Universidad Cenfotec

Maestría en Ciberseguridad

Escuela de Informática

Tema: Propuesta de Herramienta para determinar la viabilidad técnica de implementación de una Arquitectura Zero Trust

Elaborado por:

Ulate Castro, José Pablo

Mayo, 2022

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Ulate Castro José Pablo.**

Alonso Ramírez

Digitally signed by Alonso Ramírez
Date: 2022.07.08 19:35:08 -06'00'

M. Sc. Luis A. Ramírez Jiménez
Tutor

MSEG. Aissen Contreras Castro
Lector 1

ALVARO CORDERO PEÑA (FIRMA)

Firmado digitalmente por ALVARO CORDERO PEÑA (FIRMA)
Fecha: 2022.07.12 22:14:10 -06'00'

MAP. Álvaro Cordero Peña
Lector 2

San José, Costa Rica, 4 de julio de 2022

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-

Tabla de contenido

Índice de tablas

Tabla de figuras

Abstract

La transformación digital que se vive continuamente en diferentes ámbitos de la vida para mejorar los procesos, optimizar los recursos, gestionar las tareas y expandir las oportunidades hacen que sea necesario adaptarse rápidamente a las nuevas tendencias para mantenerse vigentes. La ciberseguridad no escapa a este dinamismo y los mecanismos que hace algún tiempo se consideraban seguros y adecuados, puede que ya no lo sean tanto o no se adapten a la realidad actual y la forma en cómo se hacen las cosas. Tradicionalmente, el modelo de seguridad que se planteó es un esquema perimetral, donde el principio de confianza se basa en la ubicación de los usuarios y dispositivos, como un castillo medieval rodeado por un foso. Se parte del hecho de que todos los elementos que están dentro del perímetro del castillo son confiables y que las amenazas vendrán únicamente del exterior. El problema de este enfoque es que un atacante ganara acceso a la red tendría acceso a todos los recursos dentro de ella. La arquitectura Zero Trust plantea una filosofía distinta al modelo tradicional, *no confiar nunca, verificar siempre*. La confianza que tradicionalmente se le ha dado a los usuarios y recursos dentro de la red es una vulnerabilidad (Kindervag, 2010). En la actualidad, los usuarios y los dispositivos ya no están únicamente en las instalaciones de las empresas y se han trasladado fuera del perímetro, incluso las mismas aplicaciones empresariales pueden encontrarse fuera de la red corporativa, lo que genera un entorno donde los datos pueden accederse desde cualquier lugar del mundo. La arquitectura Zero Trust busca construir defensas alrededor de cada una de las entidades

(usuarios, datos y dispositivos), sin importar el lugar donde se encuentren. La investigación se plantea dentro de un contexto innovador, pues la adopción de la arquitectura Zero Trust ha crecido paulatinamente durante los últimos años y se espera que cada vez sean más las organizaciones que se sumen a este modelo, lo que hace necesario el desarrollo de herramientas de autoevaluación que permitan a las empresas identificar los puntos de mejora para lograr una arquitectura más robusta.

Palabras clave: Zero Trust, arquitectura, usuarios, datos, red, seguridad y evaluación.

Capítulo 1. Introducción

1.1 Generalidades

Este es un trabajo de investigación aplicado, es decir, se desarrolla una propuesta que pueda aplicarse por cualquier organización que necesite evaluar su postura de seguridad en el marco de una arquitectura Zero Trust. Lo anterior a partir de un diagnóstico que les permita a los evaluadores conocer el estado actual de sus mecanismos de seguridad y encontrar los puntos de mejora.

1.2 Antecedentes del problema

La adopción de entornos en la nube por parte de las organizaciones ha crecido rápidamente incluso antes de la pandemia de COVID-19. Sin embargo, durante la pandemia, se afianzó con mayor fuerza, cambiando las estrategias y operaciones del negocio (Flexera, 2021). Esta transición acelerada hacia un modelo de negocio en la nube implica también preocupaciones para las empresas, por ejemplo, un 81 % de las personas encuestadas en el Reporte Anual del Estado de la nube de Flexera indica que la seguridad es su mayor desafío en este nuevo modelo. Muchas de estas organizaciones no han considerado esquemas de seguridad que se adecuen a los entornos en la nube, como un modelo Zero Trust. Poder identificar los requerimientos para desarrollar un entorno de nube seguro utilizando una arquitectura Zero Trust es clave para garantizar la seguridad de la información, desde una postura de seguridad más sólida e integral.

Estudios recientes indican que, para el año 2020, el 60 % de las organizaciones en Norteamérica y 40 % en el ámbito global se encontraban trabajando en proyectos de seguridad que se relacionan con Zero Trust, lo que representa un aumento de un 275 % respecto al 2019 (Okta, 2020). Este crecimiento acelerado de empresas que han iniciado el proceso de adopción de la

arquitectura Zero Trust resalta la importancia de contar con herramientas de evaluación en las diferentes áreas del modelo.

1.3 Definición y descripción del problema

Parte del dinamismo tecnológico que se vive diariamente implica modernizar los modelos y sistemas de seguridad para proteger la información de las organizaciones ante las diversas amenazas a las que se pueden ver expuestas. Como resultado de esta dinámica, la monetización de la información y el creciente modelo híbrido para el manejo de datos entre soluciones *on-premise* y aplicaciones en la nube, la idea de un modelo de seguridad perimetral empieza a sonar extraña y hasta peligrosa. Asimismo, el modelo de negocio está cada vez más centrado en los datos, por eso, las soluciones de seguridad también deben serlo (Forrester, 2019).

En la actualidad, muchas organizaciones han tenido que movilizar sus fuerzas de trabajo que tradicionalmente se han encontrado entre sus instalaciones a zonas fuera del perímetro de la red para continuar operando. Esta movilización implica un riesgo inherente de que la información pueda ser comprometida con mayor facilidad por medio de un ciberataque, pues la protección establecida en el perímetro tradicional no se ha expandido a los diferentes lugares donde las personas se han movilizado. Este escenario demanda establecer nuevas operaciones y estrategias de seguridad para mitigar este riesgo.

Ante esta nueva perspectiva han surgido nuevos modelos de seguridad, como Zero Trust, el cual se enfoca en usuarios, activos y recursos, donde no se otorga una confianza implícita a los activos o cuentas de usuario basándose únicamente en su ubicación de la red. Por el contrario, el principio del modelo Zero

Trust establece que ningún actor, sistema, red o servicio que opere fuera o dentro del perímetro de seguridad es confiable (DoD, 2021). El acceso a los datos se otorga cuando el recurso es necesario y la autenticación (tanto del usuario como del dispositivo) se lleva a cabo antes de que se establezca la conexión. El enfoque es proteger los recursos, no segmentos de red, debido a que la ubicación dentro de la red ya no se considera como el componente principal de la postura de seguridad (NIST, 2019).

Un elemento importante en el desarrollo de un modelo Zero Trust es la gestión de la identidad. Uno de los principales problemas que se observan actualmente es la facilidad para suplantar la identidad de los usuarios, los dispositivos o servicios. Antes de que una identidad intente acceder a un recurso, las organizaciones deben verificar la identidad por medio de una autenticación sólida utilizando procesos de múltiples factores, asegurar que el acceso es compatible y de uso común para la identidad, seguir siempre los principios de privilegios mínimos y controlar el acceso de esa identidad a los recursos en función de las políticas de las organizaciones (Microsoft, 2021).

Ante la inminente adopción del modelo Zero Trust por parte de las organizaciones, es importante contar con herramientas de evaluación que permitan a las empresas diagnosticar si están preparadas para migrar sus sistemas hacia esta nueva arquitectura e identificar los recursos y ajustes que sean necesarios. Es necesario que las empresas puedan evaluar el modelo una vez que se ha implementado para determinar áreas de mejora.

1.4 Justificación

Como resultado de la investigación se busca desarrollar una herramienta de autoevaluación que permita medir el estado actual de cualquier organización con respecto a los principios establecidos por la arquitectura Zero Trust, lo que permite a las empresas observar las áreas de mejora para alcanzar un diseño de seguridad más robusto. Las empresas pueden medir su nivel de madurez respecto a la implementación de un modelo Zero Trust, esto permite identificar las brechas que deben atenderse a corto, mediano y largo plazo para alcanzar un estado óptimo deseado en la protección de la información de los sistemas críticos.

La herramienta de evaluación también permite a las diferentes gerencias de la organización (General, Tecnología, Seguridad de la Información) fortalecer su estrategia de ciberseguridad empresarial. Esto se puede hacer tanto desde la perspectiva de procesos como de controles técnicos automatizados para enfrentar las amenazas de seguridad emergentes que se relacionan con el teletrabajo, nómadas digitales y procesamiento de aplicaciones en la nube.

1.5 Viabilidad

La propuesta de la herramienta evaluativa para la implementación de un modelo Zero Trust es viable en el contexto actual marcado por una aceleración digital potenciado por la pandemia de la COVID-19. En este entorno, un gran porcentaje de las fuerzas laborales se ha movido fuera del perímetro empresarial, lo que convierte herramientas como el teletrabajo y el comercio electrónico en una nueva normalidad que, a la vez, genera una serie de riesgos adicionales en el proceso de proteger la información. Por ejemplo, McKinsey ha estimado que en Estados Unidos la pandemia comprimió en 3 meses el crecimiento del comercio

electrónico que se esperaba en 10 años. Este crecimiento abrupto debe alinearse lo más pronto posible a las arquitecturas de seguridad adecuadas, por lo que es importante evaluar en cada caso cuáles son los requerimientos y las brechas que se deben atacar para considerar que los datos se encuentran en un entorno seguro.

En el ámbito nacional, Costa Rica se ha incorporado recientemente como miembro de la Organización para la Cooperación y el Desarrollo Económico (OCDE), por lo que es de vital importancia alinear las políticas de seguridad digital a las recomendaciones que se plantearon por este ente, así como reforzar la estrategia de ciberseguridad en las diferentes organizaciones del estado para posicionarse de una mejor forma frente las evaluaciones realizadas por la Organización. Una de las recomendaciones hechas al país en la evaluación del año 2017 por parte del Comité de Políticas de Economía Digital de la OCDE fue implementar metodologías para monitorear y evaluar las actividades de protección de datos personales (Micitt, 2017). Una herramienta de evaluación del modelo Zero Trust permite identificar las áreas de mejora para proteger los datos bajo un modelo robusto y actualizado, mejorar los índices de seguridad organizacional, así como fortalecer la Estrategia Nacional de Ciberseguridad.

1.5.1 Punto de vista técnico

El autor de este proyecto cuenta con la experiencia profesional y académica dentro del ámbito de la investigación, pues ha desarrollado tareas que se relacionan con diversas arquitecturas de ciberseguridad, asimismo, ha participado en el desarrollo de mecanismos de autenticación y gestión de usuarios que se alinean a la temática desarrollada. Además, cuenta con certificaciones profesionales en el campo de la seguridad de la información que le permiten comprender el área de

estudio. Por otro lado, se cuenta con la guía necesaria para abordar el proyecto con un enfoque adecuado. Dentro del proceso investigativo que se desarrolla se recopila la documentación y experiencia de autores expertos en la materia que aportan al producto de la investigación.

1.5.2 Punto de vista operativo

La herramienta de evaluación para determinar la viabilidad de implementación de una arquitectura Zero Trust es aplicable al contexto nacional, donde cualquier empresa u organización puede ejecutarla. El modelo Zero Trust es una arquitectura internacional aplicable a cualquier tipo de industria, donde incluso se encuentran diferentes soluciones operativas en el mercado. Desde este punto de vista, se considera viable desarrollar la investigación sin interrumpir las operaciones productivas de las organizaciones.

1.5.3 Punto de vista económico

El resultado de la investigación genera un producto que puede ser aplicable en cualquier empresa en el ámbito nacional, lo que hace una contribución a las estrategias de ciberseguridad utilizando modelos de nueva generación orientados a marcos de referencia disruptivos que se adapten a las necesidades de negocio actuales. La herramienta resultante como producto de la investigación es una hoja de cálculo con múltiples pestañas y diversas formas de cálculo desarrollada en una plataforma abierta, por lo que no existirán gastos adicionales para compartir el archivo con diversas organizaciones. Además, los gastos asociados con el desarrollo de la investigación, en términos de tiempo o recursos, se costean por el

autor. Por este motivo, el desarrollo de la investigación es viable desde el punto de vista económico.

1.6 Objetivos

Para la generación de este documento se utiliza la taxonomía de Benjamín Bloom del año 1956, debido a que se adapta a los requerimientos iniciales y desarrollados posteriormente alrededor de la investigación. Esto permite un desarrollo escalonado de la temática de la investigación.

1.6.1 Objetivo general

Proponer una herramienta para determinar la viabilidad técnica de implementación de una Arquitectura Zero Trust aplicable a cualquier organización o empresa.

1.6.2 Objetivos específicos

- Describir los diferentes componentes de una arquitectura basada en el modelo Zero Trust.
- Diferenciar las áreas de la organización que deben evaluarse durante el proceso de diagnóstico.
- Desarrollar la herramienta con sus parámetros de evaluación.
- Clasificar los posibles resultados de la evaluación.
- Reconocer el nivel de madurez de la organización en la adopción del modelo Zero Trust.
- Elaborar una guía de ejecución de la herramienta.

1.7 Alcances y limitaciones

1.7.1 Alcances

Como resultado de la investigación se desarrolla una herramienta que le permita a las organizaciones, sin importar su sector o actividad, autoevaluar su postura actual de ciberseguridad desde la perspectiva de una arquitectura Zero Trust.

1.7.2 Limitaciones

Debido a que el objetivo de la investigación se relaciona con el desarrollo de una propuesta de un modelo de evaluación de una arquitectura Zero Trust aplicable a cualquier organización, al terminarla no se realiza una implementación de los elementos que se proponen en ninguna empresa en particular.

1.8 Marco de deferencia organizacional y socioeconómico

En el contexto de la aceleración digital, Costa Rica ha seguido una serie de pasos para alinearse a los estándares internacionales del mercado digital para lograr el desarrollo de actividades comerciales electrónicas, así como la atracción de inversiones extranjeras en este nicho. Uno de los componentes clave para el crecimiento de este modelo de negocio es asegurar la protección de la información y el desarrollo de plataformas de operación seguras. En esta línea, el país ha liderado un trabajo regional en el marco de la Red de Gobierno Electrónico de América Latina y el Caribe, iniciativa soportada por la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), en búsqueda de ser un *hub* de ciberseguridad para toda Latinoamérica (RedGealc, 2020).

