2. *Vectores de ataque para el hurto de información en las empresas. 2017*
Nota. De Kaspersky (2017), (http://bit.ly/2OUtwbk).

Ante esto las empresas han optado por adquirir productos de seguridad informática con el fin de resguardar sus datos de intrusos. Hoy en día las empresas gestionan la seguridad de sus sistemas, orientados a la administración de la misma mediante software especializado en seguridad de la información. Sin embargo, la mayoría de estas soluciones están orientadas a cubrir vectores específicos de ataque, como pueden ser vector humano o vector software malicioso, dando lugar a que cada una ocupe un nicho de mercado ofertando sus características más destacadas (protección contra perdida

de datos, listas blancas y negras de software malicioso, protección por firmas de virus, cifrado de discos duros o carpetas) y orientando sus investigaciones y mejoras únicamente a un área específica.

Como empresa del grupo Gartner, consultora e investigadora con dedicación exclusiva a investigar y analizar las tendencias del mercado en lo concerniente a nuevas tecnologías. Sobre sus resultados, elabora un ranking más objetivo de los fabricantes con adecuadas soluciones y productos. Resultados publicados con el nombre de "cuadrante mágico de Gartner".

El "Cuadrante Mágico de Gartner" es una herramienta gráfica en que las compañías de cada industria tecnológica se ven dispuestas de acuerdo con su desempeño anual dentro de su propio nicho de mercado, y constituye un referente usado en todo el mundo para tomar decisiones de compra de nueva tecnología de información.

Desde el cuadrante mágico de Gartner presentado en la Figura 3 se tienen las principales marcas implementadas en empresas al 2021 en la cual se coloca a McAfee como una de las marcas líder, seguida de otras como Kaspersky y Symantec como visionarias.

Figura 3. *Principales marcas implementadas en empresas. 2021*
Nota. De Gartner (2021). Cuadrante Mágico de Gartner para Plataformas de Protección Endpoint, (https://www.tecnozero.com/antivirus-y-anti-ransomware/cuadrante-magico-de-gartner-epp-2021/)

En el Perú, los sectores de Educación, Gobierno y las grandes empresas, han incrementado su inversión en el año 2017 hacia el mercado corporativo de seguridad informática por la reciente alza de ataques de ransomware conocidos como Wannacry y GoldenEye registrados a nivel global el pasado mayo y junio del 2017. Entre las soluciones adquiridas están los softwares de seguridad empresarial para la detección de código malicioso desconocido o de día cero, y soluciones DLP para prevenir la fuga de información. (Gestión, 2017).

Un estudio realizado por Deloitte reveló que el 67% de los bancos peruanos sufrieron fraudes internos por sus propios empleados en el año 2014, respecto a robo de información como uno de los principales vectores de ataque, los cuales son categorizados como origen de brechas de seguridad interna. Después de la Conferencia de Seguridad Bancaria CELAES 2014 las entidades financieras involucradas acordaron nuevas medidas y técnicas para reforzar los sistemas de protección y prevención de riesgos cibernéticos. (Gestión, 2014). En la Figura 4 se aprecia de manera gráfica lo comentado.

Principales resultados por País

	Puntos destacados	2014 Latam	Argentina	Chile	Colombia	Ecuador	Guatemala	México	Perú
1	Los encuestados creen que hay un incremento en el presupuesto de seguridad de la información	78%	69%	100%	100%	100%	100%	50%	67%
2	Los encuestados creen que los gastos en seguridad de la información están alineados o por encima del plan estimado	68%	69%	67%	0%	82%	50%	50%	100%
3a	Las iniciativas de seguridad más importantes son: • Cumplimiento regulatorio y legislativo de seguridad de la información	37%	31%	0%	0%	45%	50%	38%	100%
3b	Las iniciativas de seguridad más importantes son: • Protección de Datos	32%	15%	67%	0%	18%	50%	38%	100%
4	Los encuestados han implementado o comprado servicios en la nube	44%	31%	71%	100%	27%	0%	70%	33%
5	Los encuestados han experimentado incidentes de seguridad/privacidad durante el último año	29%	23%	33%	100%	36%	0%	13%	67%

Valores más altos Valores más bajos

Figura 4. *Incidentes de Seguridad Informática en el 2014*
Nota. De "Encuesta a instituciones financieras". Gestión (2014), (http://bit.ly/2YhnhBm).

BAFING S.A.C. es actualmente líder de mercado en el rubro de seguridad informática ejecutando proyectos de integración, de tecnologías, infraestructura computacional y control automatizado para Empresas. En 2019, BAFING S.A.C., en cumplimiento con la norma ISO 27001 sobre la gestión de la seguridad de la información

en las empresas, implementa McAfee Endpoint Security y McAfee DLP para resguardar los activos importantes de la empresa almacenados en los equipos informáticos lo cual se usa hasta la actualidad. Entre el año 2019 y 2021 se percibió una serie de ataques de naturaleza ransomware, exploits de sistema operativo, herramientas rootkit que desactivan temporal o permanentemente la protección antivirus, ataques de intrusión de red y en un porcentaje elevado el origen de estos ataques se debió al descuido de operarios de la empresa que abrieron archivos infectados o descargaron herramientas de internet (BAFING S.A.C., 2021). Por lo anterior expuesto surge la necesidad de implementar una solución diferente que pueda ofrecer mayor cobertura a los escenarios de riesgo presentados por la empresa.

Los incidentes reportados en todos los casos anteriores ocasionaron pérdida de información, por robo directo de información o daño resultante al sistema informático. Se perdió dinero en reparar y reemplazar equipos, las medidas correctivas en estos casos terminan siendo costosas debido a las horas hombres empleadas, la disposición del usuario final y el poco tiempo de resolución con el que cuentan después de un incidente de esa magnitud con contraste con las mismas estrategias de protección, pero aplicadas como plan preventivo.

En la siguiente figura se muestra la cantidad de incidentes reportados por la empresa BAFING entre enero del 2019 a mayo del 2021. Se tiene que el número de incidentes ha ido en incremento siendo el año 2021 el de mayor cantidad de ataques cibernéticos con 305 incidentes registrados dentro de la institución; la proyección del año 2022 para su término podría superar los 360 incidentes.

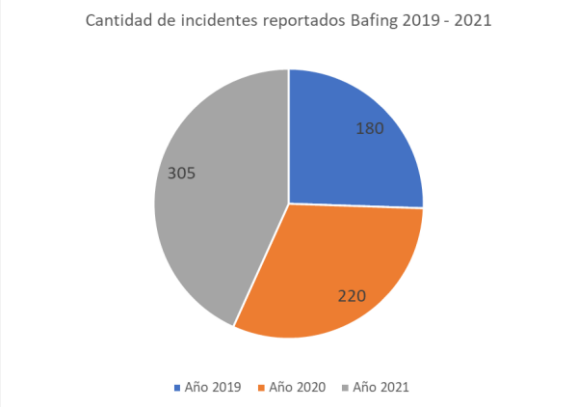

Figura 5. *Cantidad de incidentes reportados entre los años 2019 – 2021. BAFING S.A.C.*
Nota. BAFING S.A.C.

En la figura siguiente se presenta un detalle de los incidentes resueltos y no resueltos de cada año. En los casos en donde el incidente no fue resuelto por el equipo de seguridad se tuvo que formatear el equipo a fin de recuperar la administración del mismo, esta acción provocó perdida temporal del control de dispositivo y comprometió la integridad de la información registrada. Se puede percibir que la cantidad de incidentes no resueltos va en aumento lo cual hace evidente la necesidad de implementar un nuevo marco de trabajo por la constante evolución de amenazas y ataques cibernéticos que se reportaran en años posteriores

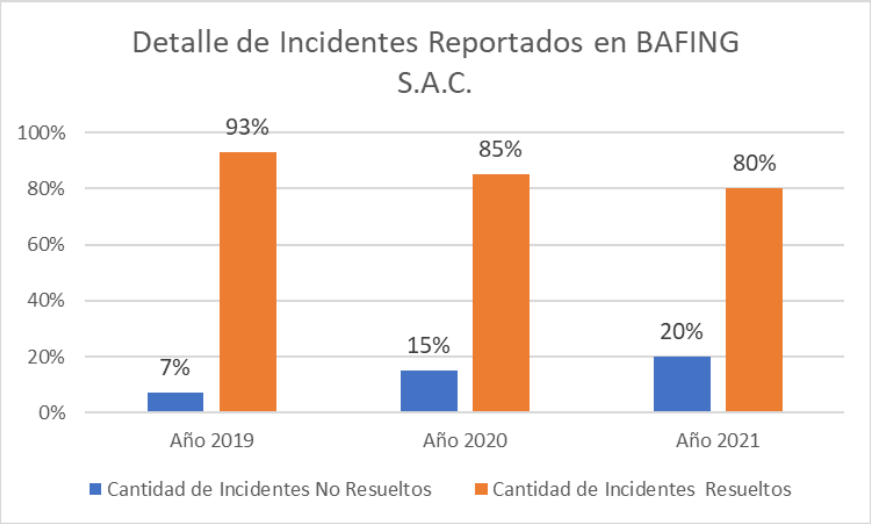

Figura 6. *Detalle de Incidentes Reportados en BAFING S.A.C. 2021*
Nota. BAFING S.A.C.

1.2. Formulación del problema

1.2.1. Problema general

¿Cuáles es el efecto del diseño de una nueva arquitectura de seguridad informática en la seguridad de la información de empresa BAFING S.A.C.?

1.2.2. Problemas específicos

a) ¿Cuál es el efecto del diseño de una nueva arquitectura de seguridad en la integridad de la información de la empresa BAFING S.A.C.?
b) ¿Cuál es el efecto del diseño de una nueva arquitectura de seguridad en la confidencialidad de la información de la empresa BAFING S.A.C.?
c) ¿Cuál es el efecto del diseño de una nueva arquitectura de seguridad en la disponibilidad de la información de la empresa BAFING S.A.C.?

1.3. Justificación de la investigación

Económica: La solución presenta una justificación económica al reducir el riesgo de infección de sistemas informáticos por ataques cibernéticos (intrusiones por troyanos, ransomware, gusanos, phishing, etc.) que en su mayoría de los casos dejan los equipos informáticos en estado inoperable y afectando a la continuidad de los servicios o la línea productiva del negocio. Lo mismo trae por consecuencia un gasto adicional por reposición de recursos y que genera un exceso en los costos de la empresa.

Legal: La solución tiene justificación legal al cumplir con los lineamientos establecidos en la NTP ISO/IEC 27001:2014 a la que la empresa debería estar sometida para asegurar los activos de su empresa con los cuales gestiona y administra información. Así mismo se cuenta con la aprobación de la empresa BAFING para el uso de los datos de los equipos auditados y su procesamiento para la realización de este proyecto (Anexo 4).

Tecnológica: La solución tiene justificación tecnológica al desarrollar un esquema integrador de tecnologías de protección para el cumplimiento de necesidades de la empresa auditada.

Metodológica: La investigación es de carácter experimental porque manipula la variable independiente "Arquitectura de Seguridad Informática" para impactar en la variable dependiente "Seguridad de Información", reforzando sus efectos.

1.4. Limitaciones de la investigación

La investigación está limitada por los siguientes parámetros: Geográficos, se desarrolló en la empresa BAFING S.A.C., ubicada en Av. del Parque Sur 560, Distrito de San Borja. Se emplearon recursos humanos para la implementación del proyecto, asimismo las labores de campo se efectuaron de manera directa por el mismo investigador. Su alcance fue directo al efectuarse en parte de las instalaciones de la empresa BAFING S.A.C. en el área de Tecnología de Información en cuyo ambiente se proporcionó un servidor de prueba para la instalación de las consolas de administración y los equipos Workstation del área de Tecnología de Información de la empresa. El periodo de implementación y análisis de resultados se efectuó en el año 2021.

1.5. Viabilidad de la investigación

Se tuvo a con disposición de equipos Workstation y servidores de prueba hábiles en el área de T.I. en BAFING S.A.C., todos los equipos cumplen con los requerimientos mínimos para la investigación especificados en el anexo 5, lo cual permitió realizar la presente investigación.

Se contó con licencias de partner de BAFING S.A.C. de las respectivas marcas dando la facultad de realizar el proyecto aprovechando todas las funciones del producto.

Se contó con autorización total por parte de la empresa para realizar cambios sobre los equipos administrados en un ambiente de pruebas, así como acceso autorizado para trabajar en esos ambientes, en tanto no afecte al funcionamiento normal y ejecución de rutinas diarias en dicha estación de trabajo.

CAPITULO II: MARCO TEORICO

2.1. Antecedentes de la investigación

Díaz-Ricardo, Yanet; Pérez-del Cerro, Yunetsi y otros (2014), desarrollan una herramienta de seguridad informática para apoyar en la gestión de información con el objetivo de centralizar, facilitar la fluidez de información y asegurar la resolución de dificultades detectadas.

> A este tipo de herramientas actualmente se les conoce como consolas de administración las cuales centralizan eventos de software remotamente y los ordenan para una fácil presentación y entendimiento a ojos del administrador de consola. La ventaja de poseer una consola de administración de software es que permite una toma de decisiones de todo un sistema en un menor tiempo al automatizar la recolección de eventos y actualizar información en tiempo real sobre los equipos informáticos remotos.

Gil Vera, Víctor y Gil Vera, Juan Carlos (2017) llegan a las siguientes conclusiones:

> La seguridad informática hace que las organizaciones protejan sus recursos financieros, así como sistemas de información, su reputación, también legal, del mismo modo los bienes tangibles e intangibles.

> El objetivo de este trabajo fue el desarrollo de un modelo simulador que evalué el nivel óptimo de seguridad que debe tener toda organización, este seria definido como una situación en la que los riesgos son controlados y cuentan con respuesta inmediata para la reducción casi total del impacto sobre el funcionamiento del negocio que le permita obtener beneficios como empresa. Para la construcción del modelo se empleó técnicas de modelaje y análisis del comportamiento de sistemas complejos de corto, mediano y largo plazo. Para la construcción del modelo se utilizó el software “POWERSIM”, integrado para construir y utilizar simuladores de negocios. Concluyendo con el modelo que, la ausencia de un plan director como guía de para proteger sus activos, la sola inversión de mucho dinero en seguridad, no garantiza que alcance niveles de seguridad satisfactorios.

Corda, María Cecilia; Viñas, Mariela y otros (2017) exponen lo siguiente:

> La innovación en tecnología trajo como consecuencia un incremento de riesgos principalmente de problemas relacionados con el acceso de la información.
>
> Su trabajo se focaliza en el ámbito de bibliotecas, como en áreas de información o documentaria. Se hizo un seguimiento y análisis de aplicación de políticas en bibliotecas de todo el país para finalmente delinear aspectos a considerar para una adecuada gestión de riesgos en el campo bibliotecario.

Monsalve-Pulido, Julián Alberto; Aponte-Novoa, Fredy Andrés y otros (2014), investigan y presentan resultados de seguridad informática de una empresa privada, así como también la implementación de un plan de gestión de vulnerabilidades acorde a las necesidades de la empresa. También investigaron sobre el inventario tecnológico de la empresa, con el fin de identificar problemas que causen vulnerabilidades que afecten la seguridad de información. Luego de seis meses de aplicación y seguimiento del plan de gestión en la organización, se evidenció una reducción del 70% en las vulnerabilidades. Del mismo modo se presentan comparativos de herramientas informáticas utilizadas en la aplicación y gestión del plan, que podrían ayudar a futuras investigaciones y adecuada elección de herramientas que permitan el monitoreo y gestión de riesgos.

Dichas herramientas hacen referencia a el uso de consolas de administración de software, las mismas actualmente incorporan funciones de recolección de data para la elaboración de inventario de equipos tecnológicos y tareas de gestión de vulnerabilidades sobre los equipos remotos administrados.

La investigación de Muñoz Hernández, Helmer; Zapata Cantero, Laura Giseth y otros (2019) muestra como la tecnología ha evolucionado gradualmente y con esto el cómo almacenar la información, como necesidad aumenta su protección de datos de información almacenados virtualmente. También se analizan riesgos, en donde la afectación de la información, como alternativas para disminuir y controlar situaciones de riesgo basados en el aplicativo de seguridad informática de sistemas contables. En la comparación realizada con los países de España y Colombia sobre capacitación,

prevención y control de delitos informáticos de una empresa en sus procesos contables de sus sistemas digitales (base datos).

