UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS “ESPOG”

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: ***RPC-SO-02-No.053-2021***

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
PROPUESTA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD EN REDES INALÁMBRICAS DE ÁREA LOCAL.
Línea de Investigación:
SEGURIDAD INFORMÁTICA
Campo amplio de conocimiento:
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Autor:
Sarango Narváez Diego Fernando
Tutor:
Recalde V Pablo M

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, Pablo M Recalde V con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: PROPUESTA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD EN REDES INALÁMBRICAS DE ÁREA.

Elaborado por: Diego Fernando Sarango Narváez, de C.I:1718014986, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2023

Firmado electrónicamente por:
PABLO MARCEL
RECALDE VARELA

_____

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Diego Fernando Sarango Narváez con C.I: 171801496, autor del proyecto de titulación denominado: PROPUESTA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD EN REDES INALÁMBRICAS DE ÁREA. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2023

_____

Firma

orcid: 0000-0003-2751-0695

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

La necesidad diaria de acceder a los servicios informáticos por medio de las redes de comunicación como uno de los principales medios para optimizar los tiempos de producción tanto de bienes como servicios se ha vuelto sin duda una de las más grandes preocupaciones de la mayoría de las organizaciones altamente competitivas.

Acorde a Molina (2017) las redes inalámbricas representan un medio para desarrollar nuevos negocios internos o externos, hacer que la producción sea más efectiva y sencilla a todos los miembros de la organización, lo cual significa es incremento sustancial en el valor de las acciones de los accionistas.

Sin embargo, las redes inalámbricas van ahora de la mano con todas las vulnerabilidades que las aqueja; según estudios que se han realizado las redes inalámbricas serán siempre uno de los principales obstáculos que las empresas enfrentan a diario y una de las principales causas será el control de tráfico de estas.

Desde 1999, se han publicado documentos en Internet que enumeran las mejores prácticas para implementar LAN inalámbricas, considerando que estas prácticas exceden ampliamente las habilidades del usuario común, es poco lo que se puede hacer para reducir las intrusiones en la red de este tipo. (Pstyga, 2022)

Esta revisión bibliográfica examina diversas formas y mecanismos de implementación de seguridad en redes inalámbricas de área local y brinda a los interesados en el tema las mejores prácticas metodológicas de implementación de seguridad de estas redes, independientemente de la medida en que dependan principalmente de los criterios del National Institute of Standards and Technology (NIST).

El trabajo presente de investigación abarca el Objetivo de Desarrollo Sostenible (ODS) número nueve, el propósito es aumentar significativamente la accesibilidad de

las tecnologías de la información y la comunicación y trabajar para garantizar un acceso a Internet asequible y universal en los países menos desarrollados para el año 2020. (ODS, 2017)

Problema de investigación

Hoy en día, garantizar la seguridad de la información en las empresas es crucial debido a las necesidades apremiantes que existen en este ámbito. De igual forma se convirtió en una necesidad primaria para generar mayores ingresos por producción y atención cuando de brindar nuestros productos o servicios se trata. (Pstyga, 2022)

Esta es la razón por la cual actualmente se ha comenzado a otorgar una importancia significativa a los servicios de seguridad de Tecnologías de la Información. Con la llegada de la pandemia «SARS COV 2» esto se volvió prioritario y obligó a implementar de forma prematura soluciones que tal vez en su momento no estuvieron preparadas para soportar la cantidad de transaccionalidad que se generó por el hecho de realizar home office y de igual manera el estudio en línea de los estudiantes.

La sociedad fue víctima de un problema que, si bien en algunas organizaciones estuvieron preparadas para este contingente, nunca se imaginó que iba a suceder de tal magnitud como pasó. (Ubierna, 2020)

¿Si se aplican las recomendaciones, sean estas referentes al marco NIST SP 800-30 o la norma ISO 27033, se puede mejorar la seguridad en las redes de área local inalámbrica?

Objetivo general

Realizar una comparativa entre el marco NIST SP 800-30 y norma ISO 27033 para la posterior implementación de seguridad en las redes inalámbricas en «Fermagri S. A».

Objetivos específicos

- Analizar varias propuestas de seguridad en redes Wireless dadas por diferentes organizaciones mundiales.
- Proponer una solución para mejorar una situación específica utilizando métodos ya existentes y comparar los resultados de dicha solución con una situación real. Esto puede implicar el uso de técnicas y herramientas existentes para optimizar procesos y mejorar la eficiencia en un área determinada.
- Encontrar las soluciones más efectivas para cubrir las demandas particulares de las empresas agropecuarias como lo es «Fermagri S. A». Esto podría significar la reorganización de los procedimientos y la adopción de tecnologías vanguardistas con el fin de mejorar la eficacia y el rendimiento.
- Sugerir la aplicación de las prácticas más efectivas que ya han sido definidas previamente. Esto puede implicar la implementación de técnicas y procesos que han sido probados y han demostrado ser exitosos en situaciones similares.

Vinculación con la sociedad y beneficiarios directos:

El fortalecimiento de conceptos sobre la seguridad informática dará un valor agregado a los altos directivos de cada institución para la mejor toma de decisiones, así mismo para que los que todavía se encuentran temerosos de realizar una inversión significativa se den cuenta de que el activo más valioso que se debe proteger en toda institución es su información.

Este trabajo de investigación coopera con el Objetivo de Desarrollo Sostenible número nueve “Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación”. (ODS, 2017)

Entre los objetivos del ODS nueve están el acceso equitativo al conocimiento y la experiencia, especialmente Internet. Con el fin de alcanzar este objetivo, las compañías pueden colaborar mediante la incorporación de la innovación en su cultura empresarial, y la transformación de productos, instalaciones, servicios, procesos productivos y gestión interna con enfoques de sostenibilidad

Al completar la investigación, se podrán ofrecer sugerencias para adoptar las mejores prácticas y controles mediante la comparación de las normas internacionales NIST e ISO 27001. La implementación de estas prácticas y controles agregará un valor significativo y aumentará el prestigio de las empresas que los apliquen.

El presente estudio brindará el mayor apoyo y dará seguridad a los datos que hoy en día es parte crítica en cualquier entidad que maneje información confidencial.

Fermagri S. A. es una empresa del sector agropecuario con sede en cinco provincias del Ecuador que su crecimiento fue acelerado en lo que lleva sus años de operación, es por este motivo que las redes se las ha realizado de manera empírica sin tener aterrizados los conceptos de seguridad en las redes inalámbricas.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

En este capítulo se encuentran las descripciones del proyecto.

1.1. Contextualización general del estado del arte

Según Shaw (2023), Wi-Fi hace referencia a las tecnologías de redes de área local inalámbrica que se basan en el estándar IEEE 802.11, y que permiten la comunicación entre dispositivos sin necesidad de cables.

Estas tecnologías emplean señales de radio para transferir información desde el dispositivo cliente hasta el punto de acceso, como el enrutador. Una vez establecida la conexión, el enrutador permite la comunicación entre otros dispositivos en la red de área local (LAN), la red de área amplia (WAN) o la red global de Internet.