En el año 2017, el Ministerio de Ciencia, Tecnología y Telecomunicaciones (Micitt) de Costa Rica presentó la Estrategia Nacional de Ciberseguridad con el

objetivo de diseñar un marco para orientar las acciones que el país puede tomar con respecto al uso seguro de las TIC, desarrollar la coordinación y cooperación entre las partes interesadas y promover medidas de educación, prevención y mitigación del riesgo de utilizar las TIC. Los esfuerzos por promover un entorno digital seguro vienen incluso de algunos en el pasado, en el año 2012 se creó un Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT) en el ámbito nacional, bajo el Micitt, por medio del Decreto n.º 37.052 para coordinar entre los diferentes interesados todo lo que se relaciona con información y seguridad cibernética y para formar un equipo de expertos en ciberseguridad. Esto con el fin de prevenir y responder a los incidentes cibernéticos contra las instituciones gubernamentales.

En el marco jurídico, Costa Rica ha mostrado importantes avances por medio de la Ley de Delitos Informáticos y la adhesión al Convenio de Budapest, este es el único instrumento internacional relativo a delitos informáticos y la prueba relacionada con los mismos, por lo que se ha acogido, de gran forma, en el ámbito internacional.

En el contexto social, el país se ha visto afectado por un importante volumen de casos de delitos cibernéticos, asociados principalmente con estafas en sucursales electrónicas bancarias y trámites en instituciones del estado, por medio de diferentes canales asociados con el *phishing*, ingeniería social y suplantación de identidad. Según los datos del Organismo de Investigación Judicial, en Costa Rica ocurre un intento de fraude electrónico cada 37 minutos, se registraron 1963 denuncias en 2017, 2795 en 2018, 3594 en 2019 y 4898 denuncias en 2020.

1.9 Estado de la cuestión

La transformación digital, acelerada por la pandemia de la COVID-19, cambió la forma en como opera el modelo de negocio de las organizaciones. La nueva normalidad que se vive invita a un entorno digitalizado y remoto, desde el comercio que ofrece sus productos en línea hasta los trabajadores que realizan sus tareas desde casa sin desplazarse a las oficinas de las empresas. Este nuevo modelo enfoca la productividad en la nube, dejando atrás arquitecturas tradicionales donde todos los datos, dispositivos y hasta usuarios se encontraban dentro del perímetro de la red organizacional. En la actualidad, el perímetro ya no existe, o bien se ha transformado en múltiples perímetros de microsegmentos de la red, donde los usuarios pueden conectarse a las redes corporativas desde cualquier lugar, en cualquier momento y desde cualquier dispositivo.

Este nuevo modelo de negocio implica también desafíos inherentes de seguridad. Ya no es suficiente un *firewall*, un analizador de tráfico o una VPN para garantizar la seguridad de la información y garantizar la identidad. El proceso de transformación digital mejora la agilidad empresarial y el flujo de información, pero amplía también la superficie de ataque y expone a las organizaciones a nuevas amenazas. Existen nuevas necesidades y requerimientos para cumplir con un modelo de seguridad robusto, adaptable y automatizado.

Zero Trust es un modelo de seguridad de red que se basa en un proceso estricto de verificación de identidad, donde solamente los usuarios y los dispositivos autenticados y autorizados pueden acceder los datos y las aplicaciones. El enfoque de la arquitectura es holístico, ya que se basa en el acceso con menos privilegios y en el principio de que ningún usuario o aplicación debe ser intrínsecamente confiable. Por el contrario, todo elemento se considera hostil y solo se establece una

relación de confianza con base en la identidad del usuario y el contexto, nunca según su ubicación en la red (Zscaler, 2021).

Las empresas deben adoptar un modelo Zero Trust para ser competitivas y asegurar los datos en entornos de nube o remotos. Para esto, es importante que puedan identificar que elementos necesitan para adoptar el modelo, diagnosticar su estado actual y evaluar como mejorar para llegar a un estado óptimo de seguridad.

1.9.1 Planificación de la revisión

Se formula en esta etapa una pregunta clara y definida del tema de investigación. Se hace una búsqueda de documentación existente en el tema con el objetivo de conocer el desarrollo académico que existe, posibles áreas de investigación y verificar que no se dupliquen los estudios realizados en otras publicaciones.

1.9.1.1 Formulación de la pregunta

La formulación de la pregunta ayuda a delimitar la búsqueda de información que sustenta el proyecto. El objetivo es encontrar respuestas que demuestren la contribución de este trabajo al campo de investigación y sea de utilidad para la población meta.

1.9.1.1.1 Foco de la pregunta

Para la presente investigación se busca centralizar la búsqueda de documentos técnicos que especifiquen los requerimientos y áreas de trabajo que deben analizarse para implementar una arquitectura Zero Trust, así como los

parámetros para medir el nivel de madurez en cada etapa del proceso de adopción del modelo.

1.9.1.1.2 Amplitud y calidad de la pregunta

Se establece en esta sección la pregunta de investigación que se desea responder, de forma clara y concisa, y que se basa en un problema por resolver. Se hace un listado de términos clave relevantes para la búsqueda de información y se consideran componentes clave como la población específica, exposición y eventos de interés. Se definen medidas por utilizar para medir el efecto con base en la pregunta a responder y el diseño de los estudios.

1. Problema

Como parte de la aceleración digital y las nuevas tendencias de negocio, muchas organizaciones han tenido que movilizar sus fuerzas de trabajo que tradicionalmente se han encontrado entre sus instalaciones a zonas fuera del perímetro de la red. Los datos y aplicaciones que tradicionalmente se almacenaban en servidores *on-premise* han migrado a soluciones híbridas o instaladas completamente en la nube, lo que hace que el acceso no se brinde por una ubicación en la red, sino validando la identidad de los usuarios, los dispositivos y los servicios.

Como solución para este nuevo modelo operacional, se han desarrollado arquitecturas aplicables a este esquema que proporcionen una mayor seguridad y garanticen la identidad y permisos de los usuarios, como Zero Trust. Sin embargo, muchas organizaciones desconocen el nivel de madurez de su postura actual de

seguridad y qué elementos o procesos se requieren para alcanzar un nivel óptimo aceptable. Las herramientas de medición y evaluación en el contexto de la arquitectura Zero Trust son escasas o no son aplicables para cualquier tipo de empresa, sin importar el tamaño o sector en el que operan.

2. Pregunta

Con la definición del problema anterior, se formula la siguiente pregunta de investigación: ¿Cuáles investigaciones se han llevado a cabo en el área de ciberseguridad para determinar la postura de una organización que desee implementar una arquitectura Zero Trust?

3. Palabras clave y sinónimos

Se hace un listado de palabras clave que se utilizan para la búsqueda e identificación de documentos y trabajos que se relacionan con la investigación. Las palabras que se seleccionaron son Zero Trust, ciberseguridad (*cybersecurity*), seguridad (*security*), herramientas de evaluación (*evaluation tool*), modelo de madurez (*maturity model*).

4. Intervención

Observar los resultados de las organizaciones que ya han adoptado una arquitectura Zero Trust y las herramientas que han utilizado para medir su funcionamiento. Extraer los artículos y documentos de mayor relevancia para la investigación y analizar los resultados.

5. Control

Al iniciar la investigación no se cuenta con una colección de estudios realizados en el área. Se inicia con una búsqueda a partir de las palabras clave que se identificaron.

6. Efectos

Se espera tener documentación suficiente con las búsquedas realizadas para entender cuáles son las áreas que deben evaluarse en una arquitectura Zero Trust, así como los criterios de evaluación.

7. Medida de salida

Para la documentación encontrada se lleva a cabo una revisión de la calidad de esta en sitios *web* especializados para este propósito.

8. Población

La población por analizar son las publicaciones que se encuentren en los repositorios de las fuentes que se seleccionaron y que tengan relación con el objetivo de la revisión de literatura.

9. Aplicación

Este tipo de investigación puede resultar de utilidad para aquellas organizaciones que tengan implementado o se encuentren en proceso de implementar el modelo Zero Trust en su arquitectura de seguridad.

10. Diseño experimental

Durante el diseño experimental se hace un análisis y clasificación de los estudios que se obtienen con base en la calidad del contenido y relevancia para la investigación.

1.9.1.2 Selección de fuentes

Se especifican en esta sección las fuentes para la identificación de estudios primarios que se utilizan para la investigación.

1.9.1.2.1 Definición del criterio de selección de fuentes

Se han tomado en cuenta para la selección de fuentes aquellas publicaciones que coincidan con las palabras claves definidas que se encuentren en sitios de investigación confiables.

1.9.1.2.2 Lenguaje de estudio

Con el objetivo de encontrar un mayor número de publicaciones relevantes se definió el idioma de búsqueda, tanto en español como en inglés.

1.9.1.2.3 Identificación de fuentes

En este apartado se describe la selección de fuentes para el desarrollo de la investigación.

1. Método de selección de fuentes

El método de selección de fuentes se basa en el respaldo con el que cuenta la fuente en el área de tecnología con respecto a la publicación de estudios y documentos investigativos.

2. Cadenas de búsqueda

Las cadenas de búsqueda que se seleccionaron para encontrar las publicaciones relevantes a la investigación son las siguientes:

intitle: “zero trust”

zero trust+evaluation tool

zero trust model+cybersecurity

zero trust+maturity model

3. Lista de fuentes

1. Google Scholar

1.9.1.2.4 Selección de fuentes después de la evaluación

Se toman en cuenta las fuentes que coincidan con los criterios de búsqueda, estén actualizadas y muestren calidad investigativa.

1.9.1.2.5 Comprobación de las fuentes

Se buscan los sitios donde se publican las fuentes para determinar su validez.

1.9.1.3 Selección de los estudios

Una vez que se seleccionaron las fuentes, se definen los estudios que sean relevantes para la investigación.

1.9.1.3.1 Definición del criterio de inclusión y exclusión de estudios

Se toman en cuenta los estudios que han coincidido con las búsquedas de las palabras clave cuando se encuentren dentro del área de investigación y con una publicación no mayor a 5 años de antigüedad.

1.9.1.3.2 Definición de tipos de estudio

Se evalúan los estudios que se relacionan con el área de investigación cuyo enfoque esté dirigido al tema de la arquitectura Zero Trust.

1.9.1.3.3 Procedimiento para la selección de los estudios

1. Utilizar la opción de búsqueda avanzada o búsqueda general disponible en las fuentes que se seleccionaron.
2. Aplicar las cadenas de búsqueda definidas utilizando las palabras clave.
3. Filtrar el rango de fechas para considerar únicamente estudios publicados entre los últimos 5 años
4. Evaluar los resultados y aplicar los criterios de selección con base en el Abstract y palabras clave del artículo.
5. Extraer y documentar la información relevante para la investigación.

1.9.2 Ejecución de la revisión

1.9.2.1 Selección de estudios iniciales

En la Tabla 1 se muestran los cuatro artículos seleccionados a partir de los criterios de búsqueda definidos en la sección anterior dentro del repositorio Google Scholar.

Título del artículo	Autores	Año	Enlace
Zero Trust Maturity Matters: Modeling Cyber Security Focus Areas and Maturity Levels in the Zero Trust Principle	Modderkolk, M.G.	2018	https://dspace.library.uu.nl/bitstream/handle/1874/364996/Thesis_MG.Modderkolk_ZeTuMM_V1.0-Public.pdf?sequence=2&isAllowed=y
Zero Trust Validation: From Practical Approaches to Theory	Bobbert, Yuri Scheerder, Jeroen	2020	https://isaca.nl/wp-content/uploads/2020/12/Bobbert-Y.-Scheerder-J.-2020-Zero-Trust-Validations_From-practical-approaches-to-theoryo.pdf

Título del artículo	Autores	Año	Enlace
Zero Trust Architecture	Rose, Scott Borchert, Oliver Mitchell, Stu Connelly, Sean	2020	https://doi.org/10.6028/NIST.SP.800-207
Implementing a Zero Trust Architecture	Kerman, Alper Borchert, Oliver Rose, Scott	2020	https://www.nccoe.org/sites/default/files/legacy-files/zt-arch-project-description-draft.pdf

Tabla 1. Índice de estudios recolectados del repositorio Google Scholar

1.9.2.2 Evaluación de la calidad de los estudios

Se presume la calidad de los artículos mencionados con base en la cantidad de filtros y evaluaciones realizados por Google Scholar.

1.9.2.3 Revisión de la selección

La selección de estudios primarios se realiza tras llevar a cabo una revisión del Abstract y contenido general incluido en cada artículo.

1.9.2.4 Extracción de información

Se consideran los siguientes elementos para la extracción de la información relevante de los estudios primarios y el cumplimiento de los objetivos de la investigación:

- Definiciones de los componentes necesarios dentro de un entorno Zero Trust.
- Herramientas de evaluación de los procesos de seguridad.
- Pasos de implementación de un modelo Zero Trust.
- Casos de uso de una arquitectura Zero Trust.

Título	Zero Trust Maturity Matters: Modeling Cyber Security Focus Areas and Maturity Levels in the Zero Trust Principle
Año de publicación	2018
Autores	Modderkolk, M.G.
Resumen	Esta investigación desarrolla un modelo de madurez a partir de la arquitectura Zero Trust que se basa en otros modelos dentro del área de ciberseguridad.

Aspectos importantes	• Definición de áreas de evaluación. • Identificación de parámetros de medida. • Propuesta de niveles de cumplimiento. • Cálculo de resultados de madurez. • Casos de estudio aplicados.

Tabla 2. Extracción de Fuente 1

Título	Zero Trust Validation: From Practical Approaches To Theory
Año de publicación	2020
Autores	Bobbert, Yuri Scheerder, Jeroen
Resumen	Este artículo describe el estado actual de implementación de Zero Trust, lo que incluye las limitaciones existentes en su adopción. Se enfoca en estrategias de visibilidad hacia las gerencias y altos mandos y propone un *framework* que se basa en tres niveles, estratégico, táctico y operativo.
Aspectos importantes	• Propuesta de un lenguaje común para que todas las partes de la organización puedan participar de la implementación del modelo. • Identificación de factores clave de éxito durante la implementación de Zero Trust. • Definición de los elementos que deben monitorearse. • Evaluación inicial que las empresas deben hacer antes de iniciar el proceso de implementación.

Tabla 3. Extracción de Fuente 2

Título	Zero Trust Architecture

Año de publicación	2020
Autores	Rose, Scott Borchert, Oliver Mitchell, Stu Connelly, Sean
Resumen	Esta publicación de la NIST contiene los conceptos importantes que se relacionan con la arquitectura Zero Trust, sus principios, componentes, escenarios de desarrollo y amenazas que se relacionan, así como un plan de migración de un modelo tradicional a uno Zero Trust.
Aspectos importantes	• Conceptos y definiciones de los componentes de la arquitectura. • Identificación de los requerimientos técnicos de implementación. • Relación existente con otros *frameworks* de NIST. • Propuesta de migración (pasos y requerimientos).