Estos riesgos informáticos se presentan como amenaza que afecta a la empresa, pudiendo tener graves consecuencias con relación a la información que se maneja. Bajo este escenario los empresarios deberían implementar estrategias para prevenir y disminuir situaciones de riesgo en seguridad de información y sean aplicadas integralmente.

Terán Bustamante, Antonia; Dávila Aragón, Griselda y otros (2019) elaboran un modelo que identifica y cuantifica diversos factores que impactan en la gestión adecuada de tecnologías e impacto en innovación. También realizan un análisis en empresas de servicios tecnológicos en México.

La Red Bayesiana presentada en el trabajo de Terán es una estructura en modelo de causa-efecto, evaluando la forma óptima o no óptima de la gestión tecnológica y múltiples factores se evidencia en la causalidad de variables que capturarán adecuadamente la interrelación de las mismas para gestionar e innovar, por razonamiento probabilístico. Resultados que precisan el capital humano, como gestionar el conocimiento y seguridad informática son factores más relevantes. En la figura 7 se presenta un modelo de causa efecto usando redes bayesianas adaptado a una situación de análisis de riesgo de ciberataque.

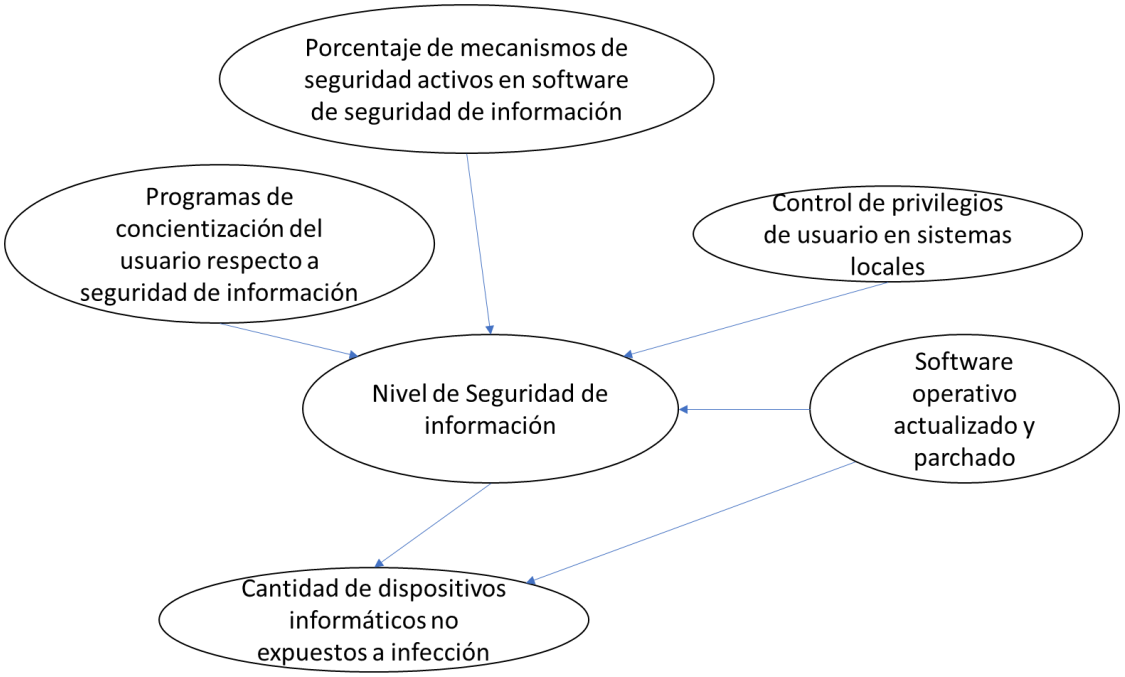

Figura 7. *Modelo de causa efecto para el análisis de riesgo de ciberataques.*
Nota. Elaboración Propia

Acosta (2015) define seguridad informática como la acción mínima de protección de recursos informáticos. Así también define sus alcances en la elaboración de políticas, procedimientos y estándares de la seguridad informática. El objetivo de dicho proyecto fue desarrollar un modelo de seguridad en base a la metodología de protección Data Loss Prevention (DLP) que pueda usarse en pequeñas y medianas empresas (PYMES). La metodología empleada fue descriptiva debido a que pretende analizar las ventajas que conlleva tener un sistema DLP en la empresa. El tipo de diseño es experimental, de enfoque mixto dado que se realizará la implementación del mismo y se medirá el efecto entre variables. Se audita e implementa una herramienta de software en los equipos clientes y en un servidor para conseguir el objetivo principal.

Los resultados obtenidos después del desarrollo del proyecto de Acosta fueron que los dos elementos que generan la pérdida de información en las Pymes es el tecnológico y el humano; por lo que al desarrollar el modelo propuesto se obtuvo una herramienta que ha permitido seguir la información clasificada en tiempo real, así como ayudar a que el trabajador comprenda la implicancia que tiene el perder la información. Asimismo, en referencia al proyecto de Acosta y empleando el cuadrante mágico de Gartner en la figura 3 se concluye que el software de McAfee Endpoint Protection fue el más adecuado para contar con un resguardo óptimo de la información para la empresa, al mismo tiempo de ser sencilla y comprensible para quien la maneja. Las directivas y herramientas

implementadas en el ambiente de prueba de la empresa ayudaron a prevenir incidentes de pérdida de datos, además de obtener un presupuesto proyectado que alcance a todos los equipos informáticos del negocio.

Arellano y Friedich (2015), en su trabajo "Seguridad informática" nos presenta las etapas de desarrollo de una política de seguridad:

- Desarrollo: Creación, revisión y aprobación de política.
- Implementación: La política es comunicada y acatada por la organización.
- Mantenimiento: Monitoreo de funcionamiento de la política implementada.
- Eliminación: La política es retirada cuando ya no se le requiere más.

El objetivo principal de la investigación de Arellano fue hacer una revisión general de los conceptos relacionados a seguridad informática y el procedimiento para la aplicación de estándares dentro de las organizaciones. La metodología empleada fue de carácter descriptiva debido a que se busca analizar las ventajas de la gestión de conocimientos sobre seguridad informática en la empresa, implementar políticas tras el análisis de las necesidades de la misma y recopilar resultados post implementación. El trabajo investigación tiene un no experimental con enfoque cualitativo, que no confronta las variables de estudio ni las manipula, en cambio las observa en su contexto natural para luego realizar conclusiones sobre las mismas. Se concluye así que, para hacer frente al creciente número de amenazas y mecanismos de ataque informático, es necesario contar con un plan organizado que priorice la cobertura de los vectores de robo de información ya conocidos para prevenir y corregir incidencias en los equipos informáticos.

León (2015) propone implementar un software de seguridad McAfee DLP para diseñar un sistema de prevención de amenazas por incidentes de fuga de información. El objetivo del proyecto fue sintetizar métodos de clasificación de información a través de herramientas software automatizadas. Metodología de investigación de tipo experimental, se utiliza el software de seguridad McAfee DLP para ejecutar reglas de control sobre la información de la empresa. El diseño de la investigación fue experimental con enfoque mixto que usó un ambiente de pruebas para las políticas implementadas.

Los incidentes tratados en el trabajo de León son interpretados como parte del resultado para determinar el nivel de seguridad con las nuevas configuraciones implementadas. Los beneficios obtenidos tras la implementación del proyecto fueron conocer cuál es la

información que está en uso, en reposo y en movimiento en la empresa y permitir consecuentemente tomar control de accesos de la misma.

Daza (2015) implemento en su tesis la solución de seguridad Kaspersky Endpoint Security en sus sistemas informáticos para cumplir con el perfil de seguridad informática propuesto a partir de la problemática de vulnerabilidad de información en su universidad.

El objetivo planteado que da pie al desarrollo del proyecto fue implementar una solución de seguridad en la red local y gestionar los equipos informáticos bajo un esquema de políticas de seguridad administrables a través de un software de administración llamado Kaspersky Security Center. La metodología también de tipo experimental, se utiliza el software de seguridad Kaspersky Endpoint Security para ejecutar reglas de protección sobre los equipos informáticos de la empresa. El diseño fue de tipo experimental con enfoque mixto dado que el proyecto se desarrolló con una muestra compuesta de equipos informáticos con personal administrativo, estudiantes y docentes de la facultad de Ingeniería de Sistemas Computacionales de la Universidad de Guayaquil donde se instala y prueba el software de protección y se configuran los controles para la información entrante y saliente que manejan los computadores de rutina. Se recaban los resultados de las encuestas realizadas a especialistas de seguridad informática de la facultad para desarrollar un perfil de seguridad informática que permita funcionar correctamente a los sistemas informáticos bajo un esquema de control y protección por políticas de seguridad. Tras el término del proyecto se concluye las falencias que existían al no contar con un esquema de seguridad basado en políticas de control y protección aplicadas de forma ordenada a grupos de equipos y usuarios. Se experimentó mejoría al contar con una protección que centraliza la información en una interfaz gráfica, la cual permite tomar decisiones en tiempo real frente a las amenazas internas y externas en la red.

Sosa (2018), en su tesis “Metodología para la elección de software de seguridad informática”.

> Establece los mecanismos de prueba para medir la eficiencia del software de seguridad informática en base al resultado de los incidentes reportados. El objetivo del proyecto pretende determinar el impacto del software de seguridad informática frente al nivel de protección de información y al riesgo de peligro de vulnerabilidad de la misma. La metodología de investigación fue experimental debido a que se emplean criterios de medición de software en los equipos auditados. La muestra

estudiada para este caso es un subgrupo de la población total de equipos informáticos, en este caso se usaron 30 computadoras con las mismas condiciones. El diseño experimental con enfoque mixto que confronta variables manipuladas deliberadamente para obtener datos tales como porcentaje de consumo de recursos del computador, tiempo de ejecución de tareas, cantidad de incidentes reportados. Los resultados se recolectan a través de gráficos de barras con datos pre-test y post-test referido a la implementación de un software de protección. Los indicadores utilizados como confidencialidad, integridad y disponibilidad de la información.

En los resultados del trabajo de Sosa se concluye que la aplicación de un método de nivel de seguridad de información permite discernir el impacto de implementación de tecnologías de protección frente a la reducción de riesgo de vulnerabilidad de información, así también conocer cuál es el grado de beneficio entre cada herramienta.

2.2. Bases teóricas

2.2.1 Seguridad informática

2.2.1.1 Concepto. - Terán, Dávila y Castañón (2019) la seguridad informática lo define como: “Observar y establecer un conjunto de técnicas, reglas, estrategias, políticas, guías, prácticas y procedimientos orientadas a la prevención, protección y resguardo de daños, alteración o sustracción de recursos informáticos de una organización” (Voutssas, 2010).

Gil, V. y Gil, J. (2017), sostiene que: “La seguridad informática protege sistemas de información, reputación, recursos financieros, situación legal, y otros bienes tangibles e intangibles de las organizaciones. La seguridad de la información protege los sistemas informáticos (…) la aplicación de medidas de seguridad debe ser planificado y racional, evitando inversiones innecesarias. Con lo que las medidas y mecanismos de protección sean efectivas, integrando en el amplio sistema de gestión de la seguridad de información”.

La seguridad informática, al igual que la seguridad que se aplica a otros entornos, minimiza riesgos de acceso y uso de sistemas no autorizado o con mala intención. Proteger los recursos informáticos de la empresa

> es el objetivo de la seguridad, como hardware, software e información. Con adopción de las medidas, la seguridad informática ayuda a cumplir sus objetivos de la empresa de proteger sus sistemas de información, reputación, legal, recursos financieros, bienes tangibles e intangibles (P. Galdaméz, 2011).
>
> En tal sentido, la gestión de seguridad informática de una organización es tarea exigente y evaluar tecnologías de seguridad también es fundamental para la gestión eficaz la seguridad de la información.
> La Tecnología de la Información (TI) debería estar en permanente extensión en todas las áreas de las empresas como factor crítico para el éxito de la economía mundial.
> Las consecuencias en la seguridad de información son ocasionadas por actores y motivos diferentes.
>
> Grupos como Hackers, empleados maliciosos, espías industriales, o terroristas profesionales, aficionados, buscan penetrar en los sistemas en busca de información o crear daños. Estos buscan aspectos vulnerables, utilizando debilidades en la cadena de seguridad de la empresa. La lucha y preocupación en hacer más seguros los sistemas de información es constante, en consecuencia, las empresas siempre buscan encontrar novedosas formas de seguridad (pp. 193-194).

Tipton (2006) define seguridad informática como la capacidad de preservar la confidencialidad, integridad y disponibilidad en los sistemas de información.

Monsalve, Aponte y Chávez (2014), indica que:

> La seguridad de información en la empresa contempla la seguridad de accesos, de periféricos, de uso de contraseñas y el control de vulnerabilidades, entre muchos. Todos requieren estudios y presupuesto para su aplicación, sea de manera preventiva o correctiva sobre seguridad, del mismo modo, es encontrar sistemas totalmente seguros es imposible, en razón que diariamente aparecen nuevos riesgos y a todo nivel.

Por otro lado, la seguridad de la información digital de la empresa depende del físico, que refiere al alojamiento de la información; el social, relacionado con la capacidad discrecional por parte del usuario de los sistemas informáticos, y el lógico, referido a las políticas de niveles de acceso y disposición. Es decir, un esquema seguro debe ajustar los niveles de integridad, disponibilidad y confidencialidad de la información, según la norma ISO 27001. En la descripción de características, están implícitas en la información, en tanto, toda empresa debe completar el ciclo de seguridad para que su información sea fluida en procesos estructurados, que constituye los denominados Sistemas de Gestión de Seguridad de la Información (SGSI).

Actualmente, determinar el grado de inseguridad de información, en contexto de análisis de riesgo y vulnerabilidad, trasciende niveles de operatividad y uso, por tanto, interpretar unidades de portabilidad y medios que facilitan su transmisión, donde nuevas configuraciones para el fraude se abren, así como el uso indebido y alteración; siendo guía del cibercrimen, inteligencia y la gestión de áreas forenses sobre la información. (p.67).

De lo revisado se tiene la seguridad informática como las herramientas que aseguran la integridad del contenido procesado, el nivel de privacidad de la data administrada y la capacidad de acceso supervisado a los activos digitales que gestionan información, minimizando el riesgo de intrusión de grupos de atacantes como hackers, espionaje corporativo, personal descontento que exponen o corrompen la información que es objetivo de resguardo. El alcance de sus lineamientos conforma hardware, software e información a fin de considerar todos los componentes que participan en los procesos de una empresa. La misma cuenta con instrumentos que miden su nivel de efectividad en un sistema o redes de sistemas. Todo sistema de gestión de seguridad de información requiere de una proyección de presupuesto a fin de considerar todos los activos que se verán involucrados en la implementación de plataformas que administren la seguridad de la información.

2.2.1.2 Arquitectura de seguridad informática

García y Martínez (2006), manifiesta que:

> Las amenazas son diversas y comprometen a los objetivos de las empresas. Ante cualquier riesgo las empresas optan por aceptarlo, actúan para reducir toda posibilidad de ocurrencia o como también la transferencia del riesgo. A toda medida para minimizar un riesgo se le denomina control de seguridad [Tipton, 2006; Witman, 2007]. Los controles de seguridad son clasificados de la siguiente manera: controles administrativos, controles lógicos y controles físicos (Tipton, 2006].
>
> Para la efectividad de los controles deben estar integrados a una *arquitectura de seguridad informática* [Tudor, 2006], por consiguiente, debe estar acorde con los objetivos de la empresa, priorizando posibles amenazas según el impacto en la empresa [Peltier, 2005; Landoll, 2005]. (p. 1).
>
> De lo revisado se concluye que arquitectura de seguridad informática son los controles de seguridad que gestionan la seguridad informática en las empresas. Un control de seguridad es el nodo único con el cual aplicamos políticas de seguridad alineadas a los objetivos de seguridad informática en la empresa según la evaluación del riesgo afrontado (evitar, aceptar, mitigar, transferir).

