ANÁLISIS DEL MODELO DE SEGURIDAD ZERO TRUST Y LAS CONSIDERACIONES GENERALES APLICABLES A CUALQUIER ORGANIZACIÓN PÚBLICA EN COLOMBIA.

JORGE LUIS GAITAN BAQUERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FUSAGASUGÁ
2022

ANÁLISIS DEL MODELO DE SEGURIDAD ZERO TRUST Y LAS CONSIDERACIONES GENERALES APLICABLES A CUALQUIER ORGANIZACIÓN PÚBLICA EN COLOMBIA.

JORGE LUIS GAITAN BAQUERO

Proyecto de Grado – Monografía presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Cesar Enrique Silva García
Director de Trabajo de Grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FUSAGASUGÁ
2022

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Fusagasugá, 31 de mayo del 2022

AGRADECIMIENTOS

A mi Madre, por su valioso apoyo incondicional y la confianza brindada. Le agradezco por su contribución en el cumplimiento de mis objetivos como persona y como profesional.

A las familias Baquero-Ortiz, por su motivación y respaldo incondicional en cada decisión y proyecto que he llevado a cabo.

A los docentes y tutores de la Universidad, por sus orientaciones y apoyo durante este proceso, sin el cual no hubiera sido posible la realización de éste trabajo y en especial, al Ingeniero Cesar Silva, quien compartió sus conocimientos y dedicó el tiempo necesario para aclarar cualquier tipo de inquietud.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ACTIVO DE LA INFORMACIÓN: Desde la óptica organizacional, es preciso decir que “son los datos que tienen significado para una entidad”[1], siendo esta la base fundamental para llevar a cabo las actividades necesarias en el cumplimiento de sus objetivos.

AMENAZA: Desde el contexto de seguridad de la información, se puede describir este concepto como la “causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización”[2]

AUTENTICACIÓN: Proceso mediante el cual se realiza la validación de credenciales ejecutado de forma correcta y adecuada en un sistema de información.

CIBERSEGURIDAD: “Es la práctica que permite defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos.”[3] De esta forma se apropian las estrategias necesarias para la protección de información en un entorno digital.

ESTÁNDARES DE SEGURIDAD: “Son una herramienta que apoya la gestión de la seguridad informática, ya que los ambientes cada vez más complejos requieren de modelos que administren las tecnologías de manera integral, sin embargo, existen distintos modelos aplicables en la administración de la seguridad.”[4]

GESTIÓN DEL RIESGO: Se entiende como aquellas “actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.”[5]

HACKEO: Este concepto es apropiado en el contexto de la informática cuando se “hace referencia a las actividades que buscan comprometer los dispositivos digitales, como ordenadores, teléfonos inteligentes, tabletas e incluso redes, se caracterizan como actividad ilegal por parte de los ciberdelincuentes, motivados por

---

[1] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN. Guía para la Gestión y Clasificación de Activos de Información. [Sitio web] Bogotá D.C: MINTIC. [Consultado: 11 julio 2021] Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

[2] ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. UNE-ISO/IEC 27000. 2 ed. Madrid, España. AENOR 2014. 30p.

[3] KASPERSKY LAB. ¿Qué es la ciberseguridad? [Sitio web] Centro de recursos. [Consultado: 11 julio 2021] Disponible https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[4] REMOLINA BECERRA, Luis. Diseño de un modelo de seguridad informática a una empresa en su sistema de monitoreo del área de tecnología. Trabajo para optar al título Ingeniero de Telecomunicaciones. Facultad de Ingeniería. Universidad Cooperativa De Colombia. 2019. 68 pp.

[5] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del riesgo. Principios y directrices. ISO 31000. Bogotá D.C.: El Instituto, 2011. 34 p.

la obtención de algún beneficio económico, por protesta, recopilación de información (espionaje), e incluso sólo por la diversión del desafío."[6]

MONITOREO: Entiéndase por las actividades de "verificación, supervisión, observación crítica o determinación continúa del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado."[7]

PERÍMETRO: En estrategias de seguridad informática, este término es utilizado para describir "el límite seguro entre el lado privado y administrado localmente de una red, a menudo la intranet de una empresa, y el lado público de una red, a menudo la conexión a Internet."[8]

SEGURIDAD DE LA INFORMACIÓN: Según lo especifica la norma ISO/IEC 27001, este concepto lo conforman tres dimensiones principales: "la confidencialidad, la disponibilidad y la integridad. Con el objetivo de garantizar el éxito empresarial sostenido así como su continuidad, y minimizar impactos, la seguridad de la información conlleva la aplicación y la gestión de medidas de seguridad adecuadas que implica la consideración de una amplia gama de amenazas."[9]

RIESGO: En relación a la informática, se expresa como la "posibilidad determinada a una amenaza pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias."[10]

USUARIO: En un concepto generalizado desde la óptica de un sistema informático puede referirse a la persona que interactúan o realiza una acción determinada, no obstante, puede estar clasificado o estandarizado conforme a unos roles preestablecidos dentro de dicho sistema.

VULNERABILIDAD: En el contexto de la seguridad de la información, se relaciona como "debilidad de un activo o control que puede ser explotada por una o más amenazas."[11]

---

[6] MALWAREBYTES. Todo sobre el hackeo. [Sitio web] [Consultado: 11 julio 2021] Disponible en: https://es.malwarebytes.com/hacker/

[7] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del riesgo. Principios y directrices. ISO 31000. Bogotá D.C.: El Instituto, 2011. 34 p.

[8] CIBERSEGURIDAD. Seguridad perimetral [sitio web]. [Consultado: 22 de julio de 2021]. Disponible en: https://ciberseguridad.com/servicios/seguridad-perimetral/#:~:text=Un%20per%C3%ADmetro%

[9] ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. UNE-ISO/IEC 27001. 2 ed. Madrid, España. AENOR 2014. 30p.

[10] ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. UNE-ISO/IEC 27000. 2 ed. Madrid, España. AENOR 2014. 30p.

[11] Ibíd., p. 17.

VERIFICAR: Visto desde la óptica de la seguridad informática, puede entenderse como “el proceso de comparar con una copia de los datos para asegurarse de que sean exactamente los mismos que los datos originales”[12] y de esta forma validar una acción.

ZERO TRUST: Desde el contexto de las redes informáticas, este concepto hace referencia cuando “supone que no se otorga una confianza implícita a los activos o cuentas de usuario basándose únicamente en su ubicación física o de red o en función de la propiedad de los activos”[13]

[12] TECNOLOGIAS INFORMACIÓN. Verificación de Datos: Principios y Métodos. [sitio web]. [Consultado: 22 de julio de 2021]. Disponible en: https://www.tecnologias-informacion.com/verificacion.html

[13] INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA. Computer Security Resource Center. [sitio web]. Gaithersburg: NIST. [Consulta: 06 de junio de 2021]. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-207/archive/2020-02-13

RESUMEN

En los notables acontecimientos de los últimos años, se observa un incremento considerable en los ataques a la información, siendo esta de vital importancia para la continuidad de un negocio o una nación. En igual proporción, los ciberataques pueden llevarse a cabo desde el interior de la organización (usuarios, redes y aplicaciones) o al exterior de la misma, sin embargo, las nuevas tendencias corporativas, como el teletrabajo o la computación en la nube, han venido evidenciando las falencias en los controles de seguridad, ya que gran parte de las estrategias están diseñadas bajo la protección de perímetro que hace la distinción de una zona de confianza donde los usuarios de una entidad pueden utilizar los dispositivos conectados a una red interna y hacer uso de las aplicaciones con el mínimo de restricciones posibles, entendiendo este comportamiento, como una brecha en la protección de los activos de la información. De esta forma, el presente trabajo pretende hacer una revisión documental sobre el modelo de seguridad de "Zero Trust" y las consideraciones de su posible implementación en las organizaciones públicas colombianas, permitiendo de esta forma brindar una perspectiva general sobre la importancia de contar con el conjunto de medidas óptimas que minimicen el riesgo de un ataque informático y el impacto que pueda tener en la estructura de negocio para una organización.

Por lo tanto, el modelo de seguridad de "Zero Trust", se define como las estrategias que se encargan de la identificación, verificación y automatización de los lineamientos de seguridad al interior de una organización que serán aplicados en los recursos tecnológicos y fundamentalmente a los usuarios. Para llevar a cabo este propósito, el modelo presenta tres pilares; verificar y asegurar, accesos limitados y el monitoreo constante.

Para la elaboración de este trabajo se establecerán como fases de investigación la construcción del estado del arte acerca de modelos de seguridad, una revisión contextual sobre el enfoque de seguridad de las organizaciones en Colombia, un consolidado documental sobre los componentes y principales características de "Zero Trust" y de esta manera finalizar, con la presentación de las consideraciones requeridas para utilizar un esquema de "Zero Trust" en las organizaciones colombianas, enfocado a la seguridad informática y el cumplimiento normativo.

Palabras claves: Análisis, activo de la información, ciberseguridad, entidades públicas, Zero Trust.

ABSTRACT

In the notable events of recent years, there has been a considerable increase in attacks on information, this being of vital importance for the continuity of a business or a nation. In the same proportion, cyberattacks can be carried out from within the organization (users, networks and applications) or outside it, however, new corporate trends, such as teleworking or cloud computing, have been showing failures in security controls, since most of the strategies are designed under perimeter protection that distinguishes between a trusted zone where users of an entity can use devices connected to an internal network and make use of applications with the least possible restrictions, understanding this behavior as a breach in the protection of information assets. In this way, this work intends to make a documentary review on the “Zero Trust” security model and the considerations of its possible implementation in Colombian public organizations, thus allowing to provide a general perspective on the importance of having the set of optimal measures that minimize the risk of a computer attack and the impact it may have on the business structure.

Therefore, the "Zero Trust" security model is defined as the strategies that are responsible for the identification, verification and automation of the security guidelines within an organization that will be applied to technological resources and fundamentally to the users. To carry out this purpose, the model has three pillars; verify and secure limited access and constant review.

For the elaboration of this work, the construction of the state of the art about security models, a contextual review on the security approach of organizations in Colombia, a consolidated documentary on the components and main characteristics of "Zero Trust” and thus finalize, with the presentation of the considerations required to use a “Zero Trust ”scheme in Colombian organizations focused on computer security and regulatory compliance.

Keywords: Analysis, information asset, cybersecurity, public entities, Zero Trust.

INTRODUCCIÓN

El auge tecnológico ha permitido la utilización de elementos capaces de ofrecer múltiples servicios en el uso y aprovechamiento de las tecnologías de la información, y como su término lo indica es aquella tecnología que se utiliza a través de las telecomunicaciones, ya sea el uso de medios digitales, Internet, redes inalámbricas, teléfonos móviles y otros sistemas de comunicación. Las TIC desempeñan un papel importante en la vida de todos en la actualidad, ya que, con la ayuda de este tipo de tecnologías, los usuarios están obteniendo gran variedad de servicios directamente en su casa, ya sea comprando o pagando cualquier tipo de factura solo usando las redes de telecomunicaciones. Las TIC proporcionan un acceso fácil a toda la información disponible y accesible en la red, incluso el acceso a la educación ha mejorado gracias al uso de las TIC.

La tecnología de las TIC juega un papel importante en todos los campos de la forma de gobierno, en el que la administración pública es uno de ellos. Las tecnologías TIC son un requisito de la actualidad, es así que la administración pública utiliza las tecnologías TIC en todos los campos ya sea para brindar servicios a los ciudadanos o brindarles la información necesaria. Por lo cual, un gran número de organizaciones desarrollan sus actividades basadas en estos recursos, tal como las organizaciones públicas, que en Colombia son denominadas como entidades públicas "que pertenecen y son administradas por el Estado, entendiendo como Estado todo lo que forma parte de una sociedad, es decir que las entidades estatales por ser parte de una sociedad trabajan en beneficio de la Nación y de la ciudadanía colombiana."[14] Sin embargo, este manejo de la información puede conllevar riesgos para las entidades donde se afectaría la confidencialidad, integridad y disponibilidad.

Entiéndase que esta misma entidad pública tiene la responsabilidad de brindar seguridad de la información, acorde con la normatividad legal vigente, la cual es percibida como la "preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas"[15]

De esta forma, la creciente masificación de servicios basados en la nube, computación móvil, Internet de las cosas (IoT) y traer su propio dispositivo (BYOD) a la fuerza laboral han cambiado el panorama tecnológico para la empresa

[14] CAMPOS FARUK. Seguridad de la información en el sector público colombiano. [sitio web]. Bogotá D.C. [Consultado: 02 de octubre de 2021]. Disponible en: http://polux.unipiloto.edu.co:8080/00002657.pdf

[15] ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. UNE-ISO/ICE 27001. 2 ed. Madrid, España. AENOR 2016. 30p.

moderna. Las arquitecturas de seguridad que se basan en firewalls de red y redes privadas virtuales (VPN) para aislar y restringir el acceso a los recursos y servicios tecnológicos corporativos ya no son suficientes para una fuerza laboral que regularmente requiere acceso a diversas aplicaciones y recursos que existen más allá de los límites de las redes corporativas tradicionales. El modelo de “Zero trust” es un enfoque holístico de la seguridad de la red, que requiere la verificación de cada persona y dispositivo que cada vez intenta acceder a recursos en una red privada. Esto sigue siendo cierto, sin importar si ese dispositivo o persona ya está dentro o fuera del perímetro de la red.

Esto resuelve muchos problemas en el modelo de seguridad de red tradicional, que se basaba en el concepto de perímetro de seguridad. El acceso a una red estaba estrictamente controlado, pero una vez dentro, las conexiones eran confiables de forma predeterminada y un atacante podría causar daños importantes. En el entorno distribuido actual, con datos y aplicaciones que se ejecutan en servicios remotos en la nube, empleados que trabajan desde casa o desde dispositivos personales, y el uso creciente de dispositivos móviles e IoT, el enfoque del perímetro de seguridad ya no es válido y está siendo reemplazado por el modelo de “Zero Trust”.

1 DEFINICIÓN DEL PROBLEMA

A lo largo de las últimas décadas, se ha contemplado la incursión de la tecnología en múltiples aspectos de la sociedad, siendo ésta un pilar en el adelanto cultural, social y económico de la vida moderna. De esta forma se han generado grandes inventos o creaciones en la forma como nos comunicamos e interactuamos con nuestros semejantes. Sin embargo, haciendo un especial énfasis en las contribuciones al sector productivo, se puede mencionar que la conformación de la internet ha dispuesto alternativas y modelos de negocios que brindan servicios especializados a toda clase de público. En este contexto, se evidencia un común denominador que enmarca la prestación de estos servicios, a "La información", la cual es considerada como un activo importante en los entornos empresariales y esencial para el funcionamiento de una estructura de negocio. Principalmente se puede consolidar en dos tipos de formatos; digital y físico donde, así mismo puede ser transmitida[16]. Por tal razón puede ser susceptible a todo tipo de amenazas y afectar la operatividad de las empresas y las partes de interés que la conforman. Por lo que se hace necesario brindar alternativas de protección y resguardo ante los riesgos internos o externos de la organización.