A medida que las redes inalámbricas se vuelven cada vez más populares, también aumentó el número de personas malintencionadas que buscan aprovecharse de ellas. Muchas de estas redes carecían de medidas de seguridad, lo que se convirtió en un problema para las empresas, ya que los empleados que se conectaban desde lugares públicos podían estar exponiendo información confidencial a cualquier persona con un receptor Wi-Fi. Para abordar esta preocupación, la Alianza Wi-Fi ha desarrollado varios protocolos de seguridad, incluyendo el último estándar, WPA3. Como resultado, los usuarios que se conectan a puntos de acceso seguros utilizando WPA y una conexión VPN bien configurada, están en gran medida protegidos contra los problemas de seguridad asociados con las redes abiertas.

De acuerdo con Reinoso (2017). Con el tiempo, se han desarrollado y perfeccionado estándares globales como son la International Organization for Standardization (ISO) y la Instituto Nacional de Normas y Tecnología (NIST) para garantizar la calidad de las redes y dispositivos e incluso su correcto funcionamiento, así mismo la protección de datos.

Con el paso del tiempo, la seguridad de la información ha ganado popularidad y ha dejado de ser considerada como un gasto para transformarse en una inversión crucial para los altos ejecutivos. Mientras que algunos países han implementado medidas de seguridad con rapidez, otros lugares han tenido un impacto menor en este ámbito.

De acuerdo con Ríos et al., (2017) la transformación de los sistemas de información a lo largo del tiempo ha generado la necesidad de contar con profesionales especializados en informática, cuya función sea evaluar el correcto funcionamiento de los sistemas, identificar posibles vulnerabilidades y aplicar medidas preventivas y correctivas para evitar la pérdida de información, la cual podría generar costos significativos para las organizaciones. Actualmente, las empresas enfrentan no sólo riesgos físicos, como robos o asaltos en sus instalaciones, sino también delitos de seguridad informática que pueden afectar la información crítica de la organización.

1.2. Proceso investigativo metodológico

A continuación, se explica el proceso de investigación a partir de los siguientes elementos.

Enfoque de la investigación

Según Fisterra (2002) se utilizará el enfoque de metodología cualitativo el cual su principal propósito es determinar la naturaleza y objetivación de los resultados y explicar por qué suceden las cosas.

Tipo de investigación

La investigación realizada es de tipo documental y comparativa, según Equipo editorial Etecé (2022) se puede explicar como una compilación de documentos de diferentes fuentes con un tema en particular. Se utilizó la investigación documental para analizar e interpretar distintas metodologías que se pueden implantar en la seguridad de las redes inalámbricas de área local.

Con la investigación comparativa se analizó y comparó las características de las normas NIST SP 800.30 e ISO 27033 para luego determinar cuál sería la que mejor se adapte a una futura implantación.

Población y muestra

El departamento de TI de la empresa Fermagri se ha seleccionado como la población de este trabajo, con el objetivo de cubrir temas relacionados con la administración, soporte y seguridad.

Figura 1.
Fórmula Muestral

$$n = \frac{N \cdot Z^2 \cdot p \cdot (1-p)}{(N-1) \cdot e^2 + Z^2 \cdot p \cdot (1-p)}$$

La población de TI son 4, aplicando la fórmula, se debe tomar a toda la población como muestra.

Para la muestra cualitativa se consultó con personas externas del área de TI que han trabajado en proyectos similares en distintas áreas. Se emplea como herramienta a las encuestas de Google forms. (Ver anexo 2)

Métodos

Método inductivo

Es una estrategia de razonamiento la cual se encarga de partir desde premisas particulares para la generación de conclusiones generales. Pérez (2008)

Aplicando este método se define si la aplicación del marco NIST SP 800-30 o la norma ISO 27033 es la más recomendable para su posterior implementación.

Método deductivo

Estrategia de razonamiento que se utiliza para inferir conclusiones lógicas a partir de premisas verdaderas. (Pérez, 2008)

Se empleó el método deductivo para el respectivo análisis del marco de seguridad NIST 800-30 y la norma ISO 27033 en el presente artículo de investigación.

1.3. Análisis de resultados

El trabajo realizado de análisis y recepción de la información en la empresa Fermagri, demostró que hay trabajo para realizar una futura implementación de procedimientos adecuados para que permitan mitigar las vulnerabilidades a las que la organización se encuentra expuesta. (Ver anexo 2)

El análisis del marco de seguridad NIST y la norma ISO 27033 que se analizaron dan como resultado que cualquiera de los dos se puede implementar, sin embargo, va a depender mucho de la inversión que se pueda realizar.

Todas las recomendaciones tanto técnicas como administrativas que se pudieron ver tanto de NIST como de ISO se pueden implementar en conjunto con el departamento de TI de la empresa Fermagri S.A., serán unas más fáciles de interpretar que otras.

Es recomendable que los puertos de la red LAN que no se encuentren en uso estén inactivos hasta que se los necesite, ya que también puede existir gente con un poco de experiencia que puede intentar hacer daño o simplemente ingresar a la red para demostrar que existen brechas que deben ser subsanadas.

CAPÍTULO II: PROPUESTA

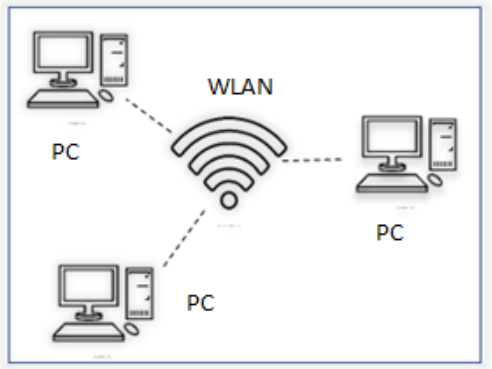
Se desarrollará la propuesta del tema de investigación que se planteó como: Propuesta metodológica para la implementación de seguridad en redes inalámbricas de área local.

2.1. Fundamentos teóricos aplicados

Teoría de redes inalámbricas

Es aquella que permite la intercomunicación entre dispositivos de una misma red sin la necesidad de cables que la conecten. (Castillo, 2020)

Figura 2.
Red Wlan



Nota. Desarrollo de autoría propia

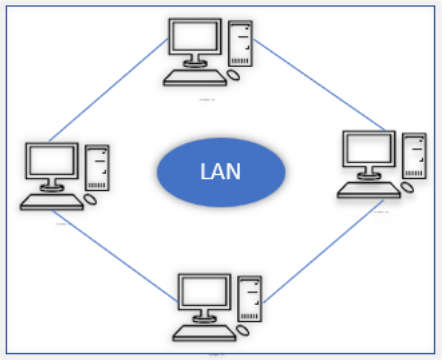
Red de área local

Red de computadoras que permiten el intercambio de información entre varios dispositivos de una misma red a nivel local, estas pueden ser de hogar o de empresas privadas. (Barbancho et al., 2020)

Según Barbancho et al., (2020), la clasificación por los criterios y tipos de redes se basa en:

- Tamaño de la red (área de distribución).
- Manera de transmitir la información (tecnología de la información).
- Propietario de la red (titularidad de la red)

Figura 3.
Red LAN



Nota. Desarrollo de autoría propia

Redes privadas

Mencionan propiedad de empresas u organismos y solo los miembros tienen la autorización de acceder a su contenido. Se puede decir que toda red LAN se considera red privada. En la actualidad se puede mencionar que existen muchas características para elaborar una red LAN, sea esta por su categoría, o certificación de puntos de red. La calidad de los materiales con los que se desarrolla el cableado estructurado que forma parte de la red LAN interfiere mucho en su rendimiento y velocidad, en la mayoría de las organizaciones se usa la categoría 6 por los costos que esta representa.