2.2.1.3 Diferencia entre Seguridad informática y Seguridad de la información

Corda, Viñas y Coria (2017), respecto a la diferencia, dicen que: Guerrero Julio y Gómez Flórez (2011, p.197) explican que: Seguridad informática son medidas preventivas y reactivas para empresas y sistemas tecnológicos a proteger y cautelar la información, y mantener la disponibilidad, confidencialidad, e integridad. Por otro lado, la seguridad de información contempla la integridad, confidencialidad y disponibilidad, como sistemas en tratamiento en la empresa. La seguridad de la información es la capacidad de preservar el nivel de confianza, de prevenir acciones ilícitas que comprometan la autenticidad, integridad,

disponibilidad y confidencialidad de la información transmitida o almacenada, y de servicios que los sistemas y redes ofrecen (p.9).

De lo comentado anteriormente; Seguridad de la Información es la característica que adquieren los sistemas cuando son capaces de gestionar y administrar a través de políticas de Seguridad Informática otros sistemas o redes de sistemas empresariales. Seguridad Informática vienen a ser los recursos empleados en ejecutar las actividades para gestionar y administrar la seguridad de la información en sistemas o redes de sistemas.

2.2.1.4 Políticas de seguridad

Dussan Cavijo (2006) dice que:

> La Política de seguridad definen aspectos de seguridad en directrices, procedimientos, normas, guías de trabajo, para adoptar a nivel local o institucional, con el propósito de estandarizar, establecer y normalizar la seguridad en lo tecnológico y humano.
> -Tecnológica: Esfuerzos para la correcta operatividad de la plataforma de software, hardware, sistemas operativos, telecomunicaciones, bases de datos y acceso a Internet.
> -Humana: Se convierten en usuarios proveedores, clientes, empleados etc.
> Enfocando los recursos y esfuerzos, ligados a la cultura empresarial y cómo se integran aspectos como la ética, mejoramiento continuo, la responsabilidad y capacitación.
> Las políticas de seguridad informática varían de una a otra empresa, los documentos incluyen exposición de motivos, personas a quien va dirigido las políticas, historial de modificaciones hechas, alguna definición de términos e instrucciones.
> Para la efectividad de la política debe contar con elementos que refuercen el proceso: Herramientas, cultura organizacional y monitoreo. Aspectos técnicos, tecnológicos y recursos financieros, son fundamentales para toda actividad de control, como retroalimentación para fortalecerlos con las mejores prácticas (pp.89-91).

Vega Velasco (2008) afirma que:

> Para implementar un sistema de seguridad se complementa con políticas de seguridad. Para ello se requiere conocer las amenazas a los recursos y a la información de la empresa, del mismo modo determinar cuál es el origen de la misma, pudiendo ser externas o internas a la empresa.
> Sería en vano solo proteger de amenazas externas, si existen amenazas internas, ejemplo, si alguien utiliza un USB infectado se podría expandir en toda la red.
> La política de seguridad es un conjunto de reglas para acceder a los recursos informáticos y a la información que gestionan y administran. Todo documento de seguridad debe ajustarse a la mejora continua y dinámica según cambios presentados en donde se crearon.
> Estas políticas son para proteger sistemas e información de la Empresa, como garantizar la confidencialidad, disponibilidad e integridad de la información. Estos documentos contemplan procedimientos para cumplir reglas, responsabilidades en todos los niveles. Por supuesto que el apoyo gerencial de la organización es fundamental.
> Estas políticas deben difundirlas a todo el personal de la empresa.
> También debe ser muy claras: El objetivo, responsables de cumplir, medidas a aplicar en caso de no cumplimiento. (pp. 67-68).

> Política de seguridad será la manera reglamentada de interpretar de manera global el cómo gestionar, implementar administrar, y medir un sistema de seguridad de la información. Para la realización de un correcto procedimiento de gestión de políticas de seguridad es necesario examinar las amenazas internas y externas a la empresa a fin de dimensionar los riesgos de seguridad que podrían enfrentar en el futuro y decidir una correcta estrategia de enfrentamiento normada de manera global.

2.2.2 Riesgo

Corda, Viñas y Coria (2017), indican que:

> El *riesgo informático* refiere a toda eventualidad que no permite cumplir ningún objetivo, es decir, daño que afecte el funcionamiento de resultados

esperados. Zulueta, Despaigne y otros (2009, pp. 7-8) consideran que, aun cuando hay criterios variados, concuerdan que el riesgo implica:

- *Incertidumbre:* Riesgo que puede ocurrir como no.
- *Efecto en los objetivos:* Si el riesgo ocurre, las consecuencias serían inevitables.

El sistema informático es considerado como seguro, si cumple algunas características:

- *Integridad*: La información solo personal autorizado puede modificarlo.
- *Confidencialidad:* La información legible para usuarios.
- *Disponibilidad:* Información disponible cuando sea necesario.
- *Irrefutabilidad:* información que conserva la propiedad de autoría verificable.

Componentes a considerar para el riesgo informático:

- Resguardo físico
- Manejo de accesos
- Resguardo de los datos
- Protección en las redes
- Organización y asignación de responsabilidades
- Análisis cuantitativo de riesgos
- Políticas de personal, medidas de higiene, salubridad y ergonomía, selección y contratación de seguros
- Aspectos jurídicos y delitos
- Estándares de ingeniería, programación y operación
- Procedimientos de auditoría interna y externa
- Seguridad de sistemas operativos, red y plan de contingencia.

Entre muchos tipos de riesgos informáticos:

Riesgos de integridad: Relacionados a la autorización, detalle exacto de entrada y de aplicativos usada por la empresa. Estos riesgos aplican en el soporte de procesamiento del negocio, presente en el lugar y momento en las partes de aplicaciones.

Riesgos de relación: Referido al oportuno manejo de información. La información y datos correctos permiten tomar decisiones correctas en el tiempo preciso en relación al riesgo analizado.

Riesgos de acceso: Enfocado en accesos no autorizados o controlados a sistemas informáticos y al manejo de datos e información en ellos. Riesgos de dispersión en el trabajo, así como los relacionados con la integridad y confidencialidad de la información de los sistemas de bases de datos.

Riesgos de utilidad: centrado en niveles de riesgo:

- El riesgo es enfrentado por direccionamiento del sistema ante la ocurrencia de problemas.
- Técnicas de recuperación o restauración para reducir indisponibilidad de sistemas.
- Copias de Seguridad y plan alternativo para controlar situaciones de adversidad operativa en el proceso de toda información.

Riesgos de infraestructura: Relacionado a la ausencia de estructuras tecnológicas para el manejo de información (redes, software, hardware, personas y procesos) causando incertidumbre en la gestión de atención de presentes y futuras necesidades del negocio con un costo eficiente. Asocia todo riesgo con procesos de información tecnológica que desarrolle, mantenga, opere y defina en un procesamiento de información y aplicación.

Riesgos de seguridad general: Sucede por no tener en cuenta los requerimientos de diseño y ejecución de los lineamientos que exigen los estándares de la International Electrotechnical Commission (IEC 950) para reducir riesgos.

El riesgo de origen tecnológico incide en metas y objetivos empresariales, causar riesgos intrínsecos por el uso de tecnología. Por tanto, el daño, falla o interrupción en el manejo de tecnologías implican pérdidas en las empresas, desgranamiento financiero, multa, acciones legales, afecta la imagen de una empresa y causa inconvenientes a nivel estratégico u operativo (pp.7-8).

Tener presente que no existe seguridad absoluta. Se puede reducir oportunidades para que un sistema sea comprometido y daños provocados por ataques.

La Gestión de riesgos informático, considera:

a) Datos: información almacenada en ordenadores informáticos.

b) Recursos: el equipamiento usado para operar en el negocio.

c) Reputación: una actividad inicial es el análisis de riesgos, realizando un modelado de amenazas. Se trata de actividades recurrentes.

Un riesgo es la combinación de activos, vulnerabilidades y atacantes. (p.12).

De lo descrito anteriormente se califica como riesgo a la característica de un sistema para ser afectado por un agente interno o externo y alterar el resultado que entrega en los procesos que ejecuta. Estos riesgos son clasificados según el medio en el que se presentan, es así como se tienen conocidos, por mencionar algunos, riesgos de acceso, riesgos de infraestructura, riesgo de utilidad, etc.

La oportunidad de sucesión del mismo se ve aumentado o reducido por la efectividad de un sistema de seguridad de la información implementado en las empresas.

2.3. Objetivos de la investigación

2.3.1. Objetivo general

Diseñar, implementar y valorar la propuesta de una arquitectura de seguridad informática en la seguridad de la información de la empresa BAFING S.A.C.

2.3.2. Objetivos específicos

a) Determinar el efecto de nueva arquitectura de seguridad informática en la integridad de la información de la empresa BAFING S.A.C.
b) Determinar el efecto de una nueva arquitectura de seguridad informática en la confidencialidad de la información de la empresa BAFING S.A.C.
c) Determinar el efecto de una nueva arquitectura de seguridad informática en la disponibilidad de la información de la empresa BAFING S.A.C.

2.4. Formulación de hipótesis

2.4.1. Hipótesis general

El diseño de una nueva Arquitectura de Seguridad Informática aumentara la seguridad de información de la empresa BAFING S.A.C.

2.4.2. Hipótesis especificas

a) La nueva arquitectura de seguridad informática incrementará la integridad de la información en la empresa BAFING S.A.C.
b) La nueva arquitectura de seguridad informática incrementará la confidencialidad de la información en la empresa BAFING S.A.C.
c) La nueva arquitectura de seguridad informática incrementará la disponibilidad de la información en la empresa BAFING S.A.C.

CAPITULO III: DISEÑO METODOLÓGICO

3.1. Diseño de la investigación

El diseño de la investigación es de pre prueba-post prueba con un solo grupo. Diagramado así:

G O_1 X O_2

Se aplica una prueba al grupo antes del tratamiento, se implementa el tratamiento y finalmente se aplica una prueba posterior al tratamiento, por lo tanto, es experimental. Esto implica manipular una variable experimental, controlada rigurosamente, y describir de qué modo o causa produce un acontecimiento o situación particular. (Hernández Sampieri, 1998, p. 136).

En este estudio la post prueba se aplicó después de seis meses de implementada la propuesta.

3.2. Tipo

Investigación de tipo es experimental pues comprende que el experimento es inducido por el investigador para introducir variables manipuladas, para controlar variación de variables y efecto en conductas observadas (Tamayo y Tamayo, 1996, p. 56).

3.3. Enfoque

La investigación es cuantitativa, pues se busca datos precisos y cuantificados para efectos de orientación. Se soporta de la Estadística para el análisis de datos.

3.4. Población

El presente estudio considera una población constituida por la cantidad de incidentes reportados en el año 2021 que está conformado por 305 incidentes que le ha acontecido al sistema de la empresa BAFING S.A.C.

Para la evaluación del estado actual del sistema y después de la implementación de la propuesta, se consideraron a los 30 trabajadores del área de tecnología informática.

3.5. Muestra

El tamaño de la muestra se estimó a través de un cálculo probabilístico de incidentes en la calculadora científica NETQUEST.COM (2021), precisando 280 casos. Se consideró la fase de pruebas desde el sistema de tickets Manage Engine Service Plus v8.1 de helpdesk de BAFING S.A.C. para el censo de incidentes resueltos y no resueltos de los productos antivirus que se auditaran. Se incluyeron los equipos del área de soporte de Tecnología de Información de BAFING S.A.C. Siendo el área de T.I. con 40 computadores los cuales fueron las plataformas en donde se analizaron las incidencias existentes en una bitácora histórica y se determinó la manera en que fueron resueltas. No fueron contemplados los equipos fuera del área de T.I. de BAFING S.A.C. por tratarse de equipos críticos para la continuidad del servicio de la empresa.

Para el caso de los trabajadores, no fue necesario tomar una muestra, pues la población es pequeña (menor o igual a 30).

3.6. Operacionalización de variables

Tabla 1

Operacionalización de Variables

Variables	Dimensiones	Indicadores	Índice
V.I. Arquitectura de seguridad informática	Control físico	• Infraestructura tecnológica (hardware, software)	Valores %
	Control lógico o técnico	• Capacidades del Software	
	Control administrativo	• Política de seguridad informática	
V.D. Seguridad de la información	Integridad	• Protección de hardware • Alteración del contenido de la información • Registro del personal autorizado • Prevención de modificaciones • Prioridad	Promedio
	Confidencialidad	• Accesibilidad de la información • Necesidad de ocultar o mantener en secreto información y /o recurso • Prevención de divulgación • Disposición de permisos • Prioridad	
	Disponibilidad	• Prevención de interrupciones • Accesibilidad • Prioridad	

Nota. Elaboración Propia

3.7. Técnicas para la recolección de datos

Para recolectar datos se utilizó las siguientes técnicas:

Entrevista: Dirigido a especialistas del campo en seguridad informática. Se documentó información acerca de las características, ventajas y desventajas de las marcas auditadas.

Análisis Documental: Revisión de reportes emitidos por la empresa u otros.

Observación: Permitió comprender los procesos por mejorar.

Encuesta/instrumento de evaluación: Administrado a los trabajadores del área de informática y trabajadores externos para a) la construcción del perfil de evaluación del software. b) evaluación del software, hardware y política por marca c) evaluar el estado actual del proceso y después de implementar la propuesta.

3.8. Técnica para el procesamiento y análisis de datos

Para el procesamiento de datos se utilizó el Paquete Estadístico para las Ciencias Sociales- SPSS 25. El análisis descriptivo de datos es mediante medidas como porcentajes, media aritmética y desviación estándar.

El análisis inferencias es mediante la Prueba T-Student de dos medias.

3.9. Aspectos éticos

El estudio es original y con la confidencialidad de información que brinda la empresa BAFING S.A.C., para lo cual se cuenta con la autorización respectiva, ubicada en el anexo 4 “Carta de autorización BAFING S.A.C.”. Se toma en cuenta el respeto a los autores y publicaciones citados en el contenido del trabajo referidos en la Referencia y Bibliografía.

CAPITULO IV: RESULTADOS

4.1. Propuesta

De acuerdo con las bases revisadas la propuesta teórica es la siguiente:

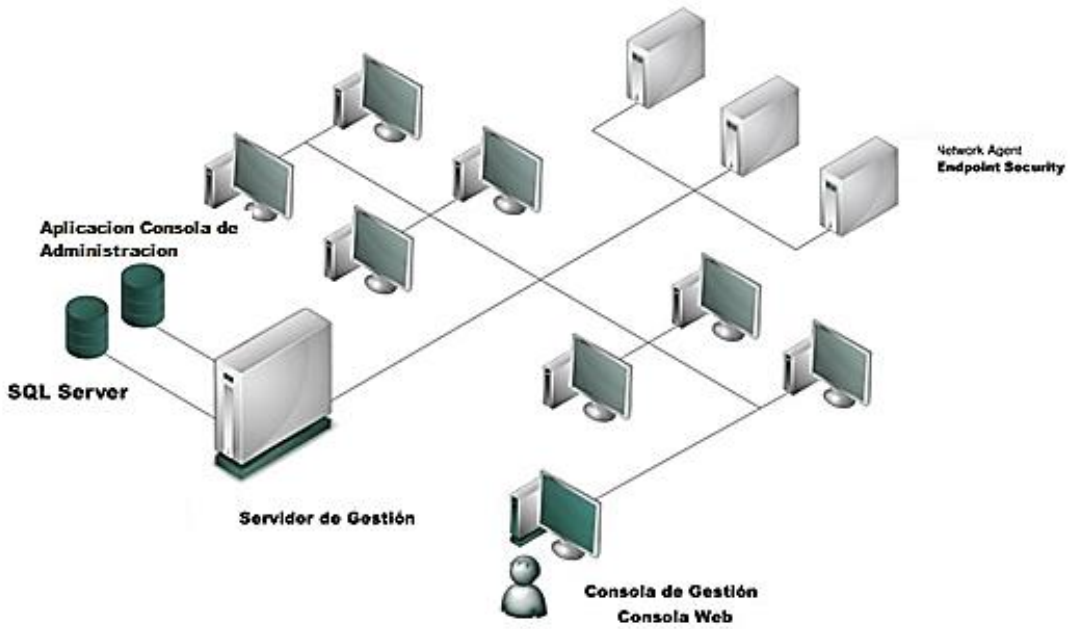

Figura 8. *Propuesta de Solución: Modelo de Arquitectura de Seguridad informática*
Nota. Elaboración Propia

Se propone un equipo servidor de Gestión que aloje las aplicaciones de consola de administración de productos de seguridad y control en una base de datos local SQL Server. El monitoreo y configuración de reglas de acceso y políticas de seguridad se realizará a través de una Consola de Gestión – Consola Web en un navegador de internet asegurando que solo el administrador de dominio pueda ingresar directamente al servidor.