En el último año, según la agencia "We are Social", se observa un incremento del 7.3% en la utilización de internet a nivel global y así mismo un aumento del 77% en las transacciones mediante el comercio electrónico. En gran proporción, puede ser consecuencia, a las condiciones y medidas sociales adoptadas por los largos periodos de confinamiento que se derivó de la pandemia del "COVID 2019"[17]. No obstante, esto generó una mayor atención a la explotación de vulnerabilidades en los sistemas de información comerciales, a tal grado que "63% de las intrusiones maliciosas en redes son resultado de datos de autenticación (nombres de usuario y contraseñas) que han sido comprometidos en otros ciberataques."[18]

Las anteriores estadísticas, deslumbra predicciones sobre los ataques que pueden llegar a sufrir una empresa y los devastadores daños que pueden afectar toda su estructura de negocio, debido a la implementación de modelos de seguridad que se basan en la protección de perímetro, dejando expuesta la información al interior de las redes corporativas, o lo que comúnmente es conocido por la zona de confianza. Tanto así que, "los límites de cualquier infraestructura corporativa se han desdibujado tanto en los últimos años que ha dado paso a un gran ecosistema

[16] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de Seguridad de la Información, Visión de conjunto y vocabulario. ISO/IEC 27000. Bogotá D.C.: El Instituto, 2014. 30 p.

[17] ORGANIZACIÓN MUNDIAL DE LA SALUD. [sitio web]. Ginebra: OMS. [Consulta: 29 de Mayo de 2021]. Disponible en: https://www.who.int/es/emergencies/diseases/novel-coronavirus-2019

[18] POGII, Nicolás. 30 Estadísticas de Seguridad Informática que importan (Actualizadas 2021) En: THE MISSING REPORT. [sitio web]. San Francisco: Autor [Consulta: 29 de Mayo de 2021]. Disponible en: https://preyproject.com/blog/es/30-estadisticas-seguridad-informatica/

conectado en el cual desconfiar de todo es lo mejor para las empresas."[19]

1.1 ANTECEDENTES DEL PROBLEMA

Es bien conocido, en la cultura en general, que conforme avanza el desarrollo tecnológico y sus brillantes facilidades en el mundo cotidiano, de forma paralela, también lo hace las metodologías para vulnerar y explotar estos sistemas o inventos que facilitan la ejecución de tareas en los entornos empresariales y domésticos. Sin embargo, en gran medida las repercusiones que puede llegar a ocurrir a las entidades comerciales, será altamente impactante para el desarrollo de su estructura de negocio, y en algunos casos puede conllevar a sanciones administrativas y legales.

Es así que, desde el inicio de la computación, se han detectado sin números de incidentes de seguridad, como por mencionar algunos casos, a finales del año 1988 "pasaría a la historia como el día en el que las reglas de internet cambiaron para siempre, evidenciando que existían vulnerabilidades informáticas que debían corregirse. El punto de partida de este progresivo cambio fue la creación, lanzamiento y rápida expansión de un malware autor replicable llamado Morris, que debe su nombre al inventor, Robert Tappan Morris, hijo de un famoso criptógrafo. Los efectos de este virus informático fueron devastadores: afectó a la actividad de los equipos, limitó las conexiones durante días y accedió a información sensible."[20] Considerando que esta acción se llevará a cabo en una entidad de servicios públicos o una cadena de suministros, el daño generado sería invalorable a la población de cualquier nación.

En cuanto a los incidentes un poco más actuales podremos encontrar, el comúnmente llamado "WannaCry", Según el portal se Eset WeliveSecurity, "Un 12 de mayo, pero del año 2017, un nuevo virus informático ponía en alerta a empresas y usuarios de todo el mundo. Gran cantidad de equipos de diferentes compañías en 150 países se veían afectados por una amenaza que se propagaba sin precedentes. El ransomware WannaCry cifraba los archivos de un equipo e inmediatamente se propagaba a otro y otro equipo en la red, explotando una vulnerabilidad que pocos habían parcheado y sin ningún tipo de intervención por parte del usuario."[21] Tuvo un alcance tan importante este incidente que, en el mismo año se reporta por parte

[19] MARCAL, David. 'Zero Trust' desconfía por naturaleza. *Revista Red seguridad.* 2020. nro 91. pp 56-58.

[20] B12 ADMARK. Los 5 ataques informáticos más famosos de la última década. [Consulta: 23 de marzo de 2022]. Disponible en: https://agenciab12.com/noticia/5-ataques-informaticos-mas-famosos-ultima-decada

[21] ESET, WE LIVE SECURITY. WannaCry: tres años después sigue siendo una amenaza activa de la cual debemos aprender. [Consulta: 20 de Julio de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2020/05/12/wannacry-tres-anos-despues-una-amenaza-activa-debemos-aprender/

de las autoridades competentes una penetración de este malware en el Instituto Nacional de Salud, generando la suspensión de múltiples servicios en su portal web.

Como si fuera poco, según estudios realizados por diversas compañías de seguridad informática acerca de las tendencias de ciberataques en el país, mencionan que “en Colombia, se encontró que los incidentes más comunes tienen que ver con malware (35%), ransomware (24%), exposición de datos internos (33%), robo de credenciales (20%) y crypto jacking (18%).[22]”

Se hace evidente que el crecimiento en la utilización de dispositivos electrónicos y la masificación del uso del internet abre la posibilidad que las entidades en Colombia, se interesen en adquirir tecnología permitiéndole fortalecer sus sistemas de seguridad tanto física como digital. No obstante, se hace necesario el estudio de nuevas metodologías que acompañen estos sistemas para brindar las alternativas necesarias a cualquier tipo de ataque o incidentes graves de seguridad.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo un modelo de seguridad basado en Zero Trust permite asegurar los activos de información en las organizaciones públicas en Colombia?

[22] SEMANA. El 76% de organizaciones en Colombia reportó incidentes en la nube. Ciberseguridad. [Consulta: 20 de julio de 2021]. Disponible en: https://www.semana.com/tecnologia/articulo/sophos-76-de-organizaciones-en-colombia-reportaron-incidentes-en-la-nube/292849/

2 JUSTIFICACIÓN

En general, los modelos de seguridad de la información, que implementan las organizaciones, están conformados por un conjunto de acciones que buscan evitar o minimizar los riesgos, que, en determinado momento, puede estar expuesta la información y de esta forma seguir los lineamientos previamente establecidos para no comprometer la continuidad del negocio y subsanar los daños recibidos. Sin embargo, el presente trabajo pretende visualizar un modelo de seguridad donde se intensifique las acciones realizadas por los mecanismos de validación, donde no se generen zonas de confianza en los sistemas y redes computacionales, presentando consideraciones que permitan menores porcentajes de daños ante posibles ataques a la información.

Por consiguiente, se construye un análisis a las estrategias enfocadas a los esquemas de seguridad mediante la adecuación de modelos de confianza cero en las organizaciones colombianas, con el fin de establecer una mirada general a dicho modelo y sus principales beneficios en la protección de la información y como estandarte mantener la confidencialidad, integridad y disponibilidad.

La relevancia de este análisis monográfico se centra en brindar opciones de seguridad a las organizaciones colombianas, debido a que las circunstancias actuales evidencian una desproporcionada amenaza latente en la explotación de vulnerabilidades, tanto en aspectos externos o internos de los sistemas computacionales y no permite hacerles frente a los atacantes. Tal es el caso, que hace unos meses una gran compañía, sufrió, lo que en los medios de comunicación llamarón “El hackeo de la historia”, al irrumpir en los sistemas de una empresa de tecnología por meses sin ser detectados y filtrar todo tipo de información valiosa para sus clientes y proveedores. En consideración del autor, es un llamado a prepararse para la peor situación, con la esperanza que ocurra la mejor de las alternativas posibles.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar las consideraciones generales de un modelo de seguridad de Zero Trust que brinda una alternativa de seguridad a los activos de la información a cualquier organización pública en Colombia, por medio de la recopilación de información y la integración de estrategias relacionadas con la protección de la información.

3.2 OBJETIVOS ESPECÍFICOS

- Examinar los conceptos y componentes básicos del modelo de seguridad mediante la búsqueda de información relacionada y la conceptualización de términos relevantes, proporcionando las características y alcance del modelo “Zero Trust” debido al poco conocimiento sobre la metodología propuesta en las instituciones públicas del país.

- Establecer las principales debilidades en la protección de los activos de la información para las entidades públicas del país, exponiendo los posibles campos de acción en la identificación de las vulnerabilidades más comunes en las organizaciones, relacionando metodologías y datos sobre las amenazas existentes, generando el contexto necesario sobre los riesgos identificados.

- Categorizar los riesgos a la información identificados previamente, mediante la relación de estrategias de protección a la información que genere soluciones factibles a la implementación de un modelo de seguridad “Zero Trust”, en virtud del contexto organizacional.

- Proponer las recomendaciones para la implementación del modelo de seguridad “Zero Trust” en cualquier entidad pública del país mediante la presentación de metodologías y estrategias que garanticen los niveles apropiados de riesgos en los activos de información, en respuesta a la creciente tendencia de ataques a la información en el país.

4 MARCO REFERENCIAL

En el presente capítulo se abordan los aspectos que fundamentan el trabajo desarrollado, brindando especificar los conceptos y metodologías que facilitan la comprensión de la temática principal.

4.1 MARCO TEÓRICO

En general las organizaciones colombianas en la actualidad, manejan o desarrollan sistemas de información como base operativa en la ejecución de sus estrategias comerciales con un alto contenido tecnológico para la gestión misional, por tal razón generarán alternativas basadas en seguridad a los diferentes activos, ya sean físicos o intangibles. Sin embargo, “la información se convierte hoy en el valor más relevante de las industrias y empresas, estos requieren de la protección, confidencialidad y que se conserven de forma íntegra. Por ello, se deben gestar estrategias de servicio que protejan esta información dentro de los estándares y regulaciones vigentes.”[23]

En ese contexto, la seguridad de la información se convierte en prioridad para cualquier entidad, entendiendo como el “conjunto organizado de acciones que tomen en cuenta la infraestructura tecnológica, organizacional, legal y demás que debe ser protegida.”[24] Por consiguiente, es importante conocer dichas acciones que contribuyen a la edificación de estrategias enfocadas a la seguridad de la información.

4.1.1 Sistema de gestión de seguridad de la información

Brindando una definición, la ISO/IEC 27000 indica que un modelo de SGSI “es un conjunto de políticas, procedimientos, guías y sus recursos y actividades asociadas, que son gestionados de manera colectiva por una organización. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos del negocio. Este enfoque está basado en una apreciación del riesgo y los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar con eficacia los riesgos. El análisis de los requisitos para la protección de los activos de información y la aplicación de controles adecuados para

[23] APONTE AGUDELO, Andrés. Modelo de seguridad para plataformas IAAS de la empresa Virgin Mobile. Trabajo de grado Especialista en seguridad informática. Bogotá D.C.: Universidad Nacional Abierta Y A Distancia. Escuela De Ciencias Básicas e Ingeniería. 2018. 95 p.

[24] RODRIGUEZ GAHONA, Guillermo. Análisis comparativo de los modelos defensa en profundidad y MSPI, para la implementación de la seguridad informática en el sector privado del país. Trabajo de grado Especialista en seguridad informática. Bogotá D.C.: Universidad Nacional Abierta Y A Distancia. Escuela De Ciencias Básicas e Ingeniería. 2020. 97 p.

garantizar la protección de estos activos de información, según sea necesario, contribuye a la exitosa implementación de un SGSI."[25]

4.1.2 Modelo de seguridad y privación de la información

El gobierno nacional de Colombia mediante diversas estrategias enfocadas en el mejoramiento de la gestión digital de los entes públicos, se ha permitido emitir diferentes políticas que fortalecen la transformación digital del estado y así mismo de las organizaciones que dependen de este. Es así, que mediante la adopción del decreto 1008 del 2018, se dan a conocer los componentes necesarios para la conformación de las políticas de la estrategia "Gobierno digital" que establece habilitadores transversales como herramienta en la integración de procesos y procedimientos enfocados en la arquitectura e infraestructura empresarial, en los servicios de los ciudadanos y de igual forma, en la seguridad de la información, lo cual podrá ser visualizado en la figura 1. Así mismo, parte fundamental de este habilitador se despliega a través del "Modelo de Seguridad y Privacidad de la Información."

Figura 1 Componentes de gobierno digital

Fuente: Tomado del sitio web https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/

[25] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de Seguridad de la Información, Requisitos. ISO/IEC 27001. Bogotá D.C.: El Instituto, 2014. 30 p.

De esta forma, acorde con la dirección de gobierno digital, este modelo "imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital."[26] Como datos a resaltar esta estrategia brinda veintiuno (21) guías acerca de desarrollo y medición de dicho modelo completando aspectos como metodología, indicadores controles y demás relacionados.

4.1.3 Modelo de defensa en seguridad en profundidad

Este término de "defensa en profundidad", se presenta como "un método que busca disminuir las vulnerabilidades en los sistemas informáticos, el cual consiste en aplicar seguridad por capas a un sistema, su función principal es de aumentar la posibilidad de detectar intrusos y disminuir las oportunidades que los intrusos logren su propósito"[27]

4.1.4 Marco de Ciberseguridad del NIST

Según NIST, "es una metodología con un enfoque para reducir el riesgo vinculado a las amenazas cibernéticas que puedan comprometer la seguridad de la información, y está compuesto por tres partes: el Núcleo del Marco, los Niveles de Implementación y los Perfiles del Marco. Cada componente del Marco refuerza la conexión entre los impulsores empresariales o de misión y las actividades de seguridad cibernética."[28]

Una vez establecido el concepto de este marco de referencia, se hace necesario contextualizar que las mejores prácticas brindadas, están enfocadas a la protección de la ciberseguridad y consta de tres componentes principales. Como lo dice la OEA, "Las Funciones son el nivel más alto de abstracción incluido en el Marco. Actúan como la columna vertebral del Framework Core en el que se organizan todos los demás elementos"[29]. Estos componentes se pueden observar e identificar en la figura 2.