Modelo OSI (*Open Systems Interconnection*)

El modelo de referencia OSI es la base principal para los protocolos de red, su principal función se basa en conseguir la interconexión de diferentes sistemas de distinta procedencia, en resumen, es un estándar de protocolos para interconexión. (Martinez, 2018)

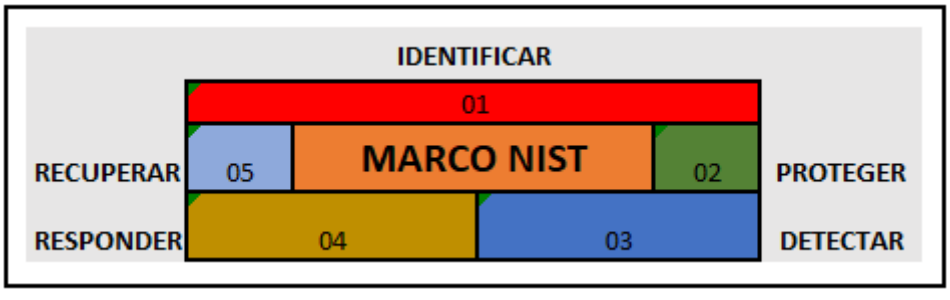
Figura 4.
Modelo OSI

Nota. Desarrollo de autoría propia

NIST

Este término se refiere a la sigla de la organización conocida como Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology), hablar del marco NIST sería muy extenso ya que abarca muchos conceptos, el marco de Ciberseguridad NIST proporciona una mejor comprensión de los riesgos a los que estamos expuestos y cómo manejarlos, así mismo, nos facilita el conocimiento para administrar, reducir y finalmente proteger tanto las redes como los datos que por ella viajan constantemente. Brinda a la organización algunas de las mejores prácticas, así mismo como realizar una inversión segura en la materia de seguridad. (*Marco de ciberseguridad del NIST*, 2019)

Figura 5.
Marco NIST



Nota. Desarrollo de autoría propia

Normas ISO

“Las normas ISO son estándares de seguridad que tienen reconocimiento a nivel internacional y fueron diseñadas para brindar asistencia a las organizaciones en la implantación de un nivel de coherencia en la prestación de servicios y en el desarrollo de productos en la industria.” (Alonso, 2020)

Figura 6.
Organización Internacional de Normalización

Fuente: Alonso (2020), Se respeta derechos de Autor

IEEE

Según las Normas IEEE (2020) se trata de una de las organizaciones más importantes del mundo en el ámbito de la ciencia y la ingeniería, cuyas siglas en inglés corresponden a Institute of Electrical and Electronic Engineers, las subfamilias de las normas 802.x son:

IEEE 802.11

De acuerdo con Martines (2018) el estándar IEEE 802.11 es un modelo utilizado para la funcionalidad de las redes de área local inalámbricas (WLAN) en dispositivos como computadoras, tablets, smartphones y otros dispositivos con capacidad para Wi-Fi.

Key Risk Indicators (KRI)

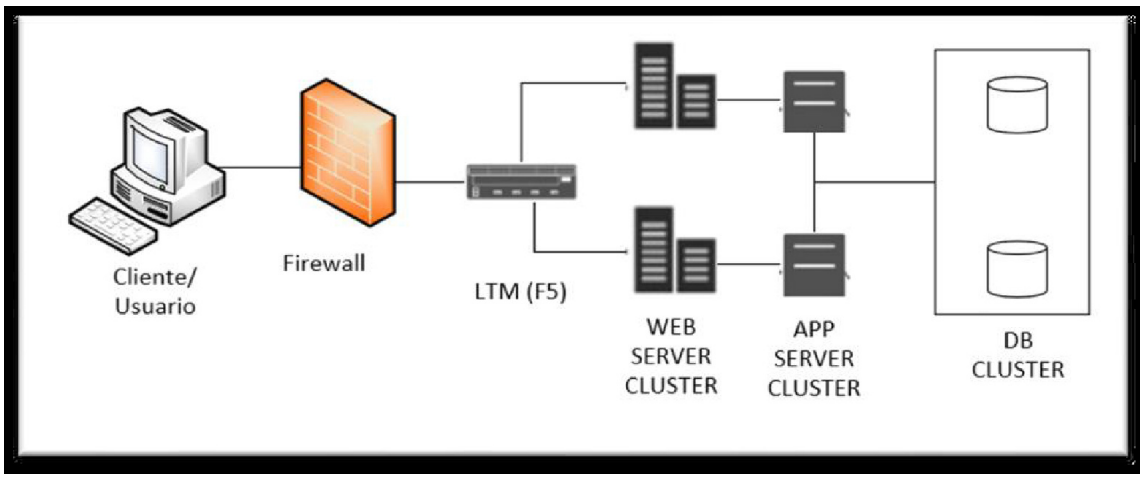
Son métricas que son utilizadas para la determinación del potencial de un riesgo eventual y tomar medidas oportunas. (Calle, 2022)

Considerando las condiciones que ISO-27001 da acerca de las redes y extrapolando el tema a las redes inalámbricas con las sugerencias de NIST, se ha propuesto la implementación de la metodología de aseguramiento en redes Wireless. El correcto análisis de las vulnerabilidades en la red LAN y la aplicación de marcos de seguridad ayudará a tener una mejora y mitigar los riesgos a los que nos encontramos expuestos día a día con el uso de la tecnología.

Firewall

Un firewall es un elemento de seguridad que busca evitar el acceso no autorizado a una red privada conectada a Internet. Su función principal consiste en analizar todos los mensajes que ingresan y salen de la red para bloquear aquellos que no cumplan con los parámetros de seguridad establecidos, al mismo tiempo que permite el control libre de las comunicaciones" (Moes, 2018).

Figura 7.
Firewall



Nota: Moes (2018), se respeta los derechos de autor.

2.2. Descripción de la propuesta

En el análisis respectivo, para la seguridad de las redes inalámbricas, se realiza la comparativa de las ventajas y desventajas entre las normas ISO 27033 y el marco de seguridad NIST de ciberseguridad, llegando a concluir que, para el caso de estudio,

puede ser implementado el marco de seguridad NIST, ya que se apega a las recomendaciones técnicas y administrativas para los tipos de empresa del sector Pymes.

En la tabla 1 podemos observar las características, ventajas y desventajas del marco de seguridad NIST SP 800 30 de seguridad

Tabla 1.
Marco NIST SP 800 30 de seguridad

NIST CFS		
Características	**Ventajas**	**Desventajas**
Implementación de sistema de gobierno y madurez	Funciona para empresas pequeñas y no reguladas.	Tiene la menor cobertura de los principales marcos de ciberseguridad.
Identificar: cuales son los activos que se quiere proteger o no, si es un activo crítico.	No tiene certificación, solo es aplicable.	
Proteger: qué controles se quieren poner en marcha.	Da mucha madurez a los procesos de seguridad.	
Detectar: Mecanismo para estar constantemente controlando y monitorizando.	Orientados al riesgo	
Responder: Si se encuentra alguna novedad tener la potestad de responder.	Monitoreo por parte de KRI	
Recuperar: regresar al principio, respaldo o imagen.	No tiene costo de implementación	

Nota: Desarrollo de autoría propia

Esta investigación aplicando el marco de referencia NIST, habla de cómo se aplica la misma y la información técnica que se debe considerar.