Tabla 4. Extracción de Fuente 3

Título	Implementing a Zero Trust Architecture
Año de publicación	2020
Autores	Kerman, Alper Borchert, Oliver Rose, Scott
Resumen	Este artículo propone una implementación práctica del modelo Zero Trust utilizando productos comerciales

	disponibles que se alinean con los principios NIST SP 800-207.
Aspectos importantes	• Ejemplos de escenarios prácticos donde se puede implementar el modelo. • Listado de los componentes generales de la arquitectura. • Identificación de requerimientos y estándares que se relacionan. • Propuesta de un mapa de control de seguridad.

Tabla 4. Extracción de Fuente 4

1.9.3 Análisis de resultados

De acuerdo con la literatura consultada en la sección anterior, se puede determinar que, aunque el concepto de Zero Trust se desarrolló hace más de una década, fue hasta hace un par de años que empezó a aumentar considerablemente el número de organizaciones que han decidido adoptar el modelo. Las razones para la inclusión de una arquitectura Zero Trust dentro del modelo de seguridad empresarial se relacionan con la transformación de los modelos de negocio y de las estrategias de manejo de la información.

La migración hacia modelos híbridos (*on-premise*/*cloud*) o incluso modelos instalados totalmente en la nube ha permitido la flexibilización de las restricciones para acceder a la información; ya no es necesario que una persona se encuentre físicamente en las instalaciones de la empresa para acceder a la red corporativa, por el contrario, ahora la información es accesible desde cualquier lugar y en cualquier momento. La pandemia de la COVID-19 aceleró todavía más esta transformación digital, impulsando modelos de teletrabajo y comercio electrónico a

niveles nunca vistos. Este nuevo escenario también implica nuevos riesgos de seguridad y expande la superficie de ataque ante posibles amenazas que quizás no se consideraron previamente, lo que hace de vital importancia adaptar el modelo de seguridad a estas nuevas necesidades de negocio.

Sin embargo, la adopción del modelo Zero Trust resulta muchas veces complicada debido a que no existe un lenguaje común en torno al mismo, en ocasiones, es dependiente del fabricante y no resulta sencillo de entender por parte de las gerencias y los altos mandos. Según las publicaciones de NIST (2019), Zero Trust carece de un *framework* común o una alineación con los *frameworks* existentes, así como un vocabulario común. Esto afecta tanto al personal operativo como administrativo, por un lado, se necesita una orientación estratégica y, por otro lado, conocimientos técnicos, dejando una brecha en la comunicación entre ambas partes. Es importante contar con herramientas que proporcionen un lenguaje entendible para todas las partes, que permitan identificar las necesidades en los diferentes niveles de la organización, así como formas de medir el cumplimiento de los requisitos por medio de medidas, controles y contrapesos.

Capítulo 2. Marco conceptual

Para el desarrollo del marco conceptual se propone una nube de conceptos basada en los resultados del estado de la cuestión, donde se buscan las palabras clave que aparezcan con mayor frecuencia. Para la nube de conceptos se utilizó la herramienta TagCrowd.

Figura 1. Nube de conceptos

A partir de la identificación de los principales conceptos desarrollados en la investigación, la relación entre ellos se puede representar a través del siguiente mapa conceptual:

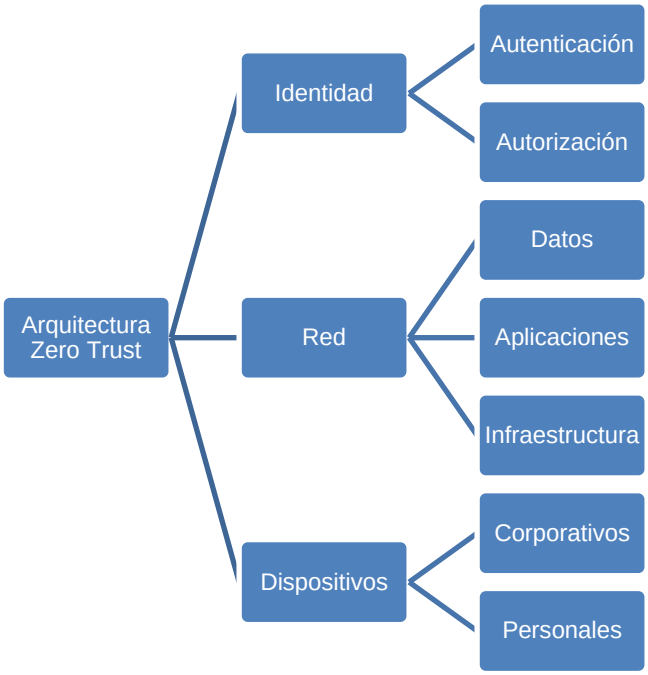


Figura 2. Mapa conceptual

En la siguiente sección se definen los conceptos relevantes en el desarrollo de la investigación:

- Identidad: puede representar personas, estaciones de trabajo, dispositivos finales o de Internet de las cosas. La identidad corresponde al plano de control de la arquitectura Zero Trust. Cuando una identidad intenta acceder algún recurso se debe verificar por medio de un proceso de autenticación que la solicitud sea válida y congruente con el tipo de recursos que esta identidad habitualmente accede y que sigue el principio de mínimos privilegios (Microsoft, 2021).
- Red: es la plataforma que permite la comunicación entre los diferentes elementos. En la arquitectura Zero Trust, las redes deben segmentarse y protegerse en tiempo real por medio de cifrado de datos punto a punto y monitoreo constante utilizando herramientas de análisis de datos (NIST, 2020). La segmentación de la red busca agregar controles en cada uno de los diferentes componentes a través de la creación de microperímetros (Palo Alto, 2019).
- Dispositivos: cuando se otorga permiso a una identidad para acceder un recurso, los datos fluyen a través de diferentes dispositivos, como computadoras, teléfonos inteligentes, tabletas, servidores (locales o en la nube), entre otros. Esto ocasiona que la superficie de ataque se expanda ampliamente, requiriendo de un monitoreo detallado y solicitando una serie de políticas mínimas de cumplimiento en cada dispositivo para poder conectarse a la red (Microsoft, 2021).

- Datos: son el elemento principal que se busca proteger en cualquier solución de ciberseguridad. Los datos deben clasificarse, etiquetarse y encriptarse, así como restringir el acceso que se basa en estos atributos (NIST, 2020).
- Aplicaciones: son las que se encargan de brindar la interfaz por la cual se consumen los datos. Pueden legarse, *on-premise*, alojadas en la nube o proveídas por terceros. Además, debe validarse el acceso y los permisos a las aplicaciones, así como analizar el tráfico que fluye a través de ellas (Palo Alto, 2019).
- Infraestructura: hace referencia al entorno donde se almacena e intercambia la información. Puede ser *on-premise*, basada en nube, híbrida, virtualizada, entre otros. Representa un elemento crítico dentro de la seguridad, pues es la base desde la cual se desarrollan los otros elementos (Microsoft, 2021).
- Autenticación: es el proceso que permite validar si una identidad puede acceder a un recurso. En el entorno Zero Trust es necesario contar con autenticación de múltiple factor, lo que disminuye el riesgo de la reutilización de usuarios y contraseñas. Una vez que la identidad se ha autenticado puede conectarse al resto de las aplicaciones por medio del proceso de *single sign-on* (SSO), lo que incrementa la productividad, pues no es necesario autenticarse en cada aplicación por separado (Akamai, 2020).
- Autorización: es el proceso de brindar permisos después de que la identidad se ha autenticado, al seguir el principio de mínimos privilegios.

Capítulo 3. marco metodológico

3.1 Tipo de investigación

La investigación por realizar se clasifica como aplicada, ya que se busca establecer una herramienta de autoevaluación para determinar el nivel de madurez de una organización en una arquitectura Zero Trust o que planifique su implementación. Esto al identificar las áreas de trabajo y su estado actual frente a la postura que se planteó en el modelo.

3.2 Alcance investigativo

El alcance investigativo que se planteó en esta investigación es descriptivo y toma como referencia la definición que planteó Vargas (2004): “Tipo de estudio que busca especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a análisis” (s. p.).

En este proyecto se pretende mostrar el estado actual de las organizaciones dentro del contexto particular de la arquitectura Zero Trust. Además, especifica propiedades, características y perfiles de las diferentes áreas de la organización que deben evaluarse utilizando la herramienta resultante de esta investigación y detallando el nivel de cumplimiento según los diferentes parámetros que se definan. Se mide de acuerdo con una escala de cumplimiento donde se describa la situación actual de la entidad y se brinda un resultado de acuerdo con la recolección de datos resultante de la herramienta de evaluación.

3.3 Enfoque

El enfoque propuesto en esta investigación es cuantitativo, pues la herramienta de evaluación que se desarrolla realiza una medición, según una escala

de cumplimiento definida, que permite categorizar cada una de las áreas de la organización involucradas dentro de la arquitectura Zero Trust de acuerdo con el nivel de madurez con el que se cuente. La escala es numérica, asigna un valor según el nivel de cumplimiento y genera un resultado que puede cuantificarse utilizando la medida de los puntos que se obtienen de la cantidad de puntos totales.

3.4 Diseño

El diseño cuantitativo propuesto para la investigación es la encuesta, pues las organizaciones deben aplicar la herramienta de autoevaluación a los encargados de cada área para medir el cumplimiento en los diferentes dominios y así validar el nivel de madurez según los parámetros establecidos.

3.5 Población y muestreo

La población definida para aplicar la herramienta de autoevaluación son los diferentes encargados de las áreas que se relacionan con la arquitectura Zero Trust. Se propone un muestreo no probabilístico por conveniencia, en el que las personas que apliquen la herramienta puedan seleccionar a los expertos de cada área que puedan brindar la información precisa y permitan obtener resultados más confiables.

3.6 Instrumentos de recolección de datos

El instrumento de recolección de datos propuesto en la investigación es el cuestionario aplicado a los encargados de cada área relacionada con la arquitectura Zero Trust. En este se evalúan diferentes aspectos de ciberseguridad que se relacionan con el modelo.

3.7 Técnicas de análisis de información

Para realizar el análisis de información se utiliza el proceso presentado en la Figura 3:

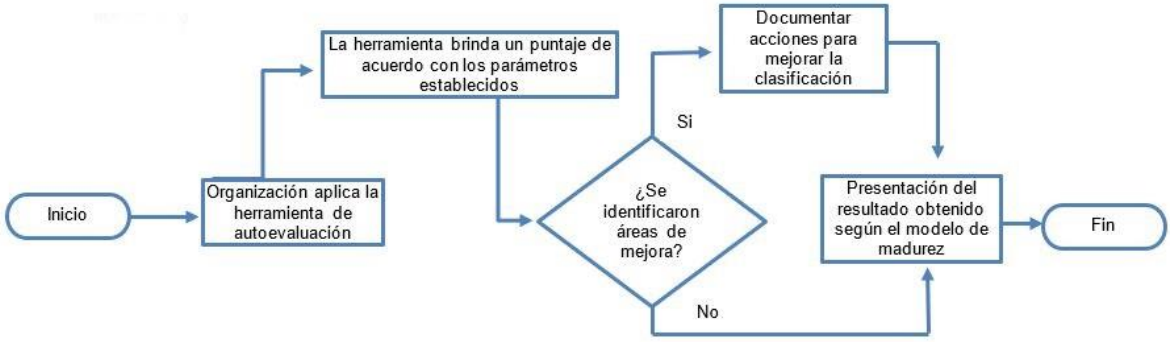


Figura 3. Diagrama de flujo de análisis de la información

Capítulo 4. Análisis del diagnóstico

En este capítulo se exponen y analizan los resultados de los instrumentos de investigación aplicados, con el fin de validar el cumplimiento de los objetivos que se plantearon al inicio de la investigación. Los resultados se obtuvieron a partir de una encuesta a diferentes personas involucradas en el área de las tecnologías de información, con el objetivo de validar la necesidad de la herramienta de evaluación para determinar la viabilidad técnica de implementación de una arquitectura Zero Trust. Con los resultados se busca presentar un diagnóstico que justifique el desarrollo de la herramienta y la validez que tiene en el proceso de adopción e implementación de un modelo Zero Trust.

4.1 Desarrollo de la encuesta

La encuesta se planteó con el objetivo de medir el conocimiento y nociones básicas en torno al modelo Zero Trust en las organizaciones, así como determinar la existencia de herramientas que permitan a las empresas conocer los requerimientos

técnicos necesarios para adoptar el modelo. A partir de esto, se desarrollaron las siguientes preguntas:

1. ¿Ha escuchado acerca del modelo Zero Trust?
2. ¿Conoce los requerimientos para que una empresa pueda adoptar un modelo Zero Trust?
3. ¿Considera que su organización está preparada para adoptar un modelo Zero Trust?
4. ¿Conoce alguna herramienta que le permita a su organización evaluar la viabilidad técnica de implementación de una solución Zero Trust?
5. ¿Conoce si en su organización se utilizan herramientas para medir el nivel de madurez de las soluciones Zero Trust?

4.2 Aplicación y análisis de la encuesta

La encuesta se aplicó en diferentes grupos de redes sociales y foros que se relacionan con el ámbito informático. Un total de 57 personas respondió el formulario, lo que representa una muestra representativa del sector tecnológico y de ciberseguridad. A continuación, se muestran los resultados en la encuesta:

Para la primera pregunta, “¿Ha escuchado acerca del modelo Zero Trust?” Un total de 45 personas respondió afirmativamente, mientras que solo 12 personas indicaron desconocer el término.

