Universidad Cenfotec

Maestría en Ciberseguridad

Escuela de Informática

Tema:
Propuesta de solución para la modernización de accesos e identidades, bajo principios de cero confianza

Elaborado por:
Danny Vargas

Fecha: Febrero, 2022

Declaración Jurada

Yo, Danny Vargas Fernández, estudiante de la Universidad Cenfotec, declaro bajo fe de juramento y consciente de las responsabilidades penales de este acto, que soy autor intelectual de la tesis o proyecto de investigación titulado: Propuesta de solución para la modernización de accesos e identidades, bajo principios de cero confianza, por lo que libero a la Universidad Cenfotec de cualquier responsabilidad en caso de que la declaración sea falsa.

Brindado en San Pedro, Montes de Oca, San José Costa Rica en el día 16 de Marzo del año 2022.

DANNY ALONSO VARGAS FERNANDEZ (FIRMA)

Firmado digitalmente por DANNY ALONSO VARGAS FERNANDEZ (FIRMA)
Fecha: 2022.03.16 11:05:09 -06'00'

Danny Vargas Fernández
2-0635-0797

Agradecimiento

Inicialmente agradezco a Dios por darme la vida, por darme las fuerzas día con día y guiarme con sabiduría y entendimiento en el proceso de mi vida laboral. También deseo agradecer a mi familia que han sido los más sacrificados, por los momentos que estuve ausente durante el desarrollo de esta carrera, y a todas las personas que me apoyaron en el proceso. Agradezco a VMware INC que me apoyó y brindó los recursos económicos, por creer en este proyecto, y sobre todo en mí. A todos los profesores que nos compartieron sus experiencias y conocimiento durante la carrera y especialmente a Alonso Ramírez, tutor de este trabajo de investigación. A todos mis compañeros de la carrera que durante estos dos años compartimos de manera virtual, pero aprendimos mucho juntos.

Dedicatoria

A todas aquellas personas que están iniciando una carrera laboral en tecnologías de información, que desean aprender de seguridad de la información y desean desarrollar un proyecto basado en principios de cero confianza.

Universidad Cenfotec
Carrera de Postgrado
Maestría en Ciberseguridad

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Vargas Fernández Danny.**

Alonso Ramírez — Digitally signed by Alonso Ramírez Date: 2022.03.08 18:27:02 -06'00'

M. Sc. Luis A. Ramírez Jiménez
Tutor

REBECA ESQUIVEL FLORES (FIRMA) — Firmado digitalmente por REBECA ESQUIVEL FLORES (FIRMA) Fecha: 2022.03.09 08:54:44 -06'00'

M. Sc. Rebeca Esquivel Flores
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA) — Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA) Fecha: 2022.03.10 18:51:15 -06'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 05 de marzo de 2022

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

Tabla de contenido

Capítulo 1. Introducción 1
1.1 Generalidades 2
1.2 Antecedentes del problema 2
1.3 Definición y descripción del problema 4
1.4 Justificación 5
1.5 Viabilidad 7
1.5.1 Punto de vista técnico 8
1.5.2 Punto de vista operativo 8
1.5.3 Punto de vista económico 9
1.6 Objetivos 10
1.6.1 Objetivo general 10
1.6.2 Objetivos específicos 10
1.7 Alcances y limitaciones 11
1.7.1 Alcances 11
1.7.2 Limitaciones 11
1.8 Marco de referencia organizacional y socioeconómico 12
1.8.1 Historia 13
1.8.2 Tipo de negocio y mercado meta 23
1.9 Estado de la cuestión 23
1.9.1 Planificación de la revisión 24
1.9.2 Ejecución de la revisión 34

Capítulo 2. Marco conceptual 37
2.1 Concepto de cero confianza 38
2.1.1 Cero confianza según Forrester 38
2.1.2 Cero confianza según National Institute of Standads and Technology (NIST) 39
2.1.3 Cero confianza según CISCO 40
2.1.4 Cero confianza según Cloud Security Alliance (CSA) 41
2.1.5 Los cinco pilares de cero confianza 41
2.2 Conceptos sobre espacios digitales 44
2.2.1 Dispositivos móviles 44
2.2.2 El internet de las cosas (IoT) 45
2.2.3 Traer su porpio dispositivo (BYOD) 45
2.2.4 Conceptos de administración unificada de dispositivos (UEM) 47
2.3 Conectividad 48
2.3.1 Perímetro definido por el software (SDP) 48

2.3.2 Conceptos sobre segmentación 49
2.3.3 Conceptos sobre microsegmentación 49
2.3.4 Redes Privadas Virtuales (VPN) 50
2.3.4 Firewall o Cortafuegos 50
2.3.6 Secure Access Service Edge (SASE) 51
2.3.6.1 Puerta de enlace segura (SWG, Segure Web Gateway)) 52
2.3.6.2 Redes de cero confianza (ZTN) 53
2.3.6.3 Agente de seguridad de acceso en la nube (CASB) 55
2.3.6.4 Cloud Firewall (Cortafuegos en la nube) 56
2.3.6.5 Firewall como servicio 57
2.4 Autenticación 57
2.4.1 Proveedores de Identidad 57
2.4.2 Identidad del usuario 59
2.4.3 Inicio de sesión único 59
2.4.4 Autenticación de dos factores 63
2.4.3.1 ¿Qué es un factor de autenticación? 63
2.4.4 Identidad como servicio (IDaaS) 64
2.4.5 Security Assertion Markup Language (SAML) 64
2.4.5.1 ¿Qué es una aserción SAML? 65
2.4.6 Autenticación Abierta (OAuth) 65

Capítulo 3. Marco metodológico 66
3.1 Tipo de investigación 67
3.2 Alcance investigativo 67
3.3 Enfoque 67
3.4 Diseño 68
3.5 Población y muestreo 69
3.6 Instrumentos de recolección de datos 70

Capítulo 4. Análisis del diagnóstico 71
4.1 Aplicación de los cuestionarios 71
4.1.1 Aplicación de cuestionarios a usuarios de las empresas 72
4.1.2 Conclusiones de los resultados 78

Capítulo 5. Propuesta de solución 80
5.1 Descubrimiento 84
5.1.1 Generación de documentos y evidencia 84
5.1.3 Sesiones de trabajo 89
Cuestionario de captura de información 90
5.1.4 Listado de requerimientos 95
5.2 Diseño 96
5.2.1 Propuesta de alto nivel 96
5.2.2 Aceptación de propuesta de solución 98

5.2.3 Diseño 99
5.2.4 Revisión del diseño 113
5.2.5 Aceptación diseño 114
5.3 Implementación 115
5.3.1 Reunión inicial del proyecto 115
5.3.2 Implementación de pre-producción 116
5.3.3 Pruebas de la solución 116
5.3.4 Fase de implementación en producción 117
5.3.5 Pruebas en ambiente de producción 117
5.3.6 Entrega a operaciones 118
5.4 Operaciones 119
5.4.1 Manuales de uso 119
5.4.2 Monitoreo de funcionamiento 120
5.4.3 Generación de reportes 120
5.5 Mejora continua 121
5.5.1 Análisis de reporte de operaciones 122

Capítulo 6. Conclusiones y recomendaciones 125
6.1 Conclusiones 125
6.2 Recomendaciones 127

Referencias bibliográficas 129

Apéndices 131
Anexo 1. Tabla de riesgos, vulnerabilidades y amenazas 132

Tabla de ilustraciones

Ilustración 1: Procedimiento de selección de estudios 32

Ilustración 2: Ejemplo de busquedas 33

Ilustración 3: Ejemplo de búsquedas 34

Ilustración 4: Nube de palabras, generado del sitio https://www.nubedepalabras.es 36

Ilustración 5: Diagrama de tipos de empresas Pyme y aspectos tecnológicos en espacios digitales 40

Ilustración 6: Ciclo del desarrollo de una arquitectura de seguridad basada en cero confianza 71

Ilustración 7: Resumen de la situación actual de la empresa. Fuente: elaboración propia 76

Ilustración 8: Resumen de propuesta hacia la gerencia. Fuente: elaboración propia 84

Ilustración 9: Cuadro de calor de los riesgos. Fuente: elaboración propia 88

Ilustración 10: Diagrama de gestión de politicas cero confianza. Fuente: elaboración propia 94

Ilustración 11: Autenticación SAML. Fuente: elaboración propia 97

Abstract

El desarrollo socioeconómico es uno de los principales indicadores de bienestar de la sociedad, de una región y de un país; conforme se continua buscando el progreso y el empoderamiento de las personas que desean mejorar sus condiciones de vida, se promueve la creación y el fortalecimiento de las micro, pequeñas y medianas empresas que permiten contribuir a ese desarrollo, mediante la generación de nuevos empleos e ingresos, además de la contribución que realizan a la competitividad del país. Asimismo, los emprendimientos promueven procesos dinámicos e innovadores, ayudan a la economía y eventualmente pueden contribuir a que las empresas existentes se vean obligadas a modificar sus estructuras para no “quedarse atrás” y aprovechen otras herramientas, como la tecnología y /o la innovación, para brindar mejores servicios y productos a sus clientes.

El objetivo de esta investigación es elaborar una propuesta de solución para la modernización de accesos e identidades, bajo principios de cero confianza. Este plan podría llegar a ser utilizado desde pequeñas hasta grandes empresas, todo depende del caso de uso.

Muchas empresas no disponen de grandes recursos para comprar equipo y sistemas para los colaboradores, por lo que la idea es ellos utilicen sus propios dispositivos en el hogar, y la empresa, por su parte, puede darles un subsidio por gastos de internet y de equipo.

Palabras clave: administración de dispositivos móviles, espacios digitales, escritorios virtuales, redes privadas virtuales, segundo factor de autenticación, prevención de pérdida de información, cero confianza, arquitectura, cifrado.

Capítulo 1. Introducción

1.1 Generalidades

Este trabajo es elaborado para que las empresas tengan una guía o herramienta para la modernización de accesos e identidades bajo principios de cero confianza, con el fin de ser utilizados en momentos de pandemia, en Costa Rica. Los datos proporcionados son información pública y los ejemplos utilizados en su medida pueden ser ficticios para brindar la confidencialidad, según sea el caso. Cuando en un ejemplo se menciona el nombre de una empresa en específico, será presentado bajo su aprobación.

1.2 Antecedentes del problema

Hoy en día, la globalización ha hecho que muchas empresas necesiten de herramientas que no solo les permitan estar conectadas con el mundo, sino que estén disponibles, para así permitir a la empresa generar ingresos.

Se ha visualizado que existen empresas que dependen de tecnologías de información , en Costa Rica, desde el año 2015, se ha celebrado su intento por la adhesión a la OCDE para participar como miembro activo de las sesiones y muchos de los comités especializados en temas del país. Para coordinar la alianza, el país ha trabajado en una serie de planes de acción que se deben cumplir en conjunto con revisiones de determinadas políticas públicas, siendo el cuarto país en América Latina detrás de Chile, México y Colombia. El ingreso es de importancia estratégica, ya que se le otorgará al país un sello de calidad y seriedad esencial para garantizar sus credenciales como un sistema de gobernanza democrática, sustentando un sólido

estado de derecho, y con estándares de gestión pública y económica coherentes basados en las mejores prácticas de los países más desarrollados del mundo.

Al crear una relación de beneficio en conjunto con países miembros se mantiene en el ámbito de la ciberseguridad los siguientes objetivos:

- Comprensión de la seguridad digital y de la responsabilidad de los distintos actores de su gestión.
- Desarrollo de una estrategia nacional para la gestión del riesgo de la seguridad digital.
- Colaboración con otras partes interesadas.
- Fomento de la cooperación internacional y de la asistencia mutua.

La Organización de Estados Americanos en conjunto con el observatorio de ciberseguridad publicaron en el año 2020 un reporte llamado “Ciberseguridad, Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe”. Este reporte contiene un modelo de madurez de ciberseguridad que fue la base de los estudios regionales de la OEA y el Banco Interamericano de Integración Económica para las regiones. Este documento se basa en cinco dimensiones:

1. Política estratégica.
2. Cultura y sociedad.
3. Educación, capacitación y habilidades.
4. Marcos legales y regulatorios.
5. Estándares, organizaciones y tecnologías.

Para medir de manera confiable la capacidad cibernética, cada dimensión se desglosa en factores, aspectos e indicadores. En cada nivel evalúa la capacidad con granularidad progresiva.

En los últimos años, diversos países de América Latina y el Caribe han sido testigos y víctimas no solo del incremento de amenazas en ciberseguridad, sino en la intensidad y sofisticación de estas, las cuales han afectado no solamente a instituciones públicas y del sector privado, sino también contabiliza a ciudadanos de estos países.

Se menciona que el incremento de las actividades ya es conocido desde un informe publicado en el 2016, donde se muestra el aumento de la penetración de las tecnologías digitales en la región y de los procesos de transformación digital.

1.3 Definición y descripción del problema

Ahora con el COVID-19 entre nosotros, muchas personas, empresas, escuelas y demás han cambiado su forma de vivir, su forma de ser, trabajar o ejecutar. Los gobiernos, en especial el de Costa Rica, han instado a las empresas tanto públicas, como privadas a hacer el uso del teletrabajo como herramienta principal para permitir que los trabajadores continúen con sus labores sin exponerse a salir de sus casas.