Según (Guías NIST: un sustento metodológico para los analistas de ciberseguridad, 2022) el marco NIST SP800-30 se considera una base metodológica para el diseño e implementación de servicios avanzados de pentesting o pruebas de intrusión, que brindan un diagnóstico completo de la red y otros aspectos relacionados.

En la tabla 2 se observa las técnicas pasivas que se emplean para la implementación de NIST.

Tabla 2.
Técnicas pasivas NIST

Técnicas del marco de seguridad NIST	
Revisión de la documentación	Evaluación de políticas y procedimientos de documentos existentes.
Revisión de registros	Evaluación de controles implementados, registro de forma detallada y adecuada según políticas.
Revisión del conjunto de reglas	Análisis de reglas de control en dispositivos de red respectivamente.
Revisión de configuración de sistemas	Evaluación de hardening de acuerdo con políticas que se han establecido previamente.
Escaneo de la red	Revisión de tráfico de la red LAN y verificación de cifrado de comunicaciones.
Comprobación de la integridad de los archivos	Detección de posibles manipulaciones en nuestra data e identificación de archivos maliciosos que se pudieran convertir en herramientas para los atacantes.

Nota. Desarrollo de autoría propia

En la tabla 3 se observan algunas ventajas y desventajas de la Norma ISO 27033.

Tabla 3.
Norma ISO 27033

ISO 27033		
Características	**Ventajas**	**Desventajas**
Se emplea para todo tipo de organización de acuerdo con las necesidades de esta.	Marco de seguridad reconocido internacionalmente.	El costo de implementación inicial es elevado.
Garantizar la seguridad de la información.	Existe certificación de la norma.	Cierto grado de complejidad
Acoger un principio global relacionado con la seguridad de la información.	Orientados al riesgo.	Puede parecer complejo interpretar la norma.
Gestionar acuerdos de confidencialidad.	Monitoreo por parte de KRI.	Delegación de responsabilidades.
Proponer políticas y procedimientos que nos permitan asegurar el intercambio de información.	Tiene costo de implementación.	
	Aumenta la confianza y el compromiso.	

Nota: Desarrollo de autoría propia

En la tabla 4 se puede observar las especificaciones de la ISO 27033.

Tabla 4.
Especificaciones de la ISO 27033

Especificaciones de la ISO 27033	
IS0 27033-1 Mapeo hacia otras redes	Identificar y analizar riesgos.
IS0 27033-2 Directrices sobre planificación.	Arquitectura de seguridad de la red.
IS0 27033-3 escenarios de red y amenazas.	Revisión de seguridad técnica y los controles de seguridad.
IS0 27033-4 Directrices sobre riesgos, puertas de enlace.	Seguridad en puertas de enlace para flujo de datos
IS0 27033-5 Directrices sobre riesgos, VPN.	Controles para accesos de usuarios remotos.
IS0 27033-6 Directrices sobre redes inalámbricas.	Controles técnicos para la comunicación entre redes inalámbricas.

Nota: Desarrollo de autoría propia

La comparación entre las normas de ciberseguridad ISO y el marco NIST hace referencia a la protección de datos y permite observar las características, ventajas y desventajas de cada una de ellas.

Se puede implementar cualquier marco o norma de seguridad, ya que las dos están aptas para ser implementadas en la empresa Fermagri S. A., sin embargo, como una de las ventajas que se muestra el marco de referencia NIST por tema de costo y siendo una empresa PYME se puede realizar la implementación de esta.

a. Estructura general

La presente propuesta está basada en los análisis que se han venido realizando, ver figura 8.

Figura 8.
Estructura general de la propuesta

Nota: Desarrollo de autoría propia

b. Explicación del aporte

Basado en los aportes de Ciberseguridad Industrial by Logitek (2019), se puede definir lo siguiente:

1. Políticas y procedimientos de seguridad: son un grupo de reglas, responsabilidades y procedimientos que establecen la forma en que una organización debe proteger su información y mantener su seguridad. Es esencial que estas políticas se comuniquen de manera clara, comprensible y accesible en toda la organización.

2. Seguridad física y del entorno: se refiere a la protección contra el acceso no autorizado de personas o atacantes a los dispositivos e infraestructuras de hardware de

la red. Para aumentar la seguridad en esta dimensión, se deben establecer barreras físicas, mecanismos de control de acceso y vigilancia, con el fin de evitar cualquier posible intrusión.

3. Defensa perimetral: se refiere a proteger los puntos de contacto entre una red interna confiable de una organización y otras redes externas o no confiables, como Internet o redes operadas por terceros. La capa de defensa perimetral se enfoca en proporcionar acceso remoto seguro a la red y prevenir que los atacantes accedan a los servicios disponibles externamente y los usen con fines maliciosos.

4. Defensa de red: protección de la red como un conjunto de medidas que buscan evitar los ataques de los intrusos que intentan acceder a ella, ya sea de forma pasiva, limitándose a monitorizar el tráfico, o activa, modificando los datos transmitidos. Para lograr este objetivo, se emplean sistemas de detección y prevención de intrusos en la red.

5. Defensa de equipos: la implementación de medidas de seguridad es fundamental para garantizar la protección de los servidores y dispositivos cliente, y entre estas medidas se destacan:

- Instale parches de seguridad para corregir vulnerabilidades conocidas.
- Deshabilite todos los servicios innecesarios para reducir la exposición de la computadora.
- Aprestar un anti-malware activo.
- Controle el tráfico entrante usando un firewall.
- Acortar la ejecución de programas innecesarios.

6. Protección de aplicaciones: Se puede garantizar la seguridad de las aplicaciones mediante la implementación de mecanismos de autenticación y autorización sólidos para controlar el acceso a ellas.

7. Protección de datos: La autenticación y la autorización, junto con el cifrado, son los métodos de protección de datos más utilizados si un atacante logra eludir todas las defensas anteriores y obtener acceso a la aplicación.

Según el análisis realizado, se determinó que las seguridades que se implementarán de base a la comparación de las metodologías ayudarán a tener los respectivos procedimientos y procesos que se emplearán para la seguridad de la red Wi- Fi en la empresa.

c. Estrategias o técnicas

Aplicando el marco de ciberseguridad NIST y estudiando la ISO 27033 se llega al siguiente detalle para implementación y llegar al objetivo del presente estudio:

Según marco de ciberseguridad NIST

- Se deben ajustar las políticas y los procesos de la organización. Fermagri S. A., debe asegurarse de tener en cuenta dentro de sus políticas institucionales los procesos de ciberseguridad y privacidad.
- Aseguramiento de los sistemas de información que están encargados del almacenamiento, procesamiento y transmisión.
- Según Toro, (2021) al aplicar la metodología NIST se la debe interpretar de la siguiente manera.
    1. Caracterización del sistema: permite establecer los límites y el alcance operacional de la evaluación de riesgos en Fermagri S. A.
    2. Identificación de amenazas: definir las fuentes por donde se sospeche que se pueda recibir un ataque. Una gran ayuda es la revisión de historiales o datos de agencias u otros medios de comunicación.
    3. Identificación de vulnerabilidades: elaborar un listado con los defectos o posibles debilidades. Aquí se puede dar como ejemplo el personal que no ha recibido la debida información con respecto a restricciones.