Una Consola de Administración es una solución que centraliza la información que recibimos de una red a través de los agentes de red (Network Agent) instalados en equipos de una empresa. A través de ella se puede realizar tareas masivas y realizar configuraciones en tiempo real para varios equipos a la vez.

Los equipos de escritorio tendrán instalado agentes de red y software de control y seguridad (Endpoint Security) sobre el cual se realizarán los cambios y actualizaciones de reglas y políticas.

Un agente de red es un software terminal que envía y recibe eventos desde la consola de administración, los mismos que son designados posteriormente al software que debe traducir el evento y aplicar o actualizar configuraciones.

Un software de control DLP es una aplicación encargada del monitoreo y control de la información en uso, información en movimiento e información en reposo en el equipo que está auditando.

Una aplicación de seguridad Antivirus es un software con mecanismos de detección y e inferencia de amenazas; estas son mayormente identificadas como virus o vulnerabilidades en el equipo que está auditando.

Para los detalles del experimento a realizar se tuvo un entorno antes de la implementación de la propuesta el cual es administrado los productos McAfee Endpoint Security y McAfee DLP. Este arreglo ya en producción es llamado a lo largo del experimento como Arquitectura BAFING. Así mismo se tuvo un entorno después de la implementación de la propuesta el cual es administrado por los productos Kaspersky Endpoint Security y McAfee MVISION DLP. Este arreglo que fue puesto en ejecución en un ambiente de pruebas controlado es llamado a lo largo del experimento como Arquitectura Hibrida debido a que probara la compatibilidad de ambos productos, de fabricantes diferentes, para trabajar en un solo ambiente tecnológico y a su vez probar las hipótesis del proyecto.

4.1.1. Diseño

4.1.1.1. Perfil de Evaluación de Software de Seguridad

A fin de obtener un perfil de evaluación se aplicó una encuesta a trabajadores de BAFING S.A.C. del área de TI y trabajadores externos a la empresa en el mismo rubro y funciones en cuanto a seguridad informática.

Se adjunta el resumen de respuestas para la construcción de un perfil de evaluación de software de seguridad en base a la pregunta número 2 del cuestionario considerando las 8 entradas con más puntaje que son: Malware, Ransomware, Exploits/vulnerabilidades de software, Ataques de día cero, Ataques de red, Fuga de información confidencial, Accesos no autorizados a equipos informáticos, Moderación de filtros de seguridad en grupos de usuarios. (ANEXO 2).

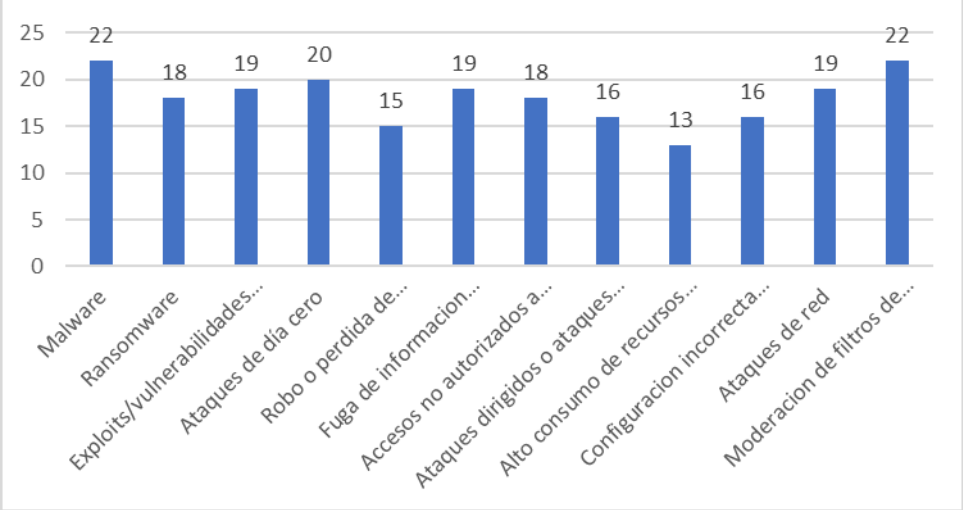

Figura 9. *Resumen de incidentes comunes en software de seguridad*
Nota. Elaboración Propia

Para la presentación grafica de resultados, se convierten a continuación los valores en módulos de protección y características de software de seguridad:

- Malware -> Protección antimalware
- Ransomware -> Protección anti-ransomware
- Exploits/vulnerabilidades de software -> Control de anomalías de software
- Ataques de día cero -> Machine learning
- Ataques de red -> Protección de amenazas de red
- Fuga de información confidencial -> Protección de datos
- Accesos no autorizados a equipos informáticos -> Cifrado de datos
- Moderación de filtros de seguridad en grupos de usuarios -> Monitoreo de usuarios

4.2. Valoración de la Propuesta

4.2.1 Valoración del software

Para la valoración de la propuesta se dispone del siguiente banco de preguntas que nos permitirá conocer los resultados de las pruebas realizadas juzgando las características del software auditado para cada caso:

1. ¿Qué producto de seguridad ENDPOINT manejan principalmente en su empresa o empresa que audita?

2. En la escala del 1 al 10 en donde 1 es muy bajo y 10 es muy alto. ¿Cómo calificaría usted la capacidad del software de seguridad ENDPOINT mencionado anteriormente para las siguientes proposiciones?, dejar en blanco si la característica mencionada no aplica a la solución que audita:
    a. Capacidad para eliminar malware y código malicioso
    b. Capacidad para eliminar amenazas tipo Ransomware
    c. Capacidad para identificar exploits de SO y vulnerabilidades de software de terceros
    d. Capacidad de autoaprendizaje para la identificación de nuevas amenazas
    e. Capacidad para prevenir amenazas de red y ataques desde fuera de la red local
    f. Capacidad para bloquear la lectura y escritura de información confidencial
    g. Capacidad para proteger y cifrar datos de usuarios con contraseñas
    h. Capacidad para establecer grupos de accesos a información critica

Se toman los siguientes valores alineados a las dimensiones estudiadas:

Tabla 2

Alineamiento Dimensiones – Características de Software de seguridad

Dimensión	Característica
Integridad	Protección Antimalware
Integridad	Protección Antiransomware
Integridad	Control de Anomalías de Software
Disponibilidad	Machine Learning
Disponibilidad	Protección de Amenazas De Red
Confidencialidad	Protección de Datos
Confidencialidad	Cifrado de Datos
Confidencialidad	Monitoreo de Usuarios

Nota. Elaboración Propia

Los criterios de evaluación son los siguientes:

Tabla 3

Criterios de evaluación de software

Criterio de evaluación	Rango de puntuación porcentual	Rango de puntuación numérico
Elevado	90%-100%	9.0-10.0
Promedio	70%-89%	7.0-8.9
Bajo	0%-69%	0-6.9

Nota. BAFING S.A.C.

A partir de los valores obtenidos en la encuesta, estos son agrupados en función de la marca de software auditada y se promedia cada característica evaluada hacia la misma.

Tabla 4

Evaluación de características de MCAFEE ENDPOINT SECURITY.

MCAFEE ENDPOINT SECURITY	Desarrollo de Característica Actual	Desarrollo de Característica Ideal	Riesgo no Cubierto
Protección Antimalware	88%	100%	12%
Protección Antiransomware	86%	100%	14%
Control de Anomalías de Software	0%	100%	100%
Machine Learning	90%	100%	10%
Protección de Amenazas De Red	88%	100%	12%
Protección de Datos	0%	100%	100%
Cifrado de Datos	0%	100%	100%
Monitoreo de Usuarios	0%	100%	100%

Nota. Elaboración Propia

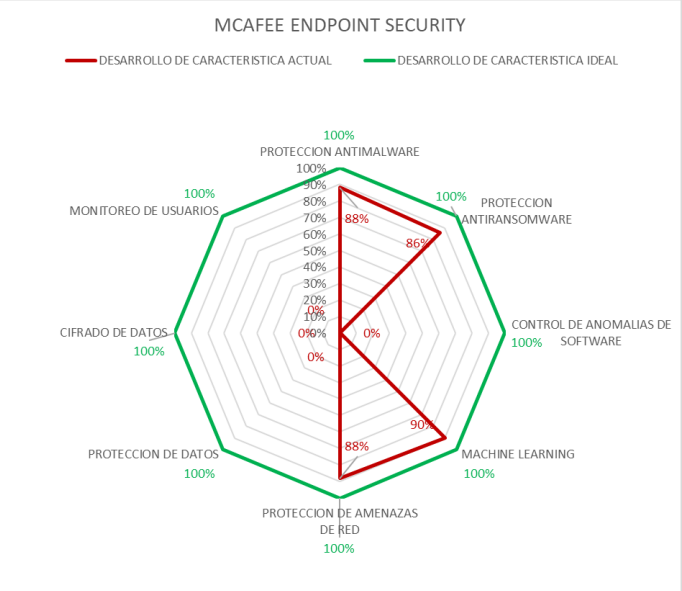

Figura 10. *Evaluación de características de MCAFEE ENDPOINT SECURITY*

Nota. Elaboración Propia

Tabla 5

Análisis de Características de MCAFEE ENDPOINT SECURITY

MCAFEE ENDPOINT SECURITY	N	Media	Desviación Estándar	Varianza
Protección Antimalware	40	8.7750	0.97369	0.948
Protección Antiransomware	40	8.6000	0.98189	0.964
Control de Anomalías de Software	40	0.0000	0.00000	0.000
Machine Learning	40	9.0000	0.81650	0.667
Protección de Amenazas de Red	40	8.8250	1.00989	1.020
Protección de Datos	40	0.0000	0.00000	0.000
Cifrado de Datos	40	0.0000	0.00000	0.000
Monitoreo de Usuarios	40	0.0000	0.00000	0.000

Nota. Elaboración Propia

Tabla 6

Análisis de Dimensiones de MCAFEE ENDPOINT SECURITY

MCAFEE ENDPOINT SECURITY	N	Media	Desviación estándar	Varianza
Integridad	120	5.7917	4.18861	17.544
Confidencialidad	120	0.0000	0.00000	0.000
Disponibilidad	80	8.9125	0.91671	0.840

Nota. Elaboración Propia

La evaluación de la solución McAfee Endpoint Security nos informa que el software tiene una cobertura parcial en cuanto a las características globales que una solución de seguridad debe tener. Se aprecia un puntaje elevado en la característica Machine Learning y puntajes promedio en las características Protección Antimalware, Protección Antiransomware y Protección de Amenazas de red. Esto se ve reflejado en un análisis de dimensiones de producto con un rendimiento bajo en integridad y confidencialidad de información y un rendimiento promedio en disponibilidad de información. La desviación y varianza percibida es muy elevada en relación a la dimensión integridad debido a que no ofrece cobertura en todas las características que engloba esta dimensión. La desviación y varianza percibida es óptima en relación a la dimensión disponibilidad debido a que ofrece cobertura total en todas las características que engloba esta dimensión.

Se concluye que el producto tiene su fortaleza en preservar la disponibilidad de la información en tanto es implementado y está en funcionamiento. Adicionalmente encuentra oportunidades de mejora en cuando a preservación de integridad de información. Se aprecia finalmente que carece de características que le permitan

preservar la confidencialidad de información por lo cual se halla la necesidad de complementar esta solución con algún otro software de protección.

Tabla 7

Evaluación de características de KASPERSKY ENDPOINT SECURITY

KASPERSKY ENDPOINT SECURITY	Desarrollo de Característica Actual	Desarrollo de Característica Ideal	Riesgo no Cubierto
Protección Antimalware	94%	100%	6%
Protección Antiransomware	94%	100%	6%
Control de Anomalías de Software	94%	100%	6%
Machine Learning	94%	100%	6%
Protección de Amenazas de Red	96%	100%	4%
Protección de Datos	71%	100%	29%
Cifrado de Datos	0%	100%	100%
Monitoreo de Usuarios	0%	100%	100%

Nota. Elaboración Propia

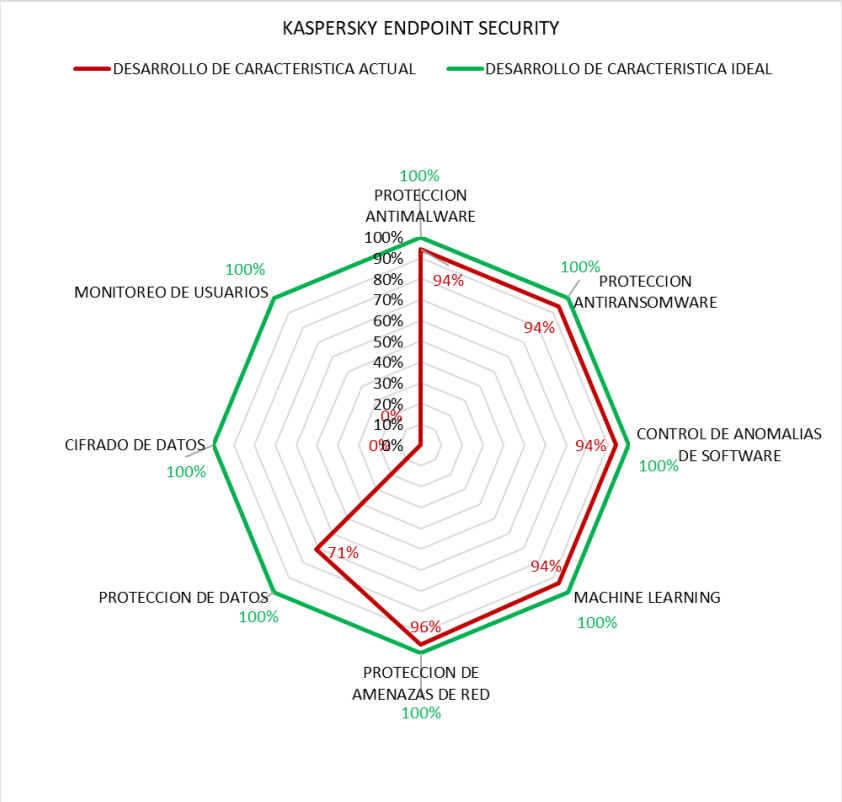

Figura 11. *Evaluación de características de KASPERSKY ENDPOINT SECURITY*

Nota. Elaboración Propia

Tabla 8

Análisis de Características de KASPERSKY ENDPOINT SECURITY

KASPERSKY ENDPOINT SECURITY	N	Media	Desviación Estándar	Varianza
Protección Antimalware	40	9.4000	0.67178	0.451
Protección Antiransomware	40	9.4000	0.70892	0.503
Control de Anomalías de Software	40	9.4000	0.77790	0.605
Machine Learning	40	9.4000	0.70892	0.503
Protección de Amenazas de Red	40	9.6000	0.54538	0.297
Protección de Datos	40	7.1000	0.90014	0.810
Cifrado de Datos	40	0.0000	0.00000	0.000
Monitoreo de Usuarios	40	0.0000	0.00000	0.000

Nota. Elaboración Propia

Tabla 9

Análisis de Dimensiones de KASPERSKY ENDPOINT SECURITY

KASPERSKY ENDPOINT SECURITY	N	Media	Desviación estándar	Varianza
Integridad	120	9.4000	0.71479	0.511
Confidencialidad	120	2.3667	3.40028	11.562
Disponibilidad	80	9.5000	0.63645	0.405

Nota. Elaboración Propia

La evaluación de la solución Kaspersky Endpoint Security nos informa que el software tiene una cobertura parcial en cuanto a las características globales que una solución de seguridad debe tener. Se aprecian puntajes elevados en las características Protección Antimalware, Protección Antiransomware, Control de Anomalías de Software, Machine Learning y Protección de Amenazas de red, y puntaje promedio en la característica Protección de Datos. Esto se ve reflejado en un análisis de dimensiones de producto como un rendimiento elevado en relación a la integridad y disponibilidad de información, sin embargo, se aprecia un rendimiento bajo para confidencialidad de información. La desviación y varianza percibida es óptima en relación a la dimensión integridad debido a que ofrece cobertura total en todas las características que engloba esta dimensión. La desviación y varianza percibida es muy elevada en relación a la dimensión confidencialidad debido a que no ofrece cobertura total en las características que engloba esta dimensión. La desviación y varianza percibida es un poco elevada en

relación a la dimensión disponibilidad debido a que ofrece cobertura parcial en todas las características que engloba esta dimensión.