El problema en resumen es que existen empresas que necesitan continuar con sus labores del día a día, mantener su información segura y permitir a sus usuarios remotos ingresar con dispositivos, conocidos o desconocidos, a las redes empresariales. Basado en ello surgen las siguientes interrogantes:

¿Estará el dispositivo asegurado?

¿La conexión es segura?

¿Cómo se maneja la información dentro del dispositivo?

Una vez conectado, ¿a qué redes o información se tiene acceso?

Estas interrogantes fomentan el problema que se le esta presentando a muchas empresas de Tecnología de Información (TI) en la actualidad, ya que están abordando

situaciones de riesgo como fuga de datos, competencia desleal, robo de información e intentos de ataques *phishing*.

Según la empresa IBM, el costo promedio de una filtración de datos es de 3.86 millones de dólares. Para una empresa de salud ha llegado a ascender hasta 7.13 millones y el costo más caro reconocido en la historia es de 8.64 millones de dólares.

La arquitectura de cero confianza viene a resolver problemas bajo la premisa de no confiar en nadie, se basa en el hecho de que las amenazas son ubicuas, existen dentro y fuera de la empresa. Dicha tecnología incluye la prevención, la detección y la respuesta en un enfoque de varias capas.

1.4 Justificación

El motivo de este proyecto de investigación es colaborar con las empresas en mantener su negocio en funcionamiento en tiempos de pandemia o crisis, como con el SARS-COV19 o posteriores pandemias, empleando herramientas digitales, las cuales los colaboradores pueden tener en sus hogares con un acceso seguro y sin hacer mucha inversión. Esto permitirá a los empleadores apoyarse con herramientas de trabajo que les siga generando ingresos y mantener firme su negocio.

Ahora que el país es parte de la OCDE debe cumplir varios aspectos en la seguridad de la información, por esta razón las entidades del gobierno deben preocuparse en cumplir con el manejo de la información, donde se almacena e incluso quien la visualiza. Por lo tanto, arquitecturas de cero confianza permitiría al gobierno trabajar de una forma más transparente, limitar el acceso y brindar seguimiento a quienes intentan acceder a los datos.

Los nómadas digitales

Son trabajadores remotos, o a distancia, que no son nacionales del lugar donde trabajan, realizan sus labores por medio de internet y se mudan de país con frecuencia, ya sea en cuestión de semanas o meses. Se caracterizan por:

1. Hacer uso de tecnología para trabajar desde cualquier país.
2. Combinar turismo con trabajo.
3. Trabajar en proyectos que no están directamente ligados al país destino.
4. No desplazar mano de obra local.
5. Depender de un patrono o empleador, o bien ser independientes o *freelancers*.

Estos trabajadores requieren flexibilidad en cuanto a tiempo de permanencia en un territorio sin perder su estatus migratorio, porque posiblemente viajarán con frecuencia. No se les debe exigir un garante o patrocinador local, pues trabajan con empleadores o clientes en el exterior. Finalmente, a los nómadas digitales les es imprescindible contar con una buena plataforma digital para realizar todos sus trámites, pues desempeñan sus funciones de manera virtual.

El Instituto Costarricense de Turismo (ICT) publicó, el 05 de marzo del 2021, que los turistas provenientes de Estados Unidos, Chile y Portugal destacan las ventajas de vivir y trabajar desde Costa Rica, demostrando que el país ha sido seleccionado por un número extraordinario de turistas que buscan un destino ideal para que se puedan alojar y trabajar remotamente. Costa Rica les ofrece seguridad durante la pandemia

y la posibilidad de combinar las labores de sus países de origen con sus clases de surf, paseos a la montaña y otras actividades naturales o culturales.

El problema radica en que esa atracción turística puede repercutir en un paraíso fiscal, ya que el proyecto de ley 22.215 evidencia que Costa Rica dejaría de percibir dinero al exonerar fiscalmente las actividades remuneradas de dichos trabajadores.

El nómada digital debe ser protegido, ya sea un trabajador que labore remotamente desde Costa Rica, o bien un colaborador costarricense que trabaje en otro país, porque la información que esas personas manejan en sus equipos es tan valiosa que las empresas no han evaluado el costo que una repercusión negativa le puede brindar a la empresa. El hecho que a un nómada digital se le extravíe el equipo o la información puede ser perjudicial para la empresa que labora o sus personas, del mismo modo que los negocios o sus clientes, la pérdida de credibilidad de la institución y hasta consecuencias legales podrían verse implicadas.

Por ejemplo, la empresa IBM publicó que en el año 2020 el costo de una filtración de datos en promedio tiene un costo de $3.86 millones y en el año 2019 tuvo un promedio de $3.92 millones. Las empresas más afectadas fueron organizaciones enfocadas en salud.

1.5 Viabilidad

El modelo de cero confianza tiene como principio nunca confiar, siempre comprobar. Aunque no es un modelo nuevo, la mayoría de las empresas hoy en día tienden a comprobar y luego confiar. Dado a esta confianza tradicional, cualquier individuo que posea las credenciales de un usuario, con ellas puede tener acceso a la información, los equipos, sitios web, dispositivos, etc. Por esta razón ese tipo de modelos no es

factible y es necesario hacer un análisis profundo para evitar la suplantación de identidad.

Por lo tanto, el objetivo de esta investigación es obtener mediante las fuentes de consulta de los fabricantes las herramientas ofrecidas, encontrar mejores prácticas y, de esta manera, proveer de una propuesta para las empresas.

1.5.1 Punto de vista técnico

En este proyecto el investigador posee las capacidades técnicas para poder explicar a los lectores temas relacionados, e implementados, sobre diferentes tecnologías en diversas empresas a nivel de América Latina. Por este motivo el propósito de esta investigación es tomar mejores prácticas de estas implementaciones y desarrollar el tema expuesto; ya que se tienen las habilidades técnicas acreditadas y certificadas por los fabricantes, además de los entrenamientos especializados para generar soluciones y propuestas que permitan crear arquitecturas bajo el principio de soluciones de cero confianza.

1.5.2 Punto de vista operativo

El desarrollo de esta investigación no afecta a las empresas, pues se trata de un tema a nivel global. La recopilación de la información se encuentra en su mayoría en sitios públicos reconocidos como la OCDE, fabricantes de arquitectura de cero confianza, así como también contenido digital ubicado en las instituciones públicas, como el Instituto Nacional de Aprendizaje, el Ministerio de Ciencia y Tecnología, y el Ministerio de Economía y Comercio.

Según la OEA, con la pandemia COVID-19 se incrementó la actividad digital en la región, este hecho ha dejado aún más en evidencia las vulnerabilidades del espacio digital de América Latina y el Caribe. El informe de *Cibercrimen ThreatMetrix* identificó

a América Latina como un foco para el fraude en la creación de cuentas, con alrededor del 20% del volumen total frente a un promedio de la industria del 12,2%.

1.5.3 Punto de vista económico

El desarrollo de este trabajo de investigación no requiere de comprar licenciamiento, equipo computacional u algún otro tipo de artefacto, sino que está orientado a la realización de horas de consultoría en investigación. Las cuales toman como ejemplo base los salarios mínimos del Ministerio de Trabajo y Seguridad Social. El salario que se toma como base es el de un licenciado en Informática, como se observa en la siguiente tabla; esta investigación no genera ningún costo económico a alguna organización, por lo tanto, se considera como un costo teórico que el investigador asumirá con horas de consultor. Además, este costo no está asociado a ninguna organización por lo que no hay salarios y comisiones que sean necesarios para el desarrollo del proyecto, ya que serán asumidos por el investigador.

Tabla 1: Salario mínimo en colones de un licenciado según MTSS

Salario anual	Salario mensual	Salario diario	Salario por hora
¢8,166,786.36	¢680,565.53	¢34028.27	¢4253.53

1.6 Objetivos

El objetivo de esta investigación consiste en proponer una metodología que actualice el principio estándar utilizado por la mayoría de las empresas, que trabajan en el concepto de comprobar y luego confiar. Este concepto puede estar obsoleto y para ello vamos a demostrar cómo actualizar a las organizaciones bajo principios de cero confianza.

Para investigación se plantearon los objetivos basados en la taxonomía original de Bloom (1956) por su robustez y su uso en el sistema educativo costarricense.

1.6.1 Objetivo general

Proponer una solución para la modernización de accesos e identidades, bajo principios de cero confianza

1.6.2 Objetivos específicos

- Conocer los fabricantes y sus productos.
- Describir los métodos modernos de accesos e identidades, así como principios de cero confianza.
- Analizar las mejores prácticas del mercado.
- Comparar las tecnologías ofrecidas en el mercado.
- Entregar una guía de implementación en principios de cero confianza.

1.7 Alcances y limitaciones

1.7.1 Alcances

En el documento se puede obtener un escrito que representa una metodología de cero confianza. Así como la elaboración de una presentación resumen para la audiencia, y una exposición de resultados de la propuesta.

1.7.2 Limitaciones

Dentro de las limitaciones que marcan el ámbito del proyecto investigativo se encuentran las siguientes:

- Falta de recursos o costos no planeados.
- Confidencialidad de la información como uno de los principios clave en la presente investigación.
- No se encuentra contemplado dentro de la explicación comentar de herramientas privadas que involucre precios, ejemplos o demostraciones, así como automatización o flujos de trabajo.
- Se limita el alcance de esta propuesta como una metodología que explique como una empresa puede desarrollar un proyecto de actualización de accesos e identidades en principios de cero confianza

1.8 Marco de referencia organizacional y socioeconómico

El año 2020, el COVID-19 obligó a 2500 millones de personas en el mundo a migrar al teletrabajo, y otros cientos de millones más al teleaprendizaje. Esta circunstancia externa e imprevisible brindó suficiente experiencia como para valorar hoy los elementos favorables y desfavorables de esta forma de empleo.

Con la pandemia muchas personas, no alfabetizadas, han perdido sus empleos, otros han tenido que adaptarse a la situación y buscar propuestas digitales, como la venta de comidas exprés, o mover sus locales comerciales a tiendas en línea.

Por otra parte, para la industria turística mundial el impacto ha sido devastador. Esto se debe a las medidas sanitarias que hicieron cerrar las fronteras, los restaurantes y los bares, ocasionando que estos últimos cerraran definitivamente o que se limitaran a bajar a la mitad su aforo según lo estipulado, asimismo, las excursiones perdieron atractivo o fueron prohibidas. Algunos países, como Costa Rica, vieron a una industria pujante adaptarse y crear promociones para el turismo nacional. A pesar del apremio económico, esta oportunidad le permitió a la ciudadanía disfrutar mucho de los parajes turísticos de nuestro país, aún en pandemia.

En la temporada alta del 2021 el turismo extranjero en el país ha caído hasta un 80% en comparación al año pasado, en ciertos destinos. Sin embargo, las agencias de alquiler de carros sirven de parámetro para saber si están teniendo una gran temporada. Lo anterior se debe a que muchos turistas se quedan por períodos más prolongados, y alquilan carro por toda su estancia para así viajar en su burbuja familiar y, por supuesto, invierten más dinero de lo que gastaba el visitante promedio que venía antes de la pandemia. Muchos de esos turistas aprovechan la estadía máxima

que les permite la visa a Costa Rica, según sus pasaportes de origen, para trabajar remotamente desde un destino tropical paradisíaco, escapando del frío invierno o de los altos picos de contagio del virus.

Los nómadas digitales son viajantes que no son 100% turistas, sino que dedican unas horas hábiles de la semana a trabajar virtualmente para sus organizaciones y el resto del tiempo disfrutan del ambiente y la vida local. Podría tratarse de las primeras señales del posturismo, donde menos visitantes realicen estancias más largas, demanden otros servicios, busquen experiencias diversas, descubran nuevas oportunidades, creen nuevo valor, produzcan mutuo beneficio del intercambio cultural, realicen encadenamientos productivos, emprendan, innoven, contraten profesionales, generen empleo, inviertan, transformen y se arraiguen.

1.8.1 Historia

En Costa Rica como en muchas otras latitudes del mundo, las pequeñas y medianas empresas constituyen un importante sector para la actividad económica del país, no solo desde el punto de vista del empleo que generan, sino también en la contribución a la producción total de la nación.

Según autores costarricenses, por ejemplo Trejos (1999), Costa Rica, como el resto de países de Latinoamérica, ha experimentado un crecimiento notorio en el sector informal, y particularmente, de la microempresa en las últimas décadas. Indica que según cifras de la Organización Internacional del Trabajo (OIT), el sector informal representó, en 1997, más del 40% del empleo no agrícola en la mayoría de los países de la región latinoamericana, donde entre 1990 y 1995, de cada 100 nuevos empleos

generados en la región, 84 responden al sector informal, principalmente al de la microempresa.

En Costa Rica, según la ley N.º 8262, una PYME se define como una unidad productiva de carácter permanente que dispone de recursos físicos estables y de recursos.

