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:
Comparativa de Métodos de Control de Acceso de una Infraestructura de Red Empresarial.
Línea de Investigación:
Seguridad Informática
Campo amplio de conocimiento:
Tecnologías de La Información y Comunicación
Autor:
Cintya Vanessa Velásquez Vivas
Tutor:
MSc. Pablo Marcel Recalde Varela

Quito – Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, Recalde Varela Pablo Marcel con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: Comparativa de Métodos de Control de Acceso de una Infraestructura de Red Empresarial.

Elaborado por: Cintya Velásquez, de C.I: 1718441346, 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., septiembre de 2022

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Velásquez Vivas Cintya Vanessa con C.I: 1718441346, autora del proyecto de titulación denominado: Comparativa de métodos de control de acceso de una infraestructura de red empresarial. 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 autora 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., septiembre de 2022

0000-0001-7262-4574

Firma

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

Con el inicio de la pandemia y la implementación del teletrabajo las empresas están mejorando la infraestructura de sus redes para extender la longitud de su red, mejorar el rendimiento, incrementar el número de usuarios e incluso segmentar la red. Todos los dispositivos y componentes que se utilizan en la red deben tener un tratamiento controlado y acceso físico restringido para su seguridad (Triviño, 2019).

A nivel mundial, el acceso a las redes se ha visto transformado principalmente por la penetración de dispositivos internos y externos, se espera que para el año 2028 los ciberataques y los ciberdelincuentes mejoren sus ataques y utilicen nuevas técnicas e inteligencia artificial para vulnerar los sistemas, hoy en día es imposible no tener conectadas a la red las infraestructuras empresariales ya sean estas alámbricas o inalámbricas y los ataques e intromisiones por accesos no autorizados y nuevas técnicas de ataque informáticos se han tornado más frecuentes (Oficina Internacional del Trabajo, 2020).

El reto de enfrentarse a la pérdida del control y soberanía de los datos, confronta con la necesidad de buscar métodos y soluciones novedosos que permitan gestionar y administrar de forma segura los dispositivos de la red para proteger los sistemas y datos críticos de una empresa de ataques (Bejarano et al., 2019).

Todos los dispositivos internos y externos que interactúan en la infraestructura de una red empresarial son un medio por el cual los hackers «black hat» podrían realizar ataques o robar información crítica de una empresa.

La seguridad es una de las bases en las que se apoya la continuidad operativa, es primordial contemplar el monitoreo y la gestión que poseen las empresas como uno de los principales aspectos que se deben priorizar para presentar los métodos de control y acceso (Zhou et al., 2021).

La implementación de métodos de control y acceso a los dispositivos que se implementen en la infraestructura de la red demandan parámetros de calidad que aseguren el buen funcionamiento, la confiabilidad, la integridad y disponibilidad de los procesos y operaciones de la empresa (Flores, 2017).

Según el nuevo informe de Kaspersky (2021) «Ajuste de la inversión: alineando los presupuestos de TI con las prioridades de seguridad», la inversión prioritaria para las empresas

es la de ciberseguridad. Hasta el año 2020 en Latinoamérica, el presupuesto para seguridad informática creció del 22% al 30% para las PYMES y para empresa más grande el crecimiento fue de 27% al 34%. Se espera que para el 2024 el presupuesto para ciberseguridad aumente en un 59%.

«El informe de evaluación de respuesta ante la crisis de la Covid-19», realizado por Schneider Electric y Oxford Business Group (OBG), asevera que la ciberseguridad ha se ha vuelto una prioridad estratégica empresarial y se pronostica que Latinoamérica incrementará su gasto anual en hardware, software y servicios de TI en un 12% anual para el 2024.

Problema objeto de investigación

Con el desarrollo de las comunicaciones, los sistemas Ciber Físicos y las tecnologías móviles, los dispositivos se han transformado en parte esencial de nuestras vidas (Chen et al., 2018). El desarrollo de la tecnología y el reto de las empresas por mejorar sus infraestructuras ha integrado en sus redes grandes cantidades de dispositivos conectados a la red generando una gran cantidad de información, (Ma et al., 2020) empeorando el problema del control de acceso inalámbrico en una red ante un desastre (Zhou et al., 2021), el bloqueo de usuarios y dispositivos no autorizados y el problema del acceso, que es esencialmente un tipo de control de acceso a la red (Zhang et al., 2017).

El Internet de las cosas (IoT) se presenta como una ventaja para los sectores industriales, pero lleva relación con el Internet antiguo por los dispositivos externos (Kuzmin, 2017) y la conexión entre estos sistemas brindando la calidad de servicio (Shi et al., 2020).

El interés y la preocupación de los investigadores y científicos por el Internet de las cosas ha ido en aumento (Yamada et al, 2016) por todos los dispositivos que interactúan con Internet y son parte de la infraestructura de una red empresarial, los sistemas cliente-servidor se acercan a un límite de rendimiento a medida que aumenta la cantidad de nodos (Berenice et al., 2017) y son un medio por el cual los hackers podrían realizar ataques o robar información crítica de una empresa (Triviño, 2019).

Con los antecedentes mencionados, hay un gran desafío en cuanto al acceso y la seguridad de las infraestructuras empresariales y se puede plantear la pregunta:

¿Qué características técnicas de seguridad tienen los métodos de control de acceso en la infraestructura de red?

Objetivo general

Realizar una comparativa de algunos métodos de control de acceso de una infraestructura de red empresarial.

Objetivos específicos

Contextualizar los fundamentos teóricos de diferentes métodos de control de acceso de red empresarial.

Determinar los mecanismos para mejorar el nivel de seguridad de acceso en la infraestructura de una red empresarial.

Desarrollar una estimación del valor aproximado que gasta anualmente en seguridad una empresa.

Vinculación con la sociedad y beneficiarios directos:

El acceso a la red desde dispositivos desconocidos se ha convertido en una gran desventaja para las pequeñas y medianas empresa que no cuentan con presupuesto para la compra de equipos de alta gama para la protección y seguridad, tomando como referencia los Objetivos de desarrollo sostenible (ODS), se centra este trabajo en el objetivo número 9 y las metas 9.1 «El desarrollo de infraestructuras confiables, sostenibles, resilientes y de calidad, para favorecer el desarrollo tanto económico como el bienestar humano, dando mayor importancia en el acceso accesible y ecuánime para todos» y la meta 9.4 « Se prevé que para el año 2030, se modernice la infraestructura y se transformen las industrias para que sean sostenibles, recurriendo a los recursos con mayor eficacia e impulsar la adopción de tecnologías y procesos industriales limpios y ambientalmente racionales, para lograr que los países tomen medidas de acuerdo con sus capacidades respectivas.»

Poniendo en práctica la investigación realizada en el presente trabajo se proporcionará a los encargados de seguridad informática, una base para escoger la mejor opción para instalar en su red, nos centraremos en el objetivo número 8 y la metas 8.3 «Impulsar políticas orientadas para el desarrollo que apoye las actividades productivas, la implementación de puestos de trabajo dignos, el emprendimiento, la creatividad y la innovación, y promover la formalización y el crecimiento de las PYMES, incluso mediante el acceso a servicios financieros».

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

Ortiz (2022) considera que la infraestructura de una red es adecuada cuando la misma se puede evaluar de manera autónoma utilizando sus propios recursos, su topología, el flujo de tráfico y las reglas de aprovisionamiento y donde cada segmento de la red tiene su propia arquitectura y sus propios protocolos.

Garbis y Chapman (2021) mencionan que una empresa debe seguir tres principios básicos para proteger los recursos de red, aplicaciones y datos como asegurarse de tener acceso a todos los recursos de forma segura, todo acceso debe estar sujeto a políticas, independientemente de la ubicación. Se debe adoptar una estrategia de privilegios mínimos y la aplicación de control de acceso estricto; realizar inspecciones y registro de todo el tráfico de la red.

Con el desarrollo de las tecnologías de la información y la comunicación (TIC), las comunicaciones y la Internet de las cosas (IoT), la cantidad de dispositivos conectados a la red y la cantidad de datos generados aumentan exponencialmente, por lo que se han desarrollado e introducido frameworks de arquitecturas de referencia de computación perimetral y todas otorgan gran importancia a la seguridad de los datos. «Sin embargo, no existe un frameworks de seguridad independiente para discutir sistemáticamente la seguridad de la informática perimetral» (Ma et al., 2020).

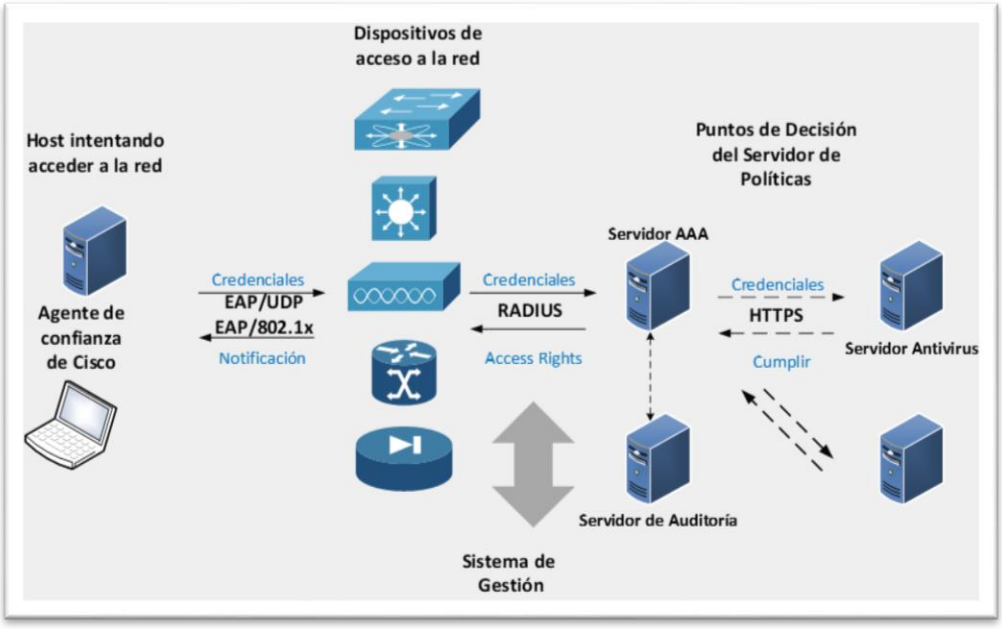
La primera tarea para proteger cualquier red es garantizar el acceso únicamente a usuarios autorizados, es crucial mejorar los mecanismos de control de acceso; por lo tanto, además de técnicas, soluciones de control de acceso, políticas de control de acceso a la red debe estar claramente definido con políticas de seguridad que deben estar respaldadas por buenas prácticas de gestión de la seguridad y determinar los mecanismos para garantizar la autenticación, confidencialidad, integridad, privacidad y seguridad de los datos (Ashcraft y Satran, 2019).