Se concluye que el producto tiene su fortaleza en preservar la integridad y disponibilidad de la información en tanto es implementado y está en funcionamiento. Tiene grandes oportunidades de mejora en tanto a preservación de disponibilidad para mejorar las características sobre las que aún tiene puntajes promedio. Tiene debilidades para preservar la confidencialidad de la información por lo cual se haya la necesidad de complementar esta solución con algún otro software de protección.

Tabla 10

Evaluación de características de MCAFEE DLP ENDPOINT.

MCAFEE DLP ENDPOINT	Desarrollo de Característica Actual	Desarrollo de Característica Ideal	Riesgo no Cubierto
Protección Antimalware	0%	100%	100%
Protección Antiransomware	0%	100%	100%
Control de Anomalías de Software	0%	100%	100%
Machine Learning	0%	100%	100%
Protección de Amenazas de Red	0%	100%	100%
Protección de Datos	84%	100%	16%
Cifrado de Datos	90%	100%	10%
Monitoreo de Usuarios	82%	100%	18%

Nota. Elaboración Propia

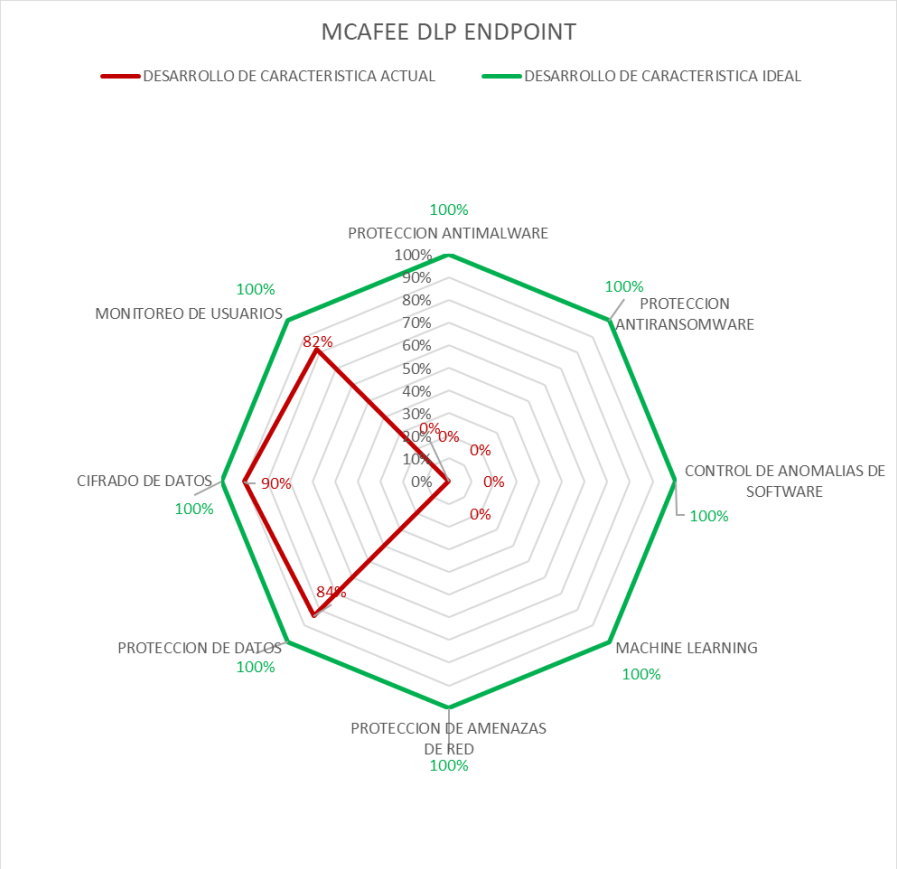

Figura 12. *Evaluación de características de MCAFEE DLP ENDPOINT*
Nota. Elaboración Propia

Tabla 1
Análisis de Características de MCAFEE DLP ENDPOINT

MCAFEE DLP ENDPOINT	N	Media	Desviación Estándar	Varianza
Protección Antimalware	40	0.0000	0.00000	0.000
Protección Antiransomware	40	0.0000	0.00000	0.000
Control de Anomalías de Software	40	0.0000	0.00000	0.000
Machine Learning	40	0.0000	0.00000	0.000
Protección de Amenazas de Red	40	0.0000	0.00000	0.000
Protección de Datos	40	8.4000	1.12774	1.272
Cifrado de Datos	40	9.0000	1.10940	1.231
Monitoreo de Usuarios	40	8.2250	1.29075	1.600

Nota. Elaboración Propia

Tabla 2

Análisis de Dimensiones de MCAFEE DLP ENDPOINT

MCAFEE DLP ENDPOINT	N	Media	Desviación estándar	Varianza
Integridad	120	0	0	0
Confidencialidad	120	8.5333	1.20874	1.461
Disponibilidad	80	0	0	0

Nota. Elaboración Propia

La evaluación de la solución McAfee DLP Endpoint nos informa que el software tiene una cobertura parcial en cuanto a las características globales que una solución de seguridad debe tener. Se aprecian un puntaje elevado en la característica de Cifrado de Datos y puntajes promedio en las características de Protección de Datos y Monitoreo de usuarios, esto se ve reflejado en un análisis de dimensiones de producto como un rendimiento promedio en relación a la confidencialidad de información y se aprecian puntajes bajos para integridad y disponibilidad de información. La desviación y varianza percibida es un poco elevada respectivamente en relación a la dimensión confidencialidad debido a que ofrece cobertura parcial en todas las características que engloba esta dimensión.

Se concluye que el producto tiene su fortaleza en preservar la confidencialidad de la información en tanto es implementado y está en funcionamiento. Tiene grandes oportunidades de mejora en tanto a preservación de confidencialidad para mejorar las características sobre las que aún tiene puntajes promedio. Se aprecia finalmente que carece de características que le permitan preservar la integridad y disponibilidad de información por lo cual se haya la necesidad de complementar esta solución con algún otro software de protección.

Tabla 3

Evaluación de características de SYMANTEC ENDPOINT PROTECTION.

SYMANTEC ENDPOINT PROTECTION	Desarrollo de Característica Actual	Desarrollo de Característica Ideal	Riesgo no Cubierto
Protección Antimalware	90%	100%	10%
Protección Antiransomware	88%	100%	12%
Control de Anomalías de Software	0%	100%	100%
Machine Learning	92%	100%	8%
Protección de Amenazas de Red	0%	100%	100%
Protección de Datos	82%	100%	18%
Cifrado de Datos	88%	100%	12%
Monitoreo de Usuarios	88%	100%	12%

Nota. Elaboración Propia

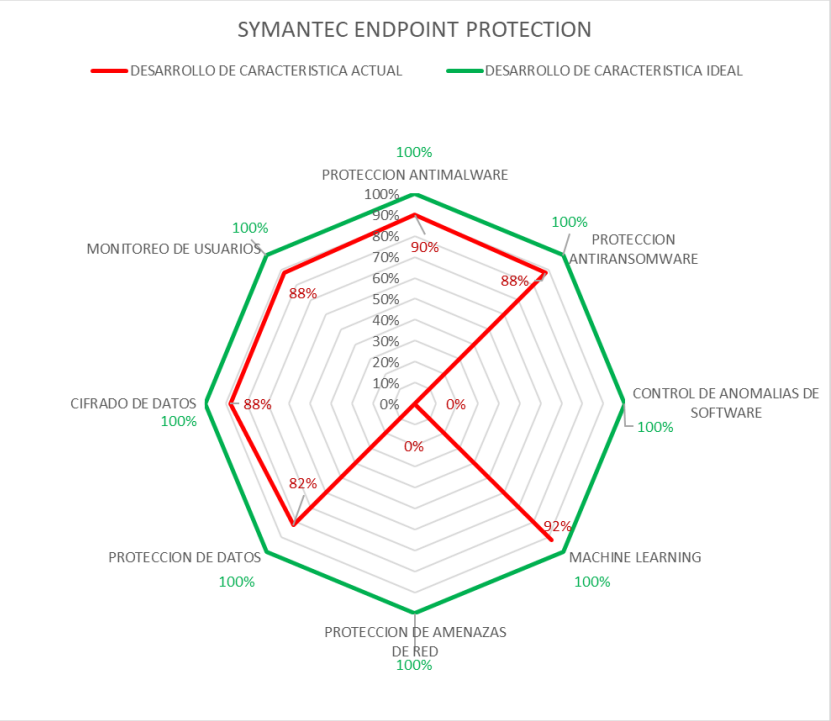

Figura 13. *Evaluación de características de SYMANTEC ENDPOINT PROTECTION*
Nota. Elaboración Propia

Tabla 14
Análisis de Características de SYMANTEC ENDPOINT PROTECTION

SYMANTEC ENDPOINT PROTECTION	N	Media	Desviación Estándar	Varianza
Protección Antimalware	40	9.0000	0.93370	0.872
Protección Antiransomware	40	8.8250	0.98417	0.969
Control de Anomalías de Software	40	0.0000	0.00000	0.000
Machine Learning	40	9.1750	0.78078	0.610
Protección de Amenazas de Red	40	0.0000	0.00000	0.000
Protección de Datos	40	8.2000	0.85335	0.728
Cifrado de Datos	40	8.7750	0.94699	0.897
Monitoreo de Usuarios	40	8.8000	0.96609	0.933

Nota. Elaboración Propia

Tabla 4

Análisis de Dimensiones de SYMANTEC ENDPOINT PROTECTION

SYMANTEC ENDPOINT PROTECTION	N	Media	Desviación estándar	Varianza
Integridad	120	5.9417	4.29049	18.408
Confidencialidad	120	8.5917	0.95702	0.916
Disponibilidad	80	4.5875	4.64892	21.613

Nota. Elaboración Propia

La evaluación de la solución Symantec Endpoint Protection nos informa que el software tiene una cobertura parcial en cuanto a las características globales que una solución de seguridad debe tener. Se aprecian puntajes elevados en las características Protección Antimalware y Machine Learning. Adicionalmente se observan puntajes promedio en las características Protección Antiransomware, Protección de datos, Cifrado de datos y Monitoreo de usuarios. Esto se ve reflejado en un análisis de dimensiones de producto con un rendimiento promedio en confidencialidad de información y un rendimiento bajo en integridad y disponibilidad de información. La desviación y varianza percibida es muy elevada en relación a la dimensión integridad y disponibilidad debido a que no ofrece cobertura en todas las características que engloba esta dimensión. La desviación y varianza percibida es óptima en relación a la dimensión confidencialidad debido a que ofrece cobertura total en todas las características que engloba esta dimensión.

Se concluye que el producto tiene su fortaleza en preservar la confidencialidad de la información en tanto es implementado y está en funcionamiento y encuentra oportunidades de mejora en cuando a preservación de integridad y disponibilidad de información.

Tabla 5

Evaluación de características de MCAFEE MVISION DLP

MCAFEE MVISION DLP	Desarrollo de Característica Actual	Desarrollo de Característica Ideal	Riesgo no Cubierto
Protección Antimalware	0%	100%	100%
Protección Antiransomware	0%	100%	100%
Control de Anomalías de Software	0%	100%	100%
Machine Learning	0%	100%	100%
Protección de Amenazas de Red	0%	100%	100%
Protección de Datos	88%	100%	12%
Cifrado de Datos	89%	100%	11%
Monitoreo de Usuarios	92%	100%	8%

Nota. Elaboración Propia

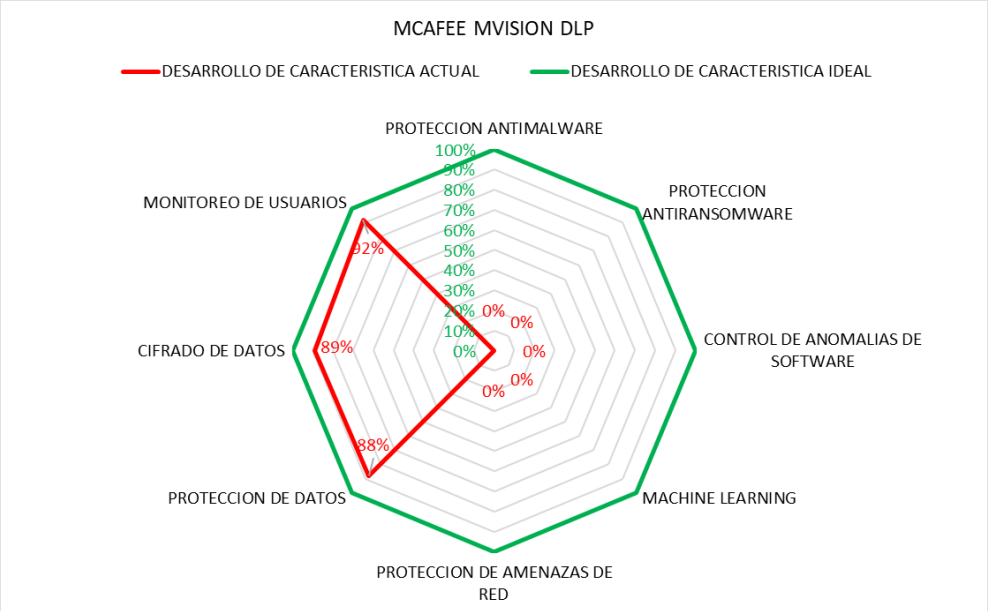

Figura 14. *Evaluación de características de MCAFEE MVISION DLP*
Nota. Elaboración Propia

Tabla 6
Análisis de Características de MCAFEE MVISION DLP

ARQUITECTURA BAFING	N	Media	Desviación estándar	Varianza
Protección Antimalware	40	0.0000	0.00000	0.000
Protección Antiransomware	40	0.0000	0.00000	0.000
Control de Anomalías de Software	40	0.0000	0.00000	0.000
Machine Learning	40	0.0000	0.00000	0.000
Protección de Amenazas de Red	40	0.0000	0.00000	0.000
Protección de Datos	40	8.8000	0.79097	0.626
Cifrado de Datos	40	8.9000	0.84124	0.708
Monitoreo de Usuarios	40	9.1500	0.80224	0.644

Nota. Elaboración Propia

Tabla 7
Análisis de Dimensiones de MCAFEE MVISION DLP

MCAFEE MVISION DLP	N	Media	Desviación estándar	Varianza
Integridad	120	0	0	0
Confidencialidad	120	8.9500	0.81838	0.670
Disponibilidad	80	0	0	0

La evaluación de la solución McAfee MVISION DLP nos informa que el software tiene una cobertura parcial en cuanto a las características globales que una solución de seguridad debe tener. Se aprecian un puntaje elevado en la característica de Monitoreo

de Usuarios y puntajes promedio en las características de Protección de Datos y Cifrado de Datos, esto se ve reflejado en un análisis de dimensiones de producto como un rendimiento promedio en relación a la confidencialidad de información y se aprecian puntajes bajos para integridad y disponibilidad de información. La desviación y varianza percibida es un optima en relación a la dimensión confidencialidad debido a que ofrece cobertura total en todas las características que engloba esta dimensión.

Se concluye que el producto tiene su fortaleza en preservar la confidencialidad de la información en tanto es implementado y está en funcionamiento. Tiene grandes oportunidades de mejora en tanto a preservación de confidencialidad para mejorar las características sobre las que aún tiene puntajes promedio. Se aprecia finalmente que carece de características que le permitan preservar la integridad y disponibilidad de información por lo cual se haya la necesidad de complementar esta solución con algún otro software de protección.

El marco de trabajo actual de BAFING es presentado implementando los productos McAfee Endpoint Security y McAfee DLP Endpoint de la suite empresarial McAfee Complete Endpoint Protection. A continuación, se presenta el resumen de resultados de su funcionamiento en el entorno tecnológico empresarial.