---

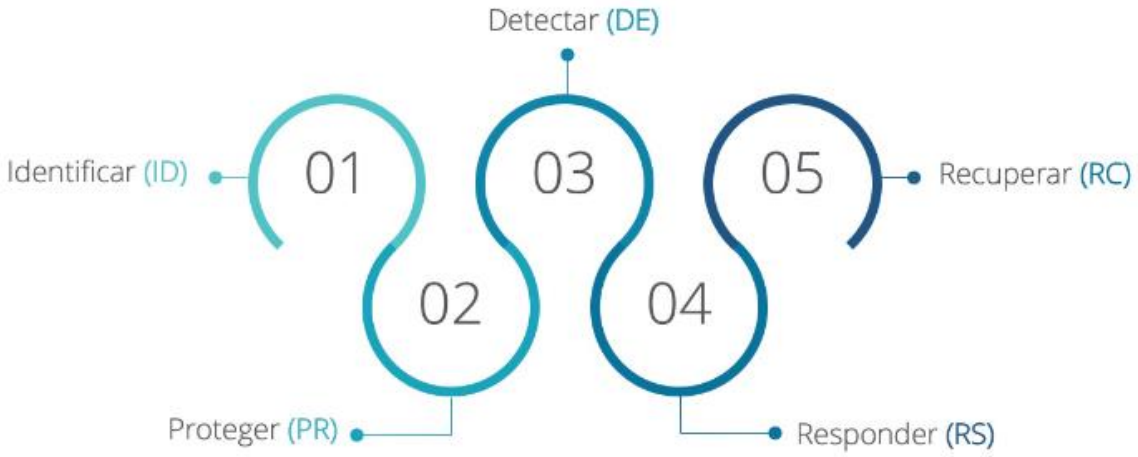
[26] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN. Gobierno Digital. [sitio web]. Bogotá D.C: MINTIC. [Consulta: 07 de junio de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

[27] GUIJARRO, Alfonso. YEPEZ, Jesica. Defensa en profundidad aplicado a un entorno empresarial. *Revista Espacios.* 2018. nro 42. pp 19-28. ISSN 0798 1015.

[28] INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA. Marco para la mejora de la seguridad cibernética en infraestructuras críticas. [sitio web]. [Consulta: 11 de Junio de 2021]. Disponible en: https://doi.org/10.6028/NIST.CSWP.04162018.

[29] ORGANIZACIÓN DE ESTADOS AMERICANOS y AWS, Ciberseguridad marco NIST, Un abordaje integral de la ciberseguridad, White papers series, Ed 5, 2019, 20 p.

Figura 2 Funciones del núcleo



Fuente: tomado de https://www.esan.edu.pe/conexion/actualidad/2019/04/30/que-es-el-cybersecurity-framework-de-nist-de-los-estados unidos/

- Núcleo del marco: Según NIST, "proporciona un conjunto de actividades para lograr resultados específicos de seguridad cibernética y hace referencia a ejemplos de orientación en cómo lograr dichos resultados"[30].

- Niveles de implementación: NIST establece que "los niveles describen el grado en que las prácticas de gestión de riesgos de seguridad cibernética de una organización exhiben las características definidas en el Marco"[31]. De esta forma los niveles proporcionan la dinámica de cómo una organización categoriza el riesgo de seguridad cibernética y los protocolos para gestionarlos.

- Perfiles: Tiene como propósito establecer la ruta para minimizar el riesgo de la ciberseguridad mediante la estructuración de funciones, categorías en una organización.

4.1.5 Arquitectura confianza cero

De acuerdo a la guía de NIST, confianza cero ("Zero trust"), "es el término para un conjunto en evolución de paradigmas de ciberseguridad que mueven las defensas de los perímetros estáticos basados en la red para centrarse en los usuarios, los

[30] INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA, Marco para la mejora de la seguridad cibernética en infraestructuras críticas, Versión 1.1, 2018, 55 p.
[31] INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA, Marco para la mejora de la seguridad cibernética en infraestructuras críticas, Versión 1.1, 2018, 55 p.

activos y los recursos. Una arquitectura de confianza cero (ZTA) utiliza principios de confianza cero para planificar la infraestructura y los flujos de trabajo industriales y empresariales. La confianza cero supone que no se otorga una confianza implícita a los activos o cuentas de usuario basándose únicamente en su ubicación física o de red (es decir, redes de área local frente a Internet) o en función de la propiedad de los activos (propiedad empresarial o personal). La autenticación y autorización (tanto de sujeto como de dispositivo) son funciones discretas que se realizan antes de que se establezca una sesión en un recurso empresarial. La confianza cero es una respuesta a las tendencias de la red empresarial que incluyen usuarios remotos, tienen su propio dispositivo (BYOD) y activos basados en la nube que no se encuentran dentro de los límites de una red de propiedad empresarial."[32]

La confianza cero se centra en proteger los recursos (activos, servicios, flujos de trabajo, cuentas de red, etc.), no en los segmentos de la red, ya que la ubicación de la red ya no se considera el componente principal para la postura de seguridad del recurso.

4.2 MARCO CONCEPTUAL

Con el propósito de brindar el contexto necesario sobre los conceptos tratados en el desarrollo del presente trabajo, a continuación, se describen los componentes más importantes en la construcción de este documento.

4.2.1 Seguridad perimetral

Este concepto se adopta y trabaja desde el ámbito de la informática, entendiendo como los mecanismos y recursos que protegen una infraestructura tecnológica de forma física y digital, pero con la particularidad que son desplegados en el exterior de los elementos a proteger.

Dicho en otras palabras, la seguridad de perímetro puede apropiarse como "el conjunto de mecanismos y sistemas relativos al control del acceso físico de personas a las instalaciones, así como la detección y la prevención de intrusiones. Cómo estas medidas de seguridad están implementadas dependen de cada organización y los requisitos de ese medio o contexto."[33] De esta forma, se puede presentar diferentes metodologías o categorías que brinda la protección. Se detallan algunas de ellas a continuación.

---

[32] INSTITUTO NACIONAL DE ESTANDARES Y TECNOLOGÍA. Computer Security Resource Center. [sitio web]. Gaithersburg: NIST. [Consulta: 06 de junio de 2021]. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-207/archive/2020-02-13

[33] UNIVERSIDAD DE LA RIOJA. Seguridad perimetral informática: objetivos y plataformas recomendables. Ingeniería y tecnología. [sitio web]. [Consulta: 25 de noviembre de 2021]. Disponible en: https://www.unir.net/ingenieria/revista/seguridad-perimetral-informatica/

- **Antivirus:** Esta plataforma se usa en dispositivos finales para limitar el ingreso de códigos de computadora maliciosos. Donde fue conocido como "un software que detectaba y en ocasiones elimina virus informáticos de los dispositivos infectados, y por lo tanto también contribuiría a detener la propagación del contenido malicioso."[34]

- **Firewall:** Según uno de los mayores fabricantes de recursos tecnológicos, este se puede definir como "un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide si permitir o bloquear tráfico específico según un conjunto definido de reglas de seguridad. Los cortafuegos han sido una primera línea de defensa en seguridad de redes durante más de 25 años. Establecen una barrera entre las redes internas seguras y controladas en las que se puede confiar y las redes externas no confiables, como Internet."[35]

- **VPN:** De la traducción de sus siglas en inglés Red Privada Virtual, esta tiene como propósito "brindar privacidad y anonimato en línea al crear una red privada desde una conexión pública a Internet. Las VPN enmascaran su dirección de protocolo de Internet (IP), por lo que sus acciones en línea son prácticamente imposibles de rastrear. Lo más importante es que los servicios VPN establecen conexiones seguras y encriptadas para brindar mayor privacidad que incluso un punto de acceso Wi-Fi seguro." Su funcionamiento se basa en la creación de una ruta protegida para el intercambio de datos.

- **Controles de identidad y acceso**: Estos mecanismos son los encargados de brindar las autorizaciones a los sistemas de información o ingreso a un espacio físicos mediante procesos de validación con una referencia previamente configurada. En la actualidad se presenta de diversas formas, sin embargo, el ejemplo más contundente hace referencia a los sistemas biométricos para el resguardo de información valiosa, donde unos rasgos como huellas digitales son almacenados en una base de datos para ser cotejados en el momento de ingreso, según sea correcta la similitud.

4.2.2 Modelo de seguridad

Un modelo de seguridad en un sistema de información es el conjunto de procedimientos para evaluar y autenticar políticas de seguridad con el fin de mapear los objetivos intelectuales de la política a un sistema de información especificando las estructuras de datos explícitas y las técnicas necesarias para implementar la

[34] ESET. Antivirus. [sitio web]. [Consulta: 25 de noviembre de 2021]. Disponible en: https://www.eset.com/es/caracteristicas/antivirus-software-que-es/#
[35] CISCO. ¿Qué es un cortafuego? [sitio web]. [Consultado: 25 de noviembre de 2021]. Disponible en: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

política de seguridad. Un modelo de seguridad generalmente se representa en matemáticas e ideas analíticas, que se asignan a las especificaciones del sistema y luego los programadores los desarrollan a través del código de programación. Se han desarrollado varios modelos de seguridad para hacer cumplir las políticas de seguridad.

4.2.3 Sistema de gestión

Existen diferentes normas y estándares internacionales que soportan y apoyan la consolidación de este concepto, como una herramienta sistemática capaz de generar y contribuir a la realización de procesos y oportunidades de mejora. Los sistemas de gestión pueden ser simples o complejos, continuos o ad hoc, estándar en toda la organización o distintos para los individuos. Y, por supuesto, diferentes sistemas de gestión pueden resultar en distintos grados de eficacia. Ciertamente, lo que funciona para una organización puede no ser óptimo para otra. Lo que es más interesante, sin embargo, es que el sistema de gestión que llevó a su organización a donde está, puede que no sea el adecuado para llevar a su organización a donde desea que esté en el futuro.

4.2.4 Desperimetrización

Desde la óptica que se desarrolla en este trabajo, este concepto implica el despliegue y ejecución de los procesos que fortalece las medidas de seguridad de una infraestructura de las tecnologías de la información. Es así que el portal web de seguridad informática, recopila la siguiente información sobre “los principales impulsores de la seguridad perimetral que ya no tiene participación en la estrategia de las empresas, es el Open Group que entre otras aportaciones desarrolló el popular modelo de arquitectura TOGAF (The Open Group Architecture Framework). A través del foro Jericó, el Open Group sostiene como propósito la desmitificación de los lineamientos que por años se han manejado alrededor de la seguridad perimetral como algo inamovible de la estrategia y los presupuestos de las empresas, esta desperimetrización involucran un mayor enfoque a la seguridad en la nube y las arquitecturas seguras de colaboración.”[36]

4.3 MARCO LEGAL

Al abordar esta temática, se considera pertinente para el desarrollo del presente trabajo conocer la normatividad legal en Colombia relacionada con la protección de la información y demás regulaciones al respecto, haciendo énfasis en la legislación para entidades públicas en el país.

[36] MAGAZCITUM. Seguridad perimetral: el debate del momento. [sitio web]. [Consultado: 25 de noviembre de 2021]. Disponible en: https://www.magazcitum.com.mx/index.php/archivos/2489

4.3.1 Ley estatutaria 1266 de 2008

"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones."[37] Esta ley tiene como objetivo reconocer el derecho constitucional a realizar un manejo de la información a los titulares de la misma, por entidades públicas o privadas.

4.3.2 Ley 1273 de 2009

"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones."[38] Esta ley comprende dos capítulos, en donde el primero estipula los delitos contra los pilares de la seguridad de la información (Confidencialidad, integridad y disponibilidad) y el segundo hace referencia a las infracciones informáticas y otros delitos relacionados.

4.3.3 Ley Estatutaria 1581 de 2012

"Por la cual se dictan disposiciones generales para la protección de datos personales."[39] Esta ley permite crear un mecanismo sólido para ejercer derechos y deberes ante todas las entidades del orden nacional en materia de datos personales, y en ese mismo sentido establece directrices claras sobre el tratamiento de la información de los titulares en Colombia.

4.3.4 Ley 1712 de 2014

"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."[40] Esta ley estatutaria emitida desde el congreso de la república, presenta la regulación sobre

---

[37] CONGRESO DE LA REPÚBLICA. Diario oficial 51698. [sitio web]. Bogotá D.C. [Consulta: 04 de mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

[38] CONGRESO DE LA REPÚBLICA. Diario oficial 51698. [sitio web]. Bogotá D.C. [Consulta: 04 de mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[39] CONGRESO DE LA REPÚBLICA. Diario oficial 51698. [sitio web]. Bogotá D.C. [Consulta: 04 de mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[40] FUNCIÓN PÚBLICA. Ley 1712 de 2014. [sitio web]. Bogotá D.C. [Consulta: 16 de enero de 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

los derechos al acceso a la información y los mecanismos para la garantía de la publicación de información.

4.3.5 Decreto 415 de 2016

“Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones”[41]. Entre la múltiple disposición y lineamientos establecido en este decreto se enmarca la necesidad de liderar la conformación de los planes estratégicos de tecnología de la información, la cual involucra intrínsecamente la adopción de políticas en materia de seguridad y calidad de la información.

4.3.6 Decreto 1008 de 2018

"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones."[42] (Sistema Único de información Normativa, 2021) Se hace especial mención a dicho decreto, ya que le transfiere facultades al Ministerio de las Tecnologías de la Información y Comunicación para estructurar y ejecutar estrategias de promover políticas que permitan dar solución a las problemáticas con el uso y manejo de las tecnologías.

[41] SISTEMA ÚNICO DE INFORMACIÓN NORMATIVA. Diario oficial. [sitio web]. Bogotá D.C. [Consulta: 16 de enero de 2022]. Disponible en https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/30020275

[42] SISTEMA ÚNICO DE INFORMACIÓN NORMATIVA. Diario oficial. [sitio web]. Bogotá D.C. [Consulta: 04 de mayo de 2021]. Disponible en: http://www.suin-juriscol.gov.co/viewDocument.asp?id=30035329

5 CONCEPTOS Y COMPONENTES BÁSICOS DE UN MODELO DE SEGURIDAD “ZERO TRUST”

Este apartado tiene como propósito describir los elementos existentes en este tipo de modelo de seguridad, brindando un enfoque histórico e ilustrativo de las políticas y esquemas que son necesarios para la conformación de una estructura de “Zero trust”.

