Revista CIES – ISSN-e 2216-0167. Volumen 15. Número 1. Año 2024. Páginas 47-61. Dirección de Investigaciones – Institución Universitaria Escolme (Medellín, Colombia)

Cyber-Security Mesh Architecture, estrategias para un despliegue en empresas colombianas

Cristian Camilo Sánchez Orozco
Administración de Sistemas Informáticos, Institución Universitaria Escolme, Medellín, Colombia, ccsanchezo@escolme.edu.co

Beatriz Elena Flórez Montoya
Docente investigador, Institución Universitaria Escolme, Medellín, Colombia, coordinacionprogramassistemas@escolme.edu.co

Recibido: 30/11/2023 - **Aceptado**: 02/02/2024 - **Publicado:** 23/04/2024

RESUMEN

Los ciberataques en Colombia han experimentado un notable aumento en los últimos años, con amenazas que van desde ataques dirigidos a entidades gubernamentales y empresas hasta actividades delictivas como el robo de datos y la extorsión en línea. Estos ciberdelincuentes utilizan diversas técnicas, como el phishing, el malware y la suplantación de identidad. Para hacer frente a esta creciente amenaza, Colombia está fortaleciendo su enfoque en ciberseguridad y colaboración entre sectores público y privado.

Además, la ISO 27000, tiene una serie de estándares internacionales que proporciona pautas y mejores prácticas para la gestión de la seguridad de la información en organizaciones colombianas, con un enfoque en la certificación de sistemas de seguridad.

Fortinet Security Fabric, una plataforma de ciberseguridad desarrollada por Fortinet se basa enla integración y colaboración entre diferentes soluciones de seguridad para proteger eficazmente redes, sistemas y datos. La combinación de la Arquitectura de Malla de Ciberseguridad, la ISO 27000 y Fortinet Security Fabric proporciona a las organizaciones una estrategia sólida para abordar las crecientes amenazas cibernéticas y proteger su infraestructurade manera efectiva.

Palabras clave: ciberdelincuentes; ciberseguridad; estrategia.

ABSTRACT

Cyberattacks in Colombia have seen a significant increase in recent years, with threats ranging from targeted attacks on governmental institutions and businesses to criminal activities such as data theft and online extortion. These cybercriminals employ various techniques, including phishing, malware, and identity theft. To counter this growing threat, Colombia is strengtheningits cybersecurity focus and fostering collaboration between the public and private sectors.

Additionally, the ISO 27000, has a series of international standards, that provide guidelines and

best practices for managing information security in Colombian organizations, with a focus on security system certification.

Fortinet Security Fabric, a cybersecurity platform developed by Fortinet, is built on the integration and collaboration of different security solutions to effectively protect networks, systems, and data. The combination of Cybersecurity Mesh Architecture, ISO 27000, and Fortinet Security Fabric provides organizations with a robust strategy to address the growing cyber threats and effectively safeguard their infrastructure.

Keywords: cybercriminals; cybersecurity; strategy.

1. INTRODUCCIÓN

En un mundo cada vez más digitalizado, la ciberseguridad se ha convertido en una preocupación global de vital importancia, y Colombia no escapa a esta realidad. El país ha experimentado un notable aumento de ciberataques en los últimos años, que abarcan desde amenazas dirigidas contra instituciones gubernamentales y empresas hasta delitos cibernéticoscomo el robo de datos y la extorsión en línea.

Ante esta creciente amenaza, Colombia está tomando medidas proactivas para desarrollar un plan estratégico que se base en las normativas vigentes. El objetivo principal de este artículo esla creación de un sistema de seguridad distribuida, alineado con los principios de la Cyber- security Mesh Architecture. Este enfoque busca consolidar la protección de la seguridad digitalen el país y se apoya en las directrices y regulaciones establecidas en la norma ISO 27000.

La ISO 27000 representa una serie de estándares internacionales relacionados con la seguridadde la información, proporcionando directrices y mejores prácticas para establecer, implementar, mantener y mejorar la gestión de la seguridad de la información en las organizaciones. Es importante destacar que la ISO 27001, en particular, es ampliamente reconocida y se utiliza para la certificación de sistemas de gestión de seguridad de la información.

A su vez, Fortinet Security Fabric se erige como una plataforma integral de ciberseguridad desarrollada por Fortinet, líder en el campo. Esta plataforma integra una amplia gama de soluciones y servicios de seguridad, proporcionando una defensa completa contra las amenazas cibernéticas. El enfoque central de Fortinet Security Fabric radica en la integración, colaboración y centralización de la gestión, lo que garantiza una protección efectiva de las redes, sistemas y datos de una organización.

En conjunto, estos elementos forman la base de una estrategia sólida y coordinada para abordarlas crecientes amenazas cibernéticas en el contexto colombiano, con el objetivo de fortalecer la seguridad digital y proteger los activos de la nación de manera efectiva.