En el artículo técnico realizado por Flores et al. (2017) señala que debido al crecimiento empresarial y tecnológico se ha puesto en evidencia la necesidad y la importancia de implementar controles de acceso a las redes. Una de las soluciones para el control de acceso es Network Access Control (NAC) cuyo enfoque es reforzar la seguridad en la red unificando tecnologías y políticas de seguridad y sistemas de autenticación.

NAC restringe el acceso a la red a dispositivos que no cumplen con los requisitos de la red, para evitar que exista una infección en la red se envían los dispositivos desconocidos a un área de cuarentena (Cisco Systems, Inc., 2022).

NAC cuenta con varias soluciones para ayudar a las organizaciones a controlar el acceso a la red. Mediante la administración del ciclo de vida de la política permite aplicar políticas a todo el conjunto operacional. Elabora perfiles de usuarios y dispositivos personales. Administra temporalmente a los usuarios mediante un portal de servicio personalizado. Comprueba el estado de seguridad mediante evaluaciones de cumplimiento de políticas a usuarios, dispositivos y sistema operativo. No necesita la atención del administrador TI para mitigar las amenazas, tiene una respuesta alta ante incidentes. Mediante API se puede integrar a otras soluciones de red (Cisco Systems, Inc., 2022).

Figura 1*:*
Componentes de NAC



Nota: Elaboración propia (2022).

Acorde a Cisco Systems, Inc. (2022) se describen los siguientes casos de uso:

NAC para usuarios-contratistas temporales. –Esta solución garantiza que los visitantes, contratistas y socios que no son parte de la organización tengan privilegios de acceso a la red diferentes a los de los empleados de planta.

NAC para BYOD. - La evolución de los dispositivos móviles ha permitido que los empleados tengan la posibilidad de trabajar de forma remota utilizando estos medios. Esta solución garantiza para BYOD el ajuste de los dispositivos de los empleados antes de acceder a la red.

NAC para Internet de las cosas (IoT). - La evolución de los dispositivos IoT se han convertido en una amenaza para las redes, ya que los atacantes utilizan estos dispositivos para acceder de forma rápida y fácil. Esta solución reduce el riesgo creado por estos dispositivos mediante la aplicación de políticas de acceso y además elabora perfiles definidos.

NAC para respuestas de incidentes. - Esta solución permite que los proveedores compartan información de componentes de seguridad de terceros, responde a alertas mediante políticas de seguridad que aísla ordenadores comprometidos.

Trusted Network Connect. - La solución Conexión de red confiable (TNC) fue promulgada y lanzada por el grupo de trabajo de Trusted Computing Group (TCG) como una arquitectura abierta para control de acceso a la red, proporciona especificaciones que permiten la verificación integral de puntos finales proporcionando confianza de interoperabilidad en entornos de múltiples proveedores y terminales. Esta arquitectura aplica políticas para el control eficaz del acceso a las infraestructuras de una red. (IBM Corporation., 2021).

Actualmente se utilizan herramientas de escaneo que permiten identificar equipos en la red, descubrir e identificar dispositivos y puertos abiertos; este tipo de herramientas se utilizan para escanear servidores de pruebas que permiten que los clientes prueben las vulnerabilidades que se tiene disponible. (Abad et al., 2019)

1.2. Proceso investigativo metodológico

Revisión bibliográfica de los principales métodos de control y acceso de una empresa de dispositivos internos y externos en infraestructura de su red.

Inicialmente se hace un análisis rápido de los métodos utilizados por las empresas, localizando las falencias de sus sistemas; se aborda con los responsables de TI identificar cómo manejan el control del acceso y la seguridad informática en las empresas.

Análisis de los elementos de la red, su infraestructura y los métodos de control y acceso implementados, riesgos y vulnerabilidades de la red.

Analizar el marco legal para garantizar la protección de datos tanto de la empresa como la información de empleados y clientes mediante la Ley Orgánica de Protección de Datos.

Métodos, técnicas e instrumentos

Para este trabajo se utilizó una encuesta que se aplicó a profesionales que sean los encargados de la seguridad de sus empresas, la encuesta estuvo compuesta por doce preguntas direccionadas a personal de TI.

Criterios y Normativas

Se presentará como antecedentes los artículos 178 y 190 del Código Orgánico Integral Penal del Ecuador.

Enfoque de la investigación

El enfoque utilizado para esta investigación será un enfoque cuantitativo, mediante una encuesta se identificará los principales métodos de control y acceso con los que cuentan las empresas en la infraestructura de su red y las vulnerabilidades a las que está expuesto.

Tipo de investigación

El tipo de investigación es de tipo no experimental.

Población y muestra

El presente trabajo está dirigido a siete pequeñas y medianas empresas, así como a profesionales que sean los encargados de la seguridad de sus empresas; y ayudar a que las corporaciones detecten los riesgos potenciales a los que se enfrentan, precisen las acciones para la mitigación de estos riesgos, analicen el costo beneficio de la implementación y consideren a uno de estos frameworks, no solo como un estándar si no como una solución que se acople a la necesidad de sus compañías. El tipo de muestreo es no probabilístico y por decisión de expertos.

1.3. Análisis de resultados

1.3.1. Comparativa de métodos de control de acceso

El escoger la opción adecuada de uno de los tres métodos de control de acceso de una infraestructura de red empresarial investigados, tiene que ser valorada mediante los pros y los contras para tomar la decisión de si es aceptable para la organización instalar la solución NAC, NAP o TNC; NAC es una solución que pueden ser beneficiosas para cualquier organización, pero esta solución no siempre se ajusta a la infraestructura de red instalada; al ser propietaria de Cisco NAC limita la operabilidad con otros fabricantes. Por su parte NAP también es una solución

propietaria de Microsoft y no está diseñada para proteger una red de usuarios que no respetan las políticas de seguridad. Por lo expuesto en el presente proyecto se destaca que la elección alternativa para pequeñas y medianas empresas es la elección de TNC; es una alternativa de código abierto y que en la actualidad quiere reemplazar a soluciones costosas y hoy en día cuenta con el apoyo de importantes empresas como: Microsoft, Juniper Networks, Sygate y Symantec. Las interfaces de TNC son realmente independientes del proveedor; todos los componentes de la arquitectura TNC han sido implementados por múltiples proveedores y estos productos han sido probados para garantizar que realmente funcionen juntos. Los clientes conservan todas las opciones y no están atados a ningún proveedor.

Independientemente de lo que decida cada organización se debe incentivar a que tomen conciencia de que es imprescindible que cuenten con un Control de Acceso a Red tanto externa como interna.

Para la validación del presente proyecto se realizó una investigación bibliográfica de los tres principales mecanismos que presenta el mercado y que se encuentran en la lucha por obtener la hegemonía en proveer los sistemas encargados de mejorar el nivel de seguridad de acceso en la infraestructura de una red empresarial, en las Tabla 1, Tabla 2 y Tabla 3 se evidencia la comparativa de los tres métodos, las ventajas y las desventajas de los métodos de control de acceso.

Tabla 1

Ventajas de los tres métodos de Control de Acceso

	VENTAJAS
NAC	Descubre cada uno de los dispositivos que se conectan a la red y controla su comportamiento. Controla quién accede a la red y restringe el número de recursos con los que puede manejar. Adapta y configura la red dinámicamente y sin intervención humana. Detecta dispositivos infectados en la red. Optimiza el consumo energético de los dispositivos. Proporcionar protección de seguridad de punto final, como software antivirus, firewall y evaluación de vulnerabilidades con políticas de aplicación de seguridad y métodos de autenticación del sistema. Controla el acceso de usuarios no conocidos o que no tienen garantías de seguridad, tales como clientes o usuarios remotos y proveedores.
TNC	Está diseñada para permitir la verificación de la postura, el monitoreo del comportamiento y la remediación no solo de los puntos finales de los usuarios, sino también de los dispositivos de infraestructura que están continuamente conectados a la red. Garantiza que todos los puntos finales de la red cumplan con las políticas de seguridad. Los dispositivos de red, los hosts de puntos finales y las aplicaciones corporativas pueden interactuar sin problemas, lo que permite una gestión de seguridad eficiente y eficaz. Los usuarios y clientes aún pueden usar sus dispositivos y plataformas favoritos, el software de detección de virus o el dispositivo de seguridad. Admite un conjunto de estándares en lugar de muchas interfaces propietarias, reduce la dependencia de soluciones de un solo proveedor y permite una flexibilidad arquitectónica que satisface las necesidades de innumerables casos de uso. Satisface las demandas de los organismos reguladores internacionales y nacionales, simplificando la interoperabilidad con otros productos de proveedores y brindar más valor a los clientes.
NAP	Determina si las computadoras cumplen con los requisitos de salud del sistema. Restringe el acceso a la red o la comunicación para clientes que no cumplen con los requisitos de salud del sistema. Proporciona las actualizaciones necesarias para permitir que la computadora corrija su estado de salud no conforme. Permite el acceso a la red siempre que la computadora del usuario cumpla con los requisitos de la política de salud. Protección de redes y dispositivos que son parte de la red mediante políticas de confianza de salud que deben cumplir los dispositivos al componer una red