5.1 CONTEXTO HISTÓRICO “ZERO TRUST”.

Los contextos históricos, permiten dilucidar una cronología y avance relacionadas a temas específicos, por tal razón se da inicio a la temática, mencionando que la información encontrada sobre los inicios de “Zero Trust”, data a mediados del año 2004, cuando un grupo de profesionales en seguridad, conforma un consorcio conocido como “El Foro de Jericó”, los cuales se autodenominan como “la agrupación de empresas multinacionales de usuarios dedicadas al desarrollo de estándares abiertos que permiten flujos de información seguros y sin fronteras entre empresas."[43] Y su principal propósito era la protección de los datos que transitan dentro y fuera de los límites de una red empresarial, llevando a popularizar el concepto de seguridad de “Desperimetrización”. Hoy en día esta asociación se fusionó con el “The Open Group Security Forum” quienes “trabajan con proveedores, consorcios y organismos de normalización para desarrollar consenso y facilitar la interoperabilidad, evolucionando e integrando especificaciones y tecnologías de código abierto”[44] y conjuntamente se encargan de preservar la documentación generada por el “El Foro de Jericó”.

Posteriormente, en el año 2010, el analista de seguridad John Kindervag perteneciente a la compañía Forrester, se encargó de popularizar el término “Zero trust”, o por su traducción al español "confianza cero", mediante la divulgación de su escrito titulado “No más centros masticables: presentamos el modelo Zero Trust de seguridad de la información”, donde relacionaba “el nuevo panorama actual de amenazas, esto ya no es una forma eficaz de hacer cumplir la seguridad. Una vez que un atacante pasa el caparazón, tiene acceso a todos los recursos de nuestra red. Hemos construido perímetros sólidos, pero los ciberdelincuentes bien organizados tienen información privilegiada y desarrolla nuevos métodos de ataque que perforan fácilmente nuestras protecciones de seguridad.”[45] De esta forma

[43] NETWORK WORLD. The Jericho Forum and its goals. Networking. [sitio web]. [Consultado: 22 de julio de 2021]. Disponible en: https://www.networkworld.com/article/2325412/the-jericho-forum-and-its-goals.html

[44] THE OPEN GROUP. Vision & Mission. [sitio web]. [Consultado: 22 de julio de 2021]. Disponible en: https://www.opengroup.org/about-us/vision-mission

[45] KINDERVAG, JHON. No More Chewy Centers: Introducing The Zero Trust Model of Information Security. Forrester Research. 2010. pp 15.

pretendía contrarrestar las amenazas de seguridad haciendo que toda la red de protección fuera omnipresente, no solo en el perímetro.

De igual forma lo acompañaron varias publicaciones relacionados al tema, como el titulado, “Incorpore la seguridad al ADN de su red: la red Zero Trust Arquitectura” el cual abarcaba, “una forma potencial en la que se podría utilizar los conceptos del modelo de Zero Trust y posiblemente implementarlo en un entorno del mundo real. Así mismo, optimizar las arquitecturas y tecnologías de seguridad para una futura flexibilidad. A medida que avanzamos hacia un mundo centrado en datos con amenazas y perímetros cambiantes, buscamos nuevos diseños de red que integren conectividad, transporte y seguridad.”[46]

Luego de este importante impulso, en 2014, la compañía Google implementó una arquitectura de confianza cero conocida como BeyondCorp. Que se fundamentó en los informes y análisis de Kindervag ayudando a cristalizar los conceptos de “Zero trust” en las comunidades de las tecnologías de la información- TI. Sin embargo, se necesitaría casi una década para que las arquitecturas de confianza cero se generalizaron, impulsadas en parte por una mayor adopción de servicios móviles y en la nube. De esta forma, en la figura 3, se muestra la línea de tiempo acerca de la evolución de este concepto metodológico y sus principales exponentes.

Figura 3 Línea de tiempo "Zero Trust"

Fuente: Tomado de https://www.wwt.com/article/what-is-zero-trust/

Para 2019, la Autoridad Técnica Nacional del Reino Unido y el Centro Nacional de Seguridad Cibernética estaban recomendando que los arquitectos de redes consideren un enfoque de confianza cero para nuevas implementaciones de TI, particularmente donde se planea un uso significativo de servicios en la nube. Siendo en ese mismo año donde NIST pública el borrador bajo la nomenclatura de “NIST800-207” como un estándar para construir arquitectura de “Zero Trust”.

[46] KINDERVAG, JHON. Build Security into Your Network's DNA: The Zero Trust Network Architecture. Forrester Research. 2010. pp 27.

5.2 COMPONENTES BÁSICOS DEL MODELO DE SEGURIDAD "ZERO TRUST".

Partiendo de la base del documento técnico escrito por John Kindervag, "en Zero Trust, no se confía en todo el tráfico de la red. Esto significa que los profesionales de la seguridad deben encargarse que se acceda a todos los recursos de forma segura independientemente de la ubicación, adopten un privilegio mínimo estratégico y hacer cumplir estrictamente el control de acceso e inspeccionar y registrar todo el tráfico."[47] Por lo tanto sería apropiado mencionar que el modelo de confianza cero es un enfoque holístico de la seguridad de la red, que requiere la verificación de cada persona y dispositivo cada vez que intenta acceder a recursos en una red privada. Esto sigue siendo cierto, sin importar si ese dispositivo o persona ya está dentro o fuera del perímetro de la red.

Así pues, Zero Trust, aplica la estrategia de suponer que está operando en un entorno de amenazas generalizadas. Un entorno que exige que evalúe y reevalúe continuamente la viabilidad de su estrategia de seguridad. A continuación, se muestran algunos comportamientos claves que podría exhibir si acepta que está operando en un entorno de amenazas generalizadas:

- **Conexiones predeterminadas.** Este podría significar el cambio más representativo de Zero Trust. Entendiendo que el mundo de las redes convencionales y algunas VPN, se asume que, si la solicitud se origina en una red conocida, debe ser segura. Se asume que los modelos que prestaban servicios de protección ayer, lo seguirán haciendo mañana. "Zero Trust exige que se abandonen esos supuestos y, en cambio, se valide y ejerza controles sobre la mayoría de aspectos relacionados al acceso lógico y físico, validando explícitamente lo que se puede y acepta las cosas que no se validen, ocasionando explícitamente que sigan siendo inciertas."[48]

- **Apertura constante de conexiones**. Un enfoque que muchos clientes han encontrado valioso para contrarrestar sus suposiciones arraigadas es asumir que todos los usuarios, dispositivos y recursos están en la Internet pública. "Algunas de las compañías más exitosas en este sentido simplemente han movido tantos recursos como sea posible a la nube, modernizando su estrategia de seguridad a medida que avanzan"[49].

[47] KINDERVAG, JHON. No More Chewy Centers: Introducing The Zero Trust Model of Information Security. Forrester Research. 2018. pp 18.
[48] THE OPEN GROUP. Zero Trust. [sitio web]. [Consultado: 22 de julio de 2021]. Disponible en: https://www.opengroup.org/forum/security/zerotrust
[49]MICROSOFT. Zero Hype. Tech community. [sitio web]. [Consultado: 22 de julio de 2021]. Disponible en: https://techcommunity.microsoft.com/t5/azure-active-directory-identity/zero-hype/ba-p/10614133

- **Validación múltiple de fuentes**. En un entorno de amenazas generalizado, la información precisa es clave. Los modelos de seguridad que dependen de múltiples fuentes de validación son mucho más sólidos: la triangulación proporciona una solución mucho más precisa que la validación de una sola fuente. De manera similar, el control que se basa en múltiples elementos (por ejemplo, usando la confianza del dispositivo, la ubicación y la autenticación fuerte,) es mejor que el que se basa en un solo aspecto del acceso.

- **Disposición a las brechas**. Se asume amenazas generalizadas, por lo tanto, algunas amenazas podrían romper las defensas. Las estrategias de contención como la administración de identidades privilegiadas, el acceso basado en roles, la separación de funciones y la segmentación de la red pueden ayudar a contener a los intrusos que accedan a las primeras capas de defensa.

- **Los estándares son seguros.** Si bien la innovación es maravillosa, una condición de seguridad (especialmente el cifrado) es que nada es demasiado seguro, pero el tiempo es un excelente indicador de buenos resultados si no ocurren infracciones. Los estándares son muy inspeccionados, muy utilizados y, sí, los estándares proporcionan una gran estrategia de seguridad.

- **Automatización**. Se debe considerar automatizar todo lo posible. Simplemente no hay suficiente personal para manejar el volumen de telemetría y ataques que enfrentará. Apoyarse de la inteligencia en la nube, el aprendizaje automático y, lo que es más importante, los mecanismos de respuesta automatizados, como el bloqueo automático de cuentas de riesgo o la prohibición del tráfico de direcciones IP incorrectas conocidas, será una estrategia que le permitirá abarcar mayor terreno informático.

5.3 PRINCIPIOS MODELO DE SEGURIDAD “ZERO TRUST”.

Tradicionalmente, es conocido en el ámbito de la infraestructura informática, dos categorías de redes, la externa; que conlleva la conexión a internet y múltiples servicios al público donde son administrados por terceros y es etiquetado como una “red no confiable”. Por otro lado, se puede encontrar la red interna, donde las empresas e instituciones consolidan recursos informáticos para proveedor servicios a sus colaboradores y empleados, donde son gestionados por un área específica de la organización, esta es conocida como “red confiable”, ya que es diseñada, implementada acorde con las necesidades y expectativas del usuario. Sin embargo, el modelo de seguridad “Zero Trust”, manifiesta que no se deben hacer distinciones o perímetros confiables, asumiendo que la red donde se transportan los datos e

información se debe considerar una zona de no confianza. Por lo tanto, a continuación, se establecen los tres principios utilizados en este modelo como se puede observar en la figura 4, categorizando cada uno de ellos con su correspondiente definición.

Figura 4 Principios del modelo

Fuente: Tomado de https://www.concurrency.com/blog/december-2020/it-will-happen-to-you%E2%80%A6-why-zero-trust-must-be-a-technology-north-star-for-2021

5.3.1 Verificar y asegurar

Haciendo a un lado el concepto de “red segura” como un entorno de confianza en los usuarios y de los dispositivos se hace necesario autenticar y autorizar siempre sobre la base de todos los puntos de datos disponibles, tales como la identidad del usuario, la condición del dispositivo, la clasificación de datos, y las anomalías, etc. Dicho desde otro contexto, “Zero Trust no depende de una ubicación, de los usuarios, los dispositivos o de las aplicaciones, que ahora con las tendencias mundiales, estas pueden estar en todas partes, por lo que se gestiona desde el interior a los usuarios adecuados para tener el acceso a las aplicaciones y los datos adecuados.

De esta forma, se establecen medidas que protejan los datos internos del abuso de información privilegiada de la misma manera que proteger los datos externos que tienen acceso a internet o a redes de dominio público.

5.3.2 Accesos limitados

Ahora bien, se hace necesario autenticar a los usuarios, saber quiénes son, dónde están y cómo acceden a los servicios y redes. Esto proporciona una validación correcta de los niveles de acceso permitidos en las infraestructuras tecnológicas, luego de ser previamente verificado.

Los controles proporcionados por el acceso condicional impactan directamente en el “verificar” y mínimo privilegio de como una condición vital. El acceso condicional se refiere a comprender que su capa de identidad es el control principal que utilizan las aplicaciones y los entornos modernos para gobernar quién tiene acceso y quién no. Zero Trust utiliza el principio de acceso con privilegios mínimos y limita a los usuarios con el acceso justo a tiempo y suficiente.

5.3.3 Revisión constante

Como parte de todo este modelo, se propone como metodología de implementación asumir que se presentan una infracción constantemente en los sistemas de información y verificar cada solicitud.

Este comportamiento permite inspeccionar continuamente el tráfico de usuarios en busca de indicios de una actividad sospechosa. En lugar de confiar en que los usuarios hagan lo correcto, se verifica que están haciendo lo correcto. “Al inspeccionar continuamente el tráfico de la red, Los profesionales de seguridad pueden identificar el comportamiento anómalo del usuario o la actividad sospechosa del usuario (por ejemplo, un usuario que realiza grandes descargas o acceder con frecuencia a sistemas o registros que normalmente no necesita para sus responsabilidades diarias)”[50]

5.4 ARQUITECTURA DE ZERO TRUST

En el pasado, cuando los usuarios salían de la red empresarial, conocida como “red confiable", se despliega una red privada virtual-VPN para extender la red empresarial a ellos. Si los atacantes pudieran robar las credenciales de un usuario, podrían acceder fácilmente a la red empresarial.

El acceso a la red de confianza cero abstrae y centraliza los mecanismos de acceso para que los ingenieros y el personal de seguridad puedan ser responsables de ellos. Otorga acceso apropiado en función de la identidad del personal y sus dispositivos, además de otro contexto como la hora y la fecha, la ubicación

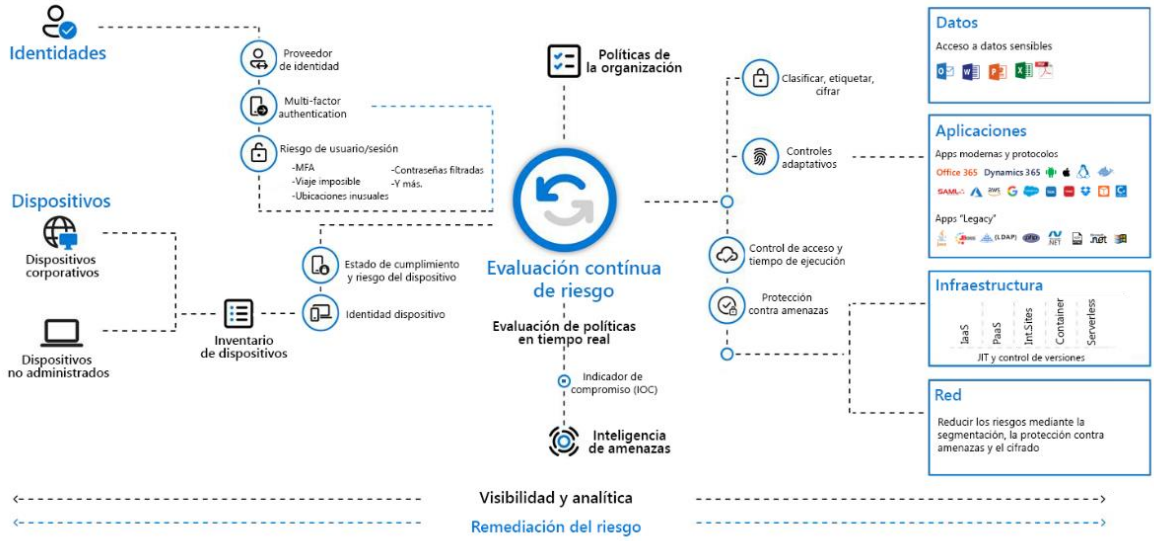
[50] KINDERVAG, JHON. No More Chewy Centers: Introducing The Zero Trust Model of Information Security. Forrester Research. 2018. pp 18.

geográfica, los patrones de uso históricos y la postura del dispositivo. El resultado es un entorno más seguro y resistente, con mayor flexibilidad y mejor supervisión.
El cambio a una fuerza laboral en gran parte remota, durante la pandemia de COVID-19 ha creado un interés sobre este modelo sobre las redes privadas virtuales. Aunque el reemplazo de VPN es un factor común para su adopción, ZTNA generalmente aumenta, en lugar de reemplazar, una VPN. Al permitir que los usuarios accedan a lo que necesitan y al cambiar a las ofertas de ZTNA basada en la nube, puede evitar la sobrecarga de su infraestructura VPN. A largo plazo, esta postura de seguridad de acceso a la red de confianza cero puede continuar utilizándose cuando el personal retome a un espacio físico laboral.