2. MARCO TEÓRICO Y/O ANTECEDENTES

El término seguridad informática ha sido objeto de estudio por algunos autores, lo que permite tener una definición más exacta; por lo tanto, es un conjunto de medidas y procedimientos, tanto

humanos como técnicos, que permiten proteger la integridad, la confidencialidad y disponibilidad de la información (Avenía, 2017). Adicionalmente, la seguridad informática se refiere a garantizar que los recursos del sistema de información de una entidad se utilicen de acuerdo con las decisiones preestablecidas. Esto implica que el acceso a la información y su modificación estén restringidos únicamente a las personas autorizadas y dentro de los límites de sus autorizaciones correspondientes (ESGinnova Group, 2015).

Trasladémonos unos años al pasado y veamos cómo ha ido cambiando el paradigma de la tecnología. Durante los años 90, las organizaciones enfrentaban un escenario tecnológico significativamente diferente al actual. En aquel entonces, el acceso a internet era limitado y las redes empresariales estaban más cerradas, con menos dispositivos conectados. Las amenazas cibernéticas eran, en cierto modo, menos sofisticadas, aun así, las organizaciones debían hacer frente a amenazas cibernéticas que podían propagarse a través de archivos compartidos y aplicaciones.

Los primeros firewalls y programas antivirus surgieron como respuestas a estos desafíos iniciales. Los firewalls, en sus primeras encarnaciones, se centraban en bloquear ciertos tipos de tráfico de red para proteger las redes internas de las organizaciones. Por otro lado, los programas antivirus se enfocan principalmente en detectar y eliminar amenazas cibernéticas específicas basadas en firmas que se propagaban a través de diversas formas de interacción digital (Apen soluciones informátiques, s.f.).

A medida que avanza la tecnología en las siguientes décadas, la conectividad global explotó yel número de dispositivos conectados a internet se multiplicó exponencialmente. Esto transformó por completo el panorama de la seguridad cibernética. Las empresas empezaron a utilizar aplicaciones y servicios en línea, lo que amplió las posibilidades de ataques y vulnerabilidades. Las amenazas cibernéticas se volvieron más sigilosas y complejas, dando lugar a una nueva generación de malware (Peláez, 2023).

En respuesta a estas amenazas emergentes, las soluciones de firewall y antivirus evolucionaron rápidamente. Los firewalls adoptaron técnicas avanzadas de inspección de paquetes y análisis de comportamiento para identificar y bloquear amenazas en tiempo real. Por otro lado, los programas antivirus se volvieron más inteligentes, utilizando algoritmos de aprendizaje automático para analizar patrones de comportamiento y detectar amenazas cibernéticas desconocidas. Sin embargo, aunque estas soluciones han avanzado considerablemente, la naturaleza en constante cambio de las amenazas cibernéticas significa que simplemente confiaren los firewalls y antivirus no es suficiente para proteger las empresas de los diferentes ataques (Fernández, 2019).

En la actualidad, las empresas han integrado tecnologías en la nube y servicios de software, lo que ha marcado un crecimiento tecnológico considerable. Esta evolución abarca desde opciones como infraestructura y hardware hasta plataformas, además de soluciones de software adaptadas a las necesidades específicas de cada empresa.

Simultáneamente, las amenazas cibernéticas han evolucionado rápidamente. Los firewalls y los programas antivirus han mejorado, adoptando técnicas avanzadas como la inspección de

paquetes, análisis de comportamiento y algoritmos de aprendizaje automático para identificar y bloquear amenazas en tiempo real. A pesar de estos avances, la naturaleza cambiante de las amenazas cibernéticas implica que simplemente depender de firewalls y antivirus no es suficiente para proteger a las empresas de los diversos ataques (Fernández, s.f.).

En este contexto, la seguridad cibernética se convierte en una prioridad crítica. Proteger datos y sistemas en un mundo digital complejo es esencial. Para las pequeñas y medianas empresas, encontrar el equilibrio entre la adopción tecnológica y la seguridad se vuelve crucial. Implementar estrategias de ciberseguridad sólidas, que incluyan no solo firewalls y antivirus, sino también medidas proactivas y educación para los empleados, es esencial para garantizar un crecimiento organizativo seguro y continuo. La colaboración entre tecnología avanzada y medidas de seguridad robustas es la clave para enfrentar las crecientes amenazas cibernéticas y mantener la integridad de las operaciones empresariales en este entorno digital dinámico (TicTac, 2023).