La diferenciación entre lo que corresponde a una pequeña y una mediana empresa está declarada dentro de la Ley de Fortalecimiento de las PYMES mediante una serie de fórmulas, las cuales tienen como variables el número de personas dentro de la empresa (PE), el valor de ventas anuales netas de la empresa en el último período fiscal (VAN), el valor neto de activos fijos netos de la empresa en el último período fiscal (AFE), y el valor neto de los activos totales netos de la empresa durante el último período fiscal (ATE) (Ley de Fortalecimiento para las PYMES, 2006).

El resultado de las fórmulas, que se da mediante “P”, indica como debe ser clasificada la empresa. Una empresa con un P menor o igual a 10 la clasifica como una microempresa; entre 10 y menor o igual al 35, una pequeña empresa; y para empresas con un P entre 36 y 100 se les clasifica como una mediana empresa. Se realiza además una diferenciación entre las empresas que son del tipo comercial o servicios y las que son industriales.

Para que una empresa entre dentro de la clasificación de PYME debe además cumplir una de las siguientes condiciones: a) tener al menos seis meses de permanencia en el mercado, b) que la persona empresaria tenga al menos dos años de experiencia en la actividad, c) que su permanencia esté asegurada, ya sea por la existencia de una franquicia y el respaldo del franquiciador, la participación en una incubadora de empresas o la existencia de contratos firmes.

La Caja Costarricense de Seguro Social realiza otra clasificación para las pequeñas y medianas empresas, en la cual se utiliza solamente el número de empleados para determinar su tamaño. De esta manera se clasifica a una microempresa como aquella que posea de 1 a 5 empleados, si tiene entre 6 a 30 trabajadores se considera una pequeña empresa, de 31 a 100 una mediana empresa y de más de 100 trabajadores una empresa grande.

La transformación digital está llamada a ser una fuerza que potencie el ejercicio de los derechos y las responsabilidades ciudadanas. Por ello, esta estrategia ocupa un lugar prioritario en la agenda de desarrollo y en el trabajo cotidiano de instituciones públicas. De forma más importante eberá ser una vivencia concreta en la innovación de las dinámicas sociales, sobre las cuales las comunidades, las empresas, las familias, y los individuos construyan, entre sí, la ruta del desarrollo y los proyectos de vida por los cuales tienen predilección.

Educación de Costa Rica en ciberseguridad

El país es reconocido por la importante inversión que se realiza en el sector educación, por mandato constitucional el país dedica el 8% del Producto Interno Bruto (PIB) a la educación.

Es un área de gran relevancia para el país, por lo tanto, la incorporación de las Tecnologías de la información y comunicación (TIC) en la educación, también se ha considerado una prioridad nacional, y se tienen diversos proyectos desde finales de los años 80.

Actualmente, el MEP, el MICITT y la SUTEL, en conjunto con otras organizaciones públicas, no gubernamentales, privadas, académicas y de la sociedad civil han implementado proyectos para cerrar las brechas en la educación a través del uso de las TIC, utilizando los recursos del Fondo Nacional de Telecomunicaciones (FONATEL). El objetivo de estas iniciativas ha sido transformar los procesos de enseñanza y aprendizaje a través del acceso universal a la conectividad de banda ancha, las tecnologías móviles y las herramientas de apoyo educativo de las TIC para profesores y estudiantes.

De acuerdo con el MICITT y la Presidencia de la República (2018) en el documento llamado estrategia de transformación digital hacia la Costa Rica del bicentenario 4.0, actualmente el 63% de las instituciones educativas de nivel secundario tiene un laboratorio de computación, en comparación con el 23% de las escuelas primarias, por lo que se están haciendo gestiones para mejorar estas cifras.

En lo que refiere a la formación de profesionales, tanto en universidades públicas como en privadas se ofrecen carreras con niveles de grado, posgrado y

especializaciones en temas vinculados con TIC; sin embargo, no necesariamente incluyen especializaciones en seguridad cibernética, a excepción de un centro educativo privado que ofrece formación a nivel de maestría.

El internet en Costa Rica

Al inicio de la década de los noventa, mientras los ticos celebraban las glorias de la primera selección de fútbol en un mundial y Mijail Gorbachov ganaba el premio nobel de la paz, en Costa Rica se informaban gracias a los cables noticiosos de las agencias internacionales de noticias, los teléfonos, telegramas y cartas.

La revolución digital hizo posible que hoy, 6 de cada 10 viviendas en el país tengan internet y que Costa Rica ocupe el tercer lugar en América Latina en el uso de las tecnologías, según el Global Information Technology Report (2015) del Foro Económico Mundial, se lideró desde la Universidad de Costa Rica (UCR) con un grupo de osados científicos que añoraban conectarse a las grandes redes de investigación que funcionaban en Estados Unidos y Europa.

Como antecedente a la llegada del internet, la UCR se alió a una red académica llamada Bitnet. Esta era una antigua red internacional de computadoras de centros de investigación que ofrecía servicios interactivos de correo electrónico y de transferencia de datos. Empleaba grandes computadoras de IBM. El Dr. Téramond había utilizado Bitnet durante sus estudios en la Universidad de Stanford y fue quien acercó esta tecnología al país apoyado por un grupo de otros ocho académicos e investigadores.

Bitnet no era la internet al que se estaba acostumbrado a utilizar, esta red ayudó a mostrar en el país los beneficios que tenían las redes de computadoras. A la iniciativa

se unieron luego científicos del Instituto Tecnológico y de la Universidad Nacional, entre otras 50 organizaciones de los países centroamericanos.

En enero de 1993 desde la Escuela de Informática de la UCR, Costa Rica se conectó por primera vez a internet. Se contaba para ello con 12 nodos y era accesible por unos 1.500 usuarios.

Con el fin de apoyar esta iniciativa se creó un grupo llamado CRNet, cuya infraestructura medular se ubicó en el Instituto Costarricense de Electricidad, en San José. La incorporación de Costa Rica a esta red fue muy temprana, pues sucedió solo dos años antes de que la WWW se posiciona realmente como una herramienta de comunicación en el mundo.

De forma paralela y hasta 1999, Radiográfica Costarricense (Racsa) apostó por otra red de computadoras llamada X.25. Esta red permitía el envío de paquetes de información y consulta de base de datos, pero no funcionaba como el internet porque era mucho más específico el tipo de consulta.

La segunda etapa del internet en el país se inició con la popularización de la herramienta y la salida de los centros académicos hacia las casas y oficinas. En 1993 La Nación se convirtió en la primera entidad privada que tuvo acceso al internet en el país, en abril de 1995, fue el primer periódico centroamericano en crear su versión en línea.

La década de los 90 fue particularmente interesante en la historia de la internet, al pasar de ser un instrumento de comunicación esencialmente entre científicos al público general, los investigadores ubican por ahí de 1997 la aparición de los primeros cafés internet del país.

La última fase del proceso se concretó en el 2005 con la inauguración de la red avanzada del ICE (RIA/Acelera) para llevar conectividad de banda ancha a lo largo y ancho del país, la cual fue promovida por el MICITT durante el periodo 2000 y 2002. Esto significó que a los usuarios se les ofrecía la experiencia de navegar por internet con mejores resultados. La oferta permitía mejorar la velocidad con la que viajaba la información.

Hoy en día las estadísticas hablan por sí solas, pues se estima que cerca del 63,9% de los hogares posee una computadora y de estos un 65,4% tiene, además, internet. El acceso desde dispositivos móviles es mayor, pues según mediciones recientes, el 86,8% de los hogares cuenta con al menos un teléfono celular.

Teletrabajo, ley de la República de Costa Rica

Ley para Regular el Teletrabajo en Costa Rica (N.º 9738), aprobada por la Asamblea Legislativa el 27 de agosto con el voto unánime de los 53 diputados presentes en el plenario.

Esta ley tiene como objetivo promover, regular e implementar el teletrabajo como un instrumento para la generación de empleo y modernización de las organizaciones públicas y privadas, a través de la utilización de tecnologías de la información y comunicación.

Según el Centro Internacional para el Desarrollo del Teletrabajo en Costa Rica cerca de 12 mil personas realizan teletrabajo, tanto en el sector público como en el privado.

El Ministro del MICITT destacó que la aprobación de esta Ley es fundamental en la estrategia de transformación digital del país, donde el trabajo ya no es visto bajo modelos tradicionales, sino bajo un paradigma donde la conectividad se convierte en

piedra angular del desarrollo económico, brindándole a la población nuevas y mejores oportunidades para innovar y aportar al crecimiento sin necesidad de trasladarse a un punto específico.

La regulación del teletrabajo traerá beneficios a los diferentes actores del mundo del trabajo, así como a las empresas o instituciones. Entre otros:

- Contribuye con la eficiencia y la modernización de la gestión, permite una mayor optimización debido al uso de las tecnologías disponibles, la reducción de costos en planta física y el aumento de la productividad.
- Promueve el empleo en los territorios, así como la atracción y retención de talento.
- Genera ahorros aproximados de ¢270 mil anuales por trabajador, en conceptos como electricidad, agua, mobiliario, espacio físico, mantenimiento y otros conceptos relacionados.
- Para las personas teletrabajadoras permite el ahorro de costos y tiempo por desplazamientos, la mejora en la conciliación de la vida personal y laboral, un aumento en las posibilidades de desarrollo personal y una mejora en la calidad de vida. Se estima en unos ¢320 mil anuales la reducción de gastos.
- Para la ciudadanía y el país, ayuda al descongestionamiento vial, dará una disminución de la huella del carbono al reducir desplazamientos.
- Contribuye con la responsabilidad ambiental y promueve la inserción laboral de poblaciones en vulnerabilidad, así como de los diferentes territorios.

La alfabetización digital en Costa Rica

La pandemia por COVID-19 ha provocado la mayor interrupción de la educación en la historia Costa Rica, al igual que muchos países en el mundo, se vio en la obligación de cerrar los centros educativos y migrar a procesos de educación a distancia y combinada, sin que el país, los centros educativos ni las familias tuvieran las capacidades pedagógicas ni los recursos tecnológicos necesarios para responder a los nuevos desafíos de la educación virtual. De esta forma, una importante cantidad de niños, adolescentes y jóvenes no pudieron continuar recibiendo clases de manera remota debido a la falta de conectividad o del equipo tecnológico necesario.

El Ministerio de Educación Pública (MEP) señala que, de una población escolar de alrededor de un millón, solo cerca del 60% ha tenido acceso a su plataforma educativa, el resto ha tenido que seguir su proceso por *WhatsApp*, recursos digitales, *offline* y materiales impresos. Asimismo, solo el 34% de la población estudiantil tiene equipo y conectividad plena, 29% tiene acceso limitado a ambos y el resto a ninguno. Esta situación también aumenta las posibilidades de repitencia e incluso de exclusión del sistema educativo, lo que pone en riesgo el desarrollo integral del estudiantado, limita sus oportunidades y les expone a sufrir diferentes formas de violencia.

Contar con una población con habilidades cognitivas y digitales adecuadas es un imperativo para competir y prosperar en la economía mundial de la cuarta revolución industrial.

Costa Rica ha dado pasos muy importantes para avanzar hacia la construcción de un país que garantice el derecho universal de toda su población al acceso y uso de las

Nuevas Tecnologías de la Información y las Comunicaciones (TICs) al impulsar políticas públicas como el Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT) 2015-2021, “Costa Rica: Una Sociedad Conectada”, el Fondo Nacional de Telecomunicaciones (FONATEL), el Programa de Hogares Conectados, los Centros Comunitarios Inteligentes (CECI) e iniciativas como la Red Educativa del Bicentenario y el Programa Nacional de Tecnologías Móviles (PNTM):Tecno@prender.

Actualmente en la Comisión de Asuntos Sociales de la Asamblea Legislativa se analiza el proyecto de ley N. º 22.206, para la creación del Programa Nacional de Alfabetización Digital (PNAD), dirigido a garantizar el acceso universal, el servicio universal, la solidaridad de telecomunicaciones, la reducción de la brecha digital, así como la alfabetización digital.

Este proyecto busca “reducir la brecha digital, garantizar mayor igualdad de oportunidades, así como el disfrute de los beneficios de la sociedad de la información y el conocimiento por medio del fomento de la conectividad, el desarrollo de infraestructura para redes fijas y/o móviles, y la disponibilidad de dispositivos de acceso y servicios de telecomunicaciones, así como la alfabetización digital para el uso productivo y significativo de la tecnología”.

Esta iniciativa de ley también permitirá al MEP y al Ministerio de Ciencia y Tecnología (MICITT) contar con los recursos económicos necesarios para impulsar programas e iniciativas que garanticen la conectividad de los hogares de las niñas, los niños y adolescentes, especialmente en las comunidades más vulnerables, reconociendo las necesidades sociales especiales de personas menores de edad, personas adultas

mayores, personas con discapacidad y población indígena, así como las necesidades de escuelas y colegios públicos y centros de prestación de servicios públicos.