La segmentación basada en la identidad, reduce la confianza implícita excesiva al permitir que las organizaciones cambien las cargas de trabajo individuales a un modelo de "denegación predeterminada" en lugar de un modelo de "permiso implícito". Utiliza reglas dinámicas que evalúan la carga de trabajo y la identidad de la aplicación como parte de la acción de permitir las comunicaciones de red.

Al iniciar una estrategia de segmentación basada en la identidad, se debe comenzar con la selección de las aplicaciones y servidores más críticos para las implementaciones iniciales y obtener un punto de partida. De esta forma en la figura 5, se presenta un ejemplo de la implementación de este tipo de segmentación basada en Zero Trust.

Figura 5 Arquitectura básica de Zero Trust



Fuente: tomado del sitio web https://www.softeng.es/es-es/blog/estrategia-zero-trust.html

Una vez que haya implementado el modelo de Zero Trust y la segmentación basada en identidad, pase a otras iniciativas para extender un enfoque de confianza cero en toda su infraestructura tecnológica. Por ejemplo, en la figura 5 se muestra un esquema básico donde se detalla cada componente en armonía con los factores de una organización y sus recursos.

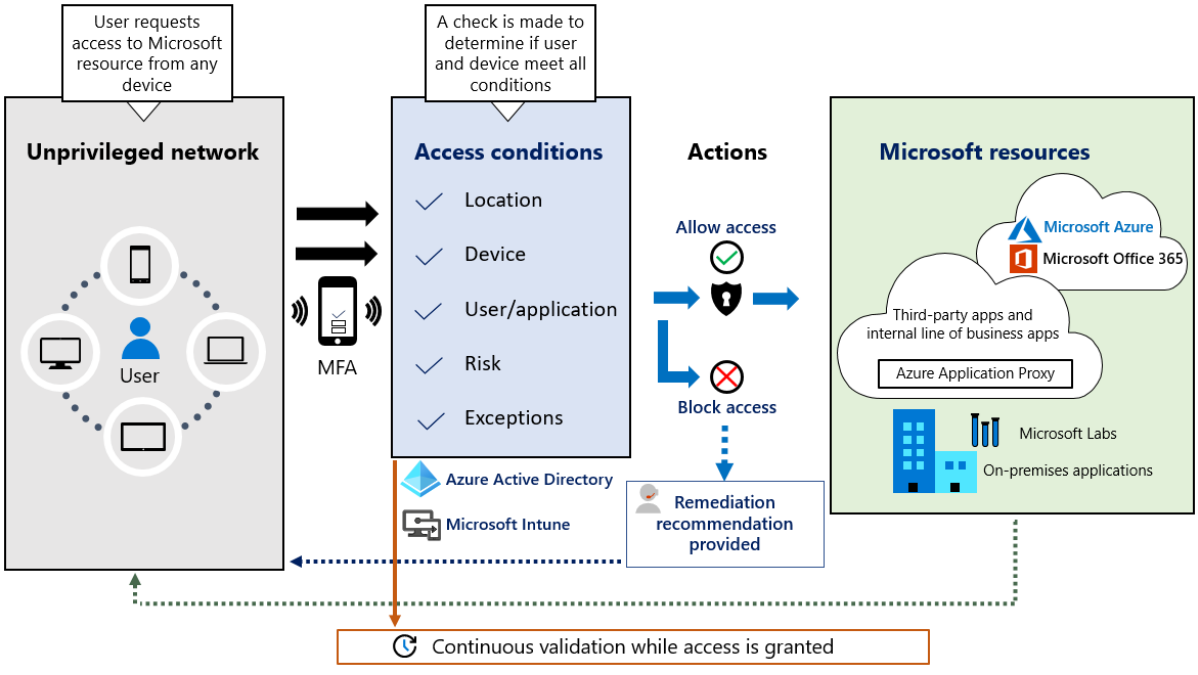
5.5 CASOS DE ÉXITO

Con el enfoque propuesto en el desarrollo del presente trabajo, a continuación, se describen algunas implementaciones sobre el modelo de seguridad “Zero Trust”, con el propósito de exponer las alternativas y metodologías aplicadas en el entorno comercial, haciendo especial énfasis en la aplicación de los principios que describe el modelo.

5.5.1 Caso Microsoft

Teniendo en cuenta que Microsoft, es un gigante tecnológico que está presente en múltiples aspectos del desarrollo y crecimiento en la industria del software, está implementando un modelo de seguridad Zero Trust para garantizar un entorno saludable y protegido mediante el uso de Internet como red predeterminada con una identidad sólida, cumplimiento con el óptimo bienestar del dispositivo y acceso con privilegios mínimos.

Figura 6 Arquitectura de Zero Trust Microsoft



Fuente: Tomado del sitio web https://www.microsoft.com/en-us/insidetrack/implementing-a-zero-trust-security-model-at-microsoft

De esta forma en la figura 6, se observa la arquitectura implementada que proporciona una referencia simplificada para el enfoque de Zero Trust. Los componentes principales de este proceso son la administración de dispositivos y la configuración de políticas de seguridad para los dispositivos, el acceso condicional de “Azure Active Directory” para la validación del estado del dispositivo y Azure AD para el inventario de usuarios y dispositivos.

El alcance propuesto por esta compañía al implementar Zero Trust, como se logra observar en la figura 6, se centró en los servicios corporativos comunes utilizados en todas las entidades, tales como empleados, socios y proveedores. La implementación de Zero Trust se centró en el conjunto básico de aplicaciones que los empleados de Microsoft utilizan a diario (por ejemplo, aplicaciones de Microsoft Office, aplicaciones de línea de negocio) en plataformas como iOS, Android, Mac OSX y Windows. Sin embargo, se proyecta que este enfoque sea amplio para incluir todas las aplicaciones utilizadas en Microsoft, de igual manera incluye cualquier dispositivo personal o de propiedad corporativa que acceda a los recursos de la empresa donde se contempla la administración a través de los sistemas de administración de dispositivos.[51]

5.5.2 Caso Google

Esta compañía, con la necesidad de brindar conexiones y ámbitos de trabajo seguros a sus programadores desde redes públicas o externas a la organización, presenta, “BeyondCorp”, su enfoque de confianza cero para el acceso y la autenticación de usuarios. Según la compañía “BeyondCorp es la implementación de Google del modelo de confianza cero. Se basa en una década de experiencia en Google, combinada con ideas y mejores prácticas de la comunidad. Al cambiar los controles de acceso del perímetro de la red a usuarios individuales, BeyondCorp permite un trabajo seguro desde prácticamente cualquier ubicación sin la necesidad de una VPN tradicional.”

BeyondCorp permite el inicio de sesión único, políticas de control de acceso, proxy de acceso y autenticación y autorización basadas en usuarios y dispositivos. Los principios de BeyondCorp son:

- Protección de la red en el borde, para que las cargas de trabajo estén aisladas de los ataques a la red y el tráfico no autorizado de Internet. Aunque un enfoque basado en barrera no es un concepto nuevo para los nativos de la nube, sigue siendo una de las mejores prácticas de seguridad. En un mundo nativo de la nube, se utiliza un enfoque de perímetro para proteger la

[51] MICROSOFT. Implementing a Zero Trust security model at Microsoft. [sitio web]. [Consultado: 30 de octubre de 2021]. Disponible en: https://www.microsoft.com/en-us/insidetrack/implementing-a-zero-trust-security-model-at-microsoft

mayor cantidad de infraestructura posible contra el tráfico no autorizado y posibles ataques de Internet, por ejemplo, ataques de denegación de servicio basados en volumen.

- No hay confianza mutua inherente entre los servicios, de modo que solo las personas que llaman conocidas, confiables y específicamente autorizadas pueden utilizar un servicio. Esto evita que los atacantes desarrollen un código que no sea de confianza para acceder a un servicio. Si un servicio se ve comprometido, evita que el atacante realice acciones que le permitan expandir su alcance. Esta desconfianza mutua ayuda a limitar el radio de explosión de un compromiso.

- Máquinas confiables que ejecutan código de procedencia conocida, por lo que las identidades de servicio están limitadas a usar solo códigos y configuraciones autorizadas, y se ejecutan solo en entornos autorizados y verificados.

- Puntos de control para la aplicación de políticas coherentes en todos los servicios. Por ejemplo, un punto de control para verificar las solicitudes de acceso a los datos del usuario, de modo que el acceso a un servicio se deriva de una solicitud validada de un usuario final autorizado, y el acceso de un administrador requiere una justificación comercial.

- Implementación de cambios simples, automatizada y estandarizada, de modo que los cambios de infraestructura se puedan revisar fácilmente para determinar su impacto en la seguridad, y se pueden implementar parches de seguridad con poco impacto en la producción.

- Aislamiento entre cargas de trabajo que comparten un sistema operativo, de modo que, si un servicio se ve comprometido, no puede afectar la seguridad de otra carga de trabajo que se ejecuta en el mismo host. Esto limita el "radio de daño" de un posible compromiso.

6 REVISIÓN GENERAL DE LAS PRINCIPALES DEBILIDADES EN LA PROTECCIÓN DE LOS ACTIVOS DE LA INFORMACIÓN PARA LAS ENTIDADES PÚBLICAS

Los ciberataques son una amenaza latente que afectan a las empresas todos los días, como lo menciona, el ex director ejecutivo de Cisco, John Chambers, "Hay dos tipos de empresas: las que han sido pirateadas y las que aún no saben que han sido pirateadas"[52]. Según diversos informes de ciberseguridad, el volumen total de incidentes se ha multiplicado en los últimos años, por lo que cada técnica utilizada y cada eslabón en la cadena de protección tiene una alta probabilidad de ser vulnerado. Y como parte del desarrollo de este trabajo a continuación se describe cada algún detonante que pueden generar un riesgo a la información.

6.1 PERSONAL DESCONTENTO

Se ha establecido en los últimos años que el activo más importante en una entidad, es la información, Sin embargo, aún se propician errores al momento de asegurar los activos mediante metodologías de perímetro, dejando brechas disponibles al atacante que podrán ser originados desde el interior de la compañía. Según INCIBE, “existe la posibilidad de que ataques intencionados o no intencionados se produzcan por diversas situaciones desde el interior de la propia empresa. En este ámbito es importante diferenciar entre insider y amenazas internas. Un insider es una persona que posee gran conocimiento de una empresa porque trabaja o trabajó en ella, y que, por su situación actual en relación a la empresa, busca cierta venganza. Esta persona es capaz de realizar acciones como el cambio de credenciales importantes, un uso inadecuado de dispositivos, etc.”[53]

6.2 PERSONAL EXTERNO

Ahora bien, cuando se hace referencia a la amenaza interna, se entiende por esa de brechas de información en los sistemas por parte de una entidad externa. Esto incluye empleados que no presentan un vínculo con la compañía, pero que tienen acceso por alguna razón y tiene la capacidad de tomar medidas que puedan dañar a la entidad, como por ejemplo introducir malware en la red o cambiar su información de inicio de sesión sin los privilegios previamente establecidos.

Entre las razones más comunes para llevar a cabo estas acciones realizadas por empleados descontentos o por amenazas internas, se encuentran:

---

[52] CISCO. ¿Cuáles son los ciberataques más comunes? [sitio web]. [Consultado: 22 de julio de 2021]. Disponible en: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

[53] INCIBE. Insider, las dos caras del empleado. [sitio web]. [Consultado: 22 de julio de 2021]. Disponible en: https://www.incibe-cert.es/blog/insider-las-dos-caras-del-empleado

- Recompensa económica.
- Espionaje empresarial.
- Sentimientos de venganza.
- Distracción de otra acción importante.
- Desconocimiento o ingenuidad.
- Cero políticas de seguridad

6.3 MANEJO INADECUADO DE LA INFORMACIÓN

La gestión de la información se centra en la gestión de información estructurada y no estructurada en cualquier formato (incluidos correos electrónicos, videos, datos encontrados en aplicaciones de línea de negocio, contenido de sitios web y redes sociales), como un activo durante todo su ciclo de vida. Esta disciplina abarca la recopilación, almacenamiento, difusión, archivo y destrucción de información, a través de la planificación, organización y estructura, procesamiento, control, evaluación y presentación de informes. La gestión de la información emplea los estándares, las políticas, los procesos, los procedimientos y la tecnología para gestionar la información de forma eficaz a nivel organizativo para llevar a cabo las actividades comerciales.

Los subconjuntos, que son altamente conocidos para la gestión de la información incluyen seguridad de la información, riesgo y cumplimiento, privacidad y protección de datos, gobernanza de la información, análisis, y gestión de registros. La mensajería instantánea está estrechamente relacionada y se superpone con la gestión de datos, los sistemas y tecnología de TI y la estrategia organizativa.

Las consecuencias de una mala gestión de la información tienen impactos a corto y largo plazo en las organizaciones, que varían en importancia. El incumplimiento de los requisitos reglamentarios es generalmente la consecuencia más conocida, que puede dar lugar a fuertes sanciones monetarias y en algunos casos daño de imagen. La falta de seguridad de la información es probablemente uno de los problemas más serios sobre los que hemos escuchado mucho en las noticias últimamente: considere los recientes ciberataques, violaciones de datos y accesos no autorizados.