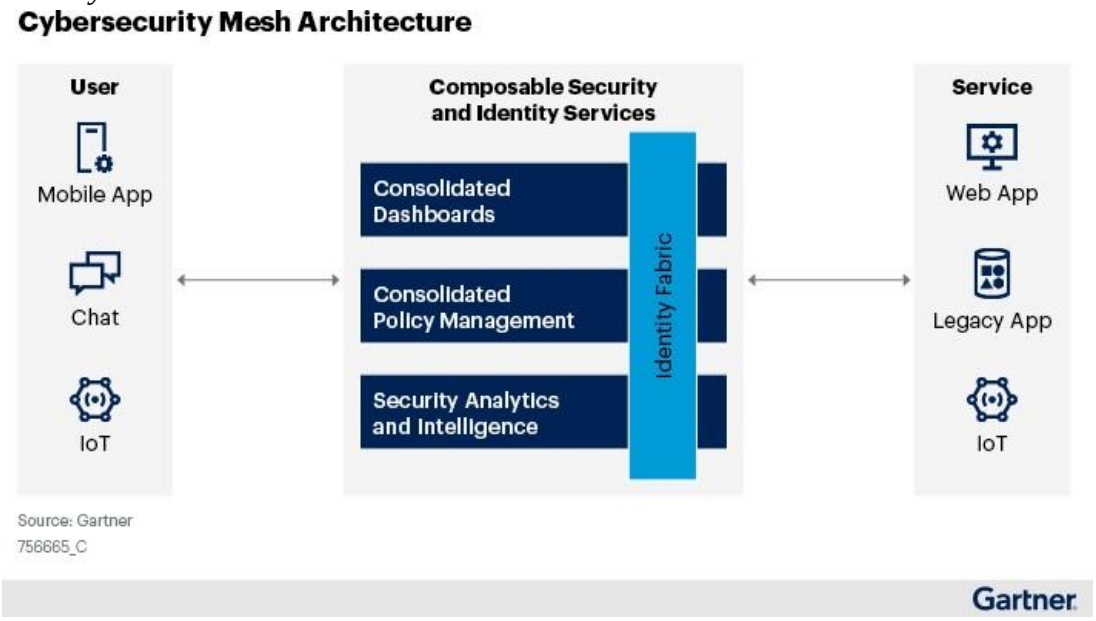
De acuerdo con Gartner la arquitectura de malla de ciberseguridad (Ciber-Security Mesh Architecture), es un ecosistema colaborativo de herramientas y controles diseñado para asegurar una empresa moderna y distribuida. Se basa en la estrategia de integrar herramientas de seguridad componibles y distribuidas al centralizar el plano de datos y control para lograr una colaboración más efectiva entre las herramientas. Los resultados incluyen capacidades mejoradas de detección, respuestas más eficientes, políticas consistentes, gestión de posturas y procedimientos, y un control de acceso más adaptable y detallado; todo ello con el fin de lograr una mayor seguridad (Gartner, s.f.a).

En la actualidad, nuestros activos digitales se hallan ampliamente dispersos en diversas ubicaciones y en múltiples entornos de nube, lo que requiere una nueva estrategia para ejercerun control distribuido. Los enfoques de seguridad convencionales se basan en productos especializados que operan de manera aislada, protegiendo los activos de manera reactiva y especializada. Esto conlleva un aumento de los costos y deja brechas significativas en la cobertura y visibilidad. Este enfoque no se ajusta a la agilidad y dispersión inherentes a la mayoría de las empresas modernas. Por tanto, la seguridad de una empresa contemporánea exige un nuevo enfoque que la conciba como un ecosistema en lugar de una colección de soluciones aisladas (González, 2023).

Ciber-Security Mesh Architecture promueve la compatibilidad, escalabilidad e integración de diferentes sistemas. Para lograr esto, se basa en un conjunto de capas fundamentales que permiten que los diversos controles de seguridad trabajen en conjunto y simplifiquen su configuración y gestión.

Imagen 1

Cybersecurity Mesh Architecture



Nota. Tomado de Gartner (s.f.b.).

Cada capa aporta un conjunto único de capacidades a la arquitectura en su conjunto:

- Analítica e inteligencia de seguridad: esta capa recopila, mapea y combina datos e información de otras herramientas de seguridad, realiza análisis de amenazas y desencadena respuestas apropiadas.

- Infraestructura de identidad: esta capa ofrece capacidades fundamentales de identidad, como la gestión del ciclo de vida, servicios de directorio, acceso adaptativo, gestión de autorización externalizada, verificación de identidad y gestión de derechos.

- Gestión consolidada de políticas, postura y procedimientos: esta capa verifica y coordina la postura de seguridad al analizar las estructuras de configuración nativa de los activos individuales y las herramientas de seguridad, y orquesta de políticas centralizadas en configuraciones de políticas nativas. También gestiona y orquesta procedimientos.

- Paneles de control consolidados: esta capa proporciona una vista compuesta del ecosistema de seguridad, lo que permite a los equipos de seguridad responder de manera más rápida y efectiva a eventos de seguridad (Stratejm, 2023).