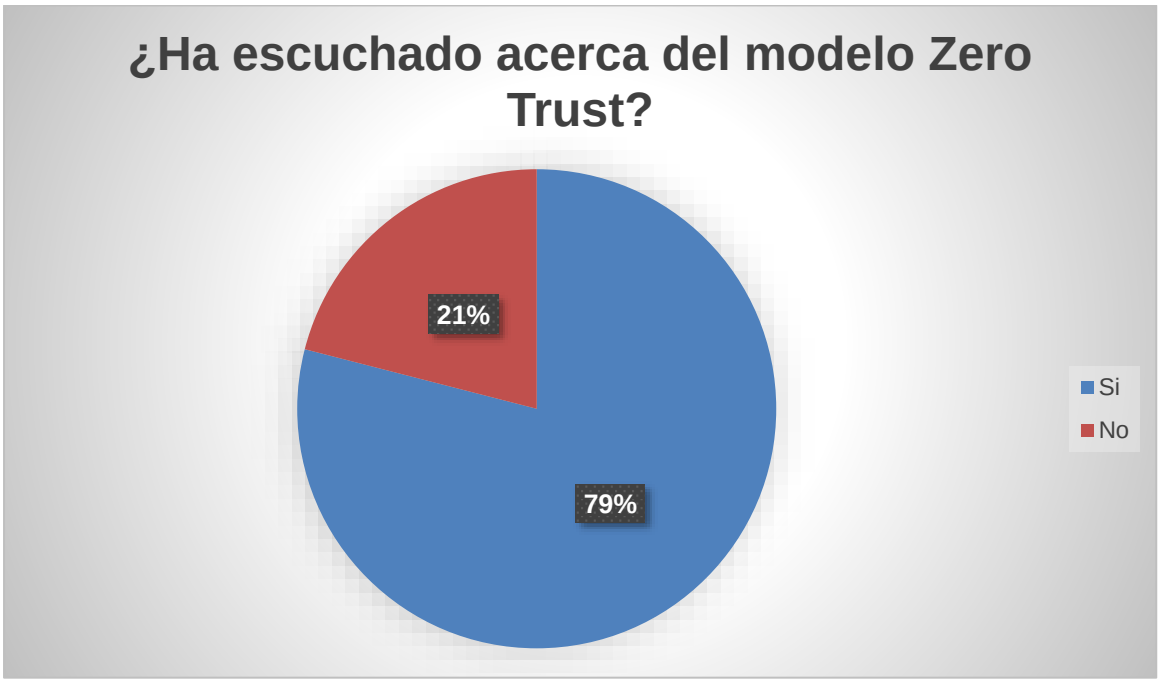


Figura 4. Gráfico porcentual de las respuestas a la pregunta: ¿Ha escuchado acerca del modelo Zero Trust?

Los resultados en esta pregunta permiten observar que la mayor parte de las personas que se relacionan con el ámbito informático tienen alguna noción del modelo Zero Trust y el término no les resulta desconocido. Esto coincide con el auge en la adopción del modelo en los últimos años, como lo muestra una encuesta aplicada por Cybesecurity Insiders y Pulse Secure a 400 personas que se encargan de la toma de decisiones en el campo de seguridad de TI a principios del año 2020, donde el 72 % de las personas encuestadas afirmó estar planeando evaluar o implementar Zero Trust en el corto plazo (Cybesecurity Insiders, 2020).

Como respuesta a la segunda pregunta, “¿Conoce los requerimientos para que una empresa pueda adoptar un modelo Zero Trust?”, un total de 7 personas respondió estar familiarizado totalmente con los requerimientos, 16 personas indicaron tener algunas nociones, mientras que 34 personas indicaron desconocer los requerimientos.

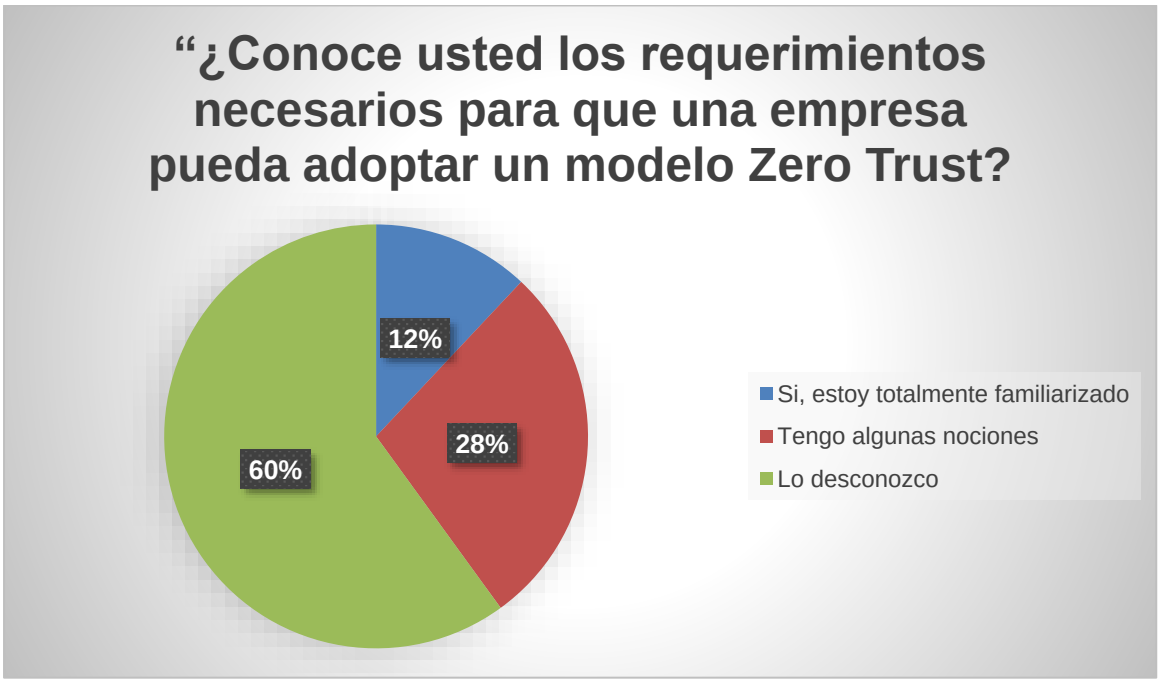


Figura 5. Gráfico porcentual de las respuestas a la pregunta: ¿Conoce los requerimientos para que una empresa pueda adoptar un modelo Zero Trust?

El análisis de estos resultados permite identificar que, aunque la mayor parte de las personas en el campo de TI han escuchado en algún momento acerca del modelo Zero Trust, los requerimientos para implementar la solución no son conocidos para la mayor parte de las personas encuestadas. Una herramienta de evaluación y viabilidad técnica de ejecución de un modelo Zero Trust permite dar una mayor claridad a los involucrados en el proceso de adopción del modelo acerca de los diferentes requerimientos técnicos necesarios.

Respecto a la tercera pregunta, “¿Considera que su organización está preparada para adoptar un modelo Zero Trust?”, un total de 4 personas respondió *Sí, cuento con las herramientas para saberlo*, 1 persona respondió *No, cuento con las herramientas para saberlo*, 21 personas indicaron desconocerlo por completo, mientras 31 personas indicaron no contar con las herramientas para saberlo.

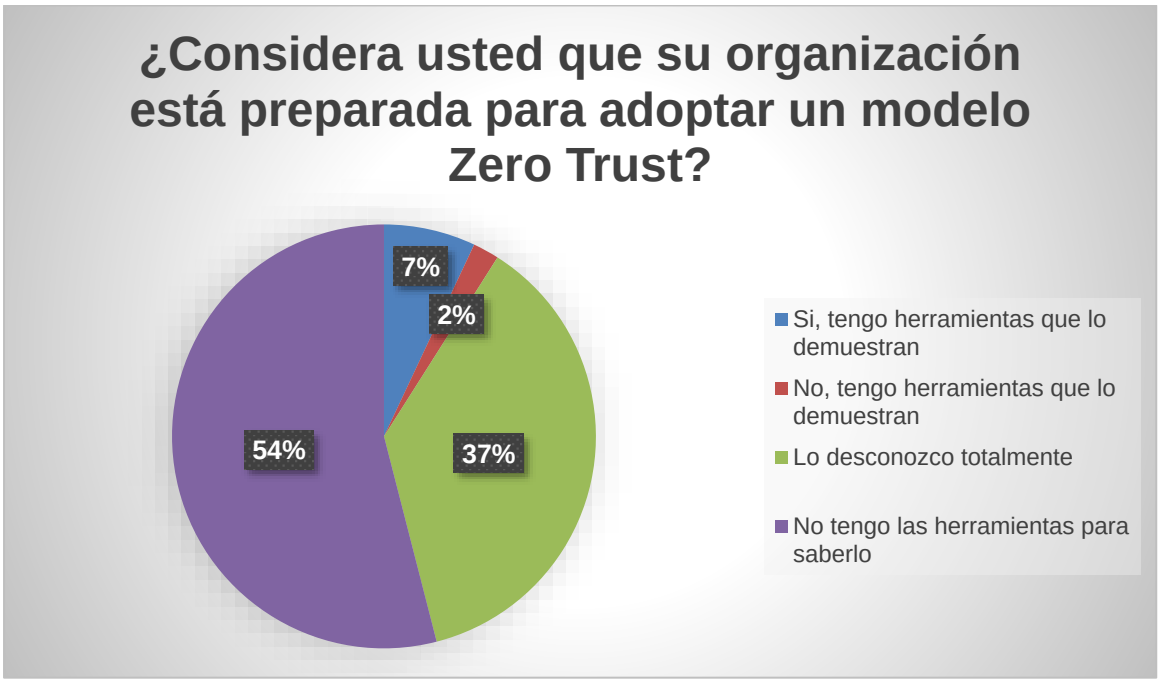


Figura 6. Gráfico porcentual de las respuestas a la pregunta: ¿Considera que su organización está preparada para adoptar un modelo Zero Trust?

Los resultados en esta pregunta reflejan que la mayor parte de las personas encuestadas no cuenta con alguna herramienta de medición para determinar si una solución Zero Trust es factible en su organización. En muchos casos, el proceso de adopción de una solución Zero Trust no es sencillo, pues se ven involucrados diversos componentes técnicos como identidades, dispositivos, aplicaciones, datos, infraestructura y redes. Por este motivo, resulta de vital importancia identificar el nivel de cumplimiento en cada uno de estos aspectos y establecer los planes de trabajo necesarios para llegar al cumplimiento en cada una de las áreas.

Para la cuarta pregunta: “¿Conoce alguna herramienta que le permita a su organización evaluar la viabilidad técnica de implementación de una solución Zero Trust?”, solamente 8 personas respondieron afirmativamente, mientras que 49 personas indicaron desconocer alguna herramienta para este fin.

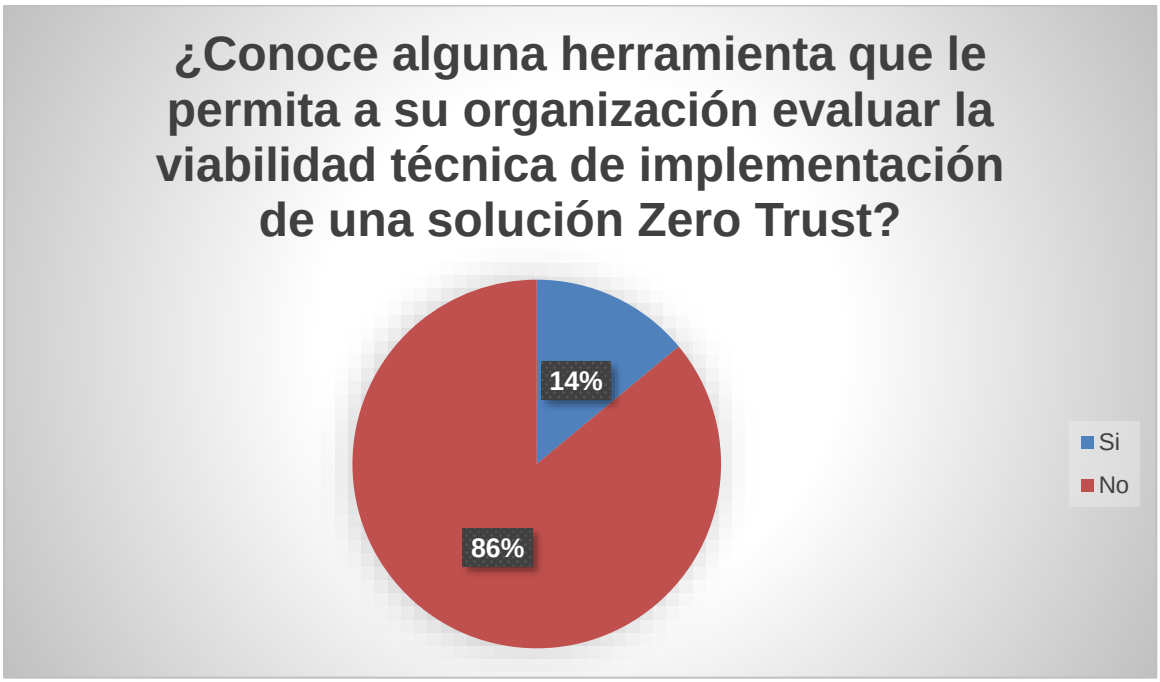


Figura 7. Gráfico porcentual de las respuestas a la pregunta: ¿Conoce alguna herramienta que le permita a su organización evaluar la viabilidad técnica de implementación de una solución Zero Trust?

Los resultados de esta pregunta se complementan con los hallazgos de la pregunta anterior, pues evidencian la falta de herramientas que permitan a las organizaciones determinar la viabilidad técnica de implementar una solución Zero Trust. Es importante que las organizaciones sean capaces de identificar cuales áreas cuentan con procesos compatibles para una eventual migración a una arquitectura Zero Trust y cuales requieren cambios en sus procesos para poder adaptarse.

Por último, en la quinta pregunta: “¿Conoce si en su organización se utilizan herramientas para medir el nivel de madurez de las soluciones Zero Trust?”, un total de 6 personas respondió afirmativamente, mientras que 51 personas indicaron no conocer ninguna herramienta.

Figura 8. Gráfico porcentual de las respuestas a la pregunta: ¿Conoce si en su organización se utilizan herramientas para medir el nivel de madurez de las soluciones Zero Trust?

Los resultados de esta pregunta reflejan que solamente un 11 % de las personas encuestadas afirma conocer que en sus organizaciones se utilizan herramientas para medir el nivel de madurez de los elementos de una solución Zero Trust, lo que evidencia la necesidad de desarrollar una herramienta que permita medir esto. Como se mencionó, la arquitectura Zero Trust está compuesta por diferentes áreas y es importante identificar las fortalezas y debilidades en cada una para que las organizaciones puedan desarrollar planes de trabajo y adoptar exitosamente el modelo.

4.3 Conclusiones del diagnóstico

A partir de los resultados en la encuesta y el análisis hecho en cada una de las preguntas, se puede determinar que es viable el desarrollo de una herramienta

que ayude a las organizaciones a conocer su postura actual y los requerimientos técnicos necesarios para adoptar exitosamente un modelo de seguridad Zero Trust.

Capítulo 5. Propuesta de solución

Como se pudo observar en el análisis del diagnóstico, muchas de las organizaciones han implementado soluciones de seguridad tradicionales a través del tiempo. Sin embargo, desconocen cuáles son los requerimientos técnicos necesarios para adoptar un nuevo modelo de seguridad y cómo sus políticas y controles actuales se acoplan o no a estos nuevos modelos.

Es evidente que la mayoría de las organizaciones ha iniciado un proceso de adopción de nuevas estrategias de seguridad para proteger de mejor forma sus activos y es probable que en muchos casos ya se cuente con alguna forma de estrategia de Zero Trust entre los controles de seguridad. Sin embargo, existen algunas brechas entre la teoría del modelo y la aplicación de este en todas sus áreas de injerencia. Zero Trust no es un producto o una solución única que las organizaciones puedan adquirir, se trata de toda una arquitectura que implica diferentes desafíos a la infraestructura actual de las organizaciones y los cambios necesarios para adoptar el modelo.