Nota. Autoría propia

Tabla 2

Desventajas de los métodos de Control de Acceso

	DESVENTAJAS
NAC	Funciona bien cuando se utilizan para controlar PC de escritorio y laptops, pero tiene problemas cuando son necesarios para supervisar otros dispositivos o usuarios dentro de la empresa. Poner una NAC podría llegar a ser muy costoso y no valer la pena para algunas compañías. Puede sobrecargarse con el exceso de información. Sólo puede controlar lo que ve. Por el gran número de puertos del switch, son difíciles de administrar. El acceso a la red se facilita cuando hay falsificación en la dirección MAC de un host. Las organizaciones establecen sus propias políticas para cada usuario, dando lugar a una gran cantidad de políticas, produciendo una gran cantidad de información innecesaria en el momento causando que NAC genere alertas falsas.
TNC	Está trabajando para consolidar un estándar. El acogerse a un código abierto es mucho más complicada. Las empresas requieren soluciones en las que no deban invertir horas de equipos de desarrollo y el gran problema es conseguir el consentimiento de todos los involucrados. Continúa ampliando la arquitectura existente para admitir capacidades y dispositivos adicionales.
NAP	No impide que los usuarios descarguen, instalen o ejecuten programas no autorizados en sus dispositivos. No ha sido diseñado para garantizar la seguridad contra accesos no autorizados sino para garantizar la integridad de la seguridad. No ha sido diseñado para proteger una red de usuarios autorizados que cargue un programa malicioso en la red o participe en otro comportamiento inapropiado.

Nota. Autoría propia

Tabla 3

Cuadro comparativo de los Métodos de Control de Acceso a la Red

Trusted Network Connect (TNC)	Network Access Control (NAC)	Network Access Protection (NAP)
TNC es una arquitectura abierta para el control de acceso a la red. Promulgada por grupo de computación confiable (TCG)	Autenticación de usuario Basado en contraseñas o certificados a través de VPN e IEEE 802.1X	Solución propietaria de Microsoft.
Diseñado para ayudar a los administradores de red a garantizar la integridad y el cumplimiento de los puntos finales y su conectividad con respecto a las políticas acordadas.	Compara las medidas con las políticas de la red para acceder.	Pensada para proteger los elementos que componen la red mediante políticas de confianza.
Puede autenticar clientes y clasificar su conexión al servidor como confiable.	Comprobación de integridad del sistema informático. Medición de la configuración antes del acceso a la red.	La plataforma de protección de acceso a la red no está disponible a partir de Windows 10
Garantiza la interoperabilidad entre puntos finales de una amplia gama de proveedores.	Existen 2 grupos los que están activamente adhiriendo a Cisco NAC y los que están desarrollando productos para trabajar junto con Cisco NAC	
Las máquinas pueden comunicar su configuración al servidor, lo que determina la confiabilidad y puede extender o restringir el acceso a los recursos de la red.	Reevalúa los sistemas informáticos aceptados en intervalos regulares.	Basa su despliegue en agentes y aplicaciones por parte del cliente y en servidores por parte de la red tanto para la verificación como para la admisión.

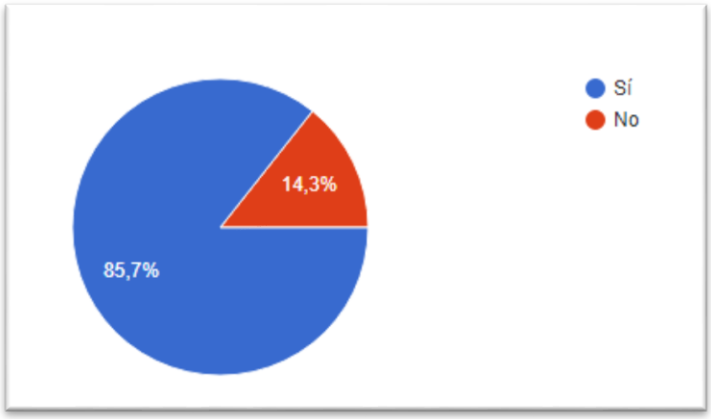
Nota. Autoría propia

1.3.2. Análisis de vulnerabilidades

Se procedió a realizar una encuesta a siete profesionales de TI encargados de la seguridad de sus empresas donde se evidencia las vulnerabilidades más importantes.

A continuación, se muestra los resultados de la encuesta:

Figura 2*:*
Pregunta 1.
¿Existe un área o persona responsable de seguridad informática y seguridad de la información de su empresa?



Nota: Tomado de Formulario de Google Encuesta de Seguridad Informática, 2022.

En relación a la primera pregunta donde se consulta si existe un área o una persona responsable de la seguridad informática y seguridad de la información la respuesta fue la siguiente: el 85,7% señalaron que Sí, un 14,3% señaló que No, se puede decir que la mayoría de las empresas consultadas tiene un área o una persona responsable, brindando un alto grado de seguridad a la infraestructura de la empresa.

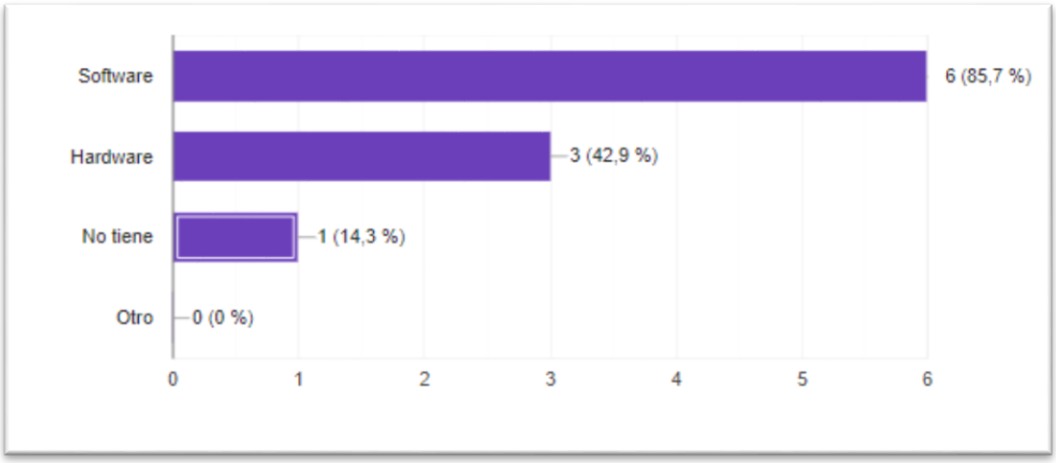
Figura 3:
Pregunta 2.

¿Quién tiene privilegios para administrar las aplicaciones internas de la empresa?

Nota: Tomado de Formulario de Google Encuesta de Seguridad Informática, 2022.

En relación a la pregunta sobre privilegios para administrar aplicaciones internas, la respuesta fue la siguiente: el 85,7% señalaron que personal de Ti es la encargada de administrar y un 14,3% señaló que todos los usuarios tienen privilegios, se puede decir que la mayoría de las empresas consultadas tienen a un responsable experto para realizar la administración, aún con este resultado se ve que algunas empresas permiten que cada usuario sea responsable de administrar aplicaciones lo que permite que personas sin conocimientos intervengan en instalar e implementar aplicaciones que pueden ser utilizadas por hackers para atacar a la red.

Figura 4:
Pregunta 3.
¿Qué tipo de herramientas de seguridad tiene implementado en su empresa?

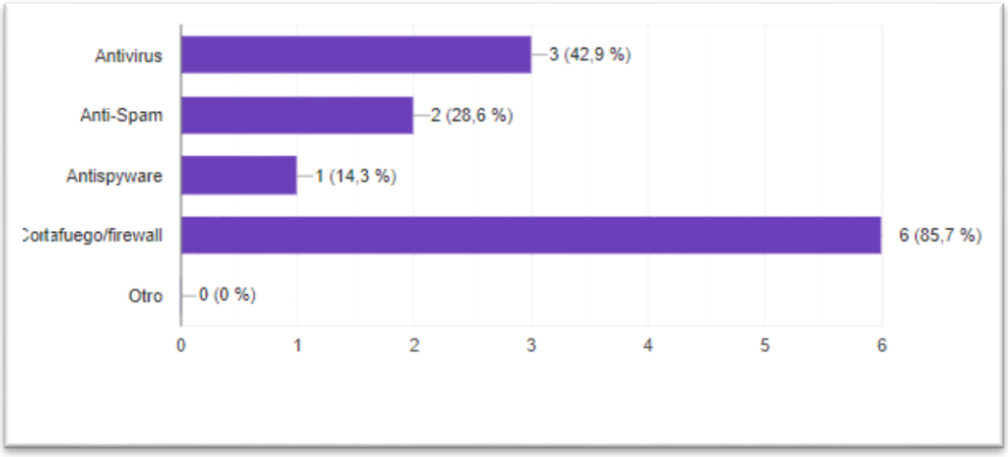


Nota: Tomado de Formulario de Google Encuesta de Seguridad Informática, 2022.