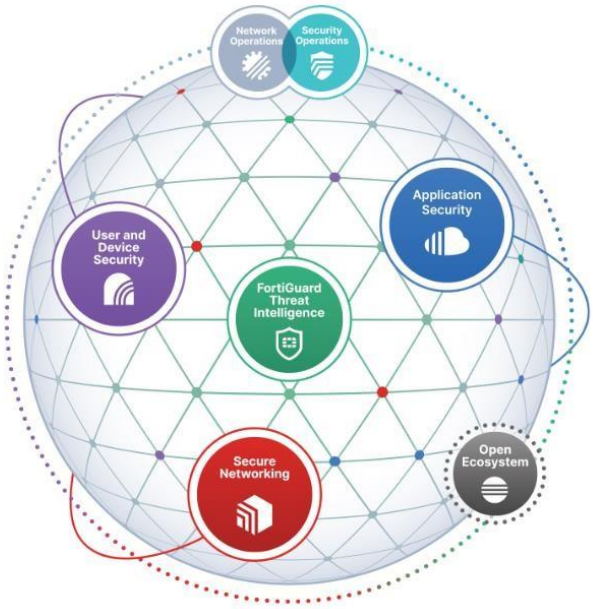
Existen numerosos proveedores de seguridad informática en el mercado, cada uno ofreciendo una amplia gama de soluciones y servicios diseñados para proteger las redes, sistemas y datos de las organizaciones contra amenazas cibernéticas. Destacando entre estas empresas se encuentra Fortinet, una empresa líder en ciberseguridad con sede en Sunnyvale, California. Fortinet es ampliamente reconocida por su solución de Cyber-Security Mesh Architecture, también conocida como "**Fortinet Security Fabric**".

Fortinet Security Fabric es una plataforma de seguridad integral que integra y coordina diferentes componentes de seguridad para proporcionar una defensa completa. Esto incluye la capacidad de compartir información en tiempo real entre dispositivos y herramientas de seguridad para una respuesta más rápida a las amenazas (Fortinet, 2021a).

Fortinet Security Fabric se basa en un sistema operativo que respalda una amplia variedad de casos de uso con más modelos de implementación que cualquier otra solución en el mercado. Estos casos incluyen entornos físicos, virtuales, en la nube y servicios integrales. Además, abarca el ecosistema y la cartera de productos más amplia de la industria, que cubre endpoints, redes y nubes. Este se basa en un conjunto de capas fundamentales que permiten que los diversos controles de seguridad trabajen en conjunto y simplifiquen su configuración y gestión (Fortinet, 2021b).

Imagen 2

Diagrama de Fortinet Security



Nota. Tomado de Fortinet (2021a).

Cada capa aporta un conjunto único de capacidades a la arquitectura Fortinet Security Fabric.

A FortiGuard | Redes Seguras | Confianza Cero | Seguridad en Nube | Gestión Centralizada | Ecosistema Abierto

Nota. Fortinet (2021a).

Cada una de estas capas ofrece soluciones y capacidades específicas para enfrentar los desafíosde seguridad. A continuación, exploraremos las soluciones de seguridad que Fortinet ofrece en el mercado, respaldadas por la colaboración y la integración promovidas por Cibersecurity Mesh Architecture.

Imagen 3

Fortinet Security Fabric Expansion

Nota. Tomado de IIJ Global (s.f.).

Una vez hablado sobre los principios fundamentales de Cyber-Security Mesh Architecture y considerando la necesidad de salvaguardar la integridad, confidencialidad y disponibilidad de la información, es crucial avanzar hacia un estándar ampliamente reconocido a nivel internacional que orienta las prácticas de seguridad en las organizaciones.

La ISO 27000, específicamente la ISO 27001, establece un conjunto de controles de seguridadde la información que las organizaciones pueden implementar para proteger sus activos de información y garantizar la confidencialidad, integridad y disponibilidad de los datos. Estos controles se agrupan en diferentes categorías y se aplican en función de los riesgos y necesidades de seguridad específicos de cada organización. A continuación, se presentan las principales categorías de controles de seguridad según la ISO 27001 (Alonso, 2023).

- **Gestión de activos:** Identificar y clasificar los activos de información, así como establecer medidas para protegerlos adecuadamente.

- **Seguridad en el personal:** Implementar prácticas de seguridad de recursos humanos, como revisiones de antecedentes y capacitación en seguridad, para garantizar la confiabilidad del personal.

- **Seguridad física y del entorno:** Proteger las instalaciones y equipos físicos donde se almacena o procesa información crítica.

- **Gestión de la continuidad del negocio:** Establecer planes y procedimientos para mantener la continuidad de las operaciones en caso de incidentes o desastres.

- **Gestión de incidentes de seguridad:** Desarrollar procedimientos para identificar, gestionar y responder a incidentes de seguridad de la información.

- **Cumplimiento legal y normativo:** Garantizar que la organización cumple con todaslas leyes y regulaciones pertinentes relacionadas con la seguridad de la información.