Tabla 8

Evaluación de características de ARQUITECTURA BAFING

ARQUITECTURA BAFING	Desarrollo de Característica Actual	Desarrollo de Característica Ideal	Riesgo no Cubierto
Protección Antimalware	86%	100%	12%
Protección Antiransomware	88%	100%	14%
Control de Anomalías de Software	0%	100%	100%
Machine Learning	91%	100%	10%
Protección de Amenazas de Red	87%	100%	12%
Protección de Datos	84%	100%	16%
Cifrado de Datos	90%	100%	10%
Monitoreo de Usuarios	82%	100%	18%

Nota. Elaboración Propia

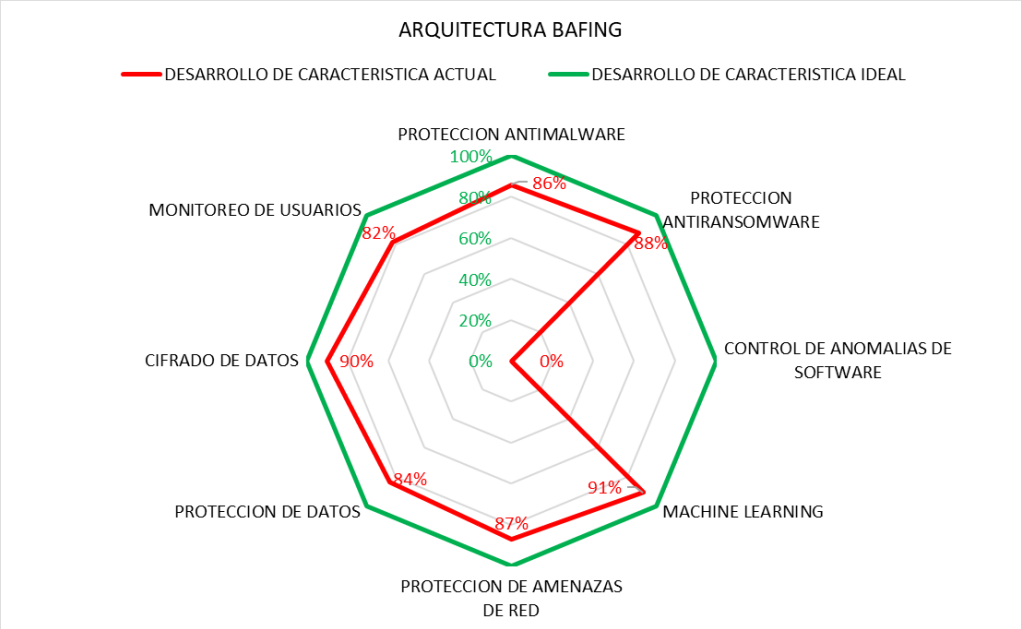

Figura 15. *Evaluación de características de ARQUITECTURA BAFING*
Nota. Elaboración Propia

Tabla 20
Análisis de Características de ARQUITECTURA BAFING

ARQUITECTURA BAFING	N	Media	Desviación estándar	Varianza
Protección Antimalware	40	8.7750	0.97369	0.948
Protección Antiransomware	40	8.6000	0.98189	0.964
Control de Anomalías de Software	40	0.0000	0.00000	0.000
Machine Learning	40	9.0000	0.81650	0.667
Protección de Amenazas de Red	40	8.8250	1.00989	1.020
Protección de Datos	40	8.4000	1.12774	1.272
Cifrado de Datos	40	9.0000	1.10940	1.231
Monitoreo de Usuarios	40	8.2000	1.26491	1.600

Nota. Elaboración Propia

Tabla 9
Análisis de Dimensiones de ARQUITECTURA BAFING

ARQUITECTURA BAFING	N	Media	Desviación estándar	Varianza
Integridad	120	5.7917	4.18861	17.544
Confidencialidad	120	8.5333	1.20874	1.461
Disponibilidad	80	8.9125	0.91671	0.840
Total		7.7458	2.1047	6.6150

Nota. Elaboración Propia

La evaluación de la solución Arquitectura BAFING nos informa que el software tiene una cobertura parcial en cuanto a las características globales que una solución de seguridad debe tener. Se aprecian puntajes elevados en las características Machine Learning y Cifrado de Datos. Tiene puntaje promedio en las características Protección Antimalware, Protección Antiransomware, Protección de Amenazas de Red, Protección de Datos y Monitoreo de Usuarios. Tiene puntaje bajo en las características Control de anomalías de Software. Esto se ve reflejado en un análisis de dimensiones de producto como un rendimiento promedio en relación a la confidencialidad y disponibilidad de información, asimismo se tiene un rendimiento bajo en integridad de información. La desviación y varianza percibida es óptima en relación a la dimensión disponibilidad debido a que ofrece cobertura total en todas las características que engloba esta dimensión. La desviación y varianza percibida es un poco elevada en relación a la dimensión confidencialidad debido a que ofrece cobertura parcial en todas las características que engloba esta dimensión. La desviación y varianza percibida es un muy elevada en relación a la dimensión integridad debido a que no ofrece cobertura en todas las características que engloba esta dimensión.

Se concluye que el producto tiene su fortaleza en preservar la disponibilidad de la información en tanto es implementado y está en funcionamiento. Encuentra grandes oportunidades de mejora en cuando a preservación de confidencialidad de información para mejorar las características sobre las que aún tiene puntajes promedio. Tiene oportunidades de mejora en la preservación de integridad de información.

La solución propuesta es un diseño de integración de software de seguridad McAfee MVISION DLP y Kaspersky Endpoint Security a fin de obtener el mejor perfil de seguridad de información a partir del funcionamiento coordinado de sus módulos de protección. A continuación, se presentan los resultados en la siguiente tabla:

Tabla 10
Evaluación de características de ARQUITECTURA HÍBRIDA.

ARQUITECTURA HIBRIDA	Desarrollo de Característica Actual	Desarrollo de Característica Ideal	Riesgo no Cubierto
Protección Antimalware	94%	100%	6%
Protección Antiransomware	94%	100%	6%
Control de Anomalías de Software	94%	100%	6%
Machine Learning	94%	100%	6%
Protección de Amenazas de Red	96%	100%	4%
Protección de Datos	88%	100%	12%
Cifrado de Datos	89%	100%	11%
Monitoreo de Usuarios	92%	100%	8%

Nota. Elaboración Propia

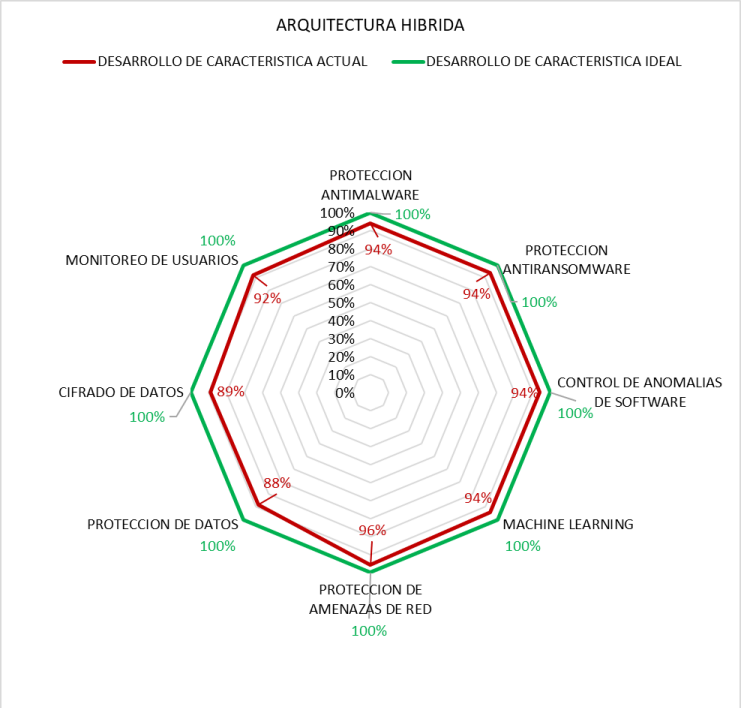

Figura 16. *Evaluación de características de ARQUITECTURA HÍBRIDA*

Nota. Elaboración Propia

Tabla 11

Análisis de Características de ARQUITECTURA HIBRIDA

ARQUITECTURA HIBRIDA	N	Media	Desviación Estándar	Varianza
Protección Antimalware	40	9.4000	0.70892	0.503
Protección Antiransomware	40	9.4000	0.74421	0.554
Control de Anomalías de Software	40	9.4000	0.59052	0.349
Machine Learning	40	9.4000	0.95542	0.913
Protección de Amenazas de Red	40	9.6000	0.49614	0.246
Protección de Datos	40	8.8000	0.79097	0.626
Cifrado de Datos	40	8.9000	0.84124	0.708
Monitoreo de Usuarios	40	9.1500	0.80224	0.644

Nota. Elaboración Propia

Tabla 12

Análisis de Dimensiones de ARQUITECTURA HIBRIDA

ARQUITECTURA HIBRIDA	N	Media	Desviación estándar	Varianza
Integridad	120	9.4000	0.67860	0.461
Confidencialidad	120	8.9500	0.81838	0.670
Disponibilidad	80	9.5000	0.76307	0.582
Total		9.2833	0.7534	0.5710

Nota. Elaboración Propia

La evaluación de la solución ARQUITECTURA HIBRIDA nos informa que el software tiene una cobertura total en cuanto a las características globales que una solución de seguridad debe tener. Se aprecian puntajes elevados en las características Protección Antimalware, Protección Antiransomware, Control de Anomalías de Software, Machine Learning, Protección de Amenazas de red y Monitoreo de Usuarios. Tiene puntaje promedio en las características Protección de Datos y Cifrado de Datos. Esto se ve reflejado en un análisis de dimensiones de producto como un rendimiento elevado en relación a la integridad y disponibilidad de información, asimismo se tiene un rendimiento promedio en confidencialidad de información. La desviación y varianza percibida es óptima en relación a la dimensión integridad, confidencialidad y disponibilidad debido a que ofrece cobertura total en todas las características que engloba esta dimensión.

Se concluye que el producto tiene su fortaleza en preservar la integridad y disponibilidad de la información en tanto es implementado y está en funcionamiento. Encuentra grandes oportunidades de mejora en cuando a

preservación de confidencialidad de información para mejorar las características sobre las que aún tiene puntajes promedio.

CAPITULO V: DISCUSION, CONCLUSIONES Y RECOMENDACIONES

5.1. Comprobación de Hipótesis

Hipótesis general

La implementación de la propuesta de seguridad informática en la Empresa aumenta la seguridad de la información.

Hipótesis específica 1

La integridad de la información después de implementar la propuesta es mayor que la integridad de la información antes de implementar la propuesta.

μ_1: Promedio de cumplimiento de la integridad de la información antes de implementar la propuesta.

μ_2: Promedio de cumplimiento de la integridad de la información después de implementar la propuesta.

a) Determinación de las hipótesis

Ho: $\mu_1 \geq \mu_2$ Ha: $\mu_1 < \mu_2$

b) Nivel de significancia

$\alpha = 0.05$

c) Prueba estadística

El estadístico a utilizar es la t de Student para diferencias de medias

$$\frac{(\bar{x}1 - \bar{x}2)}{\sqrt{\frac{{s_1}^2}{n_1} + \frac{{s_2}^2}{n_2}}} \sim t' no\ central\ con\ (n_1 - 1 + n_2 - 1)gl$$

d) Determinación de las regiones críticas (Valor teórico)

Se calcula mediante el $\mathbf{t'_{\alpha}} = -1.672$

e) Cálculos de los resultados muestrales

Tabla 25

Promedios de la Integridad Antes y Después de la implementación de la propuesta

Seguridad de la información	Antes			Después			t'_{α}	t'_{c}
	n	Media	Varianza	n	Media	Varianza		
Integridad	120	5.7917	17.544	120	9.4000	0.461	-1.672	-9.315

Nota. Elaboración Propia

f) Decisión

Como $\mathbf{t'_{\alpha}}$ = -1.672 > t'c =-9.315, se rechaza la Ho, es decir, la integridad de la información después de implementar la propuesta es mayor que la integridad de la información antes de implementar la propuesta.

Hipótesis específica 2

La confidencialidad de la información después de la implementación de la propuesta es mayor que la confidencialidad de la información antes de la implementación de la propuesta.

μ_1: Promedio de cumplimiento de la confidencialidad de la información antes de la implementación de la propuesta.

μ_2: Promedio de cumplimiento de la confidencialidad de la información después de la implementación de la propuesta.

a) Determinación de las hipótesis

Ho: $\mu_1 \geq \mu_2$ Ha: $\mu_1 < \mu_2$

b) Nivel de significancia

$\alpha = 0.05$

c) Prueba estadística

El estadístico a utilizar es la t de Student para diferencias de medias

$$\frac{(\bar{x}1 - \bar{x}2)}{\sqrt{\frac{{s_1}^2}{n_1} + \frac{{s_2}^2}{n_2}}} \sim t' no\ central\ con\ (n_1 - 1 + n_2 - 1)gl$$

d) Determinación de las regiones críticas (Valor teórico)

Se calcula mediante el $\mathbf{t'_{\alpha}}$ = -1.664

e) Cálculos de los resultados muestrales

Tabla 26

Promedios de la Confidencialidad Antes y Después de la implementación de la propuesta

Seguridad de la información	Antes			Después			t'α	t'c
	n	Media	Varianza	n	Media	Varianza		
Confidencialidad	120	8.5333	1.461	120	8.9500	0.670	-1.664	-3.127

Nota. Elaboración Propia

f) Decisión

Como t'α = -1.664 > t'c =-3.127, se rechaza la Ho, es decir, la confidencialidad de la información después de la implementación de la propuesta es menor que la confidencialidad de la información antes de la implementación de la propuesta.

Hipótesis específica 3

La disponibilidad de información después de la implementar la propuesta es mayor que la disponibilidad de la información antes de implementar la propuesta.

μ_1: Promedio de cumplimiento de la disponibilidad de la información antes de implementar la propuesta.

μ_2: Promedio de cumplimiento de la disponibilidad de la información después de implementar la propuesta.

a) Determinación de las hipótesis

Ho: $\mu_1 \geq \mu_2$ Ha: $\mu_1 < \mu_2$

g) Nivel de significancia

$\alpha = 0.05$

h) Prueba estadística

El estadístico a utilizar es la t de Student para diferencias de medias

$$\frac{(\bar{x}1 - \bar{x}2)}{\sqrt{\frac{{s_1}^2}{n_1} + \frac{{s_2}^2}{n_2}}} \sim t' no\ central\ con\ (n_1 - 1 + n_2 - 1)gl$$

i) Determinación de las regiones críticas (Valor teórico)

Se calcula mediante el **t'$_\alpha$** = -1.661

j) Cálculos de los resultados muestrales

Tabla 27

Promedios de la Disponibilidad Antes y Después de la implementación de la propuesta

Seguridad de la información	Antes			Después			t'$_\alpha$	t'$_c$
	N	Media	Varianza	n	Media	Varianza		
Disponibilidad	80	8.9125	0.840	80	9.5000	0.582	-1.661	-4.407

Nota. Elaboración Propia

k) Decisión

Como **t'$_\alpha$** = -1.661 > t'c = -4.407, se rechaza la Ho, es decir, la disponibilidad de la información después de la implementación de la propuesta es mayor que la disponibilidad de la información antes de la implementación de la propuesta.

Por lo tanto, al aceptarse como válidas las hipótesis alternativas, también es válida la hipótesis general, así, la implementación de la propuesta de seguridad informática en la empresa aumenta la seguridad de la información.