En relación a la pregunta tres sobre herramientas de seguridad, la respuesta fue la siguiente: el 85,7% señalaron que cuenta con software, un 42,9% señala que cuenta con hardware y un 14,3% no tiene ninguna herramienta de seguridad, se puede decir que la mayoría de las empresas consultadas tienen cuenta con software para seguridad, apenas 2 de las 6 empresa consultadas posee hardware para seguridad y 1 empresa no cuenta con ninguna herramienta.

Figura 5:
Pregunta 4.

¿Qué software se utiliza en la empresa para controlar software malicioso?

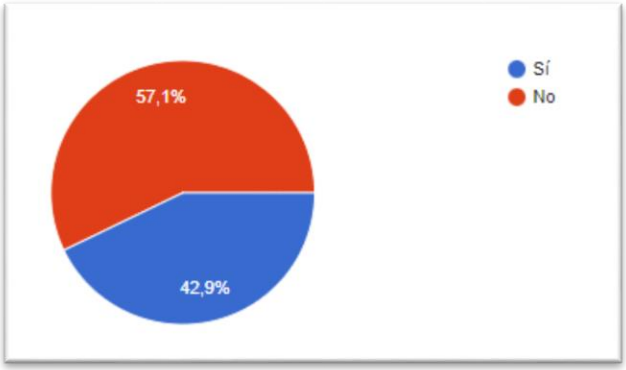


Nota: Tomado de Formulario de Google Encuesta de Seguridad Informática, 2022.

En relación a la pregunta cuatro sobre software para controlar software malicioso, la respuesta fue la siguiente: tres empresas cuentan con antivirus, dos cuentan con antispam, una cuenta con Antispyware y seis de ellas cuenta con un cortafuego o firewall, a pesar de que muchas empresas cuentan con antivirus y antispam, dentro de la seguridad es muy importante contar con antispyware ya que este permite la detección y eliminación de programas espías maliciosos.

Figura 6:
Pregunta 5.

¿Conoce las aplicaciones y dispositivos extraíbles que utilizan los empleados en la red de su empresa dentro y fuera de ella?

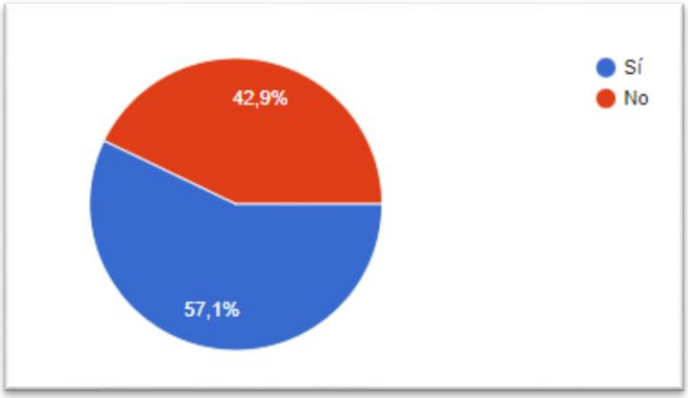


Nota: Tomado de Formulario de Google Encuesta de Seguridad Informática, 2022.

En relación a la pregunta cinco sobre aplicaciones y dispositivos extraíbles de los empleados, la respuesta fue la siguiente: 57,1% desconoce las aplicaciones y dispositivos que usan los empleados y el 42,9% conoce estos elementos, por lo cual se puede decir que la seguridad en cuanto al desconocimiento es alta y puede convertirse en una vulnerabilidad para las empresas.

Figura 7:
Pregunta 6.

¿Cuenta con algún mecanismo de control de seguridad para evitar el acceso a la red de su empresa desde dispositivos desconocidos?

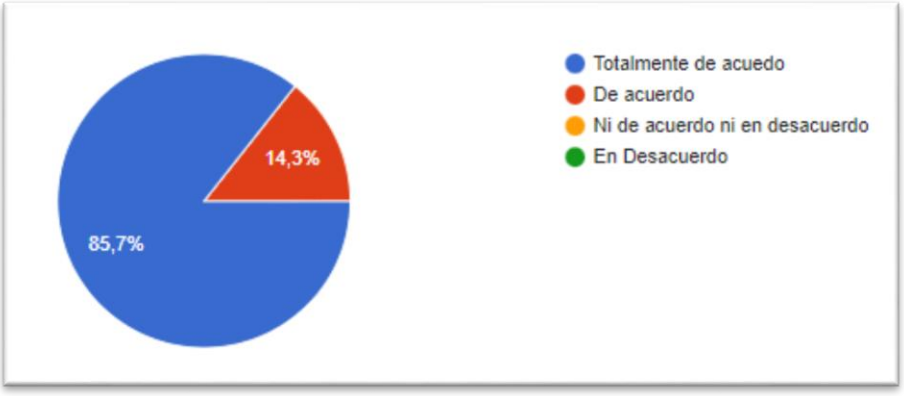


Nota: Tomado de Formulario de Google Encuesta de Seguridad Informática, 2022.

En relación a la pregunta seis sobre mecanismos de control de seguridad, la respuesta fue la siguiente: 57,1% cuenta con mecanismos y el 42,9% no cuenta con ningún mecanismo, por lo cual se puede decir que la mayoría de las empres encuestadas no está protegido ante la amenaza de intrusión a su red por dispositivos desconocidos.

Figura 8:
Pregunta 7.

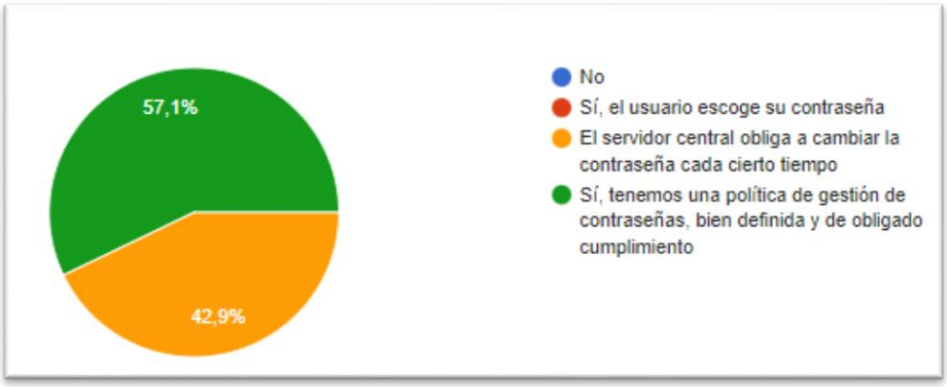
¿Cree que es necesario aplicar controles de seguridad para evitar robo o daño de información importante para la empresa?



Nota: Tomado de Formulario de Google Encuesta de Seguridad Informática, 2022.

En relación a la pregunta siete sobre aplicar controles de seguridad, la respuesta fue la siguiente: 85,7% está totalmente de acuerdo y el otro 14,3% está de acuerdo, por lo cual se puede decir que la mayoría de la empresa consideran importante aplicar controles de seguridad.

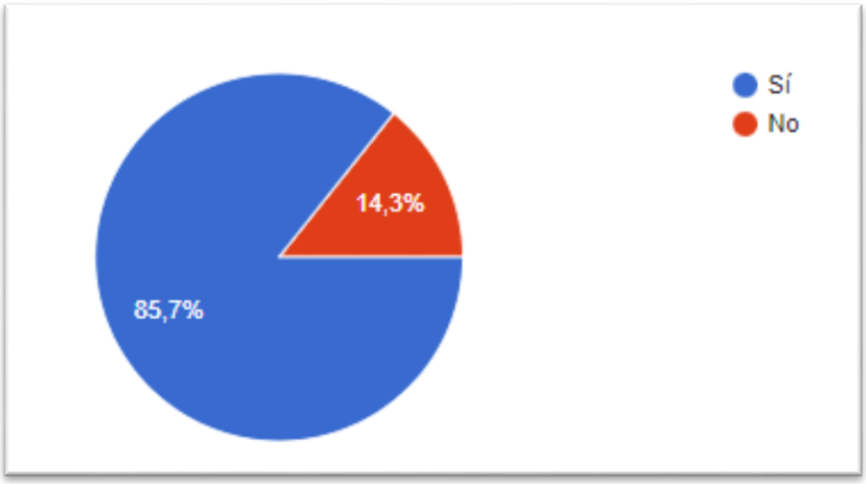
Figura 9:
Pregunta 8.
¿Tiene definido algún tipo de política de gestión de contraseñas?



Nota: Tomado de Formulario de Google Encuesta de Seguridad Informática, 2022.

En relación a la pregunta ocho sobre políticas de gestión de contraseñas, la respuesta fue la siguiente: 57,1% señala que tiene políticas de gestión bien definido y de obligado cumplimiento y el 42,9% señala que un servidor es el encargado de obligar a cambiar la contraseña, por lo cual se puede decir que la mayoría de la empresa consideran importante las políticas de gestión de contraseñas.