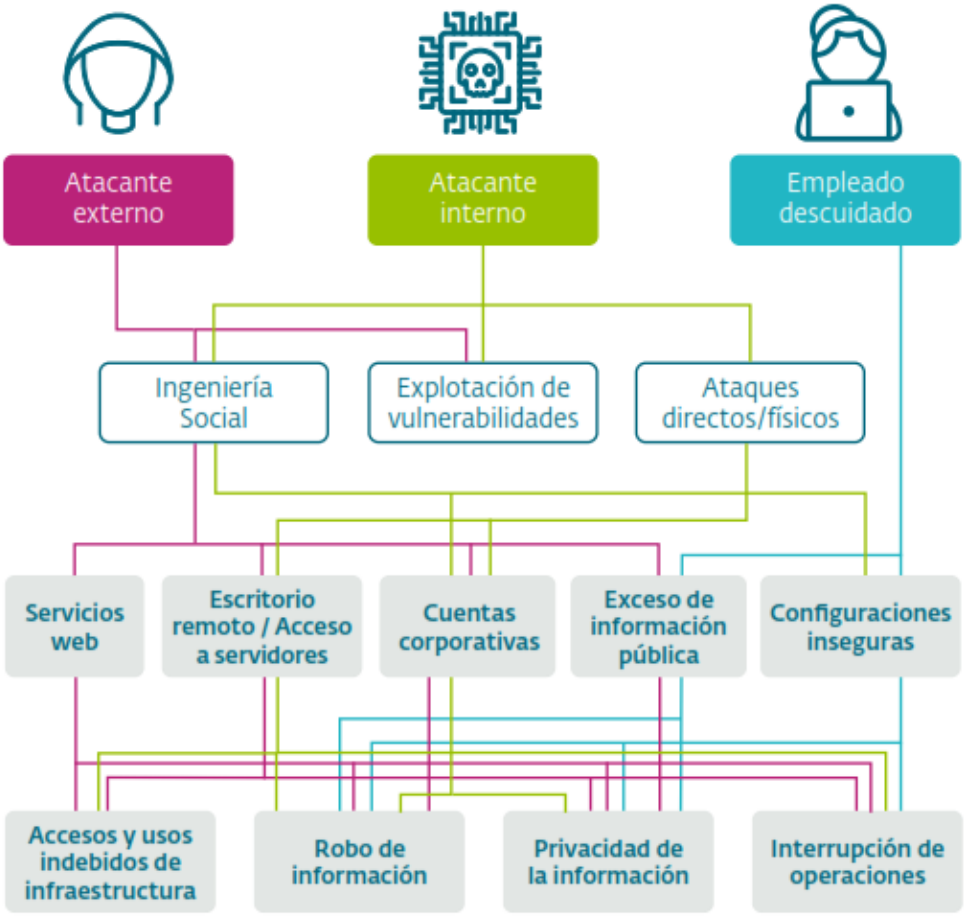
6.4 SISTEMAS DESACTUALIZADOS

En la actualidad, existen múltiples factores por lo que la entidad no pueda mantener actualizaciones constantes de su infraestructura de TI, pero desconocen que la tecnología obsoleta es más susceptible a las incursiones de seguridad. Esto podría ser cualquier cosa, desde una violación de datos cibernéticos hasta un ataque a sus activos digitales y su red. Los problemas de seguridad también ponen a su empresa

en riesgo de tiempo de inactividad. Y si se encuentra en una industria que requiere cumplimiento de seguridad, es casi imposible cumplir con estos requisitos cuando se utiliza hardware y software antiguos.

Entre los múltiples obstáculos para encontrar las soluciones pertinentes, en ocasiones ocurre que un equipo de TI no puede encontrar la mejor solución para su negocio. Puede llevar tiempo investigar y evaluar nuevas soluciones y conlleva mucho tiempo y esfuerzo por parte del personal de TI interno. Los equipos de TI a menudo se sienten abrumados hasta el punto de no tener suficiente tiempo para realizar la investigación y las evaluaciones. De esta forma como se muestra en la figura 7, se relaciona la intencionalidad de los actores principales al momento de afectar la seguridad de la información.

Figura 7 Ataques más comunes



Fuente: Tomado del sitio web https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

7 CATEGORIZACIÓN DE ESTRATEGIAS DE IMPLEMENTACIÓN DEL MODELO ZERO TRUST ACORDE AL CONTEXTO ORGANIZACIONAL

La implementación de un modelo de seguridad basado en “Zero Trust” en una organización requiere tener clara la premisa de "nunca confiar y verificar siempre", de esta forma se promulgará la protección de los datos y recursos. Es así que, a lo largo de los años, las organizaciones han incursionado en la implementación de marcos de referencia que abordan la Confianza Cero en su entorno, porque los avances tecnológicos y los cambios en la fuerza laboral de hoy en día, como las aplicaciones, los centros de datos basados en la nube, los dispositivos móviles, la modalidad de trabajo remota y mucho más, han provocado que el perímetro de la organización a nivel de red, se presente altamente afectado.

Es por esto que la implementación de un modelo de seguridad Zero Trust sugiere que las empresas no pueden confiar automáticamente en ningún usuario final que se ubiquen dentro o fuera de su perímetro, por lo tanto, se requieren privilegios estrictos, acceso de usuario y autenticación en todos los niveles para aplicaciones, dispositivos y usuarios. Dependiendo de su operación, objetivos comerciales y el tipo de sistemas heredados que utilice, no existe una solución única para todos. Sin embargo, es claro que se necesitará tiempo, recursos y la participación de toda la organización para crear una estrategia coherente y confiable. Antes de crear una hoja de ruta detallada, primero se debe conocer el grado de madurez de seguridad presente en la entidad.

7.1 FACTORES DE RIESGOS ORGANIZACIONAL

Existen metodologías, marcos de referencia, normas y estándares que evocan este concepto de contexto organizacional, como punto de partida para el despliegue u objeto de cambio en una organización. Es por tal razón que se hace necesario resaltar que este “consiste en evaluar las condiciones óptimas y las adversas que la rodean a la organización, para la preparación adecuada de modo que esas debilidades y amenazas tengan el menor impacto negativo en la empresa e impida el logro de los objetivos de la misma, así como para aprovechar las oportunidades que se presenten. Adicionalmente, permite manejar las variables que afectan a la organización y manipularlas a favor”[54]

Con lo anterior expuesto, el informe de Forrester, que se tituló “una guía práctica para una implementación de Zero Trust”, explora cinco componentes fundamentales

[54] ALIADOS EN TECNOLGÍA Y CALIDAD SAS. Lo que debes saber acerca del Contexto Organizacional: Importancia, evolución y exigencias. [sitio web]. [Consultado: 30 de octubre de 2021]. Disponible en: https://www.implementandosgi.com/estructura-alto-nive/contexto-organizacional-1/

que permite conocer y entender el punto de partida en la organización y de esta forma establecer una hoja de ruta en la migración de un sistema de seguridad tradicional, basado en el perímetro a un modelo de “Zero Trust”.

Ahora bien, con los componentes descritos y jerarquizados en la figura 8, a continuación, se brindará a cada una de estas áreas el detalle necesario para comprender los elementos prácticos de una implementación exitosa de Zero Trust.

Figura 8 Esquemas para entidades

Fuente: Tomado y adaptado de We live Security By Eset.

7.1.1 Zero trust para las personas

El componente humano suele ser el eslabón más débil en las prácticas de seguridad, ya que son víctimas de ataques de phishing o cometen errores debido a una mala gestión de contraseñas. Es fundamental alinear su estrategia con las personas de toda su organización mediante la inversión en la administración de identidad y acceder a todo su entorno local o en la nube. Con el acceso a los datos por parte de consumidores, empleados y terceros, las organizaciones necesitan desarrollar un proceso para un monitoreo consistente del acceso de los usuarios y aplicar conceptos de privilegios mínimos en todos los niveles. Esencialmente, si un usuario no necesita acceder a una función de administrador, no se debe coincidir, ya que, los usuarios con privilegios excesivos provocan más infracciones.

Por lo que se requiere implementar medidas de seguridad para cumplir con los requisitos de cumplimiento y centrarse más en la confianza cero con métodos como:

- Autenticación multifactor (MFA)
- Inicio de sesión único (SSO)

Permitiendo la automatización de tareas que fortalece las actividades de los grupos tácticos y operativos de seguridad o comúnmente llamados SOC (centro de operaciones de seguridad).

7.1.2 Zero trust para las operaciones

A medida que las organizaciones se diversificaron rápidamente en entornos de nube, la protección de las cargas de trabajo se ha convertido en una responsabilidad compartida entre el cliente y el proveedor de la nube. Según Forrester, hay tres pasos críticos que debe seguir para madurar la seguridad de la carga de trabajo, que incluyen;

- Establecer un proceso y una estructura de gobernanza de la nube: creando un proceso repetible y continuo que tenga una estructura formal para garantizar la cobertura adecuada de todas sus áreas y componentes de infraestructura que existen dentro de diferentes entornos (por ejemplo, nube local, privada y pública).

- Realizar el inventario y supervisión de las configuraciones de la carga de trabajo: utilizando soluciones de seguridad de carga de trabajo entre nubes para ayudar con la gobernanza formal (por ejemplo, CloudPassage, Qualys o Trend Micro).

- Centrarse en soluciones de gestión y seguridad nativas de la nube.

7.1.3 Zero trust para los dispositivos

El Internet de las cosas (IoT) ha hecho que la seguridad de los dispositivos conectados sea más desafiante, ya que los puntos de entrada en las redes han aumentado enormemente y han introducido más oportunidades para la explotación de vulnerabilidades con configuraciones y protocolos de comunicación inseguros. Para lograr un marco Zero Trust totalmente adoptado, los profesionales de la seguridad deben aislar, proteger y controlar todos los dispositivos conectados a la red.

A medida que desarrolla la hoja de ruta, se tiene varias sugerencias, que incluyen:

- Aplicar la segmentación de red Zero Trust a los dispositivos administrados: creando zonas o micro perímetros para aislar los dispositivos IoT de otros dispositivos o redes de TI.

- Fortalezca los dispositivos de IoT, mediante actualizaciones constantes y despliegue de componentes de seguridad.

- Reducir el riesgo de usuario creando políticas de traiga su propio dispositivo (BYOD): minimizando los problemas al negar las complicaciones que presentan los puntos finales, como eventos de malware o ransomware.

7.1.4 Zero trust para la red

Es aconsejable a cualquier tipo de organización la creación de límites mediante la segmentación lógica alrededor de los activos de la red y aumentar el aislamiento entre las segmentaciones. Esencialmente, en lugar de crear capas de controles de seguridad de afuera hacia adentro, debe proteger los datos de adentro hacia afuera trazando límites alrededor de los recursos en lugar de las redes.

Estos segmentos más pequeños, reducen la superficie de ataque para los actores malintencionados dentro de una red permitiendo solo que los puntos finales autorizados accedan a aplicaciones y datos particulares alojados en esos segmentos.

Para aumentar los controles de seguridad en la nube, se puede usar tecnología como firewalls de próxima generación para segmentar, aislar y restringir el tráfico en la red.

7.1.5 Zero Trust para los datos

Para proteger los datos, la organización primero debe descubrir y clasificar qué datos confidenciales deben protegerse, determinar dónde se encuentran y conceptualizar cómo puede defender esos datos. En Colombia el modelo de privacidad y seguridad de la información contiene una guía que genera un compendio de indicaciones útiles para clasificar y etiquetar los activos de la entidad.

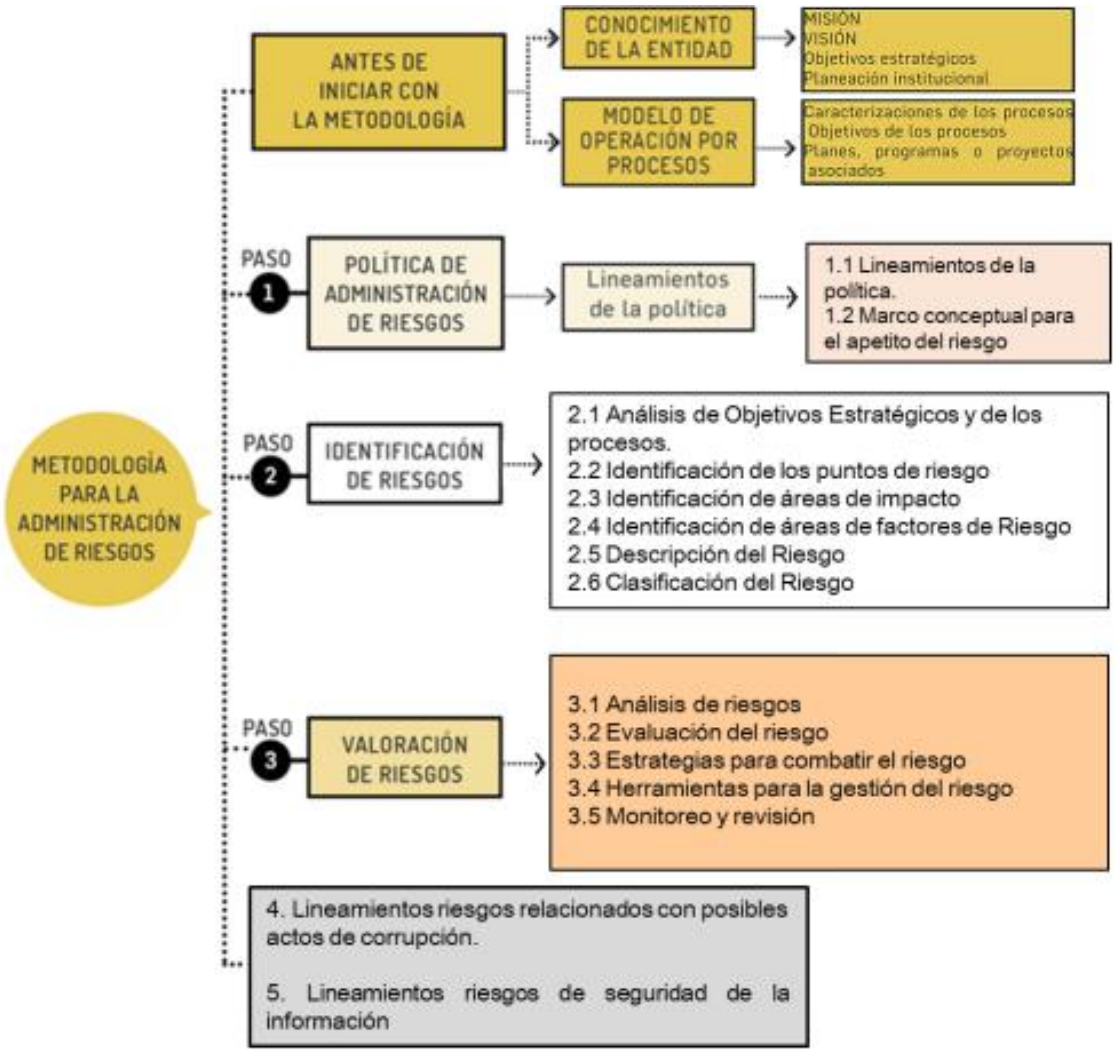
Es fundamental comprender las amenazas a las que se enfrentan los datos y cómo afectan a la entidad, y luego aplicar conocimientos contextuales para orientar las políticas y los controles.