5.2. Discusión

Estudios previos realizados coinciden con los resultados obtenidos en este trabajo. Monsalve, Aponte y Chávez (2014), con el fin de mejorar la seguridad de la información, se creó, aplico y valoro un plan de gestión de vulnerabilidades. El mismo fue realizado por fases las cuales comprenden: *Inventario de equipos, Monitoreo de vulnerabilidades y plan de acción de las vulnerabilidades en orden de prioridad, Creación de base de datos y pruebas de Remediación, Despliegue de solución y automatización y por ultimo Seguimiento y remediación de exploits reportados.* Las vulnerabilidades son clasificadas en niveles de exploit a través de tareas de análisis de las herramientas de auditoría de

seguridad, nivel alto se califica cuando el exploit está en la base de conocimientos, su modo de operación común es otorgando privilegios de usuario administrador de sistema, como consecuencia de esto, dicho código ocasiona un daño considerable hacia los dispositivos afectados. Nivel medio se califica cuando el exploit no afecta directamente al sistema operativo; en general afecta aplicativos de software de usuarios sin privilegios, con la posibilidad de escalar a administrador de sistema.

Tras un periodo de 6 meses de monitoreo de las acciones plan de trabajo para la gestión de seguridad informática formulado en la empresa BAFING, se observaron mejoras en el proceso de gestión de seguridad de la información con un diferencial de más de un 15% entre los indicadores antes del proceso y después del proceso al haber implementado la solución. Como resultado del experimento realizado se cambiaron las soluciones de software de seguridad y equipos informáticos de punto final, equipos de seguridad perimetral para disminuir las brechas de vulnerabilidades.

Gil Vera, V. y Gil Vera, J. (2017), Desarrollaron un modelo de simulación dinámica que permita modelar, examinar el comportamiento de sistemas informáticos multiniveles a través del tiempo y evaluar el nivel óptimo de seguridad. El desarrollo del mismo fue a través del software “POWERSIM”, el cual entorno integrado para el desarrollo y modelamiento de negocios. La herramienta presenta un diagrama causal de un ambiente sin lineamientos de seguridad, el cual funciona de manera reactiva cuando se reporta un incidente de seguridad informática. Las variables tomadas en el experimento fueron: criticidad de la información, exploits, intrusiones, nuevos incidentes reportados e inversión de la solución. El período de tiempo para el desarrollo del experimento fue de 6 meses con un monitoreo mensual de los resultados.

Con lo anterior presentado se concluye que se redujeron los riesgos y se elaboró un plan de acción para reforzar la protección de los equipos informaticos. Se pudo percibir el mismo efecto tras realizar la implementación de la solución ofertada en el proyecto.

5.3. Conclusiones

- Se comprobó el efecto de la nueva arquitectura de seguridad informática en la integridad de la información de la empresa BANFIG S.A.C., pues antes de la implementación de la propuesta la integridad promedio era 5.79 y después de ella la integridad promedio fue de 9.40.
- Se comprobó el efecto de la nueva arquitectura de seguridad informática en la confidencialidad de la información de la empresa BANFIG S.A.C., pues antes de la implementación de la propuesta la confidencialidad promedio era 8.53 y después de ella la confidencialidad promedio fue de 8.95.
- También, se comprobó el efecto de la nueva arquitectura de seguridad informática en la disponibilidad de la información de la empresa BANFIG S.A.C., pues antes de la implementación de la propuesta la disponibilidad promedio era 8.91 y después de ella la disponibilidad promedio fue de 9.50.
- Se comprobó el efecto de la nueva arquitectura de seguridad informática en la seguridad de la información de la empresa BANFIG S.A.C., pues antes de implementar la propuesta la seguridad promedio era 7.75 y después de ella la seguridad promedio fue de 9.28.
- Las herramientas utilizadas para el desarrollo del experimento pueden ser probadas en todo ambiente de seguridad ENDPOINT a fin de medir el nivel de seguridad de la empresa.
- Los productos ENDPOINT de seguridad de información instalados pueden convivir en un mismo sistema, siempre tomando en cuenta las consideraciones de requerimientos mínimos de cada producto individual sumado para el funcionamiento paralelo de todas las aplicaciones.
- La plantilla de requerimientos mínimos del Anexo 5 puede variar en relación a los aplicativos que se desee integrar para una nueva evaluación de productos diferentes o del mismo producto en años posteriores con relación a las actualizaciones de software del fabricante.
- La solución propuesta está disponible para empresas que dispongan de un presupuesto extendido para la inversión de seguridad de información en la

empresa que administran puesto que la gestión de esta arquitectura requiere de comprar más licencias de productos y más elementos de hardware para los equipos ENDPOINT que en el presupuesto común.

5.3.1. Conclusión Principal

Los ambientes de seguridad gestionados a través de 2 o más soluciones de seguridad ofrecen un mayor potencial de cobertura en seguridad frente a arquitecturas o plataformas conformadas por una sola suite. Por tanto, las empresas deberán buscar las combinaciones de software de seguridad, que en conjunto provean de una mayor seguridad al ambiente de TI y a sus servicios.

5.4. Recomendaciones

- La propuesta de una arquitectura de seguridad informática nueva aumenta la seguridad de la información, por lo tanto, se recomienda su implementación en la empresa.
- Es tarea permanente y de vital importancia proteger la información y recursos tecnológicos informáticos a medida que la tecnología avanza.
- Las organizaciones deberían implementar las políticas de seguridad establecidas y normadas al más alto nivel de la organización como guía de esfuerzos de protección de activos basándose en buenas prácticas o ISOs publicadas referidas a seguridad informática.
- Sobre los costos, evitar accidentes informáticos reduce costos de reposición de recursos. Consecuentemente al mejorar la seguridad de información, la cual es el motivo de estudio de esta tesis, produce un efecto reductor en los costos de la empresa sobre la adquisición de equipos informáticos. Se recomienda manejar un presupuesto extendido destinado a la gestión de arquitecturas compuestas de seguridad con 2 o más soluciones administrables (Arquitecturas Hibridas).
- En futuras investigaciones es recomendable el desarrollo de modelos de simulación para examinar el nivel de seguridad de empresa, considerando criterios involucrados con la disminución del riesgo de vulnerabilidad de información, así como también variables macroeconómicas.

- Se recomienda mejorar el hardware de los equipos (computadores y redes de comunicación de alta gamma) en los que se operara esta solución, para garantizar el correcto rendimiento de los sistemas informáticos (software y base de datos).

GLOSARIO DE TERMINOS

Acceso no autorizado: Acción por la cual una persona tiene disposición de información o recurso informático de manera indebida y contra las políticas normadas dentro de la organización y sistema en el que esta almacenado.

Administrador de consola: Rol asignado a la persona que usa una consola de administración.

Ambiente de pruebas: Ubicación física o virtual en donde se revisan los cambios que un software produce sobre el sistema anfitrión o sobre las redes de sistemas informáticos relacionados.

Antivirus: Software que detecta la presencia de virus y puede neutralizar sus efectos.

Aplicativo: Software de uso práctico y común en las estaciones de trabajo.

Ataque de día cero: Se conocen así a las vulnerabilidades de un software que aún no han sido arregladas tras su descubrimiento y que han sido explotadas por un atacante cibernético.

Código malicioso: Elemento o característica que identifica a un virus informático como tal. Parte de un programa orientado a tomar acciones que perjudican el sistema que un virus infecta.

Confidencialidad: Capacidad de un sistema de controlar los accesos de los usuarios para la visualización de información contenida en el mismo y administrar los canales sobre los cuales se comparte dicha información.

Configuración: Conjunto de valores que pueden ser asignados a un software para determinar las características de su funcionamiento.

Consola de Administración: Software que permite el control remoto de productos asociados a su marca, por lo general de naturaleza empresarial, a fin de supervisar el estado de los dispositivos vinculados, recopilar datos sobre eventos y alertas y presentarlos gráficamente a través de informes o a través de tablas ordenadas. Permite así mismo la ejecución de tareas remotas y configuraciones de productos.

Disponibilidad: Capacidad de un sistema de mantener un servicio o plataforma de trabajo, sobre la cual se gestiona y administra información, funcionando sin interrumpirse de manera no planificada y controlada.

DLP: siglas de Data Los Prevention, alude a los mecanismos de protección para prevenir fuga de información en los sistemas informáticos.

Dominio (informática): espacio de trabajo en donde un equipo asignado como "Controlador de Dominio" puede desempeñar la administración de los equipos asociados a través de políticas de funcionamiento, privilegios de usuarios, dispositivos generales conectados como impresoras y escáneres, etc.

ENDPOINT: Punto final, referido a la característica de cobertura de un producto sobre las estaciones de trabajo.

Exploits: Vulnerabilidades detectadas en un sistema o programa informático.

Fuga de información: Evento por el cual información de una organización o parte de ella queda expuesta a personas ajenas o no autorizadas al acceso de la misma. Acción y condición de la información cuando ha sido filtrada de su sistema original a medios no autorizados.

Gartner: Coloquialmente es referido al cuadrante comparativo de marcas en un determinado periodo examinando la situación actual de las mismas en el mercado sobre un nicho establecido.

Herramientas Rootkit: Conjunto de mecanismos y utilitarios para adquirir derechos de un usuario administrador de sistema en uno o varios equipos de una red.

Informática: Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras.

Integridad: Capacidad de un sistema para preservar las propiedades (consistencia, precisión y confiabilidad) de la información que gestiona y administra sin corromperse por una alteración no autorizada.

Intrusión: Apropiarse, sin razón ni derecho, de un cargo, una autoridad, una jurisdicción.

Malware: Conocido también como software malicioso, es el término que recibe cualquier programa informático que tiene código malicioso capaz de dañar u obstruir de sus funciones a un sistema, dispositivo informático o la red sobre la cual se administran los dispositivos informáticos.

Monitoreo: Referido a la recolección, análisis y uso de la información obtenida de un sistema para la administración de un sistema o redes de sistemas.

Políticas De Seguridad: Normas dedicadas a manejar una buena auditoria de la información en el contexto de seguridad informática.

PYMES: Empresa mercantil, industrial, etc., compuesta por un número reducido de trabajadores, y con un moderado volumen de facturación.

Ransomware: Software intruso que bajo la modalidad de secuestro de información encripta la data de su huésped sin autorización y luego pide recompensa por la recuperación de la misma.

Red (informática): Conjunto de equipos informáticos conectados a través de un canal de transporte de datos (cable de red, señal wifi, etc.) y que comparten información (archivos digitales) y recursos (impresoras, escáneres, etc.).

Riesgo: Probabilidad de que ocurra un evento en un sistema.

Smartphones: Equipos de telefonía móviles con capacidad de procesar almacenar y compartir información a través de uno o más canales.

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

Vulnerabilidad: Condición de un sistema de quedar expuesto a atacantes informáticos.

Workstation: Estación de trabajo, coloquialmente referido a los equipos de cómputo de escritorio y laptops.

REFERENCIAS

ACISSI (2018). *Seguridad Informatica Hacking Etico. Conocer el ataque para una mejor defensa (4a ed.).* Barcelona: Ediciones ENI. Recuperado de: http://bit.ly/2Rpiz2W

Acosta, X. R. (2015). *Desarrollo de un Modelo de Seguridad para la Prevencion de Perdida de Datos DLP, en Empresas PYMES. (tesis de Pregrado).* Universidad de las Americas, Quito. Recupeado de: http://bit.ly/33TwBfT

Agé, M., Ebel, F., Rault, R., Vicogne, F., Crocfer, R., Puche, D. y Fortunato, G. (2018). *Seguridad informática - Hacking Ético Conocer el ataque para una mejor defensa (4a ed.).* México: Ediciones ENI. Recuperado de: http://bit.ly/2Rpiz2W

Agutter, C. (2019). ITIL® 4 Essentials: Your essential guide for the ITIL 4 Foundation exam and beyond. [Mensaje en un blog]. Recuperado de:https://bit.ly/2ywFUIF

American Psychological Association. (2020) *Publication manual of the American Psychological Association* (7th ed.). Washington, DC.:Autor

Arellano, D. y Friedich, N. K. (2015). *Seguridad Informatica. (tesis de Pregrado).* Universidad Nacional de la Amazonia Peruana, Iquitos. Universidad Nacional de la Amazonia Peruana. Recuperado de:http://bit.ly/2rh1oGc

Alvarado, J (2005). *Definición de informática*. Script. Blog: Escribd. Recuperado de: https://es.scribd.com/doc/41080767/

BAFING S.A.C.. (2019). *Service Desk Plus.* Lima: BAFING S.A.C.. https://freshservice.com/latam/comparacion-helpdesk-ti/alternativa-manageengine-servicedeskplus/?tactic_id=3389092&utm

Barato, J. (2015). *El Director de Proyectos a Examen: Guía de estudio en español para la capacitación del Director de Proyectos. Preparación para el Examen PMP/CAPM del PMI según la Guía del PMBOK.* México: Ediciones Díaz de Santos. Recuperado de: http://bit.ly/2Pfvd1Y

Bohorquez, C. F. (2017). *Propuesta de seguridad de la arquitectura tecnológica en una red empresarial.* (tesis de Pregrado). Escuela Colombiana de Ingenieria, Bogota. Recuperado de:http://bit.ly/2YkovLY

Casanovas, A. (2013). *Gestión de políticas de empresa. Serie de cuadernos sobre cumplimiento legal, (5).* Recuperado de: https://bit.ly/35DOmm5

Corda, M., Viñas, M. y Coria, M. (2017). Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. *Palabra Clave* (La Plata), 7(1), 1-18. Recuperado de: http://www.redalyc.org/articulo.oa?id=350553375007

Santos, J. C. (2014). *Seguridad y alta disponibilidad*. Bogotá, Colombia: Ra-ma Editorial.

Consejo General (s.f.). *Gestión de una fuga de información*. España: Consejo General de Colegios Oficiales de Graduados Sociales de España. Recuperado de: http://graduadosocial.org/docs/Gestion-fuga-informacion-Graduado_Social.pdf

Chaparro Rueda, Y. y Guerrero Rada, J. (2017). *Guía de buenas prácticas, instrumento para desarrollar la arquitectura de tecnología informática en la Gobernación del departamento del Atlántico, con la intención de habilitar la estrategia de TI para la gestión y el gobierno de la información.* (tesis de Maestria). Universidad del Norte, Barranquilla. Recuperado de:http://bit.ly/2RnN1dH

Daza, G. (2015). *Fortalecimiento De Seguridad Del Centro De Datos De La Carrera De Ingeniería En Sistemas Computacionales, Análisis De Políticas De Seguridad Informática Propuesta De Protección Endpoint Y Control De Acceso A La Red (tesis de Pregrado).* Universidad de Guayaquil, Guayaquil. Recuperado de:http://bit.ly/2LopyVW

Defaz, J. (2017). Qué es una vulnerabilidad. [Mensaje en un blog]. Recuperado de: https://www.jesusamieiro.com/wp-content/uploads/2011/08/Que_son_las_vulnerabilidades_del_-software.pdf

De Freitas, V. y Yaber, G. (25 de Febrero de 2015). Una propuesta de arquitectura para los Sistemas Informáticos de Gestión del Conocimiento en Instituciones de

Educación Superior. *Revista Espacios*. 1(2); 2-4. Recuperado de:http://bit.ly/2PcTzcy

Deloitte. (2014). El futuro de la banca móvil en América Latina Perspectivas desde Argentina, Brasil y México. [Mensaje en un blog]. Recuperado de:https://www2.deloitte.com/content/dam/Deloitte/py/Documents/aboutdeloitte/Futuro_banca_movil2012.pdf

Díaz-Ricardo, Y., Pérez-del Cerro, Y. y Proenza-Pupo, D. (2014) Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín. *Ciencias Holguín*, XX (2), 1-14. Recuperado de: http://www.redalyc.org/articulo.oa?id=181531232002

Dussan Clavijo, C. (2006) Políticas de seguridad informática. *Entramado*, 2(1), 86-92 Recuperado de: http://www.redalyc.org/articulo.oa?id=265420388008

E-educativa. (s/f). *Definición de software*. [Mensaje en un blog]. Recuperado de: rhttp://e-ducativa.catedu.es/44700165 aula/archivos/repositorio/1000/1061/html/1_software.html#:~:text=1.,Software&text=Se%20llama%20software%20al%20conjunto,l%C3%B3gico%20de%20un%20sistema%20inform%C3%A1tico.