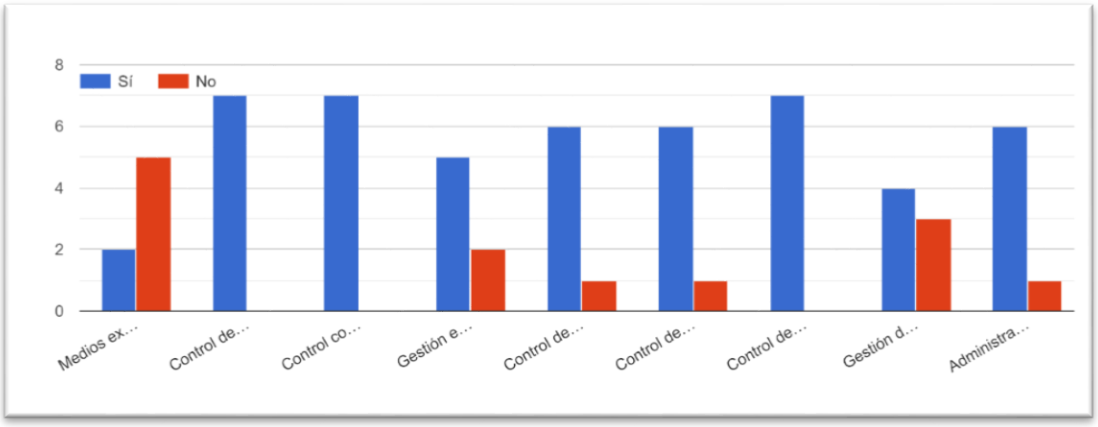
Figura 10:
Pregunta 9.
¿Dispone de servidores centrales de datos de la empresa?



Nota: Tomado de Formulario de Google Encuesta de Seguridad Informática, 2022.

En relación a la pregunta nueve sobre servidores centrales, la respuesta fue la siguiente: 85,7% señala que si dispone de servidores centrales de datos y el 14,3% señala que no dispone de servidores centrales de datos.

Figura 11*:*
Pregunta 10.
¿Existen controles de seguridad implementados en los aplicativos utilizados en la empresa?



Nota: Tomado de Formulario de Google Encuesta de Seguridad Informática, 2022.

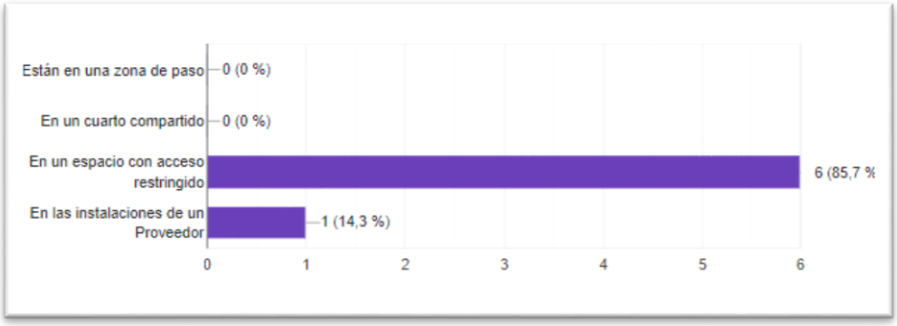
En relación a la pregunta diez sobre controles de seguridad implementados, la respuesta fue la siguiente: En relación a controles de seguridad implementados en Medios extraíbles de Datos solamente dos empresas tienen implementados controles; en relación a controles de seguridad implementados en Control de acceso: privilegios de usuarios las seis empresas señalan que tienen implementados controles; en relación a controles de seguridad implementados en Control contra software malicioso las siete empresas señalan que tienen implementados controles; en relación a controles de seguridad implementados en Gestión en la entrega de servicios de terceros dos empresas indican que no tiene implementados controles; en relación a controles de seguridad implementados en Control de Acceso a Internet solamente una empresa indica que no tiene implementados controles; en relación a controles de seguridad implementados en Control de Acceso a correo solamente una empresa indica que no tiene implementados controles; en relación a controles de seguridad implementados en Control de Acceso/seguridad de redes alámbricas e inalámbricas las siete empresas señalan que tienen implementados controles; en relación a controles de seguridad implementados en Gestión de incidentes solamente cuatro empresas tienen implementados controles; en relación a controles de seguridad implementados en Administrar permisos solamente una empresa indica que no tiene implementados controles.

Figura 12:
Pregunta 11.
¿Qué tecnologías utiliza en su empresa?

Nota: Tomado de Formulario de Google Encuesta de Seguridad Informática, 2022.

En relación a la pregunta once sobre tecnologías utilizadas, la respuesta fue la siguiente: seis empresas señalan que utilizan correo electrónico, página web y servidores propios; cinco empresas señalan que realizan teletrabajo; y seis empresas consultadas indican que cuentan con dispositivos móviles.

Figura 13:
Pregunta 12.
¿Dónde se encuentran los servidores y routers de su organización?



Nota: Tomado de Formulario de Google Encuesta de Seguridad Informática, 2022.

En relación a la pregunta doce sobre dónde se encuentran ubicados los servidores y routers, la respuesta fue la siguiente: seis empresas señalan que se encuentran ubicados en espacios con acceso restringido y una empresa indica que las instalaciones son de un proveedor.

CAPÍTULO II:

1.1. Fundamentos teóricos aplicados

Seguridad Informática: Está enfocada a la protección de elementos vulnerables del sistema informático, asegura los recursos del sistema de una organización que pueden ser software, hardware y datos; con respecto a los datos se pretende asegurar que quienes accedan y modifiquen la información de la organización sean personas acreditadas y autorizadas. (Triviño, 2019).

Infraestructura de la red. - La infraestructura de red de una empresa está compuesta por cada uno de los activos de hardware y software que permiten la conexión de red, la conexión de usuarios, procesos, aplicaciones, servicios, y redes externas hacia el Internet (Garbis y Chapman, 2021). Cuando se trata de enfrentarse a la pérdida del control y soberanía de los datos y el riesgo de seguridad, el principal objetivo de la seguridad de la infraestructura de la red es evitar y mitigar los riesgos, ante posibles ataques o amenazas a sus sistemas.

Elementos de la infraestructura de TI

Hardware. - Incluye todo el equipamiento físico tales como servidores, centros de datos, PC, computadoras personales, enrutadores, switches, routers y otros equipos.

Software. – Son todas las aplicaciones que utiliza la organización, tales como, sistemas operativos, servidores web, sistemas de gestión.

Redes. – La comunicación, la gestión y las operaciones entre sistemas externos e internos se debe a que todos los elementos de la red están interconectados.

Trusted Network Connect. – La Conexión de red de confianza por sus siglas en inglés (TNC), es una arquitectura abierta que proporciona especificaciones para la visibilidad del punto final de la red, permite monitorear y ayuda en la administración de políticas para la conocer y controlar quién y qué se conecta en su red, TNC también permiten la aplicación del control de acceso otorgando o bloqueando el acceso, para esta función se basa en la autenticación, el comportamiento del usuario, cumplimiento de dispositivos y automatización de la seguridad, ayuda con a gestionar el riesgo en una extensa gama de dispositivos informáticos que son parte de una red además de ayudar a verificar y monitorear los requisitos mínimos que están disponibles en el entorno (IBM Corporation., 2021).

TNC hace cumplir las reglas de control de acceso garantizando que únicamente los usuarios autorizados ingresen y tengan acceso a los recursos de la red.

Network Access Control. – Control de Acceso a la red por sus siglas en inglés NAC, acorde a Cisco Systems, Inc. (2022), esta tecnología está enmarcada en la seguridad en la red, mediante la aplicación de técnicas y mecanismos, determina que los dispositivos deban cumplir con requisitos predeterminados por el administrador, antes de permitir el acceso a la red y así previniendo posibles ataques y asegurar de esta forma que los dispositivos conectados a una determinada red determinada cumpla una serie de requisitos previamente establecidos por el administrador. Esta tecnología está basada en el cliente proveyendo de más detalle en la información de los dispositivos, la desventaja de esta tecnología es que se requiere la instalación de la misma en cada uno de los equipos de la red.

Funcionalidades de Network Access Control (NAC). – Acorde a Cisco Systems, Inc. (2022), esta tecnología proporciona adecuadas funciones en el registro para clientes VPN, clientes inalámbricos y dominios de directorio activo de Windows. Permite descubrir a cada dispositivo presente en la red y de esta manera permite el control del comportamiento del mismo, de esta forma puede detectar dispositivos infectados. No necesita de la intervención humana, la configuración de la red se realiza de forma dinámica. Establece un entorno seguro, mediante la aplicación de políticas de acceso.

Soluciones existentes. – Algunas empresas como CISCO y Microsoft han desarrollado estrategias, tecnología y soluciones para la interoperabilidad de los dispositivos.

Network Access Protection. - Protección de acceso a la red por sus siglas en inglés NAP, es una tecnología desarrollada por Microsoft presenta un conjunto de componentes del sistema operativo que controlan el acceso a redes privadas de una organización; pueden definir políticas para los requisitos de salud del sistema. Las políticas de NAP garantizan que estas y otras características estén implementadas y actualizadas antes de que se permita el acceso del dispositivo terminal a la red. Los dispositivos que no cumplen pueden tener su acceso restringido o bloqueado por completo. Esa plataforma por sí sola no proporciona los componentes necesarios para acumular y evaluar los atributos del estado de salida de un dispositivo, necesita agentes de estado y validadores del estado del sistema para proporcionar la validación y el cumplimento de las políticas de la red. (Candela,2020)

Con el aumento del uso de dispositivos inteligentes que se conectan a las redes empresariales, también se ha agravado el tema de las grietas de seguridad y a pesar de que existan políticas de seguridad siguen apareciendo casos de robo de información confidencial, acceso de malware que afecte la integridad de la red y la posibilidad de ataques que puedan

dañar la infraestructura de la red y perdida o daño de la información. (Abad et al., 2019), para este tema se toman en cuenta los artículos 178 y 190 de Código Integral Penal

«Artículo 178.- Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años» Código Orgánico integral Penal (COIP). Ley 0. Registro oficial del 10 de febrero de 2014 (Ecuador).

«Artículo 190.- Será sancionada con pena privativa de libertad de uno a tres años La persona que utilice fraudulentamente un sistema, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.» Código Orgánico Integral Penal [COIP]. Ley 0. Registro oficial del 10 de febrero de 2014 (Ecuador).