1.8.2 Tipo de negocio y mercado meta

Hoy en día las empresas, en su mayoría, apuestan hacia la transformación digital, desde mercados meta como farmacéuticas, sector de *retail*, sector turismo, sectores de servicio, entre otros. Todos apuestan a la innovación tecnológica lo que provoca que deban invertir en sistemas. El tipo de negocio está enfocado a cualquier empresa comercial o gubernamental, ya sea pequeña o grande y que no disponga de muchos recursos como *hardware* para distribuir una computadora a cada uno de sus colaboradores. Así como la incapacidad de mantener o pagar una consultoría de arquitectura de cero confianza o bien, cualquier empresa que desee agregar seguridad en sus sistemas, y desean moverse a los nuevos e innovadores modelos de seguridad.

1.9 Estado de la cuestión

Se hace una recopilación de documentos técnicos para identificarlos, analizarlos y mostrar parte de los resultados. Se sugirió utilizar la plantilla que presentan Biolchini, Gomes, Cruz y Horta (2005) titulado: “Una revisión sistemática a la adaptación del proceso de *Software”*. Este artículo presenta una estructura genérica de revisión sistemática, que se ilustra con detalle en el artículo de ejemplo de Blanco *et al*. (2008).

1.9.1 Planificación de la revisión

Se realiza una pregunta que sea clara y definida. Se efectúan búsquedas de documentación existente y se analiza el conocimiento académico que existe en los investigadores de este documento.

1.9.1.1 Formulación de la pregunta

Se basa en los objetivos anteriormente delimitados. La formulación de la pregunta sirve para encontrar respuestas con base en la investigación. La pregunta está compuesta por: foco de la pregunta, amplitud y calidad de la pregunta.

1.9.1.1.1 Foco de la pregunta

Es necesario la búsqueda de información, documentos técnicos y encuestas que permita tener los indicios y las respuestas de la investigación presentada en este documento.

1.9.1.1.2 Amplitud y calidad de la pregunta

El objetivo de este apartado es obtener el contexto de la pregunta de investigación, la cual se desea responder de forma clara y concisa, con base en la elaboración de un un listado de términos clave relevantes para la búsqueda de información.

1. Problema

Existen muchas empresas que desean implementar seguridad en sus redes y aplicaciones. Sin embargo, no poseen el capital para contratar a un tercero que los dirija o para adquirir equipos costosos. Muchas empresas optaron por limitarse a cerrar debido a que estaban acostumbradas a solo poder atender clientes de manera

presencial, el COVID-19 ha mostrado que una pandemia puede ocurrir en cualquier momento y el distanciamiento social debe ser necesario.

Esta investigación se centrará en brindarle una guía a todas aquellas empresas que lo consideren necesario, y de esta manera implementar una guía a bajo costo y gratuita que les permita asegurar sus redes y aplicaciones bajo principios de cero confianza.

2. Pregunta

Con la anterior definición del problema se formula la siguiente pregunta de investigación:

¿Qué deben hacer las empresas en general para implementar seguridad de cero confianza?

3. Palabras clave y sinónimos

La siguiente lista de palabras clave serán utilizadas para la búsqueda e identificación de documentos relacionados con el proyecto. Dado que la mayoría de las palabras se conocen con términos en el idioma inglés, se presenta su equivalente.

A continuación, un listado de estas palabras: tabla: *Listado de palabras*.

Tabla 1: Listado de palabras

Palabra	Equivalente en inglés	Acrónimo
Diseño	Design	
Tecnologías de información	Information Technology	IT

Cero confianza	**Zero trust**	
Dispositivo móvil	**Mobile device**	
Escritorio virtual	**Virtual desktop**	**VDI**
Red privada virtual	**Virtual Private Network**	**VPN**
VPN por aplicación	**Peer App VPN**	
Tecnología de información y comunicación	**Technology information and communication**	**TIC**
Proveedor de servicios	**Service Provider**	**SP**
Perímetro definido por *software*	**Software Defined Perimeter**	**SDP**
Administración centralizada de dispositivos	**Unified Endpoint Management**	**UEM**
Perímetro de servicio de acceso seguro	**Secure Access Gateway**	**SASE**
Traiga su propio dispositivo	**Bring Your Own Device**	**BYOD**
Teletrabajo	**Telecommuting**	
Ciber ataque	**Cyber threat**	
Aplicaciones remotas	**Remote applications**	

Administración de dispositivos móviles	**Mobile device management**	**MDM**
Internet de las cosas	**Internet of things**	**IoT**
Inicio de sesión único	**Single Sign On**	**SSO**
Cortafuegos	**Firewall**	
Red amplia definida por *software*	**Software Defined Wide Area Network**	**SD-WAN**
Política de grupo basada en objetos	**Group Base Policy Object**	**GPO**
Lenguaje de marcado para confirmaciones de seguridad	**Security Assertion Markup Language**	**SAML**
Autenticación abierta	**Open Authentication**	**OAuth**
Arquitectura de redes de cero confianza	**Zero trust network Architecture**	**ZTNA**
Arquitectura empresarial	**Enterprise Architecture**	**EA**
Identidad como servicio	**Identity as a service**	**IDaaS**
Autenticación de segundo factor	**Second factor authentication**	**SFA**

Fuente: elaboración propia

4. Intervención

Analizar ejemplos de mejores prácticas en tecnologías de cero confianza. Extraer los artículos y los documentos de mayor relevancia para la investigación y analizar los resultados obtenidos.

5. Control

Al iniciar con esta investigación no se posee base de datos histórica o información anterior que adicionar. Se inicia desde cero con las palabras claves mencionadas en la tabla anterior.

6. Efectos

Se espera obtener documentación con base en las búsquedas realizadas para entender cuáles son de las mejores herramientas y guías que ayuden a pequeñas empresas en mantener su operación aunque no todos los colaboradores estén en sus oficinas.

7. Medida de salida

Se realiza una revisión de la calidad de la documentación encontrada en sitios web especializados para tal fin.

8. Población

La población de esta investigación es cualquier empresa de capital público o privado que esté en la necesidad de asegurar sus redes y aplicaciones.

9. Aplicación

Este tipo de investigación puede resultar de utilidad para empresas pequeñas y medianas que quieran proporcionar herramientas de trabajo remoto en un ambiente de seguridad y, por supuesto, continuando con la operación regular.

10.Diseño experimental

Se realiza una selección, clasificación y depuración de los resultados obtenidos de las búsquedas. Con el fin de asegurarse que la calidad de la información y las fuentes sean de buena procedencia. Es fundamental garantizar que la información sea de confianza, así como evitar errores de uso de datos incorrectos

1.9.1.2 Selección de fuentes

Como objetivo de este apartado se especifican las fuentes identificadas para la búsqueda de estudios primarios.

1.9.1.2.1 Definición del criterio de selección de fuentes

La selección de fuentes se ha realizado con ciertos aspectos como: popularidad de los sitios, de los investigadores, respaldo técnico y teórico. También se consideran las fuentes que tengan fecha reciente y con temas actuales.

1.9.1.2.2 Lenguaje de estudio

Se utiliza para el estudio tanto el idioma español como el inglés en lo que respecta a las búsquedas; de esta manera se puede incrementar el rango de posibles resultados.

1.9.1.2.3 Identificación de fuentes

Se describe en este apartado la selección de fuentes para la documentación primaria, se hace una descripción de cómo se ejecutan las búsquedas y se provee de una lista de fuentes.

1. Método de selección de fuentes:

Se describe cómo ejecutar la búsqueda, con base en el respaldo de las fuentes. Como por ejemplo con los motores de búsquedas web.

2. Cadena de búsqueda:

Las cadenas de búsqueda utilizadas tienen combinación de "*OR*" y "*AND*". ("*architecture*" *OR* "*design*") *AND* ("*Zero trust*") *AND* ("*Virtual desktop*" *OR* "*Remote applications*" *OR* "*Remote desktop*" *OR* "*Device management*").

3. Lista de fuentes:

Debido a la calidad de los artículos académicos y de artículos recientes, de acuerdo con el tema investigado, se considera la utilización de las siguientes fuentes:

1. ACM *Digital Library*.
2. IEEE *Digital Library*.
3. *Google Scholar.*
4. *National Institute of Standards and Technology.*
5. IBM.
6. VMware.
7. Cisco.

8. Palo Alto.

9. *Forrester*.

1.9.1.2.4 Selección de fuentes después de la evaluación

De acuerdo con la lista de fuentes iniciales, las cadenas de búsqueda y los documentos obtenidos, estos ayudan a filtrar la información, permitiendo obtener los mejores resultados con base en las necesidades y los requerimientos.

1.9.1.2.5 Comprobación de las fuentes

Al momento de iniciar este documento, no se tenía experiencia o criterio certero en la selección de fuentes. A pesar de esto, se prefirieron las fuentes más utilizadas para obtener la documentación relacionada con tecnología, entre otras ramas.

1.9.1.3 Selección de los estudios

Una vez que se definieron las fuentes, se selecciona cuáles trabajos resultantes de las búsquedas serán incluidos en el análisis.

1.9.1.3.1 Definición del criterio de inclusión y exclusión de estudios

Los criterios presentados a continuación serán los que definirán si una fuente es correcta o no para el desarrollo de este proyecto de investigación.

Criterio #1

Pregunta de investigación:

¿Qué propuestas o investigaciones se han llevado a cabo en el área para favorecer espacios digitales a pequeñas empresas?

Término principal de incluisión:

Cero confianza, segundo factor de autenticación, identidad como servicio, diseño, teletrabajo, espacios digitales, escritorios virtuales, VDI, aplicaciones virtuales.

Criterios de exclusión

- Documentos de presupuestos.
- Documentos de ventas.
- Documentos obsoletos.

1.9.1.3.2 Definición de tipos de estudio

Para definir el / los tipos de estudios relacionados a la investigación se realizan las siguientes preguntas:

Pregunta de investigación	**¿Quién?**	**¿Qué?**	**¿Cómo?**	**¿Dónde?**
¿Qué propuestas o investigaciones se han llevado a cabo para asegurar las	**Páginas web, redes sociales.**	**Cero confianza.**	**Proponiendo una arquitectura, una guía para las empresas.**	**Buscadores de páginas web, sitios públicos empresariales.**

redes empresariales con principios de cero confianza?				

1.9.1.3.3 Procedimiento para la selección de los estudios

En cada una de las fuentes se realizó el siguiente proceso para definir la confiabilidad, es parte del ámbito de la investigación, y si es información necesaria para el estudio.

1- Selección de cadena de búsqueda.

2- Selección de filtros.

3- Análisis de resultados.

4- Redefinición de la búsqueda con operadores avanzados.

5- Evaluación de los resultados arrojados.

6- Selección de los resultados.

Ilustración 1: Procedimiento de selección de estudios

1.9.2 Ejecución de la revisión

A continuación, se demuestra el proceso llevado a cabo para las diferentes fuentes:

1.9.2.1 Ejecución de la selección en la fuente de ACM

Siguiendo las recomendaciones provistas por Blanco et al. (2007), se realiza la búsqueda de estudios iniciales de la siguiente manera:

Búsqueda basada en los siguientes parámetros:

- *Zero trust.*

- *Microsegmentation.*

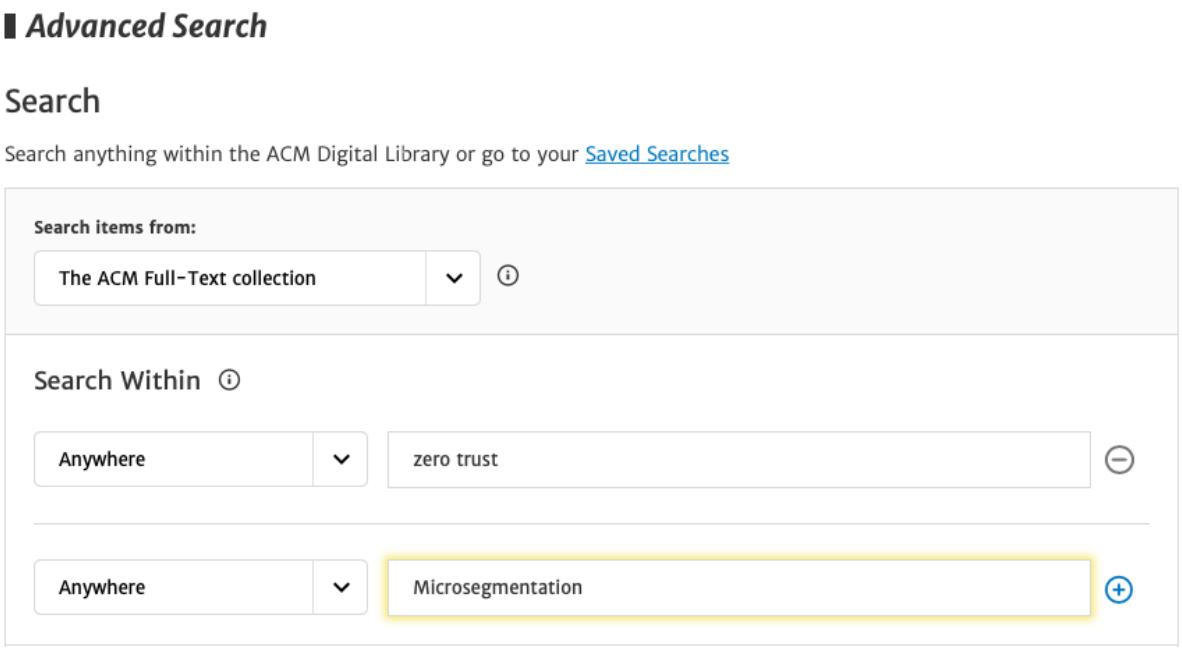


Ilustración 2: Ejemplo de búsquedas

Luego de realizar la búsqueda se encontraron 19000 distintos resultados, de los cuales se seleccionaron los siguientes artículos como referencia :