Figueroa, C. (2016). El uso del smartphone como herramienta para la búsqueda de información en los estudiantes de pregrado de educación de una universidad de Lima Metropolitana. *Educación*, 25 (49). Recuperado de: http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1019-94032016000200002

Gamboa, J. Z. (2018). Evolución de las Metodologías y Modelos utilizados en el Desarrollo de Software. *INNOVA Research Journal*. 1(2); 3-4. Recuperado de:https://bit.ly/35unzsk

García, G. y Martínez R. (2006) Análisis y control de riesgos de seguridad informática: control adaptativo Un cambio de paradigma hacia la gestión de riesgos orientada al control adaptativo. Recuperado de: http://www.rsbac.org/doc/media/rsbac-

marek2006.pdf.
http://acistente.acis.org.co/typo43/fileadmin/Revista_105/JMGarcia.pdf

Gartner. (2019). *Tecnología*. México: Gartner Peer Insights. Recuperado de: https://gtnr.it/2OS9spR

Gartner. (20 de Agosto de 2019). *gartner.com*. Recuperado de:https://gtnr.it/2OT0Mzr

Gartner. (2021). *Gartner.com*. Recuperado de: https://gtnr.it/34TI6VY

Gartner. (2020). *Seguridad*. México: About Gartner. Recuperado de: https://www.gartner.com/reviews/market/endpoint-protection-platforms/compare/product/kaspersky-endpoint-security-for-business-vs-microsoft-system-center-endpoint-protection

Grandi (2019). Auditoría de Sistema y políticas de Seguridad Informática. USA: Monografías. Com. Recuperado de: https://www.monografias.com/trabajos12/fichagr/fichagr.shtml

Gestion (31 de 07 de 2014). *gestion.pe*. Perú: Diario Gestión. Recuperado de: http://bit.ly/2YhnhBm

Gestión (09 de Agosto de 2017). *Seguirdad en empresas.* Peru: Diario Gestión. Recuperado de: http://bit.ly/2YoLENp

Gil Vera, V.; Gil Vera, J. (2017) Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica*, 22 (2), 193-197 Recuperado de: http://www.redalyc.org/articulo.oa?id=84953103011

Gomez, A. (2014). *Enciclopedia de la Seguridad Informatica.* Madrid: RA-MA. Recuperado de: http://bit.ly/33UAd10

Hernandez, R., Fernandez, C. y Baptista, P. (2015). *Metodología de la investigación.* (5° ed.). México: McGraw-Hill Interamericana. Recuperado de: http://bit.ly/2PiMrLI

Huércano Ríos, S. (2014). *Manuel de ITIL v.3, Manual Integro*. Biable: Sevilla-España.

Incibe (2019). *DLP protege tus datos contra fugas de información*. Recuperado de:https://www.incibe.es/protege-tu-empresa/blog/dlp-protege-tus-datos-fugas-informacion

Ionos (2020). Lo que hay que saber sobre el rootkit. [Mensaje en un blog]. Recuperado de: https://www.ionos.es/digitalguide/servidores/seguridad/rootkit/

Kaspersky Lab. (10 de Julio de 2017). *Seguridad*. México: *Kaspersky.com*. Recuperado de: http://bit.ly/2OUtwbk

Kaspersky Lab. (2017). The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within Kaspersky Lab. [Mensaje en blog]. Recuperado de: https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Leon, C. (2015). *Estrategias para la clasificación de la información y prevención de fuga de información. (tesis de Pregrado).* Universidad Piloto de Colombia, Recuperado de:EBogota. http://bit.ly/2rjjVS7

Lopez, P. (2010). *Seguridad Informatica.* México: Editex. Recuperado de:http://bit.ly/2Lq9ovr

Monsalve-Pulido, J.; Aponte-Novoa, F. y Chaves-Tamayo, D. (2014). Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia). *Facultad de Ingeniería*, 23 (37). 65-72. Recuperado de: http://www.redalyc.org/articulo.oa?id=413937008007

Muñoz Hernández, H.; Zapata Cantero, L.; Requena Vidal, D. y Ricardo Villadiego, Leonela (2019) Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. *Revista Venezolana de Gerencia*, vol. 2. Recuperado de: http://www.redalyc.org/articulo.oa?id=29063446029

Muñoz, J. (2017). ¿Qué es ransomware y cómo funciona el secuestro de datos? [Mensaje en un blog]. Recuperado de: https://computerhoy.com/noticias/software/que-es-ransomware-como-funciona-secuestro-datos-43513

Naz, R., Khan, M. N., & Aamir, M. (2016). Scrum-Based Methodology for Product Maintenance and Support. *International Journal of Engineering and Manufacturing*. 1(2); 1-3. Recuperado de: http://bit.ly/2Ym9mK4

Netcloud. (2019). *Ciberseguridad: Amenaza vs. Vulnerabilidad*. [Mensaje en un blog]. Recuperado de: https://netcloudengineering.com/ciberseguridad-amenaza-vulnerabilidad/

P. Galdaméz (2011). "Seguridad Informática." Actualidad TIC, pp. 1–4.

Reklaitis, V. (25 de Mayo de 2018). *marketwatch.com*. México: Marketwatch. Recuperado de: https://on.mktw.net/2YiM6wI

Rios, S. (2017). *B-able.* México: Bable. Recuperado de: http://bit.ly/2PeTTYd

Sosa, J. T. (2018). *Metodología para la elección de software de seguridad informática. (tesis de Pregrado).* Universidad Cesar Vallejo, Lima. Recuperado de: http://bit.ly/2Ln3YRO

Seguridad Informática. (2017). *Exploits. Competencias informáticas e informacionales*. México: Seguridad Informática. Recuperado de: https:/ /moodle2017-18.ua.es/moodle/pluginfile.php/80624/mod_resource/content/5/seguridad/pagina_09.htm

Tamayo y Tamayo, M. (1996). El proceso de la investigación científica. México. Limusa.

Tecnovo. (2019). *¿Qué es una workstation? Características y ventajas*. México: tecnovo.com.Recuperado de: https://tecnovo.pe/2019/07/que-es-una-workstation-caracteristicas-y-ventajas/

Terán Bustamante, A.; Dávila Aragón, G. y Castañón Ibarra, R. (2019) Gestión de la tecnología e innovación: un Modelo de Redes Bayesianas. *Economía: teoría y práctica*, (50), 63-100. Recuperado de: http://www.redalyc.org/articulo.oa?id=281161618004

Tipton, Harold F. Tipton, Micki Krause (eds.). (2006), *Information Security Management Handbook, 5th Ed.*, CRC Press.

Tirado, N. R., Álvarez Morales, E. L., & Carreño Sandoya, S. D. (2017). Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas. *Revista Publicando*.1(3); 5-6. REcuparado de: http://bit.ly/389Z04I

Técnico (2019). *¿Qué es una workstation? Características y ventajas*. México: tecnovo.com. Recuperado de: https://tecnovo.pe/2019/07/que-es-una-workstation-caracteristicas-y-ventajas/

Trigás, M. (2012), *Metodología Scrum*. España: Trill. Recuperado de: http://openaccess.uoc.edu/webapps/o2/handle/10609/17885.

Tudor Jean Killmeyer Tudor (ed.) (2006) *Information Security Architecture: An Integrated Approach to Security in the Organization*, CRC Press

Vega Velasco Walter (2008). Políticas y seguridad de la información. *Fides Et Ratio* 2(2). Recuperado de: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008

ANEXOS

Anexo 1: Matriz de Consistencia

Problema general	**Objetivo general**	**Hipótesis general**
¿Cuáles son los efectos del diseño de una nueva arquitectura de seguridad informática en la seguridad de la información de empresa BAFING S.A.C.?	Diseñar, implementar y valorar la propuesta de una arquitectura de seguridad informática en la seguridad de la información de la empresa BAFING S.A.C.	La implementación de propuesta de seguridad informática en la Empresa aumenta la seguridad de la información.
Problemas específicos	Objetivos específicos	Hipótesis especificas
¿Cuál es el efecto del diseño de una nueva arquitectura de seguridad en la integridad de la información en la empresa BAFING S.A.C.? ¿Cuál es el efecto del diseño de una nueva arquitectura de seguridad en la confidencialidad de la información en la empresa BAFING S.A.C.? ¿Cuál es el efecto del diseño de una nueva arquitectura de seguridad en la disponibilidad de la información en la empresa BAFING S.A.C.?	Determinar el efecto de una nueva arquitectura de seguridad informática en la integridad de la información de la empresa BAFING S.A.C. Determinar el efecto de una nueva arquitectura de seguridad informática en la confidencialidad de la información de la empresa BAFING S.A.C. Determinar el efecto de una nueva arquitectura de seguridad informática en la disponibilidad de la información de la empresa BAFING S.A.C.	La integridad de la información después de la implementación de la propuesta es mayor que la integridad de la información antes de la implementación de la propuesta. La confidencialidad de la información después de la implementación de la propuesta es mayor que la confidencialidad de la información antes de la implementación de la propuesta. La disponibilidad de la información después de la implementación de la propuesta es mayor que la disponibilidad de la información antes de la implementación de la propuesta.

Anexo 2: Encuesta/instrumento de evaluación

Sobre Seguridad Informática en su Empresa

Para la elaboración de perfil de evaluación.

¿Cual considera que es la causa mas probable de los incidentes reportados en su empresa o empresa que audita?

- [ ] Malware
- [ ] Ransomware
- [ ] Exploits/vulnerabilidades de software
- [ ] Ataques de día cero
- [ ] Robo o perdida de dispositivos
- [ ] Fuga de informacion confidencial
- [ ] Accesos no autorizados a equipos informáticos
- [ ] Ataques dirigidos o ataques internos
- [ ] Alto consumo de recursos de sistema
- [ ] Configuracion incorrecta del software de seguridad
- [ ] Ataques de red
- [ ] Moderacion de filtros de seguridad en grupos de usuarios
- [ ] Otro: _____

Sobre Seguridad Informática en su Empresa

Para la recolección de resultados de evaluación de software

¿Que producto de seguridad endpoint manejan principalmente en su empresa o empresa que audita?

- ○ McAfee
- ○ Kaspersky
- ○ Eset
- ○ Symantec
- ○ Otro: _____

En la escala del 1 al 10 en donde 1 es muy bajo y 10 es muy alto. ¿Como calificaría usted la capacidad del software de seguridad endpoint mencionado anteriormente para las siguientes proposiciones?, dejar en blanco si la característica mencionada no aplica a la solución que audita:

	1	2	3	4	5	6	7	8	9
Capacidad para eliminar malware y codigo malicioso	○	○	○	○	○	○	○	○	○
Capacidad para eliminar amenazas tipo Ransomware	○	○	○	○	○	○	○	○	○
Capacidad para identificar exploits de SO y vulnerabilidades de software de terceros	○	○	○	○	○	○	○	○	○
Capacidad de autoaprendizaje para la identificación de nuevas amenazas	○	○	○	○	○	○	○	○	○
Capacidad para prevenir amenazas de red y ataques desde fuera de la red local	○	○	○	○	○	○	○	○	○
f. Capacidad para bloquear la lectura y escritura de información confidencial	○	○	○	○	○	○	○	○	○
g. Capacidad para proteger y cifrar datos de usuarios con contraseñas	○	○	○	○	○	○	○	○	○
h. Capacidad para establecer grupos de accesos a información critica	○	○	○	○	○	○	○	○	○

Anexo 3: Validez de instrumentos por Jueces Expertos

Consentimiento Informado

Título de la investigación: DISEÑO DE UNA ARQUITECTURA DE SEGURIDAD INFORMÁTICA PARA INCREMENTAR LA SEGURIDAD DE INFORMACIÓN EN LA EMPRESA BAFING S.A.C. EN 2020

Tenga usted buenos días. Mi nombre es Josue Asurza Cáceres, soy tesista de la carrera de Ingeniería de Sistemas Empresariales de la Universidad Científica del Sur. Dentro de mi proceso formativo estoy desarrollando la presente investigación que tiene por finalidad Demostrar que el diseño de una arquitectura de seguridad informática puede reducir el riesgo de vulnerabilidad de información en BAFING S.A.C. La investigación está dirigida a la valoración de características de protección de software de seguridad por parte del personal de BAFING S.A.C., y consiste en realizar pruebas de seguridad en entornos controlados con software antivirus de diversos fabricantes. El tiempo de los mismos no debería exceder los 30 minutos por prueba.

Le indico que la participación en esta investigación no le provocará algún perjuicio, de ninguna manera los valores obtenidos en dichas pruebas ni su no participación en la investigación lo afectarán de forma. Por otro lado, al finalizar la investigación, compartiré con usted de forma personal los resultados de ambas evaluaciones para la consideración en la ejecución de proyectos futuros dentro de la empresa como una base de conocimientos. No se le brindará algún beneficio económico.

La participación en esta investigación es voluntaria, puede incluso retirarse de la misma luego de haber aceptado inicialmente realizar las pruebas, sin la necesidad de dar alguna explicación. Todos los datos obtenidos serán manejados exclusivamente por mí y los codificaré para que no se pierda la confidencialidad de los mismos; asimismo, no se realizarán otras investigaciones diferentes a lo detallado en este documento.

Si tuviera alguna duda adicional, puede comunicarse conmigo al correo electrónico: jasurza@bafing.com, que estaré gustosa de poder contestarle.

Como participante declaro que:

Se me ha explicado y he comprendido la naturaleza y los objetivos de la investigación presentada por Josue Asurza Caceres. Se me ha aclarado que mi participación en la investigación no me ocasionará ningún tipo de gasto. Firmo este documento como prueba de mi aceptación voluntaria habiendo sido antes informado sobre la finalidad del trabajo y que puedo retirarme de la investigación cuando yo lo decida.

Así mismo el documento otorga autorización al investigador para recolectar la información solicitada con el personal entrevistado que este sujeto a la jerarquía del área Command Center System Security de BAFING S.A.C.

Fecha: 09 de Diciembre de 2020

Apellidos y Nombres: Granados Blanco Teresa Liliana
Cargo: Jefa de soporte y mantenimiento de Systems Security

Firma: 

DNI: 72567078

Anexo 4: Constancia emitida por la institución

Carta de autorización

Señores Autoridades
Universidad Científica del Sur
Facultad de Ciencias Empresariales

Estimados Señores:

Nos es grato extenderles un cordial saludo y comunicarles que el Sr. Josue David Asurza Cáceres, estudiante de la carrera de Ingeniería de Sistemas Empresariales de la Universidad Científica del Sur, cuenta con la debida autorización para realizar su proyecto de tesis en nuestra empresa BAFING S.A.C. para que obtenga la información necesaria que le permita desarrollar su trabajo profesional.

Además, se precisa que el uso de la información que solicite es con los fines relacionados a la sustentación de su tesis y no se mostrará o divulgará información para temas no educativos.

Agradecerles por esta oportunidad de colaborar con el desarrollo académico de sus estudiantes y reiterarles nuestra más alta estima y consideración.

Atentamente

Teresa Liliana Granados Blanco
Supervisor de Equipo Command Center

Anexo 5: Requerimientos Mínimos

Servidor que administra Consola McAfee ePO 5.10.9 y Consola Kaspersky Security Center 12	
Componente	Requisitos y recomendaciones
Sistema de archivos	Partición de sistema de archivos NT (NTFS).
Espacio libre en disco	80 GB: mínimo recomendado.
Dirección IP	Utilizar direcciones IP estáticas
Memoria	Se recomienda un mínimo de 16 GB de RAM
Tarjeta de interfaz de red (NIC)	100 MB o superior
Puertos	TCP 8443; 7080; 10443; 13000; 14000; 15000
Procesador	8 Cores de 64bits; Velocidad 2,66 GHz o superior
Sistema Operativo	Windows Server 2016; Minimo
Base de Datos	SQL Server Express 2016; Minimo
Equipo cliente que gestionaran Kaspersky Endpoint Security 11.5 y McAfee DLP 11.6	
Componente	Requisitos y recomendaciones
Sistema de archivos	Partición de sistema de archivos NT (NTFS).
Espacio libre en disco	3GB; minimo recomendado
Dirección IP	Utilizar direcciones IP estáticas
Memoria	Se recomienda un mínimo de 8 GB de RAM
Tarjeta de interfaz de red (NIC)	100 MB o superior
Puertos	TCP 7080; 10443; 13000; 14000; 15000
Procesador	8 Cores de 64bits; Velocidad 2,66 GHz o superior
Sistema Operativo	Windows 10 Pro 20H2 en adelante
Software Instalado	McAfee Agent 5.7.2; Kaspersky Network Agent 12