7.2 CLASIFICACIÓN DE LOS NIVELES DE RIESGOS PARA LOS ACTIVOS DE LA INFORMACIÓN

Posteriormente de la definición de los factores descritos por el área de los riesgos presentes en cualquier entidad, se menciona que acorde con el Ministerio de Tecnologías de la Información y las Comunicaciones de la república de Colombia (MinTIC), existen diferentes lineamientos encaminados a la gestión los riesgos de Seguridad de la información, tomando como referencia los criterios de seguridad, tales como la confidencialidad, integridad y disponibilidad, con el propósito de integrar la metodología del Departamento Administrativo de la función pública (DAFP), el cual tiene como propósito “formular y promover las políticas e instrumentos en empleo público, organización administrativa, control Interno, racionalización de trámites, que van dirigidos a fortalecer la gestión de las Entidades Públicas Nacionales y Territoriales, mejorar el desempeño de los servidores

públicos al servicio del Estado, contribuir al cumplimiento de los compromisos del gobierno con el ciudadano y aumentar la confianza en la administración pública y en sus servidores."[55] De esta forma, emite la guía para la administración y gestión del riesgo donde se sugiere tres fases generales para la gestión del riesgo como se muestra en la figura 9.

Figura 9 Metodología para la administración del riesgo



Fuente: Tomado de la guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP.

[55] CONGRESO DE LA REPÚBLICA CÁMARA DE REPRESENTANTES. Departamento Administrativo de la Función Pública. Bogotá D.C. [sitio web]. [Consultado: 04 de enero de 2022]. Disponible en: https://www.camara.gov.co/departamento-administrativo-de-la-funcion-publica-0#:~:text=El%20Departamento%20Administrativo%20de%20la,P%C3%BAblicas%20Nacionales%20y%20Territoriales%2C%20mejorar

Es así, que la categorización y clasificación de los riesgos de los activos de información deben estar alineados con la normatividad para el sector comercial que aplique, es el caso que las entidades del sector estatal y públicas deberán acoger las estrategias descritas en el modelo de seguridad y privacidad de la información (MSPI) y la interrelación en las entidades transversales del estado como el modelo estándar de control interno y el modelo integrado de planeación y gestión (MIPG). En donde el análisis de riesgos debe tener en cuenta la sensibilidad de los datos procesados y almacenados por el sistema, así como respectivos criterios a evaluar.

- **Nivel alto:** "Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta." [56]

- **Nivel medio:** "Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio."[52]

- **Nivel Bajo:** "Activos de información en los cuales la clasificación de la información en todos sus niveles es baja."[52]

Para lo cual se toma como referencia, lo descrito en la guía No. 7 de gestión de riesgos del MinTIC, donde señala los siguientes niveles, que serán igualmente reflejado en la figura 10.

Figura 10 Criterios para valoración de riesgos

Fuente: Tomado guía de gestión de riesgos del MinTIC

[56] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN. Guía de gestión de riesgos. [Sitio web] Bogotá D.C: MINTIC. [Consultado: 04 enero 2022] Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150516_G7_Gestion_Riesgos.pdf

8 RECOMENDACIONES PARA PROTEGER LOS ACTIVOS DE LA INFORMACIÓN PARA LAS ENTIDADES PÚBLICAS DEL PAÍS BAJO UN MODELO DE ZERO TRUST

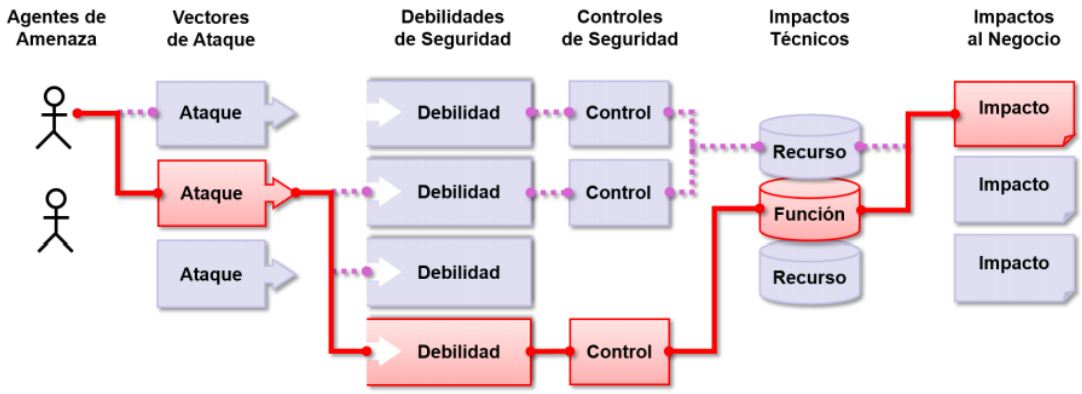
Continuando con lo expuesto en este trabajo, este capítulo aborda el consolidado de estrategias descritas anteriormente, desde el ámbito de aplicación de y puesta en marcha de los mecanismos capaces de reducir los riesgos de los activos de la información para las instituciones públicas en el país.

8.1 SEGURIDAD DE LAS APLICACIONES

La seguridad de las aplicaciones es el proceso de hacer que las aplicaciones sean más seguras mediante la búsqueda, reparación y mejora de la seguridad de las aplicaciones. Esto comúnmente se manifiesta cuando se inicia la fase de desarrollo, sin embargo, se debe incluir las herramientas disponibles y los métodos que permitan proteger las aplicaciones cuando salgan al entorno productivo. Esto es cada vez más importante a medida que los piratas informáticos dirigen su atención a los aplicativos con sus ataques de explotación de vulnerabilidades.

De acuerdo con State of Software Security Vol. 10, “el 83% de las 85.000 aplicaciones que probó tenían al menos una falla de seguridad. Muchos tenían gran cantidad identificadas, ya que su investigación encontró un total de 10 millones de fallas y el 20% de todas las aplicaciones tenían al menos una falla de alta gravedad”. No todas esas fallas presentan un riesgo de seguridad significativo, pero la gran cantidad es preocupante. Como se observa en la figura 11, algunos caminos pueden ser de difícil acceso, pero dejar expuesta esta vulnerabilidad aumenta la posibilidad de que el riesgo sea materializado y se convierta en una gran falla de funcionamiento.

Figura 11 Posibles riesgos en aplicaciones



Fuente: Tomado del sitio web https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Cuanto más rápido se fortalezcan las acciones en el proceso de desarrollo de software pueda encontrar y solucionar problemas de seguridad, más segura estará su empresa. Debido a que todos cometemos errores, el desafío es encontrar esos errores de manera oportuna. Por ejemplo, un error de codificación común podría permitir entradas no verificadas. Este error puede convertirse en ataques de inyección SQL y luego en fugas de datos si un pirata informático los encuentra.

Las API proporcionan la interfaz a través de la cual se accede a los datos. Esto incluye aplicaciones heredadas locales a modernas SaaS. Se debe reforzar la seguridad en cada una de estas aplicaciones y API para evitar la recopilación de datos y el acceso no autorizado. Se deben garantizar los permisos apropiados en la aplicación y se aconseja validar las opciones de configuración segura.

8.2 SEGURIDAD DE LA RED

Es vital comprender el concepto de seguridad en red, ya que este "combina varias capas de defensa en el perímetro y la red. Cada capa de seguridad de red implementa políticas y controles. Los usuarios autorizados tienen acceso a los recursos de red, mientras que se bloquea a los usuarios maliciosos para evitar que ataquen vulnerabilidades y amenacen la seguridad."[57] Se accede a todos los datos a través de la infraestructura de la red. Las redes deben estar segmentadas (micro segmentos), protección contra amenazas en tiempo real, monitoreo de cifrado de extremo a extremo y se deben emplear análisis para restringir el acceso de personas o dispositivos no autorizados.

8.2.1 Control de acceso

Esto se refiere a controlar qué usuarios tienen acceso a la red o secciones especialmente sensibles de la red. Con las políticas de seguridad, puede restringir el acceso a la red solo a usuarios y dispositivos reconocidos u otorgar acceso limitado a dispositivos que no cumplan con las normas o usuarios invitados.

Así mismo se puede catalogar como "el sistema autentifica la identidad del usuario mediante la verificación de las credenciales que el usuario conoce como el nombre de usuario y la contraseña. También podría ser algo que tenga el usuario como una tarjeta de identidad o una contraseña de un solo uso. Después de que el sistema verifique al usuario, la autorización es el proceso que le concede el permiso de acceso."[58]

---

[57] CISCO. ¿Qué es la seguridad de red? [sitio web]. [Consultado: 02 de septiembre de 2021]. Disponible en: https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html

[58] TREND MICRO. ¿Qué es seguridad de red? [Consultado: 02 de septiembre de 2021]. Disponible en: https://www.trendmicro.com/es_es/what-is/network-security.html

8.2.2 Segmentación de la red

La segmentación de la red, según lo menciona Trend Micro, “consiste en dividir una red en partes lógicas más pequeñas para que se puedan añadir los controles entre ellas. Así se mejora el rendimiento y la seguridad. Las redes de área local virtual (VLAN) son un método común de segmentación de la red que se lleva a cabo de forma local o utilizando una infraestructura en la nube.”[59]

La división y clasificación del tráfico de red en función de determinadas clasificaciones agiliza el trabajo del personal de soporte de seguridad cuando se trata de aplicar políticas. Las redes segmentadas también facilitan la asignación o denegación de credenciales de autorización para los empleados, lo que garantiza que nadie acceda a información que no debería. La segmentación también ayuda a las intrusiones o dispositivos potencialmente comprometidos.

8.2.3 Cifrado

Los cifrados generalmente se clasifican según cómo funcionan y cómo se utiliza su clave para el cifrado y el descifrado. Los cifrados de bloque, acumulan símbolos en un mensaje de un tamaño fijo (el bloque) y los cifrados de flujo funcionan en un flujo continuo de símbolos. Cuando un cifrado utiliza la misma clave para el cifrado y el descifrado, se conocen como algoritmos de clave simétrica. Los algoritmos o cifrados de clave asimétrica utilizan una clave diferente para el cifrado y el descifrado.

Los algoritmos de hash, según expone importante fabricante tecnológico, “se utilizan para demostrar que las letras, o los bits, no se han alterado de forma accidental. Tener el hash protegido con un cifrado le ayuda a saber que el hacker no ha cambiado el texto de forma maliciosa. El uso del hash para almacenar contraseñas, archivos de supervisión y garantizar la integridad de la comunicación de forma segura está muy extendido.”[60]

8.3 SEGURIDAD DE LA INFRAESTRUCTURA

La infraestructura que incluye todo el hardware, software, micro servicios, infraestructura de redes, instalaciones, etc., representa un vector de amenaza crítico. La gestión de la configuración, la evaluación de la versión y el uso de la telemetría para detectar ataques y anomalías ayuda a bloquear y marcar automáticamente el comportamiento de riesgo y a tomar las acciones necesarias.

[59] TREND MICRO. ¿Qué es seguridad de red? [Consultado: 02 de septiembre de 2021]. Disponible en: https://www.trendmicro.com/es_es/what-is/network-security.html
[60] Ibd 47

8.4 SEGURIDAD DE LOS DATOS

Eventualmente se toman todas las acciones para proteger los datos, que es el activo más preciado de una organización. Los datos corporativos deben categorizarse y el acceso debe restringirse. Los datos deben estar protegidos ya sea que se encuentren dentro de la organización, estén en tránsito o descargados. Debe ser clasificado, categorizado mediante el etiquetado, y encriptada para evitar el acceso no autorizado.

9 CONCLUSIONES

Se examinan los componentes y conceptos del modelo de seguridad “Zero trust” que permitió la identificación en el marco de trabajo necesario para comprender el contexto del paradigma en la seguridad de la información. Logrando observar que los enfoques de seguridad tradicionales asumen que se puede confiar en los elementos que ya están dentro de la red de una organización, esto, supone que las defensas en el perímetro de la red, como un firewall, son lo suficientemente efectivas para mantener a personas o dispositivos no deseados o no autorizados fuera de la red. Ahora con las nuevas tendencias en modalidades de trabajos y en ataques de vulnerabilidades, se comprende las características necesarias en la apropiación de los componentes básicos del modelo y el alcance del mismo en la protección de la información.

En este trabajo, se estableció que las debilidades en la protección de los activos de la información, pueden ser originadas por los intrusos internos con intenciones maliciosas causando tanto o incluso más daño que un atacante que se encuentra al exterior de la red. Donde se expone las vulnerabilidades por factores como, los empleados descontentos, que pueden interferir en los sistemas o inclusive la extracción y robo de los datos, causando un gran impacto a la estructura del negocio y los servicios que este ofrece a la comunidad.

En términos de la caracterización de los riesgos a la información, se expuso lo dictaminado por las autoridades colombianas en la gestión y valoración de riesgos a cargos de las entidades como el ministerio de las tecnologías de la información y comunicación y el departamento administrativo de la función pública, donde se establece los criterios y los niveles de impactos en el riegos de la afectación de la confidenciales, integridad y disponibles de la información en una organización pública en el país.

Se propone que mediante un enfoque del modelo “Zero Trust” ayuda a las organizaciones a hacer cumplir las políticas y los procesos que autentican, autorizan y validan continuamente a todos los usuarios y dispositivos. Se basa en la noción de que no se debe confiar en ningún usuario, dispositivo o aplicación de la red, incluso si se encuentra dentro del perímetro de seguridad de la organización. Conozca los conceptos y componentes de seguridad de confianza cero y cómo comenzar a implementar la confianza cero en la organización.

10 RECOMENDACIONES

La implementación de un modelo de seguridad basado en Zero trust, se dilucida como un proceso lento y paulatino, ya que es necesario expandir conceptos por toda la organización, con ese espíritu se sugiere a las futuras investigaciones profundizar en cada componente de la implementación de este modelo desde el ámbito de las infraestructuras críticas operadas por el estado, ya que puede abordar temáticas objetivas a los servicios esenciales mediados y soportados la tecnologías es de interés nacional.

Más allá del factor humano se encuentra el hardware. Existe una gran variedad de dispositivos móviles y computadoras personales a través de los cuales los empleados, clientes y proveedores se comunican con los sistemas de una empresa. Las políticas de traer su propio dispositivo (BYOD), el equipo de IT y la mentalidad de “siempre activo” conduce a una proliferación de propiedades, requisitos y protocolos de comunicación que deben ser rastreados y asegurados de manera continua, por lo que la relación de protocolos y equipos en la infraestructura de la organización puede ser altamente relacionado con nuevas soluciones que pueden abordar en futuras investigaciones para fortalecer los nuevos mecanismos de comunicación y de desarrollo organizacional.