#	Título	Autores	Año	URL
1	***Protection of Sensitive Data in Zero Trust Model.***	**Iftekhar Ahmed, Tahmin Nahar**	**2020**	**https://dl.acm.org/doi/10.1145/3377049.3377114**
2	***Dynamic Access Control and Authorization System based on Zero-trust architecture.***	**Jiaxuan Fei, Qui Wang**	**2020**	**https://dl.acm.org/doi/10.1145/3437802.3437824**
3	***eZTrust: Network-Independent Zero-Trust Perimeterization for***	**Zirak Zaheer, Hyunseok Chang**	**2019**	**https://dl.acm.org/doi/10.1145/3314148.3314349**

	Microservices.			
4	***Can I Reach You? Do I Need To? New Semantics in Security Policy Specification and Testing.***	**Charakampos Katsis, Fabricio Cicala**	**2021**	**https://dl.acm.org/doi/10.1145/3450569.3463558**

1.9.2.2 Ejecución de la selección en la fuente de *Scholar Google*

Al igual que en el apartado 1.9.2.1, se seleccionaron los artículos con base en las siguientes palabras:

- *Zero trust architecture.*

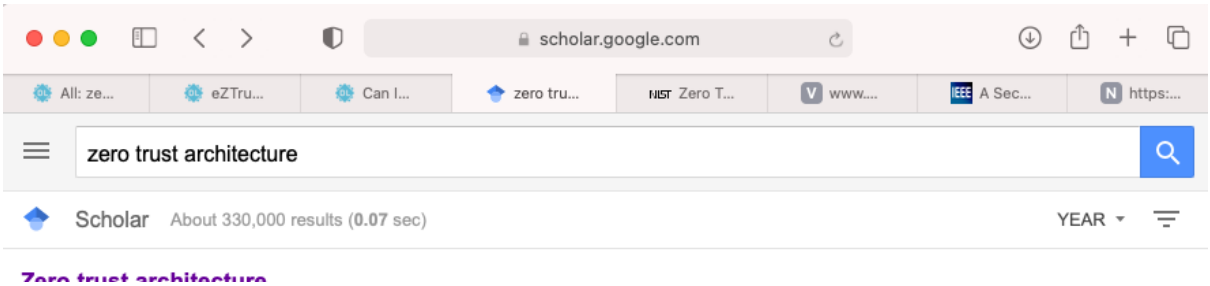


Ilustración 3: Ejemplo de búsquedas

Como se observa en la imagen anterior, se arrojaron 330,000 resultados de los cuales se seleccionaron los siguientes:

#	Título	Autores	Año	URL
1	***Build Security Into Your Network's DNA: The Zero Trust Network Architecture.***	**John Kindervag.**	**2010**	**http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf**

2	***Implementing a zero trust architecture.***	**Alper Kerman Oliver Borchert Scott Rose.**	**2020**	**https://www.nccoe.org/sites/default/files/library/project-descriptions/zt-arch-project-description-draft.pdf**
3	***Migrating to Zero Trust Architecture.***	**Songpon Teerakanok.**	**2021**	**https://www.hindawi.com/journals/scn/2021/9947347/**
4	***LCDA: Ligtweight Continuous Device to Device Authentication for a Zero Trust Architecture.***	**Syed W Shah, Arash Shaghaghi, Adnan Anwar, Robin Doss.**	**2021**	**https://www.sciencedirect.com/science/article/pii/S0167404821001759**

Capítulo 2. Marco conceptual

Con base en los resultados de las búsquedas definidas en los estados de la cuestión, se logró obtener una gran cantidad de conceptos y con el objetivo de analizar los más mencionados o relevantes, se genera la siguiente nube de palabras:

Ilustración 4: Nube de palabras, generado del sitio https://www.nubedepalabras.es

2.1 Concepto de cero confianza

2.1.1 Cero confianza según Forrester

El modelo *Zero Trust,* cuyo nombre acuñó Forrester Research, se basa en el hecho de que las amenazas son ubicuas, es decir, existen dentro y fuera de la empresa. Es fundamental incluir prevención, detección y respuesta mediante un enfoque de varias capas.

La seguridad *Zero Trust* es un modelo de arquitectura de seguridad de red basado en el principio: *"nunca confiar, siempre comprobar"*. Aunque no se trata de una teoría completamente nueva, la mayoría de los modelos de seguridad empresarial tienden más bien al concepto *"comprobar y entonces confiar"*. Con estos enfoques tradicionales, cualquiera que disponga de unas credenciales de usuario correctas podría acceder a todos los sitios web, aplicaciones o dispositivos que desee. Estos enfoques no funcionan en el panorama empresarial actual y, por eso, muchas organizaciones han sufrido ataques de *malware* y *ransomware*, así como filtraciones de datos que han afectado a sus marcas y sus ingresos.

En el año 2010 John Kindervag, que en aquel momento era analista principal de Forrester Research Inc., creó el modelo *Zero Trust Network*, o *Zero Trust Architecture*. *"En tres años, creo que Zero Trust será citado como uno de los grandes marcos en ciberseguridad"*, confiesa Chase Cunningham, analista principal de Forrester.

2.1.2 Cero confianza según National Institute of Standads and Technology (NIST)

Según NIST, cero confianza es un paradigma de ciberseguridad centrado en la protección de recursos y la premisa de que la confianza nunca se otorga implícitamente, sino que debe evaluarse continuamente. La arquitectura de confianza cero es un enfoque final para la seguridad de los recursos y los datos de la empresa que abarca la identidad (persona y no entidades personales), credenciales, gestión de acceso, operaciones, puntos finales, entornos de alojamiento, y la infraestructura de interconexión.

El enfoque inicial debe restringir los recursos para aquellos que necesitan acceder y otorgar solo los privilegios mínimos (por ejemplo, leer, escribir, eliminar) necesarios para realizar la misión. Tradicionalmente, las agencias (y las redes empresariales en general) se han centrado en la defensa del perímetro, los sujetos autenticados tienen acceso autorizado a una amplia recopilación de recursos en la red interna. Como resultado, el movimiento lateral no autorizado dentro del medio ambiente ha sido uno de los mayores desafíos para las agencias federales.

Un movimiento lateral en ciberseguridad se refiere a intentar atacar los sistemas ubicados en una misma o dominio de colición "*broacast domain*"

2.1.3 Cero confianza según CISCO

De acuerdo con el fabricante Cisco en el documento llamado "Cisco Zero Trust Architercure" presentado en el foro de Cisco Connect Vancouver (2019) cero confianza trata de un enfoque estratégico de la seguridad que se centra en el concepto de eliminar la confianza de la arquitectura de red de una organización. La confianza no es ni binaria, ni permanente. Ya no se puede asumir que las entidades internas son confiables, que se pueden administrar directamente para reducir el riesgo de seguridad o que verificarlas una vez es suficiente. El modelo de seguridad de confianza cero le pide que cuestione sus suposiciones de confianza en cada intento de acceso.

Los enfoques de seguridad tradicionales asumen que se puede confiar en cualquier elemento dentro de la red corporativa. La realidad es que esta suposición ya no es cierta gracias a la movilidad BYOD (traiga su propio dispositivo), IoT, adopción de la nube, mayor colaboración y un enfoque en la resiliencia empresarial. Un modelo de

confianza cero considera que todos los recursos son externos y verifica continuamente la confianza antes de otorgar sólo el acceso requerido.

2.1.4 Cero confianza según *Cloud Security Alliance (CSA)*

Es un concepto de seguridad de red centrado en la creencia de que las organizaciones no deben confiar automáticamente en nada, dentro o fuera de los perímetros tradicionales, y tiene como objetivo defender los activos empresariales. La implementación de *Zero Trust* requiere la verificación de cualquier sujeto o entidad que intente conectarse a los activos antes de otorgar acceso, así como la evaluación continua de las sesiones durante toda la duración de la conexión.

2.1.5 Los cinco pilares de cero confianza

La arquitectura *Zero Trust* consta de cinco pilares: confianza del dispositivo, confianza del usuario, confianza en el transporte o la sesión, confianza en las aplicaciones y en los datos. Se debe establecer confianza en cada pilar para tomar decisiones de otorgar o denegar el acceso. Al establecer la confianza en los cinco pilares puede ganar visibilidad y recopilar análisis en todos los ámbitos, ya que estos son una parte fundamental de la arquitectura *Zero Trust* y ayudan a establecer una huella más profunda y amplia en cada pilar.

Los cinco pilares son:

- Confianza del dispositivo: para que un dispositivo sea parte de la cero confianza, debe estar configurado con los siguientes elementos:

- Administración del dispositivo.
- Inventario del dispositivo.
- Autenticación del dispositivo.
- Cumplimiento del dispositivo.

- Confianza del usuario: como parte de cero confianza, se debe utilizar métodos de autenticación de usuario más seguros. Este pilar requiere un motor de acceso condicional sólido que pueda ayudar a tomar decisiones utilizando datos dinámicos y contextuales.
  - Autenticación sin contraseñas.
  - Autenticación con multi-factor.
  - Acceso condicional.
  - Puntuación de riesgo dinámico.
- Confianza de la sesión o transporte: al utilizar el principio de cero confianza de acceso, con privilegios mínimos a los recursos, se pueden limitar los derechos de acceso a los usuarios y otorgar los permisos mínimos necesarios para realizar su trabajo.
  - Microsegmentación.
  - Cifrado del transporte.
  - Protección de la sesión.
- Confianza de la aplicación: con la modernización de la autenticación de usuarios, que permite el inicio de sesión único en las aplicaciones, se obtiene seguridad y una experiencia de usuario mejorada. Para las aplicaciones tradicionales que no están diseñadas para cero confianza, se puede agregar protección en forma de aislamiento.
  - Punto de inicio de sesión único.

- Aislamiento.
- Acceso de cualquier dispositivo.

- Confianza de la información: como pilar final del modelo cero confianza debe asegurarse que los datos permanezcan seguros.
  - Prevención de la pérdida de datos.
  - Integridad.
  - Clasificación.
  - Protección de datos en reposo.

2.2 Conceptos sobre espacios digitales

De acuerdo con las fuentes consultadas y con el detalle de los resultados el siguiente diagrama muestra cómo se conceptualizan los términos más importantes arrojados en las fuentes seleccionadas.

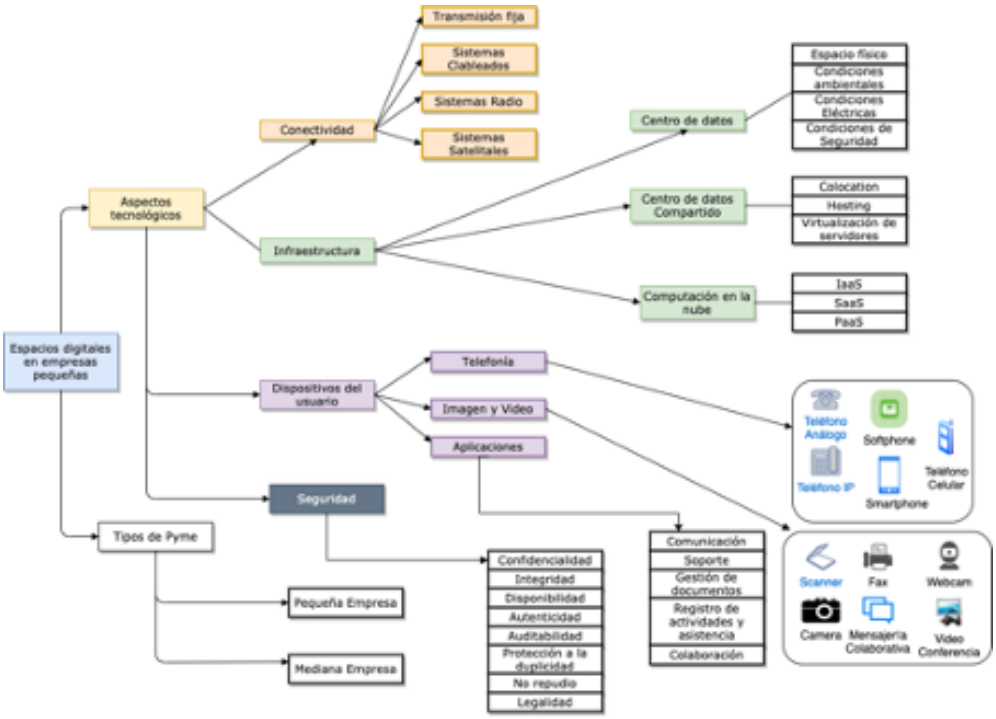


Ilustración 5: Diagrama de tipos de empresas Pyme y aspectos tecnológicos en espacios digitales

2.2.1 Dispositivos móviles

Un dispositivo móvil es un artefacto informático de bolsillo con una pantalla de visualización que funciona mediante entrada táctil o un teclado en miniatura. Los teléfonos inteligentes y las PDA (Asistente Personal Digital, por sus siglas en inglés)

son las opciones más populares en situaciones en las que se requiere una computadora, pero no se pueden usar debido a la inconveniencia del tamaño y su falta de portabilidad. Un elemento que se ha vuelto muy popular en los últimos tiempos es el *Netbook*, el cual se puede clasificar entre un dispositivo móvil y un portátil, y ha sido elegido por el gobierno español para ser utilizado por los estudiantes en las escuelas.