- **Seguridad de las comunicaciones:** Proteger las redes y sistemas de comunicación dela organización contra amenazas de seguridad.

- **Adquisición, desarrollo y mantenimiento de sistemas de información:** Garantizar que los sistemas de información se diseñen, desarrollen y mantengan de manera segura.

- **Relaciones con proveedores:** Establecer políticas y acuerdos de seguridad con proveedores y terceros que manejan información de la organización (Alonso, 2023).

Es importante destacar que, durante y después de la pandemia, se observó un notable aumentoen los ataques cibernéticos en todo el mundo. La creciente dependencia de la tecnología y la transición masiva hacia el trabajo remoto hicieron que las organizaciones y los individuos fueran más vulnerables a diversas amenazas cibernéticas. La pandemia cambió la dinámica de la ciberseguridad al exponer nuevas superficies de ataque y oportunidades para los ciberdelincuentes.

Actualmente Colombia, al igual que muchos otros países, se enfrenta a una creciente y compleja amenaza: los ataques cibernéticos. Estos ataques, que van desde el robo de datos personales hasta el sabotaje de infraestructuras críticas, han evolucionado en paralelo con el avance tecnológico y la creciente conectividad. La transformación digital ha traído consigo innumerables beneficios para la sociedad colombiana, pero también ha abierto nuevas puertaspara los ciberdelincuentes que buscan explotar vulnerabilidades en sistemas y redes.

Los sectores público y privado en Colombia han sido testigos de un aumento alarmante en la frecuencia y sofisticación de los ataques cibernéticos en los últimos años. Estos ataques no solo representan una amenaza para la seguridad nacional y la estabilidad económica, sino que también ponen en peligro la privacidad y confidencialidad de los ciudadanos y las empresas (Secnesys, 2023).

En los últimos años, el número de denuncias por ataques cibernéticos en la fiscalía general de la Nación de Colombia ha experimentado un aumento significativo, superando los 60,000 casos. Tanto el año 2022 como el transcurso del 2023 se han destacado por registrar los mayores incrementos en las cifras de ciberdelitos en el país.

En el año 2022, los sectores industriales, gubernamentales, educativos y de salud enfrentan unaola de ataques cibernéticos, representando el 67% del total de denuncias presentadas tanto por empresas del sector público como privado. Entre estos sectores, las pequeñas y medianas empresas (PYME) se encontraron en la línea de fuego, siendo las más afectadas. Esta vulnerabilidad persistente se atribuye principalmente a las estrategias de ciberseguridad deficientes implementadas en estas organizaciones.

Los estudios revelan una realidad alarmante: sólo el 7% de las PYME que experimentan un ataque cibernético logran subsistir y continuar sus operaciones. En la mayoría de los casos, estas empresas se ven obligadas a cerrar debido al impacto devastador de los ataques. Esta situación resalta la urgencia de fortalecer las medidas de ciberseguridad, especialmente entre las pequeñas y medianas empresas, para proteger la integridad de sus operaciones y asegurar su supervivencia en un entorno digital cada vez más hostil (González, 2023).

La serie ISO 27000, centrada en la seguridad de la información, ha sido ampliamente adoptadaen numerosos países alrededor del mundo, incluyendo Colombia. Cada nación tiene la flexibilidad de ajustar estas normas internacionales a sus necesidades y regulaciones locales, aunque el marco general de aplicación se mantiene constante.

En Estados Unidos y Canadá, las organizaciones emplean la serie ISO 27000 para fortalecer la seguridad de la información y cumplir con regulaciones nacionales y sectoriales. En el caso de Estados Unidos, el Instituto Nacional de Estándares y Tecnología (NIST) proporciona pautas adicionales que están alineadas con estas normas internacionales. En Canadá, estas normas son fundamentales para garantizar la seguridad de la información y cumplir con la Ley deProtección de la Información Personal y Documentos Electrónicos (PIPEDA), particularmenteen los sectores financiero y de atención médica.

En el Reino Unido, la norma ISO 27001 juega un papel crucial en la ciberseguridad y la protección de datos en diversos sectores. Ha sido incorporada en regulaciones y directrices gubernamentales, especialmente en lo que concierne a la seguridad de la información.

Dentro de la Unión Europea, la serie ISO 27000 es de importancia primordial para garantizar la protección de datos y la ciberseguridad. Está estrechamente relacionada con el Reglamento General de Protección de Datos (GDPR) de la UE y es aplicada en todos los Estados miembros, con el propósito de mantener la seguridad y la integridad de la información en un entorno cada vez más digital y conectado (ISO27000, s.f.)

En Colombia, El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) es la entidad encargada de la promoción, adopción y certificación de normas técnicas en Colombia. ICONTEC colabora estrechamente con organizaciones en Colombia para facilitar la implementación y certificación de diversas normas, incluyendo la serie ISO 27000, que se centra en la seguridad de la información.