Hoy en día, las organizaciones necesitan un nuevo modelo de seguridad que se adapte eficazmente a la complejidad del entorno moderno, abarque a la fuerza laboral móvil y proteja a las personas, los dispositivos, las aplicaciones y los datos dondequiera que se encuentren, es por este que se considera de interés para las futuras investigación ampliar el campo de aplicabilidad del presente trabajo, a los sectores tecnológicos, ya que son estos quienes brindan las oportunidad y facilidad de infraestructuras para las medianas y pequeñas empresas del país.

Los diferentes requisitos organizativos, las implementaciones de tecnología existentes y las etapas de seguridad afectan la forma en que se planifica la implementación del modelo de seguridad Zero Trust. Utilizando esta experiencia de desarrollo de las consideramos para el despliegue del modelo, se recomienda a las siguientes versiones de investigaciones apodar específicamente el contexto humano, como factor fundamental en la elaboración de políticas.

11 DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este, con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema del modelo de seguridad “Zero Trust”, puedan acceder al documento.

BIBLIOGRAFÍA

APONTE AGUDELO, Andrés. Modelo de seguridad para plataformas IAAS de la empresa Virgin Mobile. Trabajo de grado Especialista en seguridad informática. Bogotá D.C.: Universidad Nacional Abierta y A Distancia. Escuela de Ciencias Básicas e Ingeniería. 2018. 95 p.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. UNE-ISO/IEC 27000. 2 ed. Madrid, España. AENOR 2014. 30p.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. UNE-ISO/IEC 27001. 2 ed. Madrid, España. AENOR 2014. 30p.

CISCO. ¿Qué es un cortafuego? [sitio web]. [Consultado: 25 de noviembre de 2021]. Disponible en: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

CONGRESO DE LA REPÚBLICA. Diario oficial 51698. [sitio web]. Bogotá D.C. [Consulta: 04 de mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

CONGRESO DE LA REPÚBLICA. Diario oficial 51698. [sitio web]. Bogotá D.C. [Consulta: 04 de mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

CONGRESO DE LA REPÚBLICA. Diario oficial 51698. [sitio web]. Bogotá D.C. [Consulta: 04 de mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

ESET, WE LIVE SECURITY. WannaCry: tres años después sigue siendo una amenaza activa de la cual debemos aprender. [Consulta: 20 de Julio de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2020/05/12/wannacry-tres-anos-despues-una-amenaza-activa-debemos-aprender/

ESET. Antivirus. [sitio web]. [Consulta: 25 de noviembre de 2021]. Disponible en: https://www.eset.com/es/caracteristicas/antivirus-software-que-es/#

GUIJARRO, Alfonso. YEPEZ, Jesica. Defensa en profundidad aplicado a un entorno empresarial. *Revista Espacios.* 2018. nro 42. pp 19-28. ISSN 0798 1015.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del riesgo. Principios y directrices. ISO 31000. Bogotá D.C.: El Instituto, 2011. 34 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de Seguridad de la Información, Requisitos. ISO/IEC 27001. Bogotá D.C.: El Instituto, 2014. 30 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de Seguridad de la Información, Visión de conjunto y vocabulario. ISO/IEC 27000. Bogotá D.C.: El Instituto, 2014. 30 p.

INSTITUTO NACIONAL DE ESTANDARES Y TECNOLOGÍA. Computer Security Resource Center. [sitio web]. Gaithersburg: NIST. [Consulta: 06 de junio de 2021]. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-207/archive/2020-02-13

INSTITUTO NACIONAL DE ESTANDARES Y TECNOLOGÍA. Computer Security Resource Center. [sitio web]. Gaithersburg: NIST. [Consulta: 06 de junio de 2021]. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-207/archive/2020-02-13.

INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA. Marco para la mejora de la seguridad cibernética en infraestructuras críticas. [sitio web]. [Consulta: 11 de junio de 2021]. Disponible en: https://doi.org/10.6028/NIST.CSWP.04162018.

KASPERSKY LAB. ¿Qué es la ciberseguridad? [Sitio web] Centro de recursos. [Consultado: 11 julio 2021] Disponible https://latam.kaspersky.com/resource center/definitions/what-is-cyber-security

KINDERVAG, JHON. Build Security into Your Network's DNA: The Zero Trust Network Architecture. Forrester Research. 2018. pp 27.

KINDERVAG, JHON. No More Chewy Centers: Introducing The Zero Trust Model of Information Security. Forrester Research. 2018. pp 15.

MAGAZCITUM. Seguridad perimetral: el debate del momento. [sitio web]. [Consultado: 25 de noviembre de 2021]. Disponible en: https://www.magazcitum.com.mx/index.php/archivos/2489

MALWAREBYTES. Todo sobre el hackeo. [Sitio web] [Consultado: 11 julio 2021] Disponible en: https://es.malwarebytes.com/hacker/

MARCAL, David. 'Zero Trust' desconfía por naturaleza. Revista Red seguridad. 2020. nro 91. pp 56-58.

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN. Gobierno Digital. [sitio web]. Bogotá D.C: MINTIC. [Consulta: 07 de junio de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad//MSPI/

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN. Guía para la Gestión y Clasificación de Activos de Información. [Sitio web] Bogotá D.C: MINTIC. [Consultado: 11 julio 2021] Disponible en: https://www.mintic.gov.co/gestionti/615/articles-482_G5_Gestion_Clasificacion.pdf

NETWORK WORLD. The Jericho Forum and its goals. Networking. [sitio web]. [Consultado: 22 de julio de 2021]. Disponible en: https://www.networkworld.com/article/2325412/the-jericho-forum-and-its-goals.html

ORGANIZACIÓN MUNDIAL DE LA SALUD. [sitio web]. Ginebra: OMS. [Consulta: 29 de mayo de 2021]. Disponible en: https://www.who.int/es/emergencies/diseases/novel-coronavirus-2019

POGII, Nicolás. 30 Estadísticas de Seguridad Informática que importan actualizadas 2021 en: THE MISSING REPORT. [sitio web]. San Francisco. [Consulta: 29 de mayo de 2021]. Disponible en: https://preyproject.com/blog/es/30-estadisticas-seguridad-informatica/

REMOLINA BECERRA, Luis. Diseño de un modelo de seguridad informática a una empresa en su sistema de monitoreo del área de tecnología. Trabajo como ingeniero de Telecomunicaciones. Facultad de Ingeniería. Universidad Cooperativa De Colombia. 2019. 68 pp.

RODRIGUEZ GAHONA, Guillermo. Análisis comparativo de los modelos defensa en profundidad y MSPI, para la implementación de la seguridad informática en el sector privado del país. Trabajo de grado Especialista en seguridad informática. Bogotá D.C.: Universidad Nacional Abierta y A Distancia. Escuela De Ciencias Básicas e Ingeniería. 2020. 97 p.

SEMANA. El 76% de organizaciones en Colombia reportó incidentes en la nube. Ciberseguridad. [Consulta: 20 de julio de 2021]. Disponible en: https://www.semana.com/tecnologia/articulo/sophos-76-de-organizaciones-en-colombia-reportaron-incidentes-en-la-nube/292849/

SISTEMA ÚNICO DE INFORMACIÓN NORMATIVA. Diario oficial. [sitio web]. Bogotá D.C. [Consulta: 04 de mayo de 2021]. Disponible en: http://www.suin-juriscol.gov.co/viewDocument.asp?id=30035329

THE OPEN GROUP. Vision & Mission. [sitio web]. [Consultado: 22 de julio de 2021]. Disponible en: https://www.opengroup.org/about-us/vision-mission

UNIVERSIDAD DE LA RIOJA. Seguridad perimetral informática: objetivos y plataformas recomendables. Ingeniería y tecnología. [sitio web]. [Consulta: 25 de

noviembre de 2021]. Disponible en: https://www.unir.net/ingenieria/revista/seguridad-perimetral-informatica/

Resumen Analítico Especializado -RAE

Programa:	ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
Línea de Investigación:	GESTIÓN DE SISTEMAS
Título:	ANÁLISIS DEL MODELO DE SEGURIDAD ZERO TRUST Y LAS CONSIDERACIONES GENERALES APLICABLES A CUALQUIER ORGANIZACIÓN PÚBLICA EN COLOMBIA.
Autor(es):	JORGE LUIS GAITAN BAQUERO
Palabras Claves:	Análisis, activo de la información, ciberseguridad, entidades públicas, Zero Trust.
Año	2022
Descripción del trabajo:	El presente trabajo expone la recopilación de información sobre los componentes y la arquitectura de seguridad basado en el modelo de Zero Trust y las consideraciones de su posible implementación en las organizaciones públicas colombianas que desarrollen o utilice un sistema de información, permitiendo de esta forma brindar una perspectiva general sobre la importancia de contar con el conjunto de medidas optimas que minimicen el riesgo de un ataque informático y el impacto del negocio al interior de la zona definidas como perímetro en las entidades. .

Fuentes bibliográficas destacadas:

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. UNE-ISO/ICE 27001. 2 ed. Madrid, España. AENOR 2014. 30p.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. UNE-ISO/ICE 27000. 2 ed. Madrid, España. AENOR 2014. 30p.

CONGRESO DE LA REPÚBLICA. Diario oficial 51698. [sitio web]. Bogotá D.C. [Consulta: 04 de mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

CONGRESO DE LA REPÚBLICA. Diario oficial 51698. [sitio web]. Bogotá D.C. [Consulta: 04 de mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

CONGRESO DE LA REPÚBLICA. Diario oficial 51698. [sitio web]. Bogotá D.C. [Consulta: 04 de mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

KINDERVAG, JHON. No More Chewy Centers: Introducing The Zero Trust Model of Information Security. Forrester Research. 2010. pp 15.

KINDERVAG, JHON. Build Security into Your Network's DNA: The Zero Trust Network Architecture. Forrester Research. 2010. pp 27.

NETWORK WORLD. The Jericho Forum and its goals. Networking. [sitio web]. [Consultado: 22 de julio de 2021]. Disponible en: https://www.networkworld.com/article/2325412/the-jericho-forum-and-its-goals.html THE OPEN GROUP. Vision & Mission. [sitio web]. [Consultado: 22 de julio de 2021]. Disponible en: https://www.opengroup.org/about-us/vision-mission	
Descripción del problema	Los constantes cambios organizacionales, la invocación tecnología, la implementación de tecnología emergente, el crecimiento en la utilización de dispositivos electrónicos y la masificación del uso del internet abre la posibilidad que las entidades en Colombia, se interesen en adquirir tecnología permitiéndole fortalecer sus sistemas de seguridad tanto física como digital. No obstante, se hace necesario el estudio de nuevas metodologías que acompañen la implementación de estos sistemas para brindar las alternativas necesarias a cualquier tipo de ataque o incidentes graves de seguridad de la información. Por lo tanto, se hace el planteamiento del problema bajo el siguiente interrogante: ¿Cómo un modelo de seguridad basado en Zero Trust permite asegurar los activos de información en las organizaciones públicas en Colombia?
Contenido del documento:	El trabajo está compuesto con una introducción, una definición del problema con su respectiva formulación del problema, así mismo con la justificación que englóbala importancia de contar con medidas de protección de la información, seguidamente un objetivo general, donde se relaciona la finalidad del proyecto y los objetivos específicos que relata los pasos para cumplir dicho objetivo general. Posteriormente se encuentra el marco referencial que ilustra la correlación de los modeles y marcos de referencia en seguridad de la información brindando especificar los conceptos y metodologías que facilitan la comprensión de la temática principal. Seguidamente el marco teórico donde se describe los Sistema de gestión de seguridad de la información, Modelo de seguridad y privación de la información, Modelo defensa en seguridad en profundidad, Marco de Ciberseguridad del NIST para luego finalizar con el marco legal, acá se describe la normatividad que sustenta la investigación como el decreto 1008 de 2018. Así mismo se dan a conocer los conceptos y componentes básicos de un modelo de seguridad “zero trust”, sus principios y casos de estudios. Para abordar las vulnerabilidades se hace el recuento de las más comunes y las posibles estrategias para su mitigación.

Objetivo general	Analizar las consideraciones generales de un modelo de seguridad de Zero Trust que brinda una alternativa de seguridad a los activos de la información a cualquier organización pública en Colombia, por medio de la recopilación de información y la integración de estrategias relacionadas con la protección de la información.
Objetivo específicos	• Examinar los conceptos y componentes básicos del modelo de seguridad mediante la búsqueda de información relacionada y la conceptualización de términos relevantes, proporcionando las características y alcance del modelo "Zero Trust" debido al poco conocimiento sobre la metodología propuesta en las instituciones públicas del país. • Establecer las principales debilidades en la protección de los activos de la información para las entidades públicas del país, exponiendo los posibles campos de acción en la identificación de las vulnerabilidades más comunes en las organizaciones, relacionando metodologías y datos sobre las amenazas existentes, generando el contexto necesario sobre los riesgos identificados. • Categorizar los riesgos a la información identificados previamente, mediante la relación de estrategias de protección a la información que genere soluciones factibles a la implementación de un modelo de seguridad "Zero Trust", en virtud del contexto organizacional. • Proponer las recomendaciones para la implementación del modelo de seguridad "Zero Trust" en cualquier entidad pública del país mediante la presentación de metodologías y estrategias que garanticen los niveles apropiados de riesgos en los activos de información, en respuesta a la creciente tendencia de ataques a la información en el país.
Conceptos adquiridos :	El desarrollo de esta propuesta permito conocer diferentes vectores de ataques internos que nos desconocidos por muchos y exportados por personas inescrupulosas, así mismo se conoce una alternativa en la protección de los activos de la información capaz de retener ataques al interno de una organización con el propósito de reducir los riesgos y mitigar las vulnerabilidades.
Conclusiones:	Se examinan los componentes y conceptos del modelo de seguridad "Zero trust" que permitió la identificación en el marco de trabajo necesario para comprender el contexto del paradigma en la seguridad de la información. Logrando observar que los enfoques de seguridad tradicionales asumen que se puede confiar en los elementos que ya están dentro de la red de una organización, esto, supone que las defensas en el perímetro de la red, como un firewall, son lo

	suficientemente efectivas para mantener a personas o dispositivos no deseados o no autorizados fuera de la red. Ahora con las nuevas tendencias en modalidades de trabajos y en ataques de vulnerabilidades, se comprende las características necesarias en la apropiación de los componentes básicos del modelo y el alcance del mismo en la protección de la información. Se propone que mediante un enfoque del modelo “Zero Trust” ayuda a las organizaciones a hacer cumplir las políticas y los procesos que autentican, autorizan y validan continuamente a todos los usuarios y dispositivos. Se basa en la noción de que no se debe confiar en ningún usuario, dispositivo o aplicación de la red, incluso si se encuentra dentro del perímetro de seguridad de la organización. Conozca los conceptos y componentes de seguridad de confianza cero y cómo comenzar a implementar la confianza cero en la organización.