2.2.2 El internet de las cosas (IoT)

Para IBM, en pocas palabras, el internet de las cosas (Internet of things por sus siglas en inglés, IoT) es el concepto de conectar cualquier dispositivo (siempre que tenga un interruptor de encendido / apagado) a internet y a otros dispositivos conectados. Por lo tanto, IoT es una red gigante de cosas y personas conectadas, las cuales recopilan y comparten datos sobre la forma en que se utilizan y sobre el entorno que las rodea. Eso incluye una cantidad extraordinaria de objetos de todas las formas y tamaños, desde microondas inteligentes, que cocinan automáticamente su comida durante el tiempo correcto, hasta automóviles autónomos, cuyos complejos sensores detectan objetos en su camino, hasta dispositivos de *fitness* portátiles que miden su frecuencia cardíaca y la cantidad de pasos que ha dado ese día, luego se usa esa información para sugerir planes de ejercicio personalizados para usted. Incluso hay balones de fútbol conectados que pueden rastrear qué tan lejos y rápido se lanzan y registrar esas estadísticas a través de una aplicación para futuros entrenamientos.

2.2.3 *Traer su porpio dispositivo (BYOD)*

Según el fabricante de IBM el término Bring your own device (BYOD por sus siglas en inglés) significa traer su propio dispositivo. Es una política de TI que permite, y en

ocasiones alienta, a los empleados a acceder a los datos y sistemas de la empresa utilizando dispositivos móviles personales como teléfonos inteligentes, tabletas y computadoras portátiles.

Hay cuatro opciones básicas o niveles de acceso a BYOD:

- Acceso ilimitado para dispositivos personales.
- Acceso sólo a sistemas y datos no sensibles.
- Acceso con control de TI sobre dispositivos personales, aplicaciones y datos almacenados.
- Acceso que evita el almacenamiento local de datos en dispositivos personales.

Para el fabricante Citrix BYOD es la tendencia en evolución de los empleados que utilizan sus dispositivos personales para fines laborales. El dispositivo al que se hace referencia aquí podría ser una computadora portátil, un teléfono inteligente, una tableta, un disco duro portátil o cualquier dispositivo de tecnología de la información para el consumidor.

Las empresas pueden utilizar BYOD o un subconjunto de la tendencia, como BYOC (traer su propia computadora por sus siglas en inglés) . Cualquiera que sea el nivel de tecnología de consumo que una empresa permita dentro de su mayor infraestructura de TI, se aplican los mismos beneficios y riesgos.

Cuando una organización aprovecha la política BYOD debe incorporar dispositivos de propiedad de los empleados en su estrategia más amplia de gestión unificada de puntos finales (Unified endpoint management UEM, por sus siglas en inglés). El objetivo de UEM es brindarle a TI un enfoque único para administrar cualquier punto final utilizando estilos de administración tradicionales y modernos. Las partes

interesadas de TI deben comprender qué tipo de dispositivos están conectados a su infraestructura de TI para que pueda proporcionar las medidas de seguridad adecuadas y reducir la probabilidad de riesgo financiero y legal.

2.2.4 Conceptos de administración unificada de dispositivos (UEM)

Según Gartner (2021) las herramientas de gestión unificada de puntos finales (UEM) combinan la gestión de varios tipos de puntos finales en una única consola. Las herramientas de UEM realizan las siguientes funciones:

- Configurar, administrar y monitorear iOS, Android, Windows 10 y macOS, y administrar algunos puntos finales portátiles y de internet de las cosas (IoT).
- Unificar la aplicación de configuraciones, perfiles de gestión, cumplimiento de dispositivos y protección de datos.
- Proporcionar una vista única de los usuarios de múltiples dispositivos, mejorando la eficacia de la asistencia al usuario final y recopilando análisis detallados del lugar de trabajo.
- Actuar como un punto de coordinación para orquestar las actividades de las tecnologías de punto final relacionadas, como los servicios de identidad y la infraestructura de seguridad. Los proveedores de este mercado deben incluir todas las capacidades de una herramienta de gestión de clientes tradicional, proporcionar funciones de CMT específicas u ofrecer integración con una CMT de terceros.

Para VMware, Unified Endpoint Management (2020) permite que TI administre, proteja e implemente recursos y aplicaciones corporativos en cualquier dispositivo desde una única consola.

La gestión unificada de terminales es un paso más allá de la gestión tradicional de dispositivos móviles. A medida que los usuarios trabajan cada vez más de forma remota desde dispositivos tradicionales y móviles, y las empresas incorporan IoT y otras nuevas tecnologías, la gestión unificada de puntos finales ha evolucionado para resolver los problemas que encuentran los departamentos de TI modernos al proteger y conectar estos entornos.

Los departamentos de TI también enfrentan las dificultades de integrar sistemas heredados en estos nuevos dispositivos, lo que genera mayores costos de TI. La administración unificada de terminales reduce la carga de conectar estos sistemas al tiempo que reduce los costos y mitiga los riesgos.

2.3 Conectividad

2.3.1 Perímetro definido por el *software* (SDP)

Perímetro en seguridad informática se define como aquel conjunto de controles que se establecen alrededor de una infraestructura tecnológica.

Para *Cloud Security Alliance* se define como: una arquitectura de seguridad integrada que, de otro modo, sería difícil de lograr con productos de puntos de seguridad existentes, como *Network Access Control* (NAC) o *anti-malware*. Está diseñado para aprovechar componentes probados basados en estándares, como el cifrado de datos; atestación remota, seguridad de la capa de transporte mutuo, lenguaje de marcado de aserción de seguridad (SAML) y certificados X.509. La incorporación de estas y otras tecnologías basadas en estándares garantiza que SDP pueda integrarse con los sistemas de seguridad existentes de una organización.

CloudFlare indica que un perímetro definido por *software* es una forma de ocultar la infraestructura conectada a internet (servidores, enrutadores, etc.) para que las partes externas y los atacantes no puedan verla, ya sea que esté alojada en las instalaciones o en la nube. El objetivo del enfoque SDP es basar el perímetro de la red en *software* en lugar de *hardware*. Una empresa que utiliza un SDP está esencialmente cubriendo sus servidores y otra infraestructura con un manto de invisibilidad para que nadie pueda verlo desde el exterior; sin embargo, los usuarios autorizados aún pueden acceder a la infraestructura.

Un perímetro definido por *software* forma un límite virtual alrededor de los activos de la empresa en la capa de red, no en la capa de aplicación. Esto lo separa de otros controles basados en el acceso que restringen los privilegios del usuario, pero permiten un amplio acceso a la red. Otra diferencia clave es que un SDP autentica los dispositivos y la identidad del usuario.

2.3.2 Conceptos sobre segmentación

La segmentación permite que la congestión de red se reduzca de forma significativa dentro de cada segmento. Al transmitir datos dentro de un segmento, los dispositivos dentro de ese segmento comparten el ancho de banda total. Los datos que pasan entre los segmentos se transmiten a través del *backbone* de la red por medio de un puente, *router* o *switch.*

2.3.3 Conceptos sobre microsegmentación

La microsegmentación es un método para crear zonas seguras en centros de datos y despliegues en la nube, que les permite a las empresas aislar las cargas de trabajo entre ellas y protegerlas individualmente. Está dirigido a hacer que la seguridad de la red sea más granular.

2.3.4 Redes Privadas Virtuales (VPN)

Es un servicio de seguridad de internet que crea una conexión encriptada entre los dispositivos del usuario y uno o más servidores. Las VPN pueden conectar de forma segura a un usuario a la red interna de una empresa o al internet público.

Las empresas suelen utilizar una VPN para dar acceso a los empleados remotos a aplicaciones y datos internos, o para crear una única red compartida entre varias oficinas. En ambos casos, el objetivo final es evitar que el tráfico web, en particular el tráfico que contiene datos patentados se exponga en la internet abierta.

¿Por qué son necesarias las VPN para lograr esto? Tomemos a los empleados remotos como ejemplo. Cuando los empleados trabajan en las instalaciones, pueden conectar su computadora y dispositivo móvil directamente a la red interna de la empresa. Sin embargo, si un empleado trabaja de forma remota, su conexión a esa red interna debe realizarse a través de la internet pública, lo que podría exponer su tráfico a ataques en la ruta y otros métodos de espionaje de datos confidenciales. Cifrar ese tráfico con una VPN empresarial u otro servicio de seguridad lo mantiene a salvo de miradas indiscretas.

2.3.4 *Firewall* o Cortafuegos

Un *firewall* es un producto de seguridad que filtra el tráfico malicioso. Tradicionalmente, los *firewalls* se ejecutan entre una red interna confiable y una red no confiable, por ejemplo, entre una red privada e internet. Los primeros *firewalls* eran dispositivos físicos que se conectaban a la infraestructura local de una organización.

Los cortafuegos bloquean y permiten el tráfico de red de acuerdo con un conjunto de reglas internas. La mayoría de los *firewalls* permiten a los administradores personalizar estas reglas.

2.3.6 Secure Access Service Edge (SASE)

Perímetro de servicio de acceso seguro (SASE, por sus siglas en inglés) combina capacidades de redes de área amplia definidas por *software* (SD-WAN, por sus siglas en inglés) con una serie de funciones de seguridad de red, todas las cuales se entregan desde una única plataforma en la nube. De esta manera, SASE permite a los empleados autenticarse y conectarse de manera segura a los recursos internos desde cualquier lugar, y brinda a las organizaciones un mejor control sobre el tráfico y los datos que ingresan y salen de su red interna.

SASE incluye cuatro componentes de seguridad básicos:

- Puertas de enlace seguro (SWG, por sus siglas en inglés): previenen las amenazas cibernéticas y las violaciones de datos al filtrar el contenido no deseado del tráfico web, bloquear el comportamiento de los usuarios no autorizados y hacer cumplir las políticas de seguridad de la empresa. Los SWG se pueden implementar en cualquier lugar, lo que los hace ideales para proteger las fuerzas de trabajo remotas.
- Agente de seguridad de acceso a la nube (CASB, por sus siglas en inglés): realiza varias funciones de seguridad para los servicios alojados en la nube, incluida la revelación de TI en la sombra (sistemas corporativos no autorizados), la protección de datos confidenciales a través del control de acceso y la prevención de pérdida de

datos (DLP, por sus siglas en inglés) y la garantía del cumplimiento de la privacidad de los datos, mediante regulaciones.

- Acceso a la red de confianza cero (ZTNA, por sus siglas en inglés): las plataformas ZTNA bloquean los recursos internos de la vista pública y ayudan a defenderse contra posibles violaciones de datos al requerir la verificación en tiempo real de cada usuario y dispositivo para cada aplicación protegida.
- Cortafuegos como servicio (FWaaS, por sus siglas en inglés): se refiere a cortafuegos entregados desde la nube como servicio. FWaaS protege las plataformas, la infraestructura y las aplicaciones basadas en la nube de los ataques cibernéticos. A diferencia de los *firewalls* tradicionales, FWaaS no es un dispositivo físico, sino un conjunto de capacidades de seguridad que incluye filtrado de URL, prevención de intrusiones y administración uniforme de políticas en todo el tráfico de la red.

2.3.6.1 Puerta de enlace segura (SWG, Segure Web Gateway))

Una puerta de enlace web segura (SWG, por sus siglas en inglés) es un producto de seguridad cibernética que protege los datos de la empresa y hace cumplir las políticas de seguridad. Los SWG operan entre los empleados de la empresa e internet. Al igual que un filtro de agua que elimina las impurezas peligrosas del agua para que sea segura para beber, los SWG filtran el contenido no seguro del tráfico web para detener las amenazas cibernéticas y las violaciones de datos. También bloquean el comportamiento de usuario riesgoso o no autorizado.

Todos los productos SWG contienen estas tecnologías:

- Filtrado de URL.

- Detección y bloqueo *antimalware*.
- Control de aplicaciones.
- Filtrado de contenido.
- Prevención de pérdida de datos.

2.3.6.2 Redes de cero confianza (ZTN)

La industria de la seguridad reconoce que los mecanismos de defensa existentes solo tienen un éxito parcial. La ejecución de Protocolo definido por software (Software Defined Perimeter SDP, por sus siglas en inglés) se puede aplicar antes que Protocolo de transmisión / Protocolo de internet (TCP / IP, por sus siglas en inglés) y Seguridad de la campa de transporte (TLS, por sus siglas en inglés), lo que reduce la probabilidad de que estos y otros protocolos vulnerables sean utilizados como vectores de ataque por los actores de amenazas. Las implementaciones de perímetro definido por *software* crean diseños de confianza cero que evitan métodos comunes de ataque como Denegación de servicio distribuido (Distributed denial of service DDoS, por sus siglas en inglés), robo de credenciales y las diez principales amenazas notorias publicadas por *Open Web Application Security Project* (OWASP).