4. Análisis de controles: realizar una revisión de algún control actual o control planificado, aparte de realizar la lista respectiva. Se puede mencionar una bitácora de personal que tienen acceso al equipo informático a diario o que manejen información confidencial donde se use contraseñas.
5. Determinación de probabilidades, hacer un estudio para saber las posibles motivaciones para los ataques.
6. Análisis del impacto. Se busca evaluar el real riesgo y recomendar un control que pueda reducir y mitigar hasta un nivel aceptable.
7. Determinación del riesgo. Para este paso se debe conocer que tan probable es que explote una amenaza, el impacto que tendría y cuál sería su magnitud, así mismo adecuar los controles actuales y planificados. Así podremos establecer el nivel de riesgo de la organización.
8. Recomendación de controles. Cambio de contraseñas con periodicidad, actualizaciones de sistemas operativos, actualizaciones de antivirus, licenciamiento, así como la actualización de las políticas de seguridad.
9. Documentación de resultados: Presentar a la gerencia general como al departamento de TI los resultados de la valoración de los riesgos.

Según la Norma ISO 27033

- Las recomendaciones se enfocan a los controles de red que se debe mantener en una organización:
    - Monitoreo y registro.
    - Controles de acceso a la red.
    - Control de privilegios de acceso.
- Dentro de las seguridades de los servicios de red se puede implementar acuerdos con niveles de servicio o SLA, una auditoría de calidad de servicio es un modo que se puede tener visible la disponibilidad de la red así mismo como su evaluación.
- Una subdivisión de las redes con dominios distintos es decir una segregación de forma lógica e incluso puede ser física.
- Para el intercambio de información las medidas de seguridad deben definirse en función a la naturaleza del remitente y destinatarios.
- Evitar la utilización de contraseñas predeterminadas, cada router inalámbrico trae por defecto de fábrica una clave predeterminada tanto de acceso al administrador de este como para que se puedan conectar y navegar. Al momento de realizar el cambio de dicha contraseña se debe colocar una compleja para que no deba ser fácil de adivinar.
- Para evitar que el equipo muestre su presencia, se debe desactivar la opción de muestra de SSID del equipo inalámbrico hacia los usuarios finales.
- Cambiar el SSID por defecto, cambiar el nombre del SSID por defecto, para que sea complicado su localización.
- Cifrado de datos, asegurarse que se encuentre activo el cifrado de datos, la mayoría de los dispositivos son compatibles con el cifrado WPA.
- Protección contra ataques de malware e internet, la correcta instalación de un antivirus legal en los ordenadores de la organización, así como el correcto

funcionamiento de la consola de administración permitirán reducir el riesgo a ataques cibernéticos.

2.3. Validación de la propuesta

Para realizar la validación de la propuesta se detalla los métodos de seguridad que se han desarrollado según la NIST SP 800.30 y la ISO 27033

Según info@citel (s. f.) la metodología de seguridad conocida según las NIST SP 800.30 se basa en:

- **Evaluación del riesgo,** este proceso ayuda a evaluar el nivel de potencia y sus riesgos en el cual incluye:
  - Caracterización del sistema: Es un proceso que permite establecer el alcance de la evaluación de riesgos y proporciona información relevante para definir y gestionar los riesgos.
  - Detección de amenazas: Determina las mayores fuentes de amenaza que podrían exponer a vulnerabilidades.
    - Usuario: acciones no intencionales (como la entrada de datos no intencional), o acciones premeditadas (como ataques basados en la web, descargas de malware, o acceso no autorizado);
    - Natural: desastres naturales; y
    - Ambiental (como corte de energía a largo plazo).
  - Detección de vulnerabilidades: Consiste en identificar las debilidades del sistema, tales como errores o fallos, que podrían ser explotadas por posibles amenazas.
  - Análisis de control: Es un proceso que se emplea para identificar y valorar los mecanismos de control que un sistema de información tiene implementados, con el objetivo de reducir la probabilidad de que se produzca una amenaza y disminuir el impacto que ésta pueda tener en

el sistema. Se detalla ejemplos de medidas de seguridad efectivas o mitigación de riesgos:

  - Controles técnicos y no técnicos integrados en el hardware, software, o firmware del computador, como políticas de seguridad, procedimientos de trabajo, así como la seguridad del personal y la seguridad del medio ambiente.
  - Controles preventivos tales como, derechos para usuarios (control de acceso), encriptación y validación.
  - Listado de verificación para conocer si se cumplió o no los requisitos de seguridad.

- La probabilidad se puede calcular evaluando tres elementos clave: la capacidad y motivación de las posibles fuentes de amenaza, la naturaleza de la vulnerabilidad en cuestión y la efectividad de las medidas de control existentes. Al considerar estos factores, se puede clasificar la probabilidad de la amenaza como alta, media o baja.
- Análisis de impacto: Es un proceso que consiste en priorizar los niveles de impacto que pueden tener las amenazas en los recursos de información de una organización. Para llevar a cabo este análisis, es necesario asignar cada riesgo a los componentes arquitectónicos del sistema y determinar la magnitud del impacto que tendría sobre los activos. Posteriormente, se determina la magnitud del impacto, que puede ser alto, medio o bajo, en caso de que la amenaza sea exitosa. Esto permite realizar una evaluación cualitativa o cuantitativa y priorizar los riesgos según su importancia para la organización.
- Determinación del riesgo: Evaluación del nivel de riesgo del sistema de información. En base a lo siguiente se calcula:
  - Probabilidad de origen de amenaza.
  - Tamaño del efecto.

        - Ajuste de las medidas de seguridad para disminuir o suprimir el riesgo.
    - Recomendaciones de control: El objetivo de este proceso es disminuir el nivel de riesgo hasta alcanzar un nivel aceptable, para lo cual se realiza una evaluación de riesgos. Es fundamental llevar a cabo un análisis de costo-beneficio para evaluar si la inversión en la implementación de los controles recomendados justifica la reducción del riesgo obtenida. Esto es un aspecto importante dentro del proceso de gestión de riesgos y contribuye a garantizar la seguridad de los activos de la organización.
    - Los resultados obtenidos, que incluyen la identificación de amenazas y vulnerabilidades, la evaluación del riesgo y las recomendaciones para el control, se registran en un informe formal. Este informe tiene como objetivo servir como herramienta de apoyo en la toma de decisiones relacionadas con cambios en políticas y procedimientos, presupuestos y sistemas con el fin de reducir y remediar posibles pérdidas.

- **Reducción del riesgo:** Se trata de un enfoque estructurado para mitigar los riesgos, que implica la identificación, evaluación y priorización de medidas adecuadas para reducir los riesgos detectados durante la evaluación de riesgos. La aplicación de las mejores prácticas puede variar según la organización involucrada.
    - Tomar el riesgo: aceptar el riesgo potencial y continuar con la actividad u operación o utilizar controles para reducirlo a un nivel aceptable.
    - Evitar el riesgo: eliminar la causa o el efecto.
    - Reducir el riesgo: implementar controles para minimizar el impacto que genere una amenaza.
    - Transferir el riesgo: Utilizar alternativas para cubrir esas pérdidas, ejemplo, las pólizas de seguros.

Luego de identificar los posibles controles que se pueden aplicar según su viabilidad y que tan efectivos puedan ser, se debe realizar un análisis de costo-beneficio que pueda usarse para determinar las medidas de control apropiadas a los cuales se deben asignar recursos. Este punto busca demostrar que la inversión asignada reducirá el nivel de riesgo y este será justificado.