Es en este punto donde la propuesta de esta investigación pretende ayudar a las organizaciones a observar si es viable la implementación técnica de los conceptos de Zero Trust, cuáles son los requerimientos en cada una de las áreas y en qué etapa de madurez se encuentra la organización en cada uno. Es importante acotar que la propuesta desarrollada en esta sección es una herramienta de evaluación en diferentes áreas puntuales en torno al modelo Zero Trust, que permite

a las organizaciones determinar los aspectos técnicos necesarios que debe cumplir y el nivel de cumplimiento en cada uno, mas no representa una guía de implementación completa para la organización.

5.1 Modelo de la solución

Para el desarrollo de la herramienta de evaluación del modelo Zero Trust se analizaron y compararon diferentes modelos propuestos en la industria, con el objetivo de identificar las áreas de trabajo donde la herramienta debe aplicarse. Los modelos analizados comprendieron los propuestos por las siguientes empresas u organizaciones, Microsoft, Palo Alto, Cisco, Zscaler y CISA. En la siguiente tabla se muestran las áreas de trabajo propuestas por cada una de estas organizaciones:

Modelo	**Áreas de trabajo propuestas**
Microsoft	• Identidad • Dispositivos • Datos • Aplicaciones • Infraestructura • Red
Palo Alto	• Identidad • Dispositivos • Acceso • Transacciones

Cisco	• Personal • Cargas de trabajo • Lugar de trabajo
Zscaler	• Proveedores de nube • Identidad y autenticación • Dispositivos • Reportes y análisis de datos
CISA	• Identidad • Dispositivos • Red • Aplicaciones • Datos

Tabla 5. Modelos de áreas de trabajo Zero Trust

A partir de la información obtenida de los diferentes modelos, se llevó a cabo un análisis para determinar las coincidencias entre las diferentes propuestas y determinar el mejor enfoque para aplicar la herramienta. Como resultado se decidió utilizar de referencia el modelo que planteó Microsoft, donde se identifican seis áreas de trabajo, identidad, dispositivos, datos, aplicaciones, infraestructura y red. Este modelo presenta una segmentación de áreas de trabajo que se ajusta a la herramienta de evaluación, lo que permite evaluar diferentes elementos técnicos agrupados en categorías correspondientes a cada una de estas áreas con el nivel de detalle adecuado.

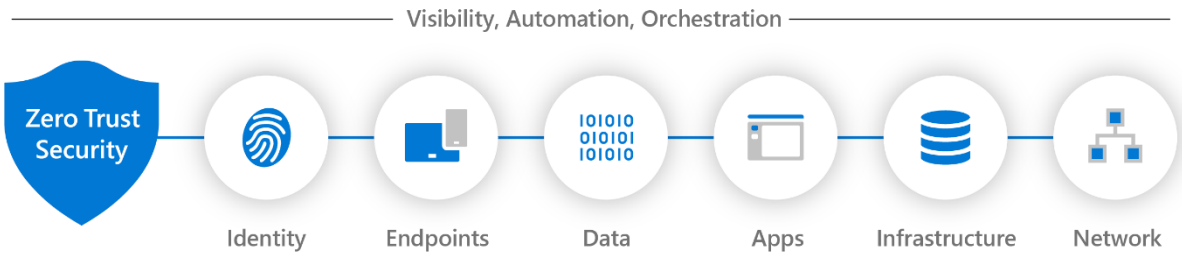


Figura 9. Áreas de trabajo del modelo Zero Trust de Microsoft.

Fuente: https://docs.microsoft.com/en-us/security/zero-trust/

Como se puede observar, el modelo propone seis áreas de evaluación donde la herramienta debe aplicarse.

1. Identidad. En esta área deben validarse los controles necesarios para garantizar el acceso seguro a los recursos por medio de mecanismos de autenticación confiables, aplicables a los ambientes de trabajo modernos donde coexisten las aplicaciones y datos *on-premise,* ambientes híbridos y soluciones alojadas en la nube. En el marco de Zero Trust es importante evaluar la implementación de soluciones de múltiple factor de autenticación (MFA) y de un único inicio de sesión (SSO).
2. Dispositivos. La superficie de ataque de las organizaciones ha crecido con la inclusión de múltiples dispositivos capaces de conectarse a la red y acceder a datos e información sensible. Muchos de estos dispositivos pueden no administrarse por con políticas de seguridad de las organizaciones dejándolos fuera del alcance de las actualizaciones de seguridad necesarias y requerimientos mínimos que deben cumplir para poder conectarse a la red. Es importante evaluar los controles en

esta área para optimizar la administración de dispositivos capaces de conectarse a la red.

3. Datos. Con los nuevos paradigmas de acceso a la información, colaboradores a distancia y manejo de datos en aplicaciones con base en la nube, es importante evaluar los controles que permitan proteger estos datos, tanto en reposo como en movimiento. Es importante clasificar y etiquetar la información según su sensibilidad para determinar los controles necesarios, tanto en las soluciones locales como en la nube.
4. Aplicaciones. Para obtener un máximo provecho de las aplicaciones y servicios, es importante que las organizaciones puedan simplificar el acceso y mantener el control sobre ellas. En esta área es relevante validar los controles que se relacionan con los permisos y accesos a estas aplicaciones, utilizando información analítica basada en datos históricos que permitan definir tendencias y detectar eventos anómalos, así como monitorear las acciones que los usuarios realizan y validar configuraciones seguras entre las aplicaciones.
5. Infraestructura. La evaluación en esta área no se limita a la infraestructura física de la organización, sino que se deben contemplar distintos tipos de tecnologías que pueden incluir el *hardware*, *software*, máquinas virtuales, infraestructura basada en la nube, servicios, entre otros. Los controles por evaluar en esta sección incluyen las herramientas de prevención y monitoreo de los diferentes componentes ante un potencial ataque, la respuesta que deben tener ante eventos que puedan comprometer el funcionamiento adecuado y

las políticas de administración que permitan una configuración segura en toda la infraestructura.

6. Red. Como se ha mencionado, el diseño de la red empresarial ha dejado de ser un elemento aislado con muros a su alrededor para protegerlo, por el contrario, se ha convertido en una colección de dispositivos y redes interconectadas a través de la nube y distribuidas alrededor del mundo. Los controles de red deben validar la protección dentro de este nuevo modelo que se basa en microperímetros, lo que asegura la encriptación de los datos en movimiento y una integración los perímetros definidos por *software* (SDP) en reemplazo de las de tradicionales VPN.

5.2 Etapas propuestas en la solución

Para la aplicación de la herramienta propuesta se sugiere una serie de etapas que permitan a las organizaciones diagnosticar, evaluar y mejorar en el proceso de adopción del modelo Zero Trust. Los resultados en cada una de las etapas permitirán a las organizaciones identificar el nivel de madurez en cada una de las diferentes áreas evaluadas y determinar el plan de acción correspondiente. Las etapas propuestas son las siguientes, análisis de la situación actual, evaluación del nivel de madurez, hallazgos y recomendaciones, implementación de controles y mejora continua.

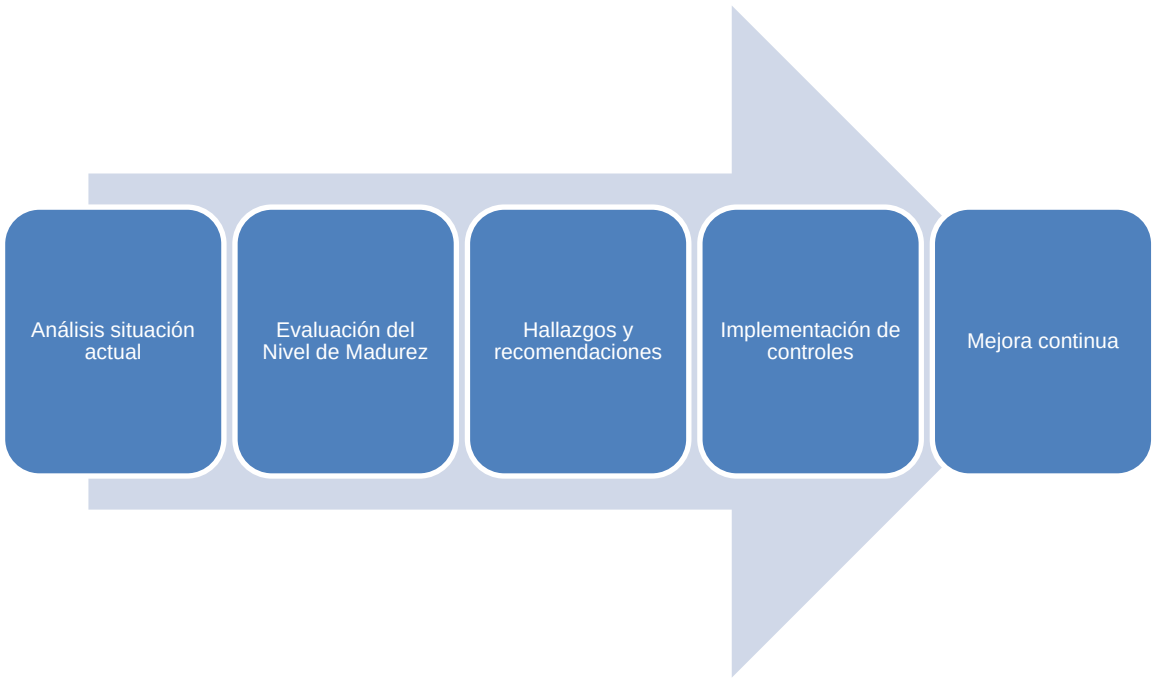


Figura 10. Etapas de aplicación de la herramienta de evaluación.

5.2.1 Etapa de análisis de la situación actual

En la fase de análisis de la situación actual las organizaciones pueden aplicar el instrumento de evaluación para conocer su postura actual y determinar la viabilidad de implementar una solución Zero Trust. En esta primera etapa se abordan preguntas generales respecto a las diferentes áreas evaluadas. Se pretende dar una visión general de los requerimientos técnicos necesarios para iniciar el proceso de adopción del modelo. En esta sección no se define un puntaje según las respuestas obtenidas, sino que se busca brindar una visión general de los diferentes elementos técnicos que la organización debe considerar en cada área del Modelo Zero Trust. A continuación, se muestran las preguntas de diagnóstico que permiten evaluar la situación actual:

Área	Pregunta
Identidad	¿Los usuarios de la organización se autentican por medio de mecanismos de múltiple factor a los sistemas? ¿Las aplicaciones de la organización utilizan un sistema único de inicio de sesión (SSO)? ¿La gestión de permisos se basa en el principio de privilegios mínimos?
Dispositivos	¿Los dispositivos que se conectan a la red corporativa se encuentran registrados? ¿Existe un método para garantizar que los dispositivos cumplen con los requisitos de seguridad para poder conectarse a la red? ¿Se ha desarrollado alguna política de prevención de pérdida de datos en los dispositivos?
Red	¿Las redes se encuentran segmentadas para prevenir el movimiento lateral? ¿La comunicación punto a punto viaja encriptada? ¿Existen mecanismos de monitoreo y detección de tráfico no habitual?
Datos	¿Existe una política de clasificación de datos según su sensibilidad? ¿Se han establecido controles para determinar si los datos pueden compartirse a terceros? ¿Los datos sensibles se encuentran encriptados?
Aplicaciones	¿El acceso a las aplicaciones se basa en políticas? ¿Las aplicaciones críticas de negocio se monitorean en tiempo real para prevenir ataques o actividades anómalas? ¿El acceso a las aplicaciones está limitado únicamente a los usuarios que las requieren?
Infraestructura	¿Existe un plan de respuesta a incidentes? ¿Se utilizan herramientas de monitoreo y recolección de registros de eventos? ¿Los privilegios de administración a los equipos se otorgan por un tiempo definido?

Tabla 6. Preguntas que se desarrollaron durante la fase de análisis de la situación actual

5.2.2 Etapa de evaluación del nivel de madurez

La fase de evaluación del nivel de madurez pretende medir el nivel de cumplimiento de la organización según la implementación de controles en las diferentes áreas del modelo. Para la evaluación de cada uno de los elementos técnicos seleccionados se utiliza la escala de medición basada en los niveles de madurez propuestos en el estándar CMM:

Niveles de madurez que se basan en el estándar CMM		
0	Inexistente	El control aplica, pero no se definió ninguna acción, política o procedimiento
1	Inicial	El control se encuentra en un estado inicial, no está definido totalmente ni documentado
2	Repetible	El control cuenta con herramientas o procedimientos asociados, se obtienen resultados consistentes
3	Definido	El control está documentado, con políticas y procedimientos definidos y estandarizados, con revisiones periódicas
4	Administrado	El control se monitorea con métricas e indicadores
5	Optimizado	El control tiene una mejora continua, con un alto nivel de automatización

Tabla 7. Niveles de madurez que se basan en el estándar CMM

Para realizar la evaluación se definió una serie de categorías y subcategorías entre las áreas de trabajo del modelo Zero Trust que se planteó, esto con el objetivo de medir el nivel de madurez en cada una de estas secciones aplicando la escala presentada. Los elementos por evaluar se muestran en la siguiente tabla:

Área	Categoría	Subcategoría
Identidad	Autenticación	Los sistemas utilizan autenticación de factor múltiple (MFA)
		Los sistemas permiten la autenticación sin contraseñas (utilizando algún método alternativo como MFA)
		Los sistemas utilizan un esquema SSO
	Autorización	Los sistemas otorgan permisos que se basan en el grupo al que pertenece el usuario
		Los permisos se administran bajo el principio de privilegios mínimos y separación de tareas
		Las acciones de los usuarios se registran en una bitácora de eventos
	Acceso Contextual	Los sistemas utilizan un acceso condicional según la ubicación del usuario
		Los sistemas solicitan un método de autenticación adicional cuando un usuario utiliza un dispositivo nuevo
		Los sistemas utilizan un acceso condicional que se basa en el análisis de comportamiento en tiempo real
Dispositivos	Registro	Los dispositivos que se utilizan se registran ante el proveedor de identidad
		Los dispositivos se inspeccionan para garantizar que cumplen con los requerimientos mínimos establecidos
		Los dispositivos se administran desde una solución MDM (Mobile Device Management)
		Los dispositivos cuentan con sus unidades de disco duro encriptadas