ICONTEC desempeña un papel fundamental en la promoción y regulación de estándares de seguridad de la información en el país. A través de sus servicios de capacitación y certificación, ayuda a las organizaciones colombianas a cumplir con las normativas nacionales e

internacionales, fortaleciendo así la protección de información sensible y promoviendo la seguridad de la información (Business Intelligent, s.f.).

En 2022, se publicó una actualización significativa de la norma ISO 27000, la cual reemplazó la versión del año 2013. Esta norma proporciona una guía esencial de buenas prácticas para la implementación de controles relacionados con la gestión de riesgos de seguridad de la información.

Entre los cambios más destacados en la actualización de la norma ISO se incluyen:

Un cambio en su título, que refleja un alcance más amplio: "Seguridad de la información, ciberseguridad y protección de la privacidad - controles de seguridad de la información".

Una estructura revisada que incorpora un total de 93 controles, organizados en 4 dominios principales: Organizacional (37 controles), Personas (8 controles), Físico (14 controles) y Tecnológico (34 controles).

Estos cambios en la norma ISO 27000 reflejan la evolución de las mejores prácticas en seguridad de la información, ciberseguridad y protección de la privacidad, y proporcionan una guía más completa y actualizada para las organizaciones que buscan garantizar la seguridad de su información en un entorno digital en constante cambio (Grajales, 2022).

En relación con el proceso de transición a la nueva versión ISO 27001, se establecen las siguientes etapas:

- La norma ha sido publicada el 25 de octubre de 2022.

- Todas las entidades de certificación deben atravesar un proceso de acreditación conforme a la nueva versión del estándar. Por lo tanto, no será posible certificar nuestro Sistema de Gestión de Seguridad de la Información (SGSI) bajo ISO 27001:2022 hasta que estas entidades estén debidamente preparadas. Se estima que las empresas certificadoras estuvieran listas durante el primer semestre de 2023.

- Las organizaciones tendrán la oportunidad de obtener una certificación inicial o renovar su certificado bajo la norma ISO 27001:2013 hasta el 25 de abril de 2024.

- Todos los certificados emitidos conforme a la norma ISO 27001:2013 mantendrán su validez hasta el 25 de octubre de 2025, lo que representa un período de tres años a partir de la publicación de la nueva versión.

Las auditorías de transición se centrarán en los siguientes aspectos clave:

- Realizar un análisis de las brechas de seguridad en relación con ISO/IEC 27001:2022, y determinar si es necesario realizar cambios en el Sistema de Gestión de Seguridad de la Información (SGSI) del cliente.

- Verificar y actualizar la Declaración de Aplicabilidad (SOA).

- Analizar y actualizar el plan de tratamiento de riesgos.

- Evaluar la implementación y efectividad de los nuevos controles y las modificaciones introducidas por la organización.

Estas etapas y enfoques son esenciales para garantizar una transición exitosa a la nueva versiónde la norma ISO 27001 y asegurar que los sistemas de gestión de seguridad de la información cumplan con los requisitos actualizados (Ingertec, 2022).

3. METODOLOGÍA O DESCRIPCIÓN DEL PROCESO

En esta sección, se proporcionará un análisis detallado de la metodología que ha dado forma al presente artículo. Se abordará el proceso consultivo, cubriendo tanto la teoría como las prácticas de implementación, junto con las consideraciones técnicas esenciales para aplicar esteconcepto de seguridad en las empresas. Esta metodología ofrece un enfoque estructurado para afrontar desafíos y lograr resultados que impacten de manera positiva en la ciberseguridad de las empresas en Colombia.

En la búsqueda por mejorar la ciberseguridad en empresas colombianas, se decidió abordar una serie de temas claves. Se comenzó inicialmente con la norma ISO 27000, explorando sus estándares y directrices que proporcionan una base sólida para la seguridad de la información. Estaba claro que comprender estos estándares era fundamental para avanzar en el objetivo.

Sin embargo, antes de aplicar estos estándares, se necesitaba conocer la realidad de las amenazas cibernéticas en Colombia. Por lo que se exploraron los datos relevantes sobre ciberataques en el país. Los resultados destacaron un aumento en la sofisticación de estos ataques, subrayando la necesidad de medidas más avanzadas para proteger la información crítica.

El siguiente paso fue explorar la teoría de la Arquitectura de Malla de Ciberseguridad. Esta arquitectura ofrecía una solución dinámica y descentralizada para enfrentar las amenazas en constante evolución. Sin embargo, aún se debía elegir al proveedor adecuado de CyberSecurity Mesh Architecture.

Se realizó una minuciosa comparación entre varios proveedores y después de un análisis, se seleccionó a Fortinet como el mejor candidato. La robustez de su Security Fabric y su historialen ciberseguridad me convencieron de que era la elección adecuada.