Valor aproximado que gasta anualmente en seguridad una empresa. - Según refleja la investigación de Kaspersky (2021), el presupuesto de TI dedicado para seguridad y ciberseguridad en PYMES de Latinoamérica ha pasado de $114,000 a $250,000, y de $13 millones a $20 millones para grandes empresas. Solo ente el año 2019 y 2020. Una empresa pequeña gasta anualmente un 18% de su presupuesto total de tecnologías de información en seguridad, lo que representa un valor entre $1,000 y $5,000. En Latinoamérica el presupuesto en seguridad informática hasta el año 2021 ascendió a 29% del presupuesto total de TI; la expectativa para el año 2024 para todas las empresas de Latinoamérica es que el presupuesto para seguridad informática aumente en 16%; como se puede observar en la Figura 14; la proyección hasta el 2024 asegura que el gasto de las empresas en ciberseguridad ascienda y a los ocho mil millones de dólares.

A pesar de las altas expectativas sobre inversión en ciberseguridad, se espera que, para el año 2024, el 9% de las PYMES y el 13.5% de las grandes empresas latinoamericanas reduzcan su gasto en seguridad informática, aduciendo que los altos directivos no ven la necesidad de invertir en temas de ciberseguridad y otros explican que esos temas han sido asumidos por empresas de outsourcing.

Figura 14:
Cálculo del presupuesto de seguridad informática.

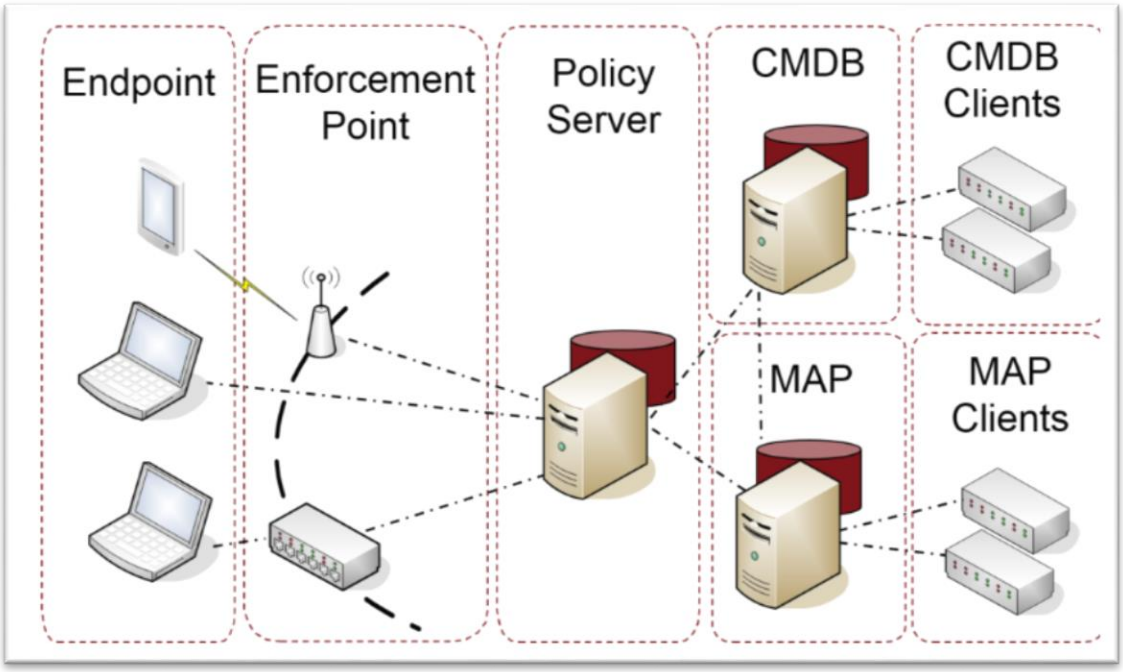
Nota: Tomado de https://calculator.kaspersky.com, 2021. Se respetan todos los derechos del autor.

1.2. Descripción de la propuesta

En el análisis de los métodos de control de acceso se realiza una tabla comparativa entre los tres principales métodos de control de acceso a la red (Tabla 3), las ventajas de cada método (Tabla 1) y las desventajas de cada método (Tabla 2), llegando a la conclusión que la más adecuada, puede ser TNC, ya que es la más completa porque además de que es una arquitectura abierta, ofrece la posibilidad de interoperabilidad de los dispositivos finales de cualquier fabricante; el costo beneficio de la implementación de la arquitectura TNC, se considera porque no solo es un estándar si no como una solución que se acopla a la necesidad de las organizaciones. La meta de TNC es reemplazar a las soluciones NAC y NAP que son propietarias de dos marcas que no interactúan libremente.

Estructura general

Figura 15:
Arquitectura TNC



Nota: Tomado de Trusted Network Communications, 2021. Se respetan todos los derechos del autor.

a. Explicación del aporte

En la Figura 15 se puede ver la infraestructura de un frameworks TNC, en el desarrollo de la propuesta de este proyecto se desarrolló una comparativa para encontrar las ventajas y desventajas de los tres métodos de control de acceso analizados, por este motivo que se propone TNC como la elección alternativa para pequeñas y medianas empresas.

b. Técnicas

En el presente trabajo se utilizó técnicas de investigación bibliográfica para indagar sobre los conceptos del tema escogido y revisar trabajos desarrollados previos a esta investigación; para este trabajo se utilizó la herramienta encuesta que se aplicó a los profesionales que sean los encargados de la seguridad de sus empresas, la encuesta estuvo compuesta por 12 preguntas direccionadas a personal de TI, las opiniones brindadas se podrán visualizar en el Anexo 1.

1.3. Validación de la propuesta

Para la validación de la propuesta se mostrará los conceptos generales, principales componentes, requisitos generales de TNC.

Según un nuevo estudio de Trusted Network Communications (2021) debido al gran avance de las empresas y organización, además de la evolución constante del entorno informático, TCG desarrollo el estándar Conexión de red de confianza (TNC), fue desarrollada originalmente como un estándar para el control de acceso a la red, donde su principal objetivo era aplicar políticas al punto final de varios proveedores; a partir del año 2009 se anunciaron especificaciones ampliadas para incluir automatización en la seguridad de TNC, donde se incluyen sistema de control industrial (ICS) y seguridad (SCADA), además el monitoreo y cumplimiento de políticas a los puntos finales. Esta arquitectura sigue en continua evolución, ampliando el actual sistema de extremo a extremo para casos de uso tradicionales y otras áreas emergentes como infraestructura de red, Internet de las cosas (IoT), movilidad y aplicaciones en la nube entre otras.

Las especificaciones habilitadas de TNC:

Visibilidad de la red: ¿quién está en la red y a qué intenta acceder?

Cumplimiento del punto final: ¿los dispositivos en la red son seguros y el comportamiento del usuario y dispositivo es apropiado?

Cumplimiento de la red: la capacidad de bloquear usuarios, dispositivos y comportamientos no autorizados y otorgar niveles apropiados de acceso a los dispositivos autorizados.

Automatización de la seguridad: compartir información en tiempo real sobre el entorno sin exponer datos.

¿Por qué escoger TNC?

Los estándares de TNC integran componentes de seguridad en el terminal, la red y los servidores en una defensa inteligente, receptiva y coordinada.

El uso de protocolos y esquemas estandarizados ofrece beneficios tanto para los usuarios como para los implementadores de soluciones tecnológicas. Para los usuarios, el uso de protocolos examinados públicamente ayuda a proteger los datos en tránsito, reduce la dependencia de soluciones de un solo proveedor y permite una flexibilidad arquitectónica que satisface las necesidades de innumerables casos de uso. Para los implementadores, los

estándares pueden ayudar a satisfacer las demandas de los organismos reguladores internacionales y nacionales, simplificar la interoperabilidad con otros productos de otros fabricantes y brindar más valor a los clientes.

Los estándares TNC:

Brindan una amplia gama de beneficios: Los estándares de TNC tienen un historial probado en la entrega de soluciones interoperables para abordar la seguridad de terminales, redes y servidores.

Se implementan ampliamente en escenarios de producción reales. Una amplia gama de clientes de muchos sectores (gobierno, atención médica, finanzas, comercio minorista y educación, entre otros) se benefician de las soluciones de seguridad interoperables basadas en estándares TNC.

Son completamente independientes del proveedor. Las soluciones basadas en TNC aprovechan la infraestructura de red existente en un entorno de producción, agregando valor a la inversión existente.

Son flexibles; admiten una amplia gama de opciones de evaluación (identidad, salud, comportamiento y ubicación; seguridad basada en hardware y software; y evaluación y monitoreo previos y posteriores a la admisión). Los estándares de TNC también se adaptan a cambios rápidos y pueden adaptarse al panorama de seguridad en evolución.

¿Cómo funciona la arquitectura?

TNC facilita la recopilación de información sobre un punto final y la entrega segura de esa información a otros componentes del entorno.

Elementos clave:

Puntos finales: Son cualquier entidad, física o virtual, que se puede conectar a una red.

Puntos de aplicación: Consumen las decisiones de control de acceso de un servidor de políticas y las aplican a las solicitudes de los puntos finales.

Servidores de políticas: Recopilan y evalúan la información sobre la postura de los puntos finales y toman decisiones de control de acceso basadas en el contexto de los puntos finales y comunican esas decisiones a los puntos de aplicación.

Bases de datos de gestión de la configuración (CMDB): almacenan las mediciones recogidas de los puntos finales.

Puntos de acceso a metadatos (MAP): Proporciona una coordinación centralizada para los productores y consumidores de información sobre redes y seguridad.

Clientes MAP: Publican, buscan y se suscriben a las actualizaciones sobre información de puntos finales y entornos a través de un MAP.