	Protección de datos	Los dispositivos móviles cuentan con algún acceso biométrico (huella o reconocimiento facial)
		Se utiliza la detección de amenazas basada en la evaluación de riesgos de los dispositivos en tiempo real
Red	Conexiones remotas	Se utiliza un perímetro definido por *software* (SDP) para establecer los microperímetros de la red
		Se encriptan todas las comunicaciones punto a punto por medio de certificados
		Se utiliza un agente de confianza entre las conexiones desde una aplicación privada y un usuario autorizado
	Automatización	Se utilizan mecanismos automatizados que se basan en Machine Learning para la protección ante amenazas
		Se definen reglas de acceso a las aplicaciones mediante un WAF (Web Application Firewall)
		Existen mecanismos para detectar tráfico anómalo que se basa en comportamiento
Datos	Clasificación	Existe una taxonomía para la clasificación de los datos
		Se encuentra definida una política de clasificación de los datos
		Existe una estrategia de clasificación y etiquetado de datos
	Políticas de acceso	Los controles de acceso a los datos se definen con base en su sensibilidad
		Los datos sensibles se encuentran encriptados para prevenir el acceso no autorizado
		Existe una política para los datos que deben compartirse con terceros
	Prevención de pérdida de información	Existe un mecanismo de monitoreo y alerta para evitar que datos sensibles se copien a un USB
		Existe un mecanismo de monitoreo y alerta para evitar que datos sensibles se envíen por correo electrónico
		Existe un mecanismo de monitoreo y alerta para evitar que datos sensibles se suban a sitios compartidos
Aplicaciones	Políticas de acceso	Los controles de acceso a las aplicaciones están definidos por políticas individuales a cada una
		El acceso se basa en análisis en tiempo real según el usuario, la ubicación, el dispositivo y la aplicación
		Se utiliza un App Proxy para brindar acceso a las aplicaciones locales
	Gestión en la nube	Las aplicaciones alojadas en la nube cumplen con la política de configuración organizacional
		Se cuenta con un CASB capaz de brindar visibilidad completa dentro de todas las aplicaciones
		Se monitorea constantemente la postura de seguridad de las aplicaciones para garantizar su debido cumplimiento
Infraestructura	Administración	El acceso de administración a los dispositivos está dado por un límite de tiempo específico (Just-in-Time)
		Se registran las acciones de los administradores y se envían alertas ante administraciones sospechosas
		Se utiliza telemetría para detectar ataques o anomalías
	Gestión de vulnerabilidades	Existe una solución SIEM para obtener y analizar registros de eventos de múltiples fuentes
		Se utiliza análisis de comportamiento para detectar amenazas
		Existe una plataforma SOAR para automatizar la respuesta ante amenazas

Tabla 8 Evaluación de madurez de las áreas del modelo Zero Trust

A partir de los resultados en la etapa de evaluación, la herramienta brinda un reporte con las calificaciones obtenidas en cada área. Este reporte servirá como insumo a la organización para identificar los puntos fuertes y las áreas de mejora de los diferentes componentes de la arquitectura Zero Trust.

5.2.3 Etapa de hallazgos y recomendaciones

La siguiente etapa para considerar es la de hallazgos y recomendaciones, donde se analizan los datos que se obtienen en la sección anterior como resultado de la aplicación de la herramienta de evaluación al identificar, tanto los puntos fuertes como las áreas de mejora dentro del Modelo Zero Trust. Los hallazgos deben ir acompañados de recomendaciones que sean aplicables a las diferentes áreas y que permitan establecer mejoras en cada una.

5.2.4 Etapa de implementación de controles

Las recomendaciones que se plantearon para cada uno de los hallazgos servirán como insumo a la siguiente etapa de implementación de controles. Se deben establecer los controles necesarios para cerrar las brechas que se identificaron en las áreas de trabajo en busca de un nivel óptimo de implementación. Los controles que deban implementarse pueden incluir una definición o cambio de alguna política organizacional, la adquisición de algún dispositivo o servicio, la

tercerización de algún proceso por medio de un proveedor o la automatización de alguna tarea.

5.2.5 Etapa de mejora continua

Por último, la etapa de mejora continua busca la evaluación constante de las diferentes áreas del Modelo Zero Trust, lo que permite encontrar puntos de mejora y generar planes de acción en busca de fortalecer el nivel de madurez de cada uno de los elementos evaluados. Para esto, las organizaciones pueden volver a la etapa de evaluación del nivel de madurez y repetir el proceso.

5.3 Ejemplo del proceso utilizando un caso de uso

Para ejemplificar el uso de la herramienta y el abordaje en cada una de las diferentes etapas del proceso de evaluación, se utiliza un caso de uso para una empresa ficticia y brindar una guía de ejecución del proceso en sus diferentes etapas.

5.3.1 Análisis de la situación actual

En primera instancia, la empresa debe realizar el análisis de la situación actual, por medio del diagnóstico que brinda la herramienta de evaluación. En esta etapa se contestan las preguntas según la realidad actual de la organización, como se muestra en la siguiente tabla:

Área	Pregunta	Respuesta
Identidad	¿Los usuarios de la organización se autentican por medio de mecanismos de múltiple factor a los sistemas?	Sí

	¿Las aplicaciones de la organización utilizan un sistema único de inicio de sesión (SSO)?	A veces
	¿La gestión de permisos se basa en el principio de privilegios mínimos?	A veces
Dispositivos	¿Los dispositivos que se conectan a la red corporativa se encuentran registrados?	A veces
	¿Existe un método para garantizar que los dispositivos cumplen con los requisitos de seguridad para poder conectarse a la red?	A veces
	¿Se ha desarrollado alguna política de prevención de pérdida de datos en los dispositivos?	No
Red	¿Las redes se encuentran segmentadas para prevenir el movimiento lateral?	No
	¿La comunicación punto a punto viaja encriptada?	A veces
	¿Existen mecanismos de monitoreo y detección de tráfico no habitual?	A veces
Datos	¿Existe una política de clasificación de datos según su sensibilidad?	Sí
	¿Se han establecido controles para determinar si los datos pueden compartirse a terceros?	Sí
	¿Los datos sensibles se encuentran encriptados?	A veces
Aplicaciones	¿El acceso a las aplicaciones se basa en políticas?	Sí
	¿Las aplicaciones críticas de negocio se monitorean en tiempo real para prevenir ataques o actividades anómalas?	A veces
	¿El acceso a las aplicaciones está limitado únicamente a los usuarios que las requieren?	A veces
Infraestructura	¿Existe un plan de respuesta a incidentes?	Sí
	¿Se utilizan herramientas de monitoreo y recolección de registros de eventos?	Sí
	¿Los privilegios de administración a los equipos se otorgan por un tiempo definido?	No

Tabla 9. Resultados en el análisis de la situación actual

En esta primera etapa, los resultados muestran un panorama general respecto a los requerimientos generales de una arquitectura Zero Trust, por lo que las preguntas respondidas afirmativamente representan concordancia y alineamiento con el modelo; aquellas en las que se respondió con la opción de *a veces* son elementos donde se cuenta con algunas nociones, pero todavía se debe trabajar en el fortalecimiento de los controles y políticas asociados; mientras que las respuestas respondidas de manera negativa indican un primer plano de acción para la organización, puntualizando los elementos técnicos que no se alinean con el modelo Zero Trust.

En este caso en particular, la entidad debe en primera instancia desarrollar una política para la prevención de pérdida de datos en los dispositivos, pues el diagnóstico indica que no la tiene y es un elemento necesario dentro de la estrategia de seguridad. Se identificó que la arquitectura de la red no previene el movimiento lateral de los usuarios una vez que tienen acceso, por lo que una de las primeras acciones debe ser el diseño de una solución que prevenga este problema. Por último, se identificó que los permisos de administración a los dispositivos no se otorgan por tiempo definido, lo que invita a la organización a replantear la forma en la que estos se otorgan.

5.3.2 Evaluación del nivel de madurez

La segunda etapa consiste en una evaluación más detallada del nivel de madurez de cada uno de los controles en las seis áreas definidas en la investigación. A continuación, se muestra la evaluación realizada en este ejemplo:

Área	Categoría	Subcategoría	Evaluación
Identidad	Autenticación	Los sistemas utilizan autenticación de factor múltiple (MFA)	*Repetible*
		Los sistemas permiten la autenticación sin contraseñas (utilizando algún método alternativo como MFA)	*Inexistente*
		Los sistemas utilizan un esquema SSO	*Repetible*
	Autorización	Los sistemas otorgan permisos que se basan en el grupo al que pertenece el usuario	*Definido*
		Los permisos se administran bajo el principio de privilegios mínimos y separación de tareas	*Inicial*
		Las acciones registradas por los usuarios se registran en una bitácora de eventos	*Repetible*
	Acceso Contextual	Los sistemas utilizan un acceso condicional según la ubicación del usuario	*Inexistente*
		Los sistemas solicitan un método de autenticación adicional cuando un usuario utiliza un dispositivo nuevo	*Definido*

		Los sistemas utilizan un acceso condicional que se basa en el análisis de comportamiento en tiempo real	*Administrado*
Dispositivos	Registro	Los dispositivos que se utilizan se registran ante el proveedor de identidad	*Definido*
		Los dispositivos se inspeccionan para garantizar que cumplen con los requerimientos mínimos establecidos	*Administrado*
		Los dispositivos se administran desde una solución MDM (Mobile Device Management)	*Administrado*
	Protección de datos	Los dispositivos cuentan con sus unidades de disco duro encriptadas	*Optimizado*
		Los dispositivos móviles cuentan con algún acceso biométrico (huella o reconocimiento facial)	*Inicial*
		Se utiliza la detección de amenazas basada en la evaluación de riesgos de los dispositivos en tiempo real	*Definido*
Red	Conexiones remotas	Se utiliza un perímetro definido por *software* (SDP) para establecer los microperímetros de la red	*Definido*
		Se encriptan todas las comunicaciones punto a punto por medio de certificados	*Administrado*
		Se utiliza un agente de confianza entre las conexiones desde una aplicación privada y un usuario autorizado	*Repetible*
	Automatización	Se utilizan mecanismos automatizados que se basan en Machine Learning para la protección ante amenazas	*Definido*
		Se definen reglas de acceso a las aplicaciones mediante un WAF (Web Application Firewall)	*Repetible*
		Existen mecanismos para detectar tráfico anómalo que se basa en comportamiento	*Inicial*
Datos	Clasificación	Existe una taxonomía para la clasificación de los datos	*Optimizado*
		Se encuentra definida una política de clasificación de los datos	*Administrado*
		Existe una estrategia de clasificación y etiquetado de datos	*Definido*
	Políticas de acceso	Los controles de acceso a los datos se definen con base en su sensibilidad	*Definido*
		Los datos sensibles se encuentran encriptados para prevenir el acceso no autorizado	*Administrado*
		Existe una política para los datos que deben compartirse con terceros	*Administrado*
	Prevención de pérdida de información	Existe un mecanismo de monitoreo y alerta para evitar que datos sensibles se copien a un USB	*Definido*
		Existe un mecanismo de monitoreo y alerta para evitar que datos sensibles se envíen por correo electrónico	*Repetible*

		Existe un mecanismo de monitoreo y alerta para evitar que datos sensibles se suban a sitios compartidos	*Repetible*
Aplicaciones	Políticas de acceso	Los controles de acceso a las aplicaciones están definidos por políticas individuales a cada una	*Repetible*
		El acceso se basa en análisis en tiempo real según el usuario, la ubicación, el dispositivo y la aplicación	*Definido*
		Se utiliza un App Proxy para brindar acceso a las aplicaciones locales	*Inexistente*
	Gestión en la nube	Las aplicaciones alojadas en la nube cumplen con la política de configuración organizacional	*Inicial*
		Se cuenta con un CASB capaz de brindar visibilidad completa dentro de todas las aplicaciones	*Inicial*
		Se monitorea constantemente la postura de seguridad de las aplicaciones para garantizar su debido cumplimiento	*Repetible*
Infraestructura	Administración	El acceso de administración a los dispositivos está dado por un límite de tiempo específico (Just-in-Time)	*Definido*
		Se registran las acciones de los administradores y se envían alertas ante administraciones sospechosas	*Administrado*
		Se utiliza telemetría para detectar ataques o anomalías	*Inicial*
	Gestión de vulnerabilidades	Existe una solución SIEM para obtener y analizar registros de eventos de múltiples fuentes	*Repetible*
		Se utiliza análisis de comportamiento para detectar amenazas	*Definido*
		Existe una plataforma SOAR para automatizar la respuesta ante amenazas	*Repetible*

Tabla 10. Resultados en la evaluación del nivel de madurez

Los resultados en esta segunda etapa le permiten a la organización observar sus puntos fuertes y sus áreas de mejora. Es importante identificar los elementos que no cumplen o cumplen parcialmente con la estrategia de Zero Trust para desarrollar un plan de mejora e implementación de nuevos controles. La herramienta brinda también un gráfico que muestra el nivel de madurez por cada una de las áreas evaluadas.