Se debe considerar lo siguiente:

- La implementación de nuevos controles y su impacto.
- La no implementación de nuevos controles y su impacto.
- Listado de costos para implementación:
    - Hardware.
    - Software.
    - Políticas y procedimientos.
    - Personal y capacitación.
- Los costos y beneficios se analizan en función de la importancia crítica del sistema y los datos.

Después de llevar a cabo estas comparaciones, se puede decidir si se deben o no implementar medidas de control de riesgos.

- **Análisis y evaluación:** se debe tener en cuenta que es muy probable que la red, así como los componentes y el software, muy probablemente cambiarán al transcurrir el tiempo. Esto significa que surgirán nuevos riesgos y los previamente mitigados pueden volver surgir siempre que la infraestructura y las operaciones de procesos comerciales estén en su lugar.

Al realizar la evaluación de este proceso se debe considerar lo siguiente:

- Continuar con el plan actual.
- Plan de contingencia.
- Nueva planificación.
- Cerrar el riesgo.

Actualmente las redes de comunicaciones son uno de los puntos más importantes que en cualquier organización no puede faltar, muchas empresas asignan valores menores para el tema de seguridad ya sea este por problemas de flujo o liquidez sin embargo se exponen a ataques en sus redes y muchas veces estos vienen desde dentro de la organización.

Así mismo, como se han vuelto bien necesarias, son uno de los puntos más vulnerables, motivo por el cual se busca por medio de la comparación de normas ISO 27033 o marcos de seguridad NIST SP 800-30 tratar de mitigar esta problemática.

Se emplea un caso de estudio en particular para la empresa Fermagri S. A. de la cual se hizo un levantamiento previo de información obteniendo resultados que nos permiten dar las recomendaciones respectivas.

Propuesta

Luego de la comparativa entre las dos metodologías tanto NIST como ISO, se propone:

Según la norma NIST SP 800 30:

- Identificación de los activos de mayor criticidad.
- Realizar un alcance operacional de evaluación de riesgos.
- Identificar las fuentes por donde se sospeche se pueda recibir el ataque.
- Elaborar una matriz de riesgos mediante una matriz de impacto.
- Elaborar un estudio de los posibles motivos para recibir un ataque.
- Analizar el riesgo real al que se encontraría expuesto la empresa y los controles necesarios.

Según la norma ISO 27033:

- Controles de red tales como (monitoreo y registro de la red, controles de acceso, permisos y privilegios de administración).
- Subdivisión o segmentación de la red de acuerdo con la necesidad.
- Uso de herramientas de control de correo electrónico (AntiSpam).
- Cambio de contraseñas predeterminadas de cada router.
- Ocultar el SSID y realizar el cambio de nombre por defecto.
- Asegurarse que el cifrado se encuentre con WPA.
- Correcta instalación y configuración de antivirus en la organización.

CONCLUSIONES

La comparativa realizada entre el marco de seguridad NIST SP 800-30 y la norma ISO 27033 se puede concluir que, si bien los dos marcos de seguridad son viables para su aplicación, está dependerá de las necesidades que la empresa quiera cubrir.

Uno de los beneficios que se puede obtener al aplicar cualquiera de los dos marcos de seguridad es que serán de gran ayuda para la detección temprana de cualquier intrusión con el monitoreo constante de la red y uso de programas para mantener en marcha las operaciones del negocio.

Según el análisis de la comparativa la mejor opción que se puede implementar en la empresa Fermagri S. A. es el marco de seguridad NIST, este marco se ajusta para empresas de la sección Pymes y así mismo el costo de implementación es muy bajo, adicional su método de implementación es más sencillo en comparación con la ISO 27001.

Debido a la falta de los procedimientos adecuados en la actualidad, la implementación de las medidas de seguridad según el marco de seguridad NIST puede ser un poco incómoda para los usuarios, pero en última instancia será necesario.

RECOMENDACIONES

Según la comparativa del marco de seguridad NIST SP 800-30 y la norma ISO 27033 se pueden implementar controles en las redes tanto técnicos como administrativos.

Con la finalidad de que se realice una conexión segura de nuestra red es recomendable realizar un estudio actual técnico del funcionamiento de los dispositivos de la empresa y seguir los lineamientos que el marco de seguridad NIST SP 800-30 recomienda.

Se recomienda socializar los procesos y procedimientos al todo el personal para que conozca las restricciones y posibles soluciones a problemas que se nos muestre en la red.

Según el marco de seguridad NIST SP 800-30 recomienda realizar un escaneo pasivo con frecuencia para complementar las medidas de seguridad, este escaneo pasivo no afecta a los dispositivos.

BIBLIOGRAFÍA

Calle, J. P. (2022, 6 octubre). *¿Qué son los indicadores clave de riesgo (KRI)?* Recuperado 20 de agosto de 2022, de https://www.piranirisk.com/es/blog/que-es-un-indicador-clave-de-riesgo-kri

Canalnews. (2021, octubre 7). *Cumbre de Ciberseguridad 2021. Canal News Ecuador.* https://canalnewsecuador.com/2021/10/07/cumbre-de-ciberseguridad-2021/

Carhuaz Malpartida, K. F. (2021). *La seguridad en redes inalámbricas*. http://repositorio.une.edu.pe/handle/20.500.14039/5393

Castillo, J. A. (2020, marzo 7). WLAN: *Qué es, definición, estándar 802.11 y diferencias con LAN.* Profesional Review; Miguel Ángel Navas. https://www.profesionalreview.com/2020/03/07/wlan-que-es/

Ciberseguridad Industrial by Logitek. (2019, noviembre 8). Estrategia de Defensa en profundidad en ciberseguridad industrial (I). Ciberseguridad Industrial, by Logitek. https://www.ciberseguridadlogitek.com/estrategia-de-defensa-en-profundidad-en-ciberseguridad-industrial/

Equipo editorial Etecé. (2022, 31 agosto). *Ejemplos de Investigación Documental*. Investigación documental. Recuperado 24 de febrero de 2023, de https://www.ejemplos.co/investigacion-documental/

Guía: Investigación cuantitativa y cualitativa—Fisterra. (2002, 27 de mayo). Recuperado 6 de septiembre de 2022, de https://www.fisterra.com/formacion/metodologia-investigacion/investigacion-cuantitativa-cualitativa/

Guías NIST: un sustento metodológico para los analistas de ciberseguridad. (2022, 14 de junio). Tarlogic Security. https://www.tarlogic.com/es/blog/guias-nist-sustento-metodologico-para-ciberseguridad/

Investigación documental. Autor: Equipo editorial, Etecé. De: Argentina. Para: *Concepto.de*. Disponible en: https://www.ejemplos.co/investigacion-documental/. Última edición: 31 de agosto de 2022. Consultado: 20 de febrero de 2023

ISO 27002 Punto por punto A13 Seguridad de las comunicaciones. (s. f.). ISO 27001. Recuperado 12 de agosto de 2022, de https://normaiso27001.es/a13-seguridad-en-las-comunicaciones/

9788428343138 - JULIO BARBANCHO CONCEJERO - paraninfo.es. (2020). https://www.paraninfo.es/catalogo/9788428343138/redes-locales-3-%C2%AA-edicion-2020