Finalmente, se realizó la comparación de diferentes implementaciones de Security Fabric en diversos entornos empresariales. Esto permitió adaptar las soluciones de Fortinet a las necesidades específicas de las empresas en Colombia, brindando una defensa sólida contra las crecientes amenazas cibernéticas.

Con un conocimiento profundo de la norma ISO 27000, una comprensión más profunda de las amenazas locales, la teoría de la Arquitectura de Malla de Ciberseguridad y una elección sólida

de proveedor, se pudo liderar la transformación de la ciberseguridad en las empresas colombianas, contribuyendo a un entorno digital más seguro y resistente.

4. ANÁLISIS DE RESULTADOS O HALLAZGOS

De acuerdo con los datos encontrados, estos revelan un paisaje intrigante en el ámbito de la seguridad de la información, específicamente en torno a la norma ISO 27000. A través de investigaciones recientes y estadísticas actuales, se ha logrado obtener una visión minuciosa sobre la implementación y el impacto de esta norma en Colombia.

Se encontró, por ejemplo, que un número significativo de organizaciones en el país ha adoptadola ISO 27000 como marco de referencia para fortalecer sus sistemas de gestión de la seguridadde la información. Este fenómeno refleja no solo una creciente conciencia sobre la importancia de la ciberseguridad, sino también un compromiso tangible con la mejora continua en la protección de datos sensibles.

Asimismo, destaca el hecho de que la última actualización de la norma ha generado un impacto palpable en la forma en que las empresas colombianas abordan las amenazas cibernéticas. La adaptación a los cambios introducidos en la normativa revela la capacidad de las organizaciones para evolucionar con el panorama de la seguridad de la información.

No obstante, es crucial señalar que, a pesar de estos avances notables, no todas las empresas colombianas han abordado de manera uniforme la implementación de la norma ISO 27000. Algunas aún no han adoptado plenamente este marco, lo que subraya la diversidad de enfoques y desafíos que persisten en el ámbito de la seguridad de la información en el país.

Durante el proceso de investigación, se encontraron casos que ilustran la creciente relevancia de enfoques innovadores de 'Cyber-security Mesh Architecture' en empresas colombianas. Un claro ejemplo fue una organización que, al enfrentarse a la expansión de su infraestructura a través de múltiples ubicaciones geográficas, optó por implementar un esquema de protección con Fortinet Security Fabric. Esta decisión permitió una interconexión más efectiva de sus sistemas, adaptándose así a un entorno cada vez más distribuido.

Otro caso notable fue el de una empresa que experimentó un aumento significativo en los ataques cibernéticos sofisticados. Al adoptar la 'Security Fabric', lograron establecer una red cohesiva y adaptable que mejoró su capacidad para detectar y mitigar amenazas de manera más eficiente.

Estos casos concretos subrayan la aplicabilidad práctica de estas innovaciones en situaciones específicas. En un contexto colombiano donde la tecnología avanza rápidamente y las amenazas cibernéticas se vuelven más complejas, la adopción de estos enfoques no solo se convierte en una estrategia viable, sino en un componente crucial para diseñar estrategias de seguridad informática efectivas y personalizadas.

5. CONCLUSIONES

Teniendo en cuenta la adopción de la norma ISO 27000 en Colombia, es evidente que esta serie de estándares ha desempeñado un papel esencial en la mejora de la seguridad de la información en el país. Al considerar su aplicación, se destaca su contribución a la creación de sistemas de gestión de la seguridad de la información robustos y uniformes en diversas organizaciones colombianas. Esto es especialmente relevante en un entornodigital en constante cambio.

La norma ISO 27001, en particular, ha sido ampliamente empleada en Colombia, lo que ha permitido garantizar la integridad, confidencialidad y disponibilidad de la información en una variedad de sectores. Al evaluar su impacto, es claro que la norma ha elevado los estándares de seguridad de la información en el país, fortaleciendo la resiliencia cibernética y protegiendo los activos de información crítica.

Considerando la creciente importancia de la ciberseguridad en un mundo digital en constante evolución, la Arquitectura de Malla de Ciberseguridad (Ciber-Security Mesh) se presenta como una innovación clave para proteger los activos de información de manera más dinámica y descentralizada. Al mismo tiempo, la norma ISO 27000, en su serie de estándares y directrices, proporciona un sólido marco para la gestión de la seguridad de la información.