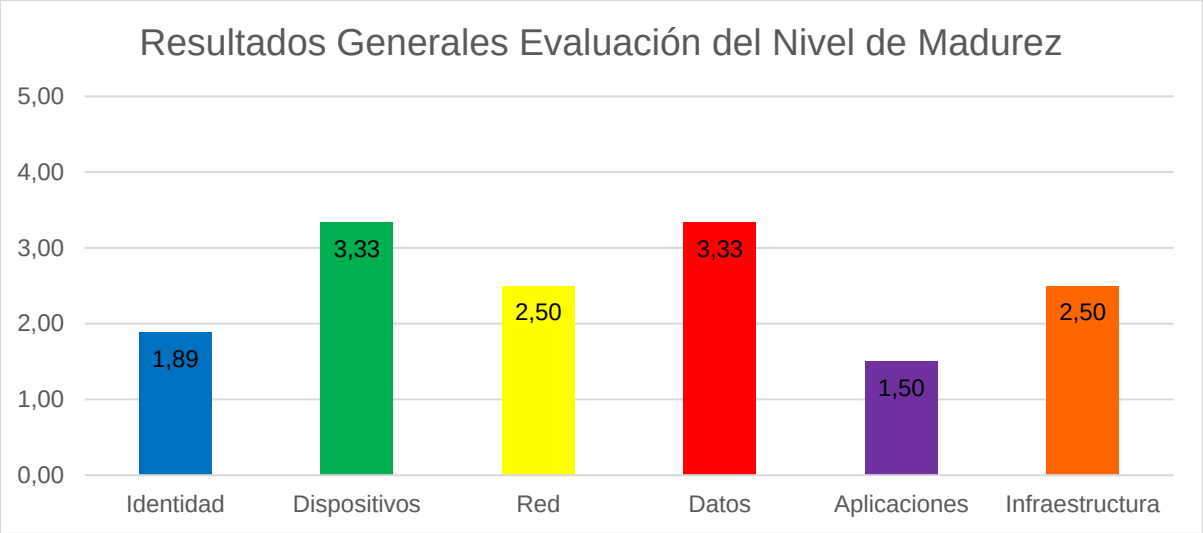


Figura 11. Gráfico con los resultados generales de la evaluación del nivel de madurez

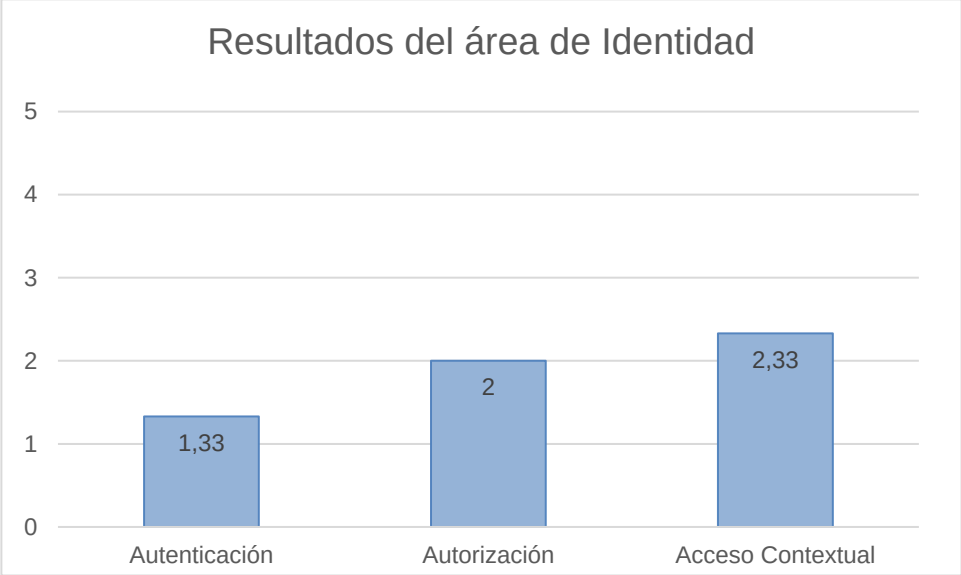


Figura 12. Gráfico con los resultados de la evaluación del nivel de madurez del área de identidad

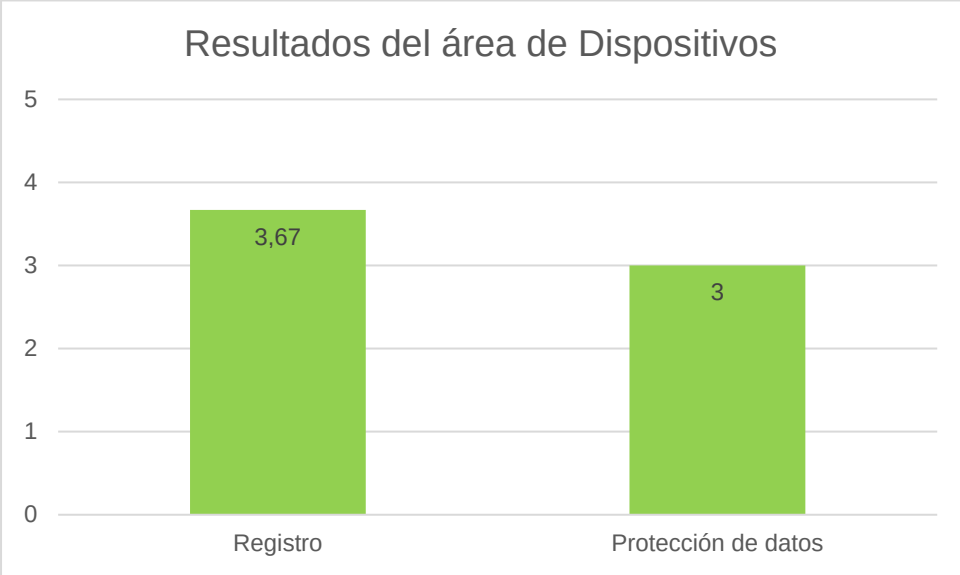


Figura 13. Gráfico con los resultados de la evaluación del nivel de madurez del área de dispositivos

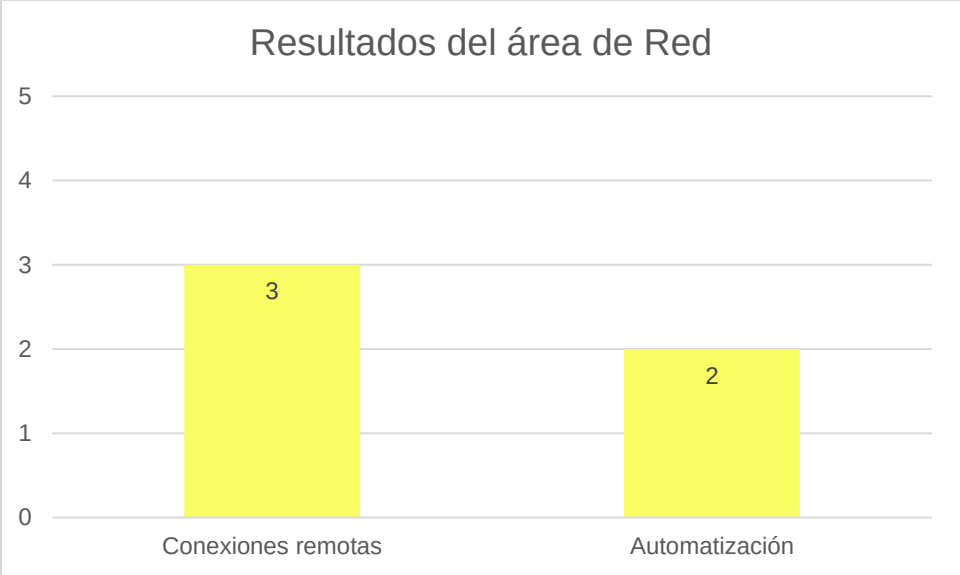


Figura 14. Gráfico con los resultados de la evaluación del nivel de madurez del área de red

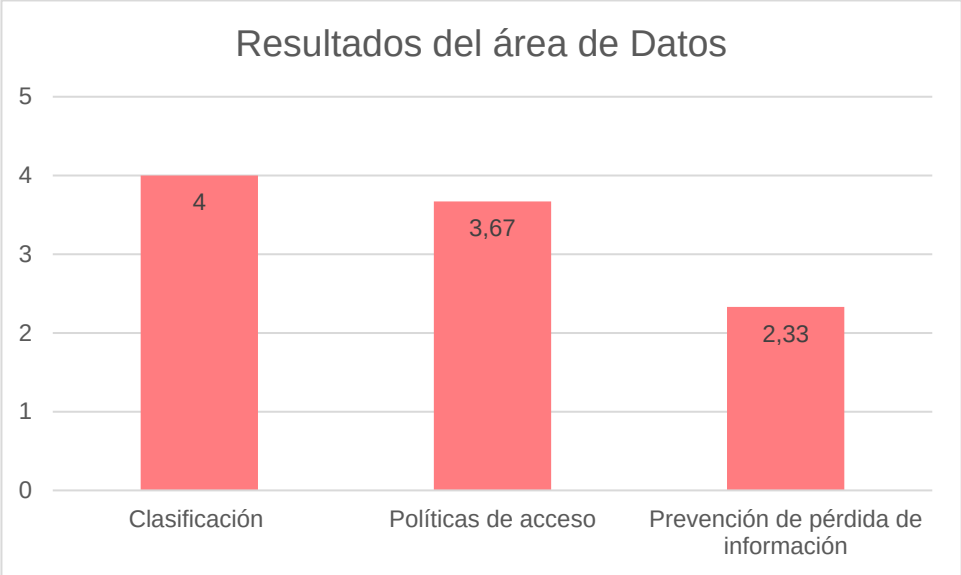


Figura 15. Gráfico con los resultados de la evaluación del nivel de madurez del área de datos

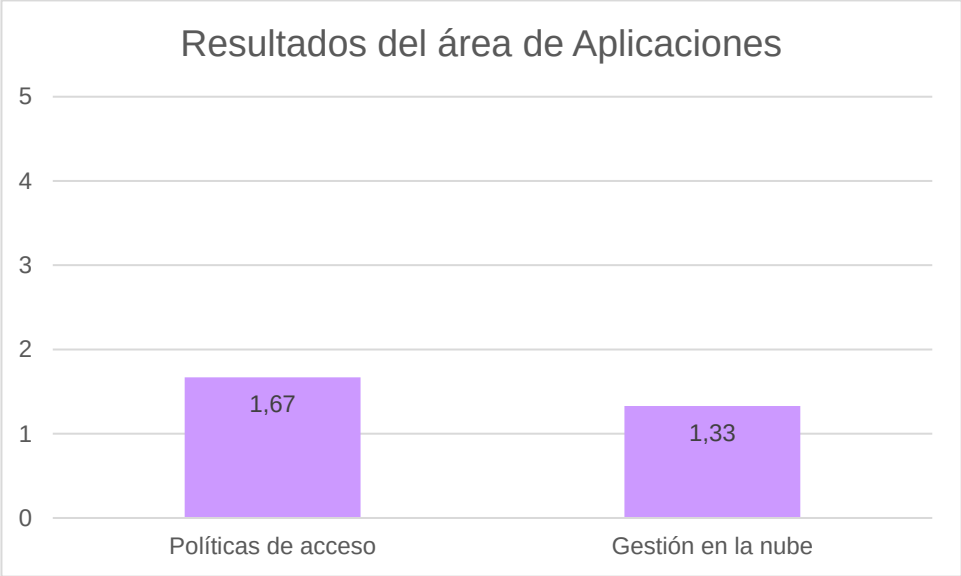


Figura 16. Gráfico con los resultados de la evaluación del nivel de madurez del área de aplicaciones

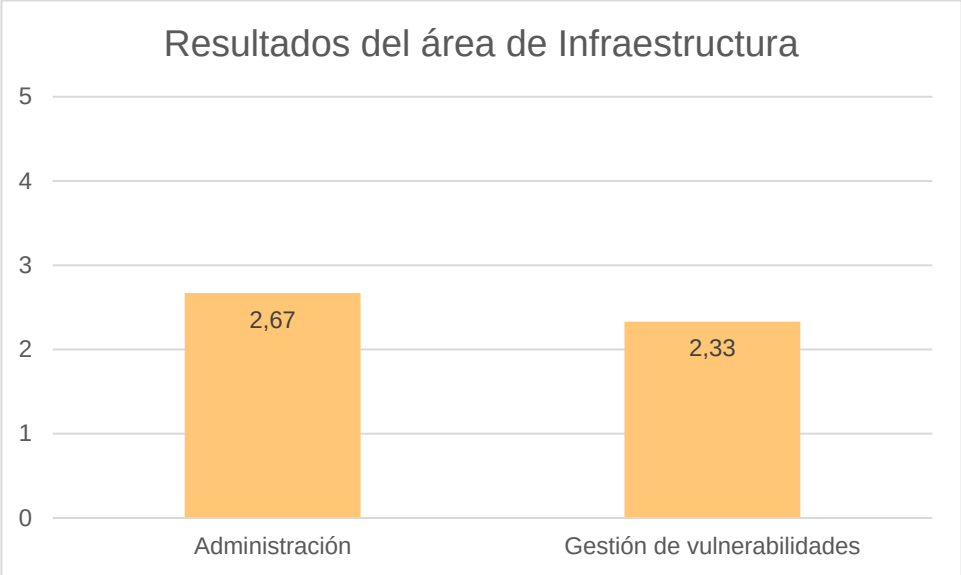


Figura 17. Gráfico con los resultados de la evaluación del nivel de madurez del área de infraestructura

5.3.3 Hallazgos y recomendaciones

Los datos que se obtienen durante la evaluación son los que permiten pasar a la siguiente etapa identificando los hallazgos y sus recomendaciones. A partir de los hallazgos, la organización debe priorizar, según sus objetivos estratégicos, cuáles son las áreas en las que debe trabajar a corto, mediano y largo plazo. Al tomar como ejemplo la evaluación realizada en este caso de uso, la entidad puede tener como objetivo atacar aquellas áreas donde los controles son inexistentes. Por ejemplo, en el área de Identidad se encontraron dos controles con una evaluación Inexistente. Los controles catalogados como inexistentes incluyen el uso de mecanismos de autenticación sin contraseñas y el acceso condicional de acuerdo con la ubicación del usuario. Las recomendaciones para la organización deben

incluir la implementación de estos controles desde niveles básicos y pasando por diferentes etapas de pruebas.

5.3.4 Implementación de controles

Una vez que se identifican los hallazgos y habiendo analizado las recomendaciones propuestas, la organización debe implementar los controles. En esta etapa de implementación, después de analizar las opciones disponibles para cumplir con los requerimientos de Zero Trust, se aplican las soluciones que mejor se adecuen a la realidad de la empresa. Por ejemplo, para el control de autenticación sin contraseñas, la entidad puede implementar una solución a través de una aplicación autenticadora de un tercero que genere un OTP y lo envíe a un dispositivo registrado. La implementación de este control puede requerir varias etapas, pues debe aplicarse en última instancia a todas las aplicaciones y sistemas que se utilizan en la organización.

5.3.5 Mejora continua

La última etapa consiste en aplicar la mejora continua, la cual se alcanza evaluando y midiendo periódicamente. La herramienta de evaluación puede utilizarse nuevamente para medir la evolución en la madurez de los controles aplicados después de cierto tiempo. Para el caso en estudio, una vez que el control de autenticación sin contraseñas se ha implementado, la evaluación de este aumentará y el resultado de madurez es mayor.

5.4 Resultados de la solución

La aplicación de la herramienta de evaluación permite identificar las fortalezas y debilidades de la estrategia de ciberseguridad respecto a un marco de referencia Zero Trust, lo que ayuda a las organizaciones a determinar dónde se encuentran en la escala de madurez de las diferentes áreas evaluadas y validar qué se debe mejorar o cambiar. Los resultados pueden servir de guía a las empresas para definir los controles que deben implementarse y las políticas y estrategias que se deben definir para aumentar el nivel de madurez del modelo de ciberseguridad que se utiliza.

Capítulo 6. Conclusiones y recomendaciones

6.1 Conclusiones

La arquitectura Zero Trust es una estrategia de ciberseguridad moderna compuesta por controles y políticas en diversas áreas de la organización. No es una solución sencilla o un producto específico en el mercado. Por este motivo, el proceso de adopción y transición hacia un modelo más robusto, que se adapte a los requerimientos actuales y brinde la seguridad necesaria ante los nuevos modelos de negocio, manejo de la información, accesibilidad de los datos y amenazas potenciales, es una tarea de múltiples etapas para las organizaciones. Además, es importante contar con una guía que referencie los elementos técnicos necesarios en cada área de trabajo.