López, A. (s/f). Anexo 13. Iso27000.es. Recuperado el 25 de febrero de 2023, de https://www.iso27000.es/iso27002_13.html

Marco de ciberseguridad del NIST. (2019, abril 16). *Comisión Federal de Comercio*. https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist

Martínez, J. L. (2018, noviembre 15). El modelo OSI. PRORED. https://www.prored.es/el-modelo-osi/

Moes, T. (25 de Marzo de 2018). SoftwareLab. Obtenido de SoftwareLab ORG: https://softwarelab.org/es/que-es-un-firewall/

Morán, M. (s. f.). *Consumo y producción sostenibles. Desarrollo Sostenible.* Recuperado 4 de agosto de 2022, de https://www.un.org/sustainabledevelopment/es/sustainable-consumption-production/

NIST Cybersecurity Framework vs ISO 27001. (2020). Segu-Info - *Ciberseguridad desde 2000*. Recuperado 12 de agosto de 2022, de http://blog.segu-info.com.ar/2018/03/nist-cybersecurity-framework-vs-iso.html

Pérez Porto, J. (10 de noviembre de 2008). *Definición de método inductivo - Qué es, Significado y Concepto*. Definicion.de. Última actualización el 5 de julio de 2021. Recuperado el 24 de febrero de 2023 de https://definicion.de/metodo-inductivo/

Pstyga, N. (2022, 21 marzo). *Ciberseguridad: todos podemos ser víctimas.* IQ Latino. https://iqlatino.org/ciberseguridad-todos-podemos-ser-victimas/

Ríos, N. R. T., Morales, E. L. Í., & Sandoya, S. D. C. (2017). *Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas*. Revista Publicando, 4(10 (2)), 462–473. https://revistapublicando.org/revista/index.php/crv/article/view/367

Seguridad en redes inalámbricas wlan: *Metodología para la implementación de seguridad en redes inalámbricas version_2.0.* (s. f.). Recuperado 29 de abril de 2022, de http://miseriwlan.blogspot.com/2006/08/metodologia-para-la-implementacion-de.html

Seguridad en redes wifi: *Una guía de aproximación para el empresario.* (2019, mayo 14). INCIBE. https://www.incibe.es/protege-tu-empresa/blog/seguridad-redes-wifi-guia-aproximacion-el-empresario

Shaw, K. (2023, enero 20). *¿Qué es el Wi-Fi y por qué es tan importante?* Computerworld.es. https://www.computerworld.es/telecomunicaciones/que-es-el-wifi-y-por-que-es-tan-importante

Soto, M. G. (2019, septiembre 1). *NIST: Ciberseguridad holística….* Medium. https://marvin-soto.medium.com/nist-ciberseguridad-hol%C3%ADstica-ce4b3911dae7

Toro, R. (2021, agosto 26). *Metodología NIST SP 800 – 30 para el análisis de Riesgos en SGSI. PMG SSI - ISO 27001.* https://www.pmg-ssi.com/2021/08/metodologia-nist-sp-800-30-para-el-analisis-de-riesgos-en-sgsi/

Universidad del Azuay. (s. f.). Universidad del Azuay. Recuperado 12 de agosto de 2022, de https://www.uazuay.edu.ec/sistemas/teleprocesos/laninalambricas

WIFI - *Comunicación Inalámbrica.* (s. f.). Recuperado 17 de agosto de 2022, de https://www.aulaclic.es/articulos/wifi.html

ANEXOS

ANEXO 1

Se procede al levantamiento de la información en la empresa Fermagri para realizar una propuesta de implementación de seguridad.

PUNTOS	SI	NO
¿Posee detectado los activos de mayor criticidad?		X
¿Tiene los SSID Ocultos?		X
¿Todos los puertos de red se encuentran abiertos?		X
¿Posee red administrada?		X
¿Posee red segmentada?		X
¿Tiene procedimientos definidos?		X
¿Tiene implementado algún marco de seguridad?		X

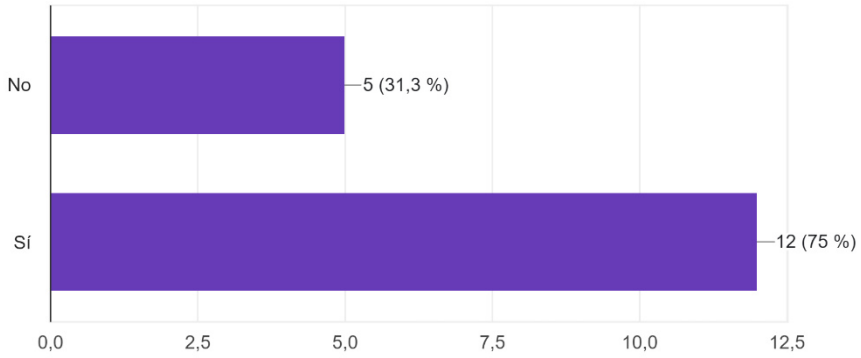
ANEXO 2

Tabulación de respuesta de encuesta realizada

Se realiza una encuesta a personal de TI de diferentes organizaciones para poder medir un poco el conocimiento que se tiene a nivel de seguridad.

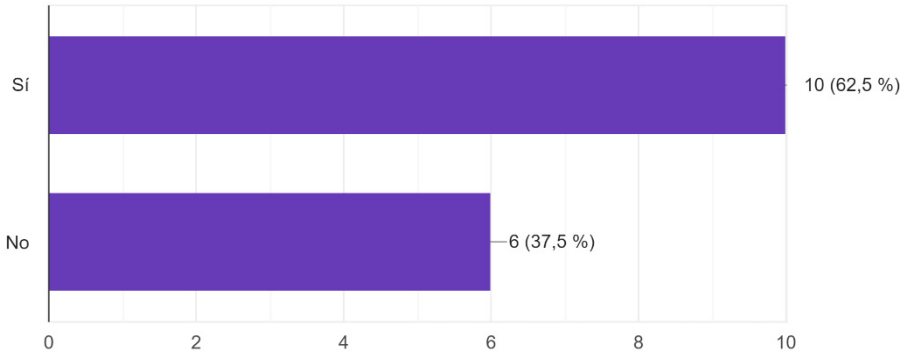
¿Su organización cuenta con un plan de seguridad de redes?

16 respuestas



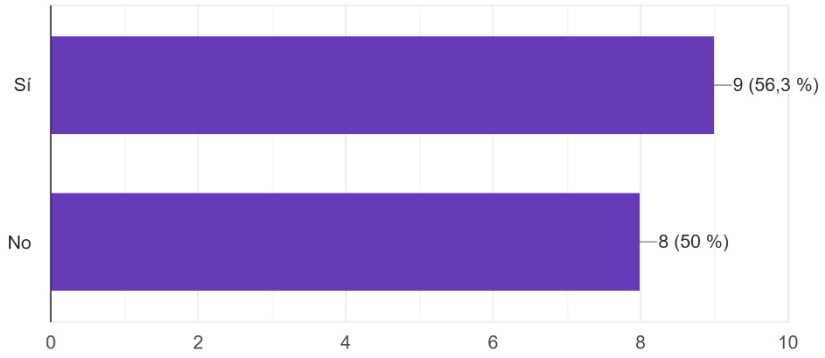
¿Se han identificado los activos de información crítica en su organización?