El Fortinet Security Fabric es una plataforma integral de ciberseguridad que aborda una amplia gama de desafíos en materia de seguridad. A lo largo de sus diversas capas, ofrece soluciones y capacidades específicas para proteger los activos de una organización en todas las áreas críticas, desde los dispositivos finales hasta las redes y la nube. La fortaleza del Security Fabric radica en su capacidad para centralizar y coordinar la gestión de la seguridad, lo que permite una respuesta más eficaz a las amenazas y una mayor visibilidad de la postura de seguridad de la organización en su conjunto. Además, su enfoque en la integración y colaboración entre diferentes componentes de seguridad lo hace adecuado para entornos cibernéticos en constante evolución, en línea con los principios de la Cibersecurity Mesh Architecture. En resumen, el Fortinet Security Fabric, respaldado por la arquitectura de Cibersecurity Mesh, es una herramienta poderosa para fortalecer la seguridad de una organización en el panorama de amenazasactual.

La combinación de estas dos fuerzas ofrece a las organizaciones una poderosa estrategia para enfrentar las crecientes amenazas cibernéticas. La Arquitectura de Malla de Ciberseguridad se adapta a un entorno digital en constante cambio, permitiendo un enfoque más eficiente en la protección de datos y sistemas. La ISO 27000, por su parte, establece las bases para una gestión integral de la seguridad de la información, lo que garantiza que las organizaciones cumplan con los estándares y mejores prácticas en seguridad.

6. REFERENCIAS

Alonso, C. (27 de febrero de 2023). *ISO 27000 y el conjunto de estándares de Seguridad de la Información*. https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/

Apen soluciones informátiques. (s.f.). ¿Qué es un firewall? https://apen.es/glosario-de-%20informatica/firewall/#:~:text=Historia%20firewall,unas%20redes%20separadas%20

de%20otras

Avenía, C. (2017). *Fundamentos de seguridad informática*. Fondo editorial Areandino.

Business Intelligent. (s.f.). ISO 27000. http://www.business-intelligent.com/iso27000.pdf

ESGinnova Group. (21 de mayo de 2015). ISO 27001: ¿Qué significa la Seguridad de la Información? https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/#:~:text=La%20Seguridad%20de%20la%20Informaci%C3%B3n%2C%20seg%C3%BAn%20ISO27001%2C%20se%20refiere%20a,Audio%20y%20v%C3%ADdeo%2C%20etc

Fernández, S. (s.f.). Ciberseguridad en la Era de la Inteligencia Artificial: La Revolución de la Defensa Digital. Age2 Expertos en ti. https://www.age2.es/noticias/ciberseguridad-inteligencia-artificial/

Fernández, Y. (17 de octubre de 2019). *Firewall: qué es un cortafuego, para qué sirve y cómo funciona*. Xataka Basics. https://www.xataka.com/basics/firewall-que-cortafuegos-sirve-como-funciona

Fortinet. (13 de marzo de 2021a). Fortinet Fabric-Ready Program Fortinet Security Fabric Interoperability Program for Technology Alliance Partners. https://www.fortinet.com/content/dam/fortinet/assets/brochures/Fortinet-Fabric-Partner-Program.pdf

Fortinet. (1 de abril de 2021b). Fortinet's Security Operating System. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf

Gartner. (s.f.a). Cybersecurity Mesh. https://www.gartner.com/en/information-technology/glossary/cybersecurity-mesh

Gartner. (s.f.b.). Cybersecurity Mesh Architecture. https://www.gartner.com/resources/738000/738083/Figure_1_Cybersecurity_Mesh_Layers.png?%20reprintKey=1-2BMK6Q70

González, D. (2023). *Ciberataques en Colombia siguen en aumento en el 2023*. Intexus. https://blog.intexus.la/ciberataques-en-colombia-en-el-2023

Grajales, L. (1 de marzo de 2022). *Todo lo que debes saber sobre la nueva versión de la ISO 27002:2022*. B.SECURE. https://www.b-secure.co/blog/todo-lo-que-debes-saber-sobre-la-nueva-version-de-la-iso-270022022

IIJ Global. (s.f.). Integrated Fortinet Solutions. https://ap.iij.com/integrated-fortinet-solutions/

Ingertec. (2022). Nueva Versión ISO 27001:2022. https://ingertec.com/nueva-version-iso-27001-

2022/

ISO27000. (s.f.). *Certificación*. https://www.iso27000.es/certificacion.html#section5b

Peláez, B. (27 de octubre de 2023). *DoS y DDoS: Impacto y consecuencias*. Listopro Community. https://community.listopro.com/dos-y-ddos-impacto-y-consecuencias/

Secnesys. (18 de octubre de 2023). Ciberseguridad en el Trabajo Remoto. https://es.linkedin.com/pulse/ciberseguridad-en-el-trabajo-remoto-secnesys-kewwe?trk=public_post_feed-article-content

Stratejm. (2 de agosto de 2023). Cybersecurity Mesh Architecture (CSMA) – A Quick Guide. https://stratejm.com/cybersecurity-mesh-quick-guide/

TicTac. (2023). IA para la protección y prevención de amenazas. Informe anual de ciberseguridad. https://www.ccit.org.co/wp-content/uploads/estudio-anual-de-ciberseguridad.pdf