Uno de los factores más importantes en cualquier proceso de cambio es conocer con detalle el estado actual de la organización. El caso de las estrategias de ciberseguridad no es la excepción, pues resulta imprescindible describir las políticas y controles actuales para determinar los siguientes pasos a partir de la infraestructura con la que se cuenta e identificar las carencias que se deben atender con mayor prioridad para adoptar los nuevos modelos. Como se mencionó, Zero Trust es una estrategia que comprende múltiples áreas del esquema de ciberseguridad de la organización, por lo que es primordial evaluar el panorama actual y los objetivos de negocio para iniciar la etapa de transición.

Es importante mantener una evaluación constante en las diferentes áreas una vez que el proceso de transición ha iniciado para medir la madurez de los controles que se implementan e identificar las áreas que deben mejorarse u optimizarse. Asimismo, la máxima de William Thomson Kelvin afirma que *lo que no se define no se puede medir y lo que no se puede medir no se puede mejorar*, cada una de las áreas involucradas en la estrategia de ciberseguridad debe identificarse y evaluarse periódicamente. Las amenazas cibernéticas se transforman y evolucionan de manera continua, lo que obliga a los controles de seguridad a mantenerse actualizados y de acuerdo con las nuevas exigencias y posibles superficies de ataque. La medición de la madurez en cada una de las áreas involucradas permite medir ese nivel de solidez y robustez en los controles y políticas que se han implementado, así como identificar aquellas áreas donde se requieren mejoras con mayor prioridad.

El proceso de mejora continua permite establecer objetivos y metas en plazos definidos, optimizar los procesos y controles y alcanzar un mayor nivel de madurez. Para esto, es prioritario contar con herramientas de evaluación que puedan

aplicarse de manera periódica y se ajusten a los objetivos y requerimientos de cada organización. Es importante también que estas herramientas sean claras y concisas en los elementos que se están evaluando para obtener resultados fiables que sirvan como insumo en la toma de decisiones y el desarrollo de la estrategia de ciberseguridad.

6.2 Recomendaciones

En este apartado se incluyen algunas recomendaciones aplicables a las organizaciones en proceso de adoptar un modelo de ciberseguridad alineado al modelo Zero Trust. En primera instancia, es importante conocer la terminología técnica asociada para explicar de una manera más eficaz los beneficios de la implementación de un modelo Zero Trust a las diferentes unidades de negocio, así como las implicaciones que tendrían los potenciales cambios en la experiencia de uso de los usuarios.

Una de las tareas más importantes es identificar y clasificar los activos de la organización. Debe estar claro qué es lo que se busca proteger, dónde se almacena la información y cómo está clasificada. Además, se debe identificar el tipo de dispositivos que utilizan los usuarios y establecer una línea base del flujo de información por un tiempo establecido.

Es importante también proponer casos de uso específicos para los usuarios, donde se ejemplifiquen las principales diferencias en el proceso, los beneficios que se pueden adquirir y el riesgo de no realizar los cambios propuestos. En este apartado se pueden incluir experiencias, tanto positivas como negativas, que se hayan observado en otras organizaciones.

No existe una receta o fórmula mágica que funcione para todas las organizaciones de esta forma, por lo que es necesario identificar de forma clara los objetivos que se tienen a corto, mediano y largo plazo, el presupuesto disponible para el desarrollo del modelo y las áreas de trabajo prioritarias. Es recomendable haber realizado un diagnóstico de la situación actual de la empresa, que incluya un análisis de riesgos y una proyección del retorno de la inversión.

Existen múltiples soluciones en el mercado que ofrecen controles alineados con un modelo Zero Trust, por lo que es recomendable analizar y estudiar cuál es el que se adapta mejor a las necesidades de cada empresa según sus objetivos y presupuesto.

Por último, las actividades que se relacionan con el proceso de adopción y mejora de la estrategia Zero Trust deben someterse a un ciclo de gestión que permita mantener los controles y las políticas actualizadas ante los constantes escenarios de cambio en el mundo de la seguridad de la información.

En síntesis, las recomendaciones que se sugieren a partir del desarrollo de la herramienta para determinar la viabilidad de implementación de una arquitectura Zero Trust son las siguientes:

- Identificar y clasificar los activos de la organización
- Evaluar los controles actuales
- Identificar los datos sensibles y la información que se desea proteger

- Establecer líneas base durante plazos definidos para conocer el flujo de datos e interacciones habituales en los sistemas y aplicaciones.
- Definir políticas de acceso y gestión de dispositivos.
- Automatizar procesos de respuesta a incidentes.
- Construir casos de uso para las diferentes áreas del modelo.
- Analizar las soluciones del mercado para identificar la que mejor se adapte a las necesidades de la entidad.
- Gestionar un ciclo de mejora continua para aumentar la madurez del modelo Zero Trust a través del tiempo.

Referencias

Akamai. (2020). *How To Guide: Zero Trust Security Transformation*. https://www.akamai.com/site/en/documents/white-paper/how-to-guide-zero-trust-security-transformation.pdf

Cybersecurity Insiders. (2020). *Zero Trust Adoption Report*. https://www.cybersecurity-insiders.com/wp-content/uploads/2020/01/2019-Zero-Trust-Security-Report_Generic.pdf

DoD. (2021). *Department of Defense (DOD) Zero Trust Reference Architecture*. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

Flexera. (2021). *Flexera 2021 State of the Cloud Report*. https://resources.flexera.com/web/pdf/Flexera-State-of-the-Cloud-Report-2021.pdf

Forrester. (2019). *A Practical Guide To A Zero Trust Implementation*. https://www.forrester.com/report/a-practical-guide-to-a-zero-trust-implementation/RES157736

Kindervag, J. (2010). *Build security into your network DNA: The zero trust network architecture*. Forrester Research Inc. http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf

Micitt. (2017). *Protección de datos personales*. https://micitt.go.cr/sites/default/files/7.-infografia-proteccion-de-datos-personales.pdf

Microsoft. (2021). *Zero Trust Maturity Model*. https://download.microsoft.com/download/f/9/2/f92129bc-0d6e-4b8e-a47b-288432bae68e/Zero_Trust_Vision_Paper_Final%2010.28.pdf

NIST. (2019). *Zero Trust Architecture*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

OKTA. (2020). *The State of Zero Trust Security in Global Organizations*. https://www.okta.com/sites/default/files/pdf/zero-trust-security-in-global-org.pdf

Palo Alto. (2019). *Understanding Zero Trust Terminology*. https://www.paloaltonetworks.com/resources/zero-trust

RedGealc. (2020). *Costa Rica mejora en temas de ciberseguridad*. https://www.redgealc.org/contenido-general/noticias/costa-rica-mejora-en-temas-de-ciberseguridad/

Zscaler. (2021). *The Network Architect Guide to Adopting a Zero Trust Network Access Service*. https://www.zscaler.com/resources/white-papers/network-architects-guide-to-zero-trust-network-access.pdf

Anexos

Anexo 1. Herramienta de evaluación de madurez Zero Trust

Nombre de la empresa

Herramienta de evaluación de Madurez Zero Trust

Herramienta de evaluación de Madurez Zero Trust

Tabla de Contenidos

Versiones

Versión	Actualizado por	Fecha de Modificación	Descripción del cambio
1.0	Jose Pablo Ulate	18/4/2021	Creación del documento

Resumen

Este documento es un instrumento para la evalaución de madurez del Modelo Zero Trust en las empresas

Matriz de evaluación de la Situación Actual de la Empresa

Área	Pregunta	Respuesta
Identidad	¿Los usuarios de la organización se autentican por medio de mecanismos de múltiple factor a los sistemas?	
	¿Las aplicaciones de la organización utilizan un sistema único de inicio de sesión (SSO)?	
	¿La gestión de permisos se basa en el principio de privilegios mínimos?	
Dispositivos	¿Los dispositivos que se conectan a la red corporativa se encuentran registrados?	
	¿Existe un método para garantizar que los dispositivos cumplen con los requisitos de seguridad para poder conectarse a la red?	
	¿Se ha desarrollado alguna política de prevención de pérdida de datos en los dispositivos?	
Red	¿Las redes se encuentran segmentadas para prevenir el movimiento lateral?	
	¿La comunicación punto a punto viaja encriptada?	
	¿Existen mecanismos de monitoreo y detección de tráfico no habitual?	
Datos	¿Existe una política de clasificación de datos según su sensibilidad?	
	¿Se han establecido controles para determinar si los datos pueden ser compartidos a terceros?	
	¿Los datos sensibles se encuentran encriptados?	
Aplicaciones	¿El acceso a las aplicaciones está basado en políticas?	
	¿Las aplicaciones críticas de negocio están siendo monitoreadas en tiempo real para prevenir ataques o actividades anómalas?	
	¿El acceso a las aplicaciones está limitado únicamente a los usuarios que las requieren?	
Infraestructura	¿Existe un plan de respuesta a incidentes?	
	¿Se utilizan herramientas de monitoreo y recolección de registros de eventos?	
	¿Los privilegios de administración a los equipos se otorgan por un tiempo definido?	

Niveles de Madurez basados en el estándar CMM		
0	Inexistente	El control aplica, pero no se ha definido ninguna acción, política o procedimiento
1	Inicial	El control se encuentra en un estado inicial, no está totalmente definido ni documentado
2	Repetible	El control cuenta con herramientas o procedimientos asociados, se obtienen resultados consistentes
3	Definido	El control está documentado, con políticas y procedimientos definidos y estandarizados, con revisiones periódicas
4	Administrado	El control es monitoreado con métricas e indicadores
5	Optimizado	El control tiene una mejora continua, con un alto nivel de automatización

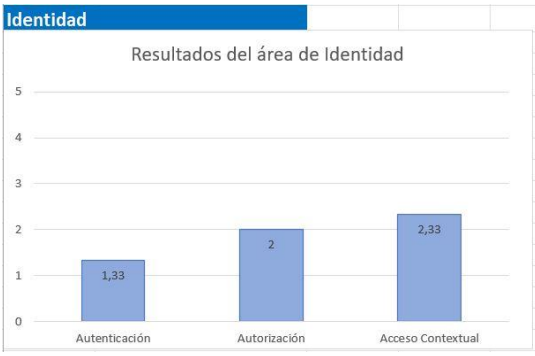
Matriz de evaluación de madurez

Área	Categoría	Subcategoría	Evaluación
Identidad	Autenticación	Los sistemas utilizan autenticación de factor múltiple (MFA)	
		Los sistemas permiten la autenticación sin contraseñas (utilizando algún método alternativo como MFA)	
		Los sistemas utilizan un esquema SSO	
	Autorización	Los sistemas otorgan permisos que se basan en el grupo al que pertenece el usuario	
		Los permisos se administran bajo el principio de privilegios mínimos y separación de tareas	
		Las acciones registradas por los usuarios se registran en una bitácora de eventos	
	Acceso Contextual	Los sistemas utilizan un acceso condicional según la ubicación del usuario	
		Los sistemas solicitan un método de autenticación adicional cuando un usuario utiliza un dispositivo nuevo	
		Los sistemas utilizan un acceso condicional que se basa en el análisis de comportamiento en tiempo real	
Dispositivos	Registro	Los dispositivos que se utilizan se registran ante el proveedor de identidad	
		Los dispositivos se inspeccionan para garantizar que cumplen con los requerimientos mínimos establecidos	
		Los dispositivos se administran desde una solución MDM (Mobile Device Management)	
	Protección de datos	Los dispositivos cuentan con sus unidades de disco duro encriptadas	
		Los dispositivos móviles cuentan con algún acceso biométrico (huella o reconocimiento facial)	
		Se utiliza la detección de amenazas basada en la evaluación de riesgos de los dispositivos en tiempo real	
Red	Conexiones remotas	Se utiliza un perímetro definido por *software* (SDP) para establecer los microperímetros de la red	
		Se encriptan todas las comunicaciones punto a punto por medio de certificados	
		Se utiliza un agente de confianza entre las conexiones desde una aplicación privada y un usuario autorizado	

	Automatización	Se utilizan mecanismos automatizados que se basan en Machine Learning para la protección ante amenazas	
		Se definen reglas de acceso a las aplicaciones mediante un WAF (Web Application Firewall)	
		Existen mecanismos para detectar tráfico anómalo que se basa en comportamiento	
Datos	Clasificación	Existe una taxonomía para la clasificación de los datos	
		Se encuentra definida una política de clasificación de los datos	
		Existe una estrategia de clasificación y etiquetado de datos	
	Políticas de acceso	Los controles de acceso a los datos se definen con base en su sensibilidad	
		Los datos sensibles se encuentran encriptados para prevenir el acceso no autorizado	
		Existe una política para los datos que deben compartirse con terceros	
	Prevención de pérdida de información	Existe un mecanismo de monitoreo y alerta para evitar que datos sensibles se copien a un USB	
		Existe un mecanismo de monitoreo y alerta para evitar que datos sensibles se envíen por correo electrónico	
		Existe un mecanismo de monitoreo y alerta para evitar que datos sensibles se suban a sitios compartidos	
Aplicaciones	Políticas de acceso	Los controles de acceso a las aplicaciones están definidos por políticas individuales a cada una	
		El acceso se basa en análisis en tiempo real según el usuario, la ubicación, el dispositivo y la aplicación	
		Se utiliza un App Proxy para brindar acceso a las aplicaciones locales	
	Gestión en la nube	Las aplicaciones alojadas en la nube cumplen con la política de configuración organizacional	
		Se cuenta con un CASB capaz de brindar visibilidad completa dentro de todas las aplicaciones	
		Se monitorea constantemente la postura de seguridad de las aplicaciones para garantizar su debido cumplimiento	
Infraestructura	Administración	El acceso de administración a los dispositivos está dado por un límite de tiempo específico (Just-in-Time)	
		Se registran las acciones de los administradores y se envían alertas ante administraciones sospechosas	
		Se utiliza telemetría para detectar ataques o anomalías	
	Gestión de vulnerabilidades	Existe una solución SIEM para obtener y analizar registros de eventos de múltiples fuentes	
		Se utiliza análisis de comportamiento para detectar amenazas	

		Existe una plataforma SOAR para automatizar la respuesta ante amenazas	

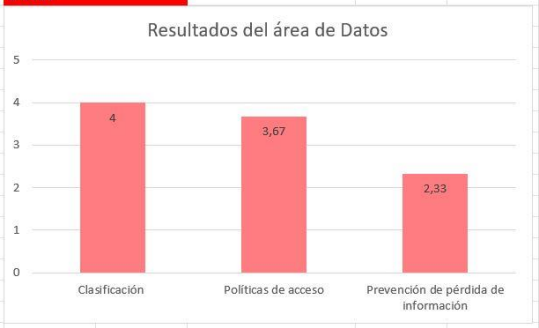
Identidad



Dispositivos

Red

Datos



Aplicaciones

Infraestructura