Una misma entidad puede asumir varios roles; por ejemplo, un servidor de políticas puede ser también un cliente de punto de acceso a metadatos (MAP) y un cliente de bases de datos de gestión de la configuración (CMDB).

Para IBM Corporation (2021). Existen cuatro componentes principales de Conexión de red de confianza (TNC).

Servidor de red de confianza (TNC).- Es el encargado de identificar y verificar a los clientes que se van añadiendo a la red.

Gestión de parches de (TNC). - El servidor de Trusted Network Connect (TNC) se integra con el Asistente de gestión de actualización de servicios (SUMA) y cURL para proporcionar una solución de gestión de parches.

Cliente de red de confianza (TNC).- Es el encargado de proporcionar la información necesaria para el servidor de TNC para que realice la verificación.

Referenciador de IP de red de confianza. - El servidor (TNC) inicia automáticamente la verificación de los clientes que son parte de la red. El referenciador de IP detecta los nuevos clientes a los que da servicio envía sus direcciones IP al servidor de TNC. El servidor de TNC verifica el cliente en lo que respecta a la política que está definida.

El servidor (TNC) identifica los clientes que se añaden a la red e inicia una verificación sobre ellos.

El cliente TNC proporciona la información de nivel de conjunto de archivos requerida al servidor para su verificación. El servidor determina si el cliente está en el nivel configurado por el administrador. Si el cliente no está conforme, el servidor del TNC notifica al administrador la corrección necesaria.

El servidor TNC inicia las verificaciones de los clientes que intentan acceder a la red. El servidor del TNC carga un conjunto de verificadores de medidas de integridad (IMV) que pueden

solicitar las medidas de integridad de los clientes y verificarlas. El servidor del TNC es un marco que carga y gestiona varios módulos IMV. Para verificar un cliente, se basa en las IMV para solicitar información a los clientes y verificarlos.

Requisitos del TNC. - Para utilizar plenamente todas las funciones de cada componente del TNC, debe comprobar que los requisitos mínimos están disponibles en su entorno.

1.4. Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 4

Matriz de Articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
La Conexión de red de confianza (TNC)	Estándar para el control de acceso a la red, donde su principal objetivo es aplicar políticas al punto final.	La metodología utilizada fue la Bibliográfica.	Fuente bibliográfica	Es una alternativa de código abierto y que en la actualidad quiere reemplazar a soluciones costosas y hoy en día cuenta con el apoyo de importantes empresas	Se desarrolló una comparativa para encontrar la mejor alternativa para pequeñas y medianas empresas.
Análisis de elementos de la red	Identificar los controles de seguridad utilizados en la empresa	Se determina las características de los dispositivos	Encuesta	57,1% desconoce las aplicaciones y dispositivos que usan los empleados y el 42,9% conoce estos elementos.	Se utilizó la herramienta encuesta que se aplicó a los profesionales de TI.

Nota: Elaboración propia, 2022.

CONCLUSIONES

En la investigación sobre la comparativa de métodos de control de acceso de una infraestructura de red empresarial, se pudo evidenciar los beneficios que cada uno de estos métodos ofrece; toda empresa tiene la opción de escoger el mejor método que mejor se acople a sus necesidades y a reducir costos, aumentando la competitividad y la productividad; la arquitectura TNC, se considera como una solución que se acopa a las necesidades de las PYMES por el costo beneficio de la implementación.

A pesar de que la elección de una alternativa de código abierto es rechazada por las grandes empresas por el tema de inversión de tiempo de su equipo de desarrollo, la ventaja de instalar TNC es que se acopla a infraestructuras preexistentes; gracias al apoyo de grandes empresas los componentes de la arquitectura TNC pueden ser implementados por múltiples proveedores sin la necesidad de estar atado a una marca o proveedor específico.

Es importante que la comunidad educativa añada a sus mallas curriculares el desarrollo de alternativas de código abierto, permitiendo dar soporte a organizaciones y empresas además de que se establece relaciones para la creación de plazas de trabajo.

Se identificó y contextualizó los fundamentos teóricos aplicados en el proyecto sobre los métodos de control de acceso y se determinó los tres principales mecanismos que ofrece el mercado para mejorar el control de acceso de la infraestructura de una red empresarial.

Se utilizó métodos investigativos tales como los bibliográficos, descriptivos y la aplicación de herramientas como una encuesta para determinar los mecanismos para mejorar el nivel de seguridad de acceso en la infraestructura de una red empresarial; fundamentalmente la aplicación de los tres principios, aplicación de políticas, la adopción de una estrategia de privilegios mínimos y la aplicación de control de acceso estricto; acorde a la encuesta se determinó que muchas empresas toman mucho en cuenta la implementación de los controles de seguridad tales como privilegios de usuarios, gestión en la entrega de servicios de terceros, el control de acceso internet y a correos, control de acceso y seguridad de redes alámbricas e inalámbricas y la administración de permisos.

Acorde a la encuesta realizada se evidencia que un 57,1% de las empresas desconocen que aplicaciones y dispositivos extraíbles utilizan sus empleados dentro de sus redes ya sea en las propias instalaciones o fuera de ella; muchas empresas no tienen implementados controles de seguridad para medios extraíbles.

Según el estudio se ha determinado que el gasto para seguridad hasta el 2020 en pequeñas y medianas empresas supero los doscientos cincuenta mil dólares, el gasto anual de una pequeña empresa se encuentra entre los mil y cinco mil dólares; para el año 2024 la expectativa para Latinoamérica es que el presupuesto para seguridad informática aumente en 16% y el gasto anual en temas de hardware, software y servicios TI aumente un 12 %**.**

RECOMENDACIONES

Se recomienda seguir analizando los métodos de control de acceso y los mejores mecanismos de seguridad para la PYMES, debido a que este tipo de empresas son la más vulnerables y no cuentan con presupuesto para mantenerse a salvo de ataques.

Se recomienda incentivar a las PYMES a que tomen conciencia y utilicen todas las opciones disponibles para reforzar sus sistemas de protección, que no dejen de lado el Control de Acceso a Red tanto externa como interna, que en lo posible recurran a las soluciones de seguridad de acceso gratuitas.

Es imprescindible que se motive a las empresas y organizaciones a comprender los beneficios que les puede ofrecer contar con mecanismos para mejorar el nivel de seguridad en sus redes; enfocarse en que cada uno de los elementos que se utilizan en la red deben tener un tratamiento controlado.

Se recomienda realizar una actualización del presente trabajo, continuando con mejoras que ayuden a reforzar el desarrollo de infraestructuras fiables, sostenibles, resilientes y de calidad, para apoyar el desarrollo económico de la PYMES.

Es recomendable que las universidades sean un apoyo para las organizaciones y empresas, en temas de desarrollo de códigos abiertos; como respaldo para que las empresas analicen el costo beneficio de una implementación que ayude a mitigar riesgos, ante posibles ataques o amenazas a sus sistemas, se debe preparar a profesionales para que tengan los conocimientos y las habilidades necesarias.

Esta visión sustenta el propósito general de la Estrategia Nacional de Ciberseguridad para asegurar que todos los actores, incluyendo el Gobierno Nacional, las organizaciones públicas y privadas, la academia y la sociedad civil en Ecuador, hagan un uso responsable y seguro del entorno digital, a través del fortalecimiento de la cultura y sus capacidades para identificar y gestionar los riesgos de ciberseguridad de las actividades derivadas del uso de la información

digital, maximizando los beneficios en la seguridad de los servicios para los ciudadanos y generando mayor prosperidad económica, política y social.

BIBLIOGRAFÍA

Abad Parrales, W. Cañarte Rodríguez, T. Villamarín Cevallos, M. Menzones Santana, H. Delgado Pilozo, Á. Toalá Arias, F. Figueroa Suárez, J. & Romero Castro, V. (2019*). La ciberseguridad práctica aplicada a las redes, servidores y navegadores web* (Vol. 59).

Ashcraft, A. Satran, M. (2019, agosto 23). *Network Access Protection*. Microsoft.com. Recuperado el 07 de febrero de 2022 de https://docs.microsoft.com/en-us/windows/win32/nap/network-access-protection-start-page

Banco Interamericano de Desarrollo & Organización de los Estados Americanos. (2020). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe.* https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Bejarano, J. Garces, O. Morales Reséndiz, R. Palmer, A. Martins de Almeida, G. Marangunich, J. Castaño, J. Rueda, S. Linares Vásquez, M, Ortiz-Casas, C. Colmenares Duque, A. Rincon, J. Quijano, A. Barrera, M & Castiblanco, S. (2019). *Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina.*

Candela Quijije, W. D. (2020). *Estudio de la Tecnología NAC para mejorar la seguridad en redes de área local. Caso de estudio: Cooperativa de la Policía Nacional Agencia Matriz*. [Tesis de maestría, Pontificia Universidad Católica del Ecuador]. Repositorio Institucional – Pontificia Universidad Católica del Ecuador.

Cisco Systems, Inc. (2022) *¿Qué es el control de acceso a la red?* https://www.cisco.com/c/es_mx/products/security/what-is-network-access-control-nac.html

Flores, J. (2017). *Análisis de las Soluciones de Control de Acceso a la Red (NAC) para mejorar la seguridad externa e interna de redes corporativas.* [Tesis de maestría, Escuela Superior Politécnica De Chimborazo]. Repositorio Institucional – Escuela Superior Politécnica De Chimborazo.

Garbis, J. & Chapman J. (2021). *Network Infrastructure.* Pp. 93–103 in Zero Trust Security. Springer.