El perímetro definido por *software* hace que los activos sean invisibles e impide el acceso hasta que la identidad asociada se autentica y autoriza con éxito, para acceder a estos activos para una implementación probada de confianza cero. En términos prácticos, cero confianza es la filosofía detrás de la arquitectura perímetro definido por *software* (SDP). Los principios básicos de SDP son: "No asuma nada, no crea en nadie, verifique todo, derrote las amenazas". Si bien SDP cero confianza está destinado a aplicarse en la capa de red 3 del Modelo de interconexión de sistemas abiertos (OSI, , por sus siglas en inglés) de la Organización Internacional de Normalización (ISO), en vista de patrones de arquitectura comunes, como

aplicaciones que acceden a servicios de nube híbrida, se debe tener cuidado de aplicar ZTN lo más cerca posible del perímetro de un dominio, para garantizar un rendimiento óptimo y evitar una latencia de servicio innecesaria.

Según *CloudFlare Zero Trust Network Access* (ZTNA) es la tecnología que permite implementar un modelo de seguridad *Zero Trust*. Es un modelo de seguridad de TI que asume que las amenazas están presentes tanto dentro como fuera de una red. En consecuencia, *Zero Trust* requiere una verificación estricta para cada usuario y cada dispositivo antes de autorizarlos a acceder a los recursos internos.

ZTNA es similar al enfoque de perímetro definido por el *software* (SDP) para controlar el acceso. En ZTNA, como en SDP, los dispositivos conectados no son conscientes de ningún recurso (aplicaciones, servidores, etc.) en la red que no sean los que están conectados.

Por ejemplo, primeramente imagine un escenario en el que cada residente obtiene una guía telefónica con los números de teléfono de todos los demás residentes de su ciudad, y cualquiera puede marcar cualquier número para comunicarse con cualquier otra persona; ahora imagine un escenario en el que todo el mundo tiene un número de teléfono que no figura en la lista y un residente tiene que saber el número de teléfono de otro residente para poder llamarlos. Este segundo escenario ofrece algunas ventajas: no hay llamadas no deseadas, no hay llamadas accidentales a la persona equivocada y no hay riesgo de que personas sin escrúpulos usen la guía telefónica de la ciudad para engañar o estafar a los residentes.

ZTNA es como el segundo escenario. Pero en lugar de números de teléfono, usa direcciones IP, aplicaciones y servicios “no listados”. Establece conexiones uno a uno entre los usuarios y los recursos que necesitan, como cuando dos personas que necesitan comunicarse entre sí intercambian números de teléfono. Pero a diferencia de dos personas que intercambian números, las conexiones de ZTNA deben volver a verificarse y recrearse periódicamente.

2.3.6.3 Agente de seguridad de acceso en la nube (CASB)

Un agente de seguridad de acceso a la nube, (Cloud Access security Broaker CASB, por sus siglas en inglés), es una empresa que ayuda a proteger los servicios alojados en la nube de otras empresas. Mantienen las aplicaciones corporativas de *software* como servicio (*SaaS*), junto con los servicios de infraestructura como servicio (Infrastructure as a service IaaS, por sus siglas en inglés) y plataforma como servicio (Platform as a Service PaaS, por sus siglas en inglés), a salvo de ataques cibernéticos y fugas de datos. Normalmente, los CASB ofrecen sus servicios como *software* alojado en la nube, aunque algunos CASB también ofrecen programas locales o dispositivos de *hardware* locales.

Varias tecnologías de seguridad diferentes caen bajo el resguardo de *CASB*, y este normalmente ofrecerá estas tecnologías juntas en un paquete integrado. Estas tecnologías incluyen descubrimiento de TI en la sombra, control de acceso y prevención de pérdida de datos (Data loss preventiion DLP, por sus siglas en Inglés), entre muchas otras.

Gartner define cuatro "pilares" para los agentes de seguridad de acceso a la nube:

- Visibilidad: los CASB ayudan a descubrir "TI en la sombra": sistemas y procesos, especialmente servicios en la nube, que no están documentados oficialmente y que pueden introducir riesgos de seguridad desconocidos.
- Seguridad de los datos: los CASB evitan que los datos confidenciales abandonen los sistemas controlados por la empresa y ayudan a proteger la integridad de esos datos. Las tecnologías relevantes para esta área incluyen control de acceso y prevención de pérdida de datos (DLP).
- Protección contra amenazas: los CASB bloquean las amenazas y los ataques externos, además de detener las fugas de datos. La detección *antimalware*, el *sandboxing*, la inspección de paquetes, el filtrado de URL y el aislamiento del navegador pueden ayudar a bloquear los ataques cibernéticos.
- Cumplimiento: debido a que la nube está tan dispersa y no está bajo el control de una empresa, puede ser difícil para las empresas que operan en la nube cumplir con requisitos reglamentarios estrictos como SOC 2, HIPAA o GDPR. Dentro de ciertas industrias y regiones, las empresas que no cumplan corren el riesgo de sufrir sanciones y multas. Al implementar fuertes controles de seguridad los CASB ayudan a las empresas que almacenan datos y ejecutan procesos comerciales en la nube a lograr el cumplimiento normativo.

2.3.6.4 Cloud Firewall (Cortafuegos en la nube)

Un *firewall* en la nube es un producto de seguridad que, como un *firewall* tradicional, filtra el tráfico de red potencialmente malicioso. A diferencia de los *firewalls* tradicionales estos se alojan en la nube. Este modelo entregado en la nube para *firewalls* también se llama *FireWall-as-a-Service* (FWaaS).

Los *firewalls* basados en la nube forman una barrera virtual alrededor de las plataformas, la infraestructura y las aplicaciones en la nube, al igual que los *firewalls* tradicionales forman una barrera alrededor de la red interna de una organización, y también pueden proteger la infraestructura local.

2.3.6.5 Firewall como servicio

FireWall-as-a-Service (FWaaS) es otro término para los *firewalls* en la nube. Al igual que otras categorías "como servicio", *software*, servicio SaaS o infraestructura como servicio (IaaS), FWaaS se ejecuta en la nube y se accede a él a través de internet, el proveedor del servicio se encarga de mantenerlo en operaciones del día dos.

2.4 Autenticación

La autenticación es un componente importante del control de acceso. Es la práctica de seguridad de confirmar que alguien es quien dice ser. Un viajero que muestra su pasaporte a un agente de aduanas es un ejemplo.

En el ámbito de la ciberseguridad, el ejemplo más común de autenticación es iniciar sesión en un servicio en la web, como iniciar sesión en *Gmail* en un navegador web o iniciar sesión en la aplicación de *Facebook*. Cuando un usuario proporciona una combinación de nombre de usuario y contraseña, el servicio puede confirmar estos detalles y usarlos para autenticar al usuario.

2.4.1 Proveedores de Identidad

Según CloudFlare un proveedor de identidad (Identity Provider IdP o IDP, por sus siglas en inglés) almacena y gestiona las identidades digitales de los usuarios. Hay que pensar en un IdP como una lista de invitados, pero para aplicaciones digitales y

alojadas en la nube en lugar de un evento. Un IdP puede verificar las identidades de los usuarios mediante combinaciones de nombre de usuario, contraseña y otros factores, o simplemente puede proporcionar una lista de identidades de usuarios que otro proveedor de servicios (como un SSO) verifica.

Los IdP no se limitan a verificar usuarios humanos. Técnicamente, un IdP puede autenticar cualquier entidad conectada a una red o sistema, incluidas las computadoras y otros dispositivos. Cualquier entidad almacenada por un IdP se conoce como "principal" (en lugar de "usuario"). Sin embargo, los IdP se utilizan con mayor frecuencia en la computación en la nube para administrar las identidades de los usuarios.

¿Porqué los IdP son necesarios?

La identidad digital debe rastrearse en algún lugar, especialmente para la computación en la nube, donde la identidad del usuario determina si alguien puede acceder o no a datos confidenciales. Los servicios en la nube necesitan saber exactamente dónde y cómo recuperar y verificar la identidad del usuario.

Los registros de las identidades de los usuarios también deben almacenarse de forma segura para garantizar que los atacantes no puedan utilizarlos para hacerse pasar por usuarios. Un proveedor de identidad en la nube generalmente tomará precauciones adicionales para proteger los datos del usuario, mientras que un servicio que no se dedique únicamente a almacenar la identidad puede almacenarlos en una ubicación no segura, como un servidor abierto a internet.

2.4.2 Identidad del usuario

La identidad del usuario digital está asociada con factores cuantificables que pueden ser verificados por un sistema informático. Estos factores se denominan "factores de autenticación". Los tres factores de autenticación son:

- Conocimiento: algo que sabe, como un nombre de usuario y una contraseña.
- Posesión: algo que se tiene, como un teléfono inteligente
- Cualidades intrínsecas: algo que se posee como la huella digital o un escaneo de retina

Un IdP solo puede usar uno de estos factores para identificar a un usuario, o los tres. El uso de más de uno se denomina autenticación multifactor (MFA).

2.4.3 Inicio de sesión único

El inicio de sesión único (Single Sign On SSO, por sus siglas en inglés) es una tecnología que combina varias pantallas de inicio de sesión de aplicaciones diferentes en una sola pantalla o consola. Con el SSO un usuario solo tiene que ingresar sus credenciales de inicio de sesión (nombre de usuario, contraseña, etc.) una vez en una sola página para acceder a todas sus aplicaciones SaaS. El SSO se usa a menudo en un contexto empresarial, cuando las aplicaciones de usuario son asignadas y administradas por un equipo de TI interno. Los trabajadores remotos que utilizan aplicaciones SaaS también se benefician del uso de SSO.

Por ejemplo: si a los clientes que ya habían sido admitidos en un bar se les pidiera que mostraran su tarjeta de identificación, para demostrar su edad, cada vez que intentaran comprar bebidas alcohólicas adicionales, ocasionaría que algunos clientes se frustraran rápidamente con los controles continuos e incluso podrían intentar eludir estas medidas introduciendo sus propias bebidas a escondidas.

Sin embargo, la mayoría de los establecimientos solo verifican la identificación del cliente una vez y, luego, sirven al cliente varias bebidas en el transcurso de la noche. Esto es algo así como un sistema SSO: en lugar de establecer su identidad una y otra vez, un usuario establece su identidad una vez y luego puede acceder a varios servicios diferentes.

El SSO es un aspecto importante de muchas soluciones de control de acceso o administración de identidad y acceso (Identity and Access Management IAM, por sus siglas en inglés). La verificación de la identidad del usuario es fundamental para saber qué permisos debe tener cada usuario.

Además de ser mucho más simple y conveniente para los usuarios, el SSO se considera más seguro. Esto puede parecer contradictorio: ¿cómo puede ser más seguro iniciar sesión una vez con una contraseña, en lugar de varias veces con varias contraseñas? Los defensores de SSO citan las siguientes razones:

Contraseñas más seguras: dado que los usuarios solo tienen que usar una contraseña, el SSO les facilita crear, recordar y usar contraseñas más seguras. * En

la práctica, este suele ser el caso: la mayoría de los usuarios utilizan contraseñas más seguras con el SSO.

Sin contraseñas repetidas: cuando los usuarios tienen que recordar contraseñas para varias aplicaciones y servicios diferentes, es probable que se establezca una condición conocida como "fatiga de contraseñas": los usuarios reutilizarán las contraseñas en todos los servicios. Usar la misma contraseña en varios servicios es un gran riesgo de seguridad, porque significa que todos los servicios son tan seguros como el servicio con la protección de contraseña más débil: si la base de datos de contraseñas de ese servicio se ve comprometida, los atacantes pueden usar la contraseña para piratear a todos los usuarios; así como otros servicios también. El SSO elimina este escenario al reducir todos los inicios de sesión a un solo inicio de sesión.

Mejor aplicación de la política de contraseñas: con un solo lugar para el ingreso de contraseñas, el SSO proporciona una forma para que los equipos de TI apliquen fácilmente las reglas de seguridad de contraseñas. Por ejemplo, algunas empresas requieren que los usuarios restablezcan sus contraseñas periódicamente. Con el SSO los restablecimientos de contraseñas son más fáciles de implementar: en lugar de restablecimientos constantes de contraseñas en varias aplicaciones y servicios diferentes, los usuarios solo tienen una contraseña para restablecer (si bien se ha cuestionado el valor de los restablecimientos regulares de contraseñas, algunos equipos de TI aún los consideran una parte importante de su estrategia de seguridad).
Autenticación multifactorial: la autenticación multifactor (Multi factor authentication MFA, por sus siglas en inglés) se refiere al uso de más de un factor de identidad para

autenticar a un usuario. Por ejemplo, además de ingresar un nombre de usuario y contraseña, es posible que un usuario tenga que conectar un dispositivo USB o ingresar un código que aparece en su teléfono inteligente. La posesión de este objeto físico es un segundo "factor" que establece que el usuario es quien dice ser. La MFA es mucho más seguro que confiar solo en una contraseña. El SSO permite activar MFA en un solo punto en lugar de tener que activarlo para tres, cuatro o varias docenas de aplicaciones, lo que puede no ser factible.