16 respuestas



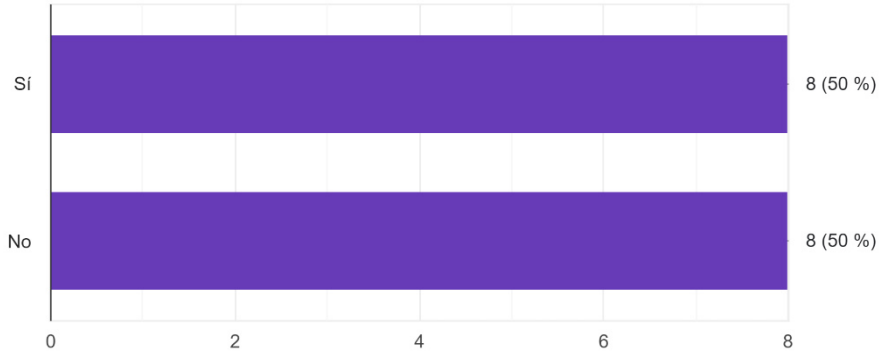
¿Se han realizado evaluaciones de riesgos de seguridad de redes en su organización?

16 respuestas



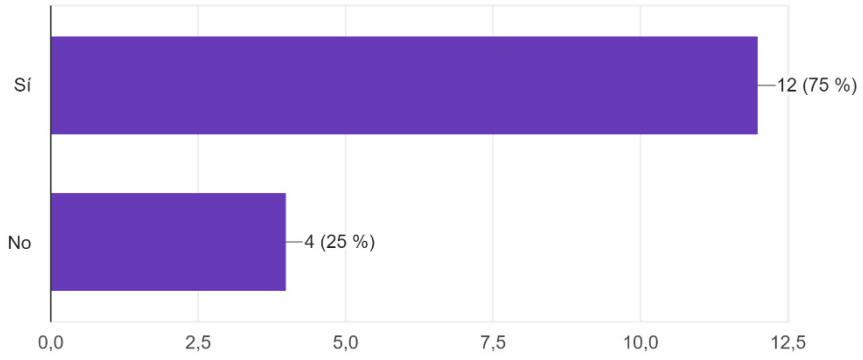
¿Su organización cuenta con políticas de seguridad de redes establecidas?

16 respuestas



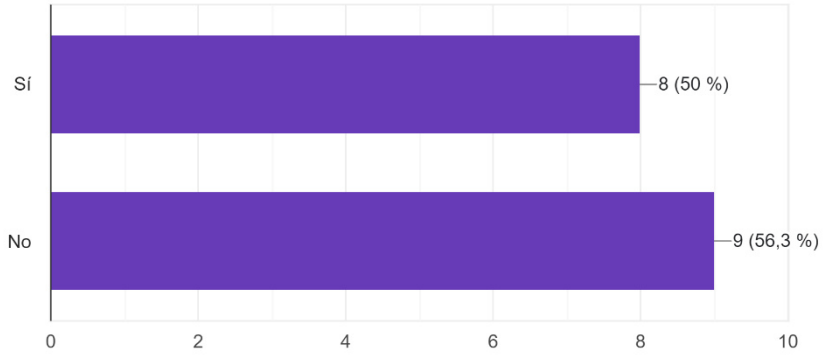
¿Se han implementado medidas de control de acceso para restringir el acceso no autorizado a la red?

16 respuestas



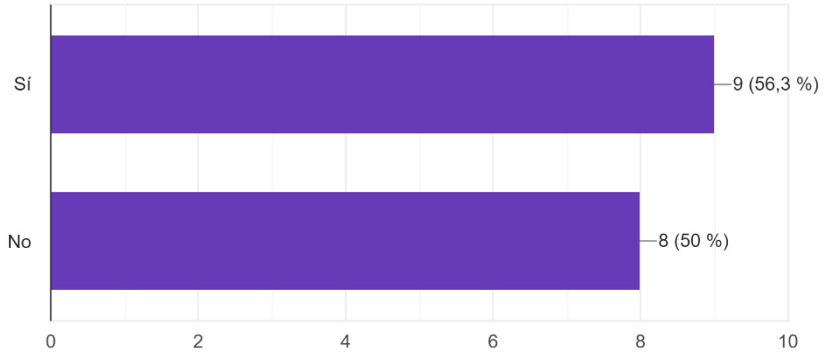
¿Se han implementado medidas de seguridad para proteger la integridad y confidencialidad de los datos de la red?

16 respuestas



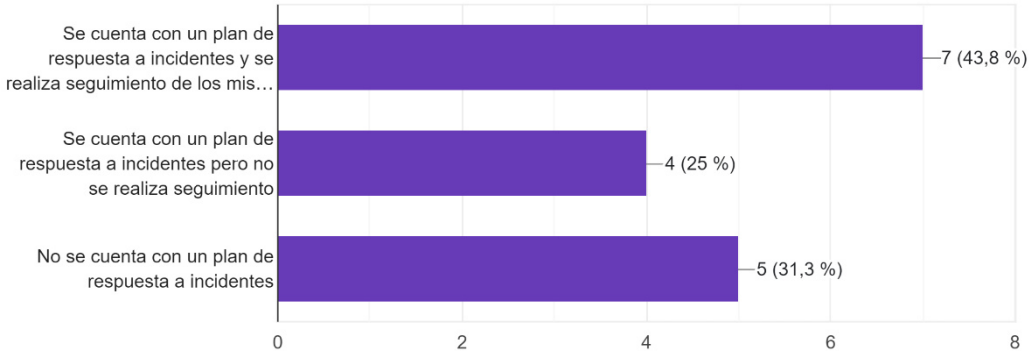
¿Se han realizado auditorias y pruebas de penetración de forma periódica para evaluar la seguridad de la red?

16 respuestas



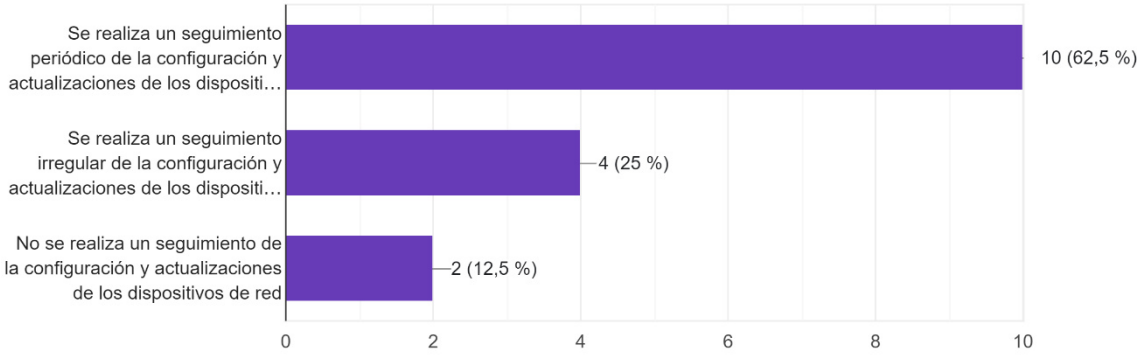
¿Cómo se manejan los incidentes de seguridad en la red?

16 respuestas



¿Cómo se asegura de que los dispositivos de red estén configurados de forma segura y se hayan aplicado las actualizaciones de seguridad necesarias?

16 respuestas



¿Cómo se gestiona la seguridad de los dispositivos móviles que acceden a la red de la organización?

16 respuestas