IBM Corporation. (5 de marzo de 2021). *Trusted Network Connect concepts*. Corporación IBM. Recuperado el 10 de diciembre de 2021 de https://www.ibm.com/docs/en/powersc-standard/1.2?topic=tnc-concepts.com

Jácome, S. (2018). *Implementación de un prototipo de control de registros de acceso mediante tecnología NFC.* [Tesis de ingeniería, Universidad Tecnológica Israel]. Repositorio Institucional –Universidad Tecnológica Israel.

Kaspersky. (2021, 21 febrero). *El presupuesto en ciberseguridad aumenta en empresas, pese a los recortes por COVID-19.* Recuperado 10 de agosto de 2022, de https://latam.kaspersky.com/about/press-releases/2021_el-presupuesto-en-ciberseguridad-aumenta-en-empresas-pese-a-los-recortes-por-covid-19

Kuzmin, A. (2017). *Blockchain-Based Structures for a Secure and Operate IoT.* Pp. 1–7 in 2017 Internet of Things Business Models, Users, and Networks. IEEE.

Ma, B. Ye, Z. Zhang, X. Chen, J. Zhou, Y. & Xiia, Q. (2020). *Security of Edge Computing Based on Trusted Computing. Pp. 132–37 in Proceedings - 2020 6th International Symposium on System and Software Reliability, ISSSR 2020*. Institute of Electrical and Electronics Engineers Inc.

Oficina Internacional del Trabajo. (2020). *El Teletrabajo Durante La Pandemia de COVID-19 y Después de Ella Guía Práctica.* edited by I. del T. Oficina. Suiza.

Ortiz Pérez, J. S. (2022). *Análisis y estudio preliminar para la optimización de la infraestructura de red de la información y comunicación de la empresa constructora INGPRA.* [Tesis de ingeniería- Universidad Santo Tomás.] Repositorio Institucional –Universidad Santo Tomás.

Shi, Y. Zhang, Y. & Chen, J. (2020). *Cross-layer QoS enabled SDN-like publish/subscribe communication infrastructure for IoT*. China Communications, 17(3), 149-167. doi: 10.23919/JCC.2020.03.013.

Simbaña, Y. (2020). *Implementación de una red LAN con acceso WAN, en la empresa GMS, administrada de acuerdo con la norma establecida por el Instituto SANS-SysAdmin Audit, Networking and Security Institute*. [Tesis de ingeniería, Universidad Tecnológica Israel]. Repositorio Institucional –Universidad Tecnológica Israel

Triviño, Ignacio. (2019). *Seguridad y Alta Disponibilidad.* Pp. 1–22 in Seguridad y alta disponibilidad, editado por J. Moreno Pérez.

Trusted Network Communications. (2021, 5 marzo). *Trusted Computing Group*. Recuperado 2 de agosto de 2022, de https://trustedcomputinggroup.org/resource/trusted-network-communications-faq

Ugarte, C. (2018). *Diseño de un Sistema de control de acceso en redes WLAN/VLAN.* [Tesis de ingeniería, Universidad Politécnica de Madrid]. Repositorio Institucional – Universidad Politécnica de Madrid

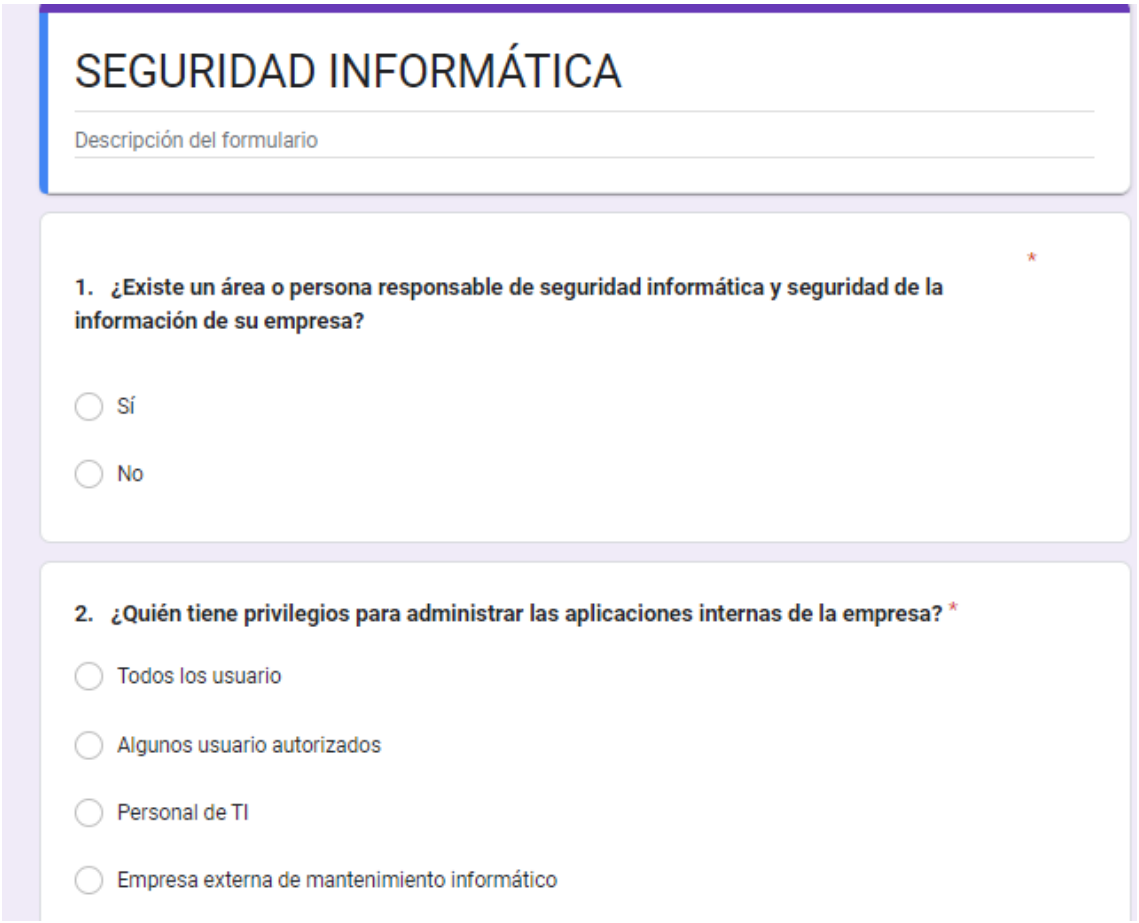
Ynzunza, Carmen. Izar, J. Bocarando, J. Aguilar, Felipe & Larios, Martin. (2017). *El Entorno de La Industria 4.0: Implicaciones y Perspectivas Futuras Implications and Perspectives of Industry 4.0.*

Zhou, H., Wang, X., Umehira, M., Chen, X., Wu, C., & Ji, Y. (2021). *Wireless access control in edge-aided disaster response: A deep reinforcement learning-based approach*. IEEE Access, 9, 46600-46611.

ANEXOS

ANEXO 1

FORMATO DE ENCUESTA



SEGURIDAD INFORMÁTICA

Descripción del formulario

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

- ○ Sí
- ○ No

2. **¿Quién tiene privilegios para administrar las aplicaciones internas de la empresa?** *

- ○ Todos los usuario
- ○ Algunos usuario autorizados
- ○ Personal de TI
- ○ Empresa externa de mantenimiento informático

3. ¿Que tipo de herramientas de seguridad tiene implementado en su empresa? Puede seleccionar varias alternativas

- [ ] Software
- [ ] Hardware
- [ ] No tiene
- [ ] Otro

4. ¿Qué software utiliza en la empresa para controlar software malicioso? Puede seleccionar varias alternativas *

- [ ] Antivirus
- [ ] Anti-Spam
- [ ] Antispyware
- [ ] Contrafuego/firewall
- [ ] Otro

5. ¿Conoce las aplicaciones y dispositivos extraíbles que utilizan los empleados en la red de su empresa dentro y fuera de ella? *

- ( ) Si
- ( ) No

6. ¿Cuenta con algún mecanismo de control de seguridad para evitar el acceso a la red de su empresa desde dispositivos desconocidos? *

- ( ) Si
- ( ) No

7. **¿Cree que es necesario aplicar controles de seguridad para evitar robo o daño de información importante para la empresa?** *

- ◯ Totalmente de acuedo
- ◯ De acuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ En Desacuerdo

8. **¿Tiene definida algún tipo de política de gestión de contraseñas?** *

- ◯ No
- ◯ Sí, el usuario escoge su contraseña
- ◯ El servidor central obliga a cambiar la contraseña cada cierto tiempo
- ◯ Sí, tenemos una política de gestión de contraseñas, bien definida y de obligado cumplimiento

9. **¿Dispone de servidores centrales de datos de la empresa?** *

- ◯ Sí
- ◯ No

10. ¿Existen controles de seguridad implementados en los aplicativos utilizados en la empresa? *

	Sí	No
Medios extraíbles de Datos	○	○
Control de acceso:privilegios de ...	○	○
Control contra software malicioso	○	○
Gestión en la entrega de servicio...	○	○
Control de Acceso a Internet	○	○
Control de Acceso a correo	○	○
Control de Acceso/seguridad de ...	○	○
Gestión de Incidentes	○	○
Administrar permisos	○	○

11. ¿Qué tecnologías utiliza en su empresa? Puede seleccionar varias alternativas *

- ☐ Correo electrónico
- ☐ Página web
- ☐ Servidor(es) propio(s)
- ☐ Teletrabajo
- ☐ Dispositivos móviles (tablet / smartphone / portátiles) con información de empresa

12. ¿Dónde se encuentran los servidores y routers de su organización? *

- ☐ Están en una zona de paso
- ☐ En un cuarto compartido
- ☐ En un espacio con acceso restringido
- ☐ En las instalaciones de un Proveedor