Punto único para hacer cumplir el reingreso de contraseña: los administradores pueden hacer cumplir el reingreso de credenciales después de un cierto período de tiempo para asegurarse de que el mismo usuario todavía esté activo en el dispositivo en el que inició sesión. Con el SSO se tiene un lugar central desde el que hacer esto para todas las aplicaciones internas, en lugar de tener que utilizarlo en varias diferentes, pues es posible que algunas no sean compatibles.

Gestión de credenciales internas en lugar de almacenamiento externo: normalmente las contraseñas de los usuarios se almacenan de forma remota, no gestionada por aplicaciones y servicios que pueden seguir o no las mejores prácticas de seguridad. Sin embargo, con el SSO se almacenan internamente en un entorno sobre el que un equipo de TI tiene más control.

Menos tiempo perdido en la recuperación de contraseñas: además de los beneficios de seguridad anteriores, el SSO también reduce el tiempo perdido para los equipos internos. El TI tiene que dedicar menos tiempo a ayudar a los usuarios a recuperar o restablecer sus contraseñas para docenas de aplicaciones, y los usuarios dedican menos tiempo a iniciar sesión en varias aplicaciones para realizar su trabajo. Esto tiene el potencial de aumentar la productividad empresarial.

2.4.4 Autenticación de dos factores

La autenticación de dos factores, abreviada como 2FA, es un proceso de autenticación que requiere dos factores diferentes para establecer la identidad. En pocas palabras, significa exigir que un usuario demuestre su identidad de dos formas diferentes antes de otorgarle acceso.

2.4.3.1 ¿Qué es un factor de autenticación?

Los factores de autenticación son diferentes métodos de verificación de identidad. Algunos factores de autenticación de uso común para 2FA incluyen:

- Conocimiento: es un dato que solo el usuario debe conocer, como una contraseña o la respuesta a una pregunta de seguridad.
- Posesión: este factor depende de que el usuario mantenga la posesión física de un objeto. Por ejemplo, una llave de hardware que puede generar códigos de acceso o un dispositivo móvil al que se pueden enviar códigos.
- Datos biométricos: estos son rasgos biológicos únicos del usuario que se pueden utilizar en la autenticación. Los ejemplos incluyen huellas dactilares, escáneres de retina e identificación facial.
- Ubicación: las herramientas basadas en la ubicación, como el GPS, se pueden utilizar para restringir la autenticación a los usuarios dentro de una región geográfica específica.

Cabe señalar que requerir dos instancias del mismo factor de autenticación no califica como 2FA. Por ejemplo, solicitar una contraseña y una pregunta de seguridad sigue siendo una autenticación de factor único. Ambos pertenecen al factor conocimiento.

2.4.4 Identidad como servicio (IDaaS)

Identidad como servicio, o (Identity as a Service IDaaS, por sus siglas en inglés) se refiere a una amplia variedad de servicios alojados en la nube para la Gestión de identidad y acceso (IAM, por sus siglas en inglés). Básicamente, IDaaS es una categoría de funciones tecnológicas que tienen que ver con la identidad del usuario y están alojadas en la nube. Los proveedores de IDaaS ayudan a garantizar que los usuarios sean quienes dicen ser, lo que en última instancia impide que los ciberdelincuentes y otros usuarios no autorizados accedan a datos confidenciales.

2.4.5 Security Assertion Markup Language (SAML)

Es una forma estandarizada de indicar a las aplicaciones y servicios externos que un usuario es quien dice ser. SAML hace posible la tecnología de inicio de sesión único (SSO) al proporcionar una forma de autenticar a un usuario una vez y luego comunicar esa autenticación a múltiples aplicaciones. La versión más actual de SAML es SAML 2.0.

Por ejemplo, se puede pensar en la autenticación SAML como una tarjeta de identificación: una forma corta y estandarizada de mostrar quién es alguien. En lugar de realizar una serie de pruebas de ADN para confirmar la identidad de alguien, es posible simplemente echar un vistazo a su tarjeta de identificación.

En informática y redes uno de los principales desafíos es lograr que los sistemas y dispositivos creados por diferentes proveedores para diferentes propósitos funcionen

juntos. Esto se denomina “interoperabilidad”: la capacidad de diferentes máquinas para interactuar entre sí, a pesar de sus diferentes especificaciones técnicas. SAML es un estándar interoperable: es una forma ampliamente aceptada de comunicar la identidad de un usuario a los proveedores de servicios en la nube.

2.4.5.1 ¿Qué es una aserción SAML?

Una aserción SAML es el mensaje que le dice a un proveedor de servicios que un usuario ha iniciado sesión. Las aserciones SAML contienen toda la información necesaria para que un proveedor de servicios confirme la identidad del usuario, incluida la fuente de la aserción, la hora en que se emitió y las condiciones que hacen válida la afirmación.

Como ejemplo en una afirmación de SAML como el contenido de una referencia para un candidato a un puesto: la persona que proporciona la referencia dice cuándo y durante cuánto tiempo trabajó con el candidato, cuál fue su función y su opinión sobre este. Con base en esta referencia, una empresa puede tomar una decisión sobre la contratación del candidato, al igual que una aplicación SaaS o un servicio en la nube pueden permitir o denegar el acceso de los usuarios según una afirmación de SAML.

2.4.6 Autenticación Abierta (OAuth)

Es un estándar técnico para autorizar a los usuarios. Es un protocolo para pasar la autorización de un servicio a otro sin compartir las credenciales de usuario reales, como un nombre de usuario y una contraseña. Con OAuth un usuario puede iniciar sesión en una plataforma y luego estar autorizado para realizar acciones y ver datos en otra plataforma.

OAuth es uno de los métodos más comunes que se utilizan para pasar la autorización de un servicio de inicio de sesión único (SSO) a otra aplicación en la nube, pero podría utilizarse entre dos aplicaciones cualesquiera. Otros protocolos también pueden realizar esta función, aunque OAuth es uno de los más utilizados.

Como ejemplo: se puede visualizar que un visitante llega a una casa cuando el propietario no está allí, y en lugar de enviarle al visitante una llave de la casa, el propietario le envía un código temporal para ingresar a una caja de seguridad que contiene la llave. OAuth funciona de manera similar. En OAuth una aplicación envía a otra aplicación un *token* de autorización para otorgar acceso a un usuario, en lugar de enviar las credenciales del usuario.

Capítulo 3. Marco metodológico

3.1 Tipo de investigación

Como el objetivo general de este proyecto es proponer una metodología para la creación de una arquitectura basada en principios de cero confianza. El tipo de investigación es la evaluativa. Dado que se recoge información y se desea emitir un criterio mediante una propuesta.

3.2 Alcance investigativo

De acuerdo con los tópicos de esta investigación se eligieron los siguientes tipos de investigación:

- **Exploratorio:** se desea familiarizar a las empresas sobre cómo pueden brindar acceso a sus colaboradores, hay información en muchas fuentes hasta el momento no se ha logrado ubicar un documento enfocado a Costa Rica que sea formal, unificado y con recomendaciones.

3.3 Enfoque

La propuesta del enfoque es cualitativa, dado que se buscan resultados ya realizados y se toman como referencia, no se espera comprobar dichos resultados.

Se basa en criterios de calidad y credibilidad, con información de mejores prácticas ya aplicadas entre instituciones y fuentes reconocidas como por ejemplo los fabricantes.

La generalización es utilizada dado a que las tecnologías cambian día con día y eventualmente una mejor práctica para el presente año, sea distinta al año 2022.

El siguiente diagrama cosiste en una propuesta de como se abordará el tema de la investigación. La idea es poder conocer las arquitecturas de cero confianza de

múltiples fabricantes, evaluar los requerimientos, mantenimiento, operación y tratar de dar una propuesta que sea fiable, económica y concisa para las empresas.

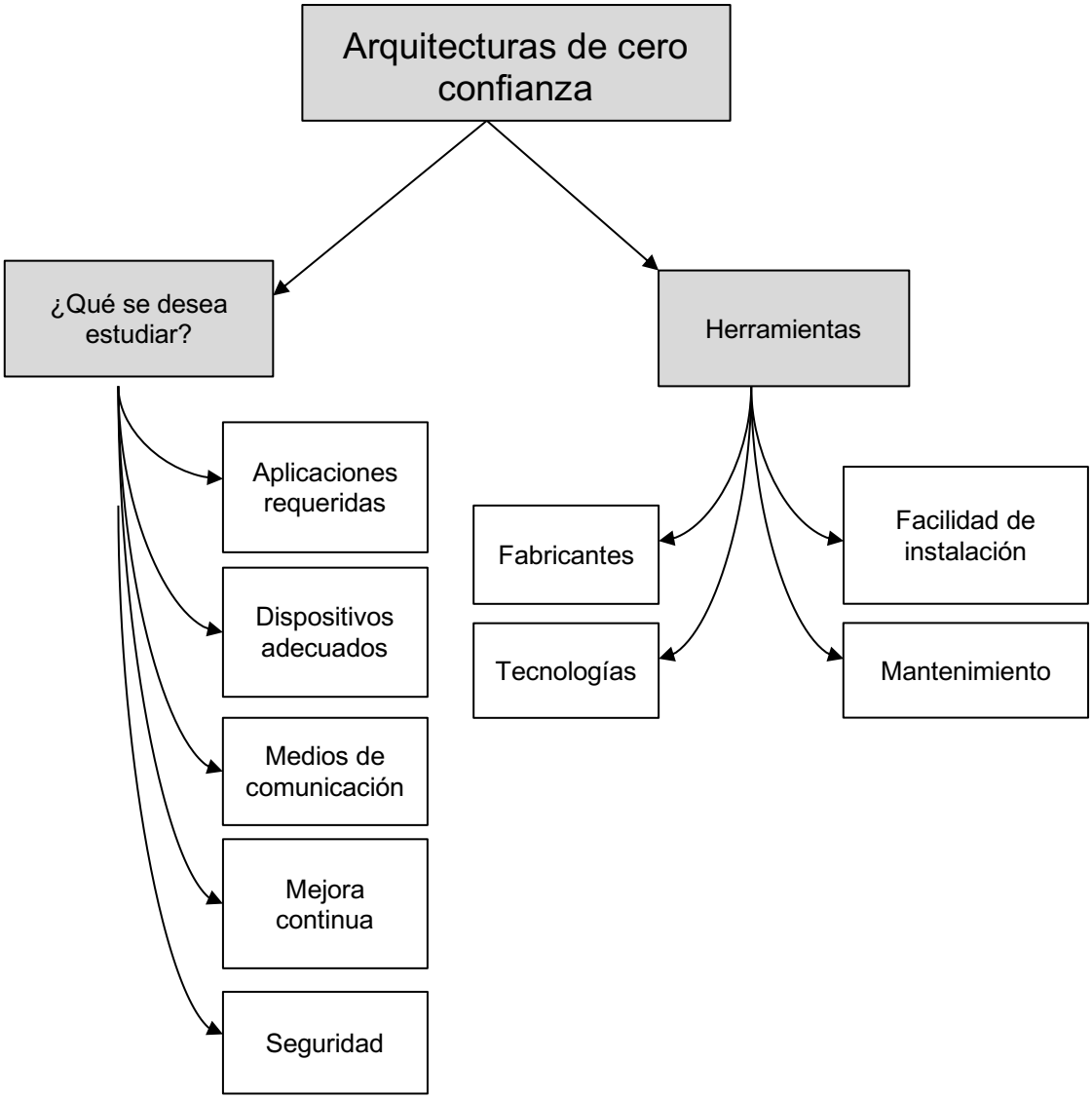


Figura 4: Paradigma naturalista. Fuente: Elaboración propia

3.4 Diseño

El diseño definido en la presente investigación es experimental de tipo pospruebas con un grupo de control que alimente las pruebas. Con base a los resultados se desea obtener un foco de la población. Se desea que de los resultados se obtenga una

pincelada de la situación actual y que se permita tener una orientación de como están las empresas hoy en día en temas de seguridad bajo principios de cero confianza.

Para lograr el objetivo se desarrollarán los siguientes pasos:

- Investigación del mercado.
- Identificación de información relevante de arquitecturas de cero confianza de fabricantes, entes internacionales y certificadores que muestren pasos a implementar una arquitectura similar.
- Limpieza de datos y selección de resultados de las cadenas de búsqueda.
- Interpretación de datos obtenidos.
- Análisis final y conclusiones.

3.5 Población y muestreo

En relación con la alta adopción de las tecnologías durante la pandemia, se identifica que hoy en día muchas personas utilizan métodos de comunicación hacia sus empresas. Muchas personas trabajan desde sus casas y las oficinas están cerradas. Lo que ha hecho que los dispositivos estén conectados a redes desconocidas para las organizaciones.

La población se ve reflejada en cualquier usuario que utilice herramientas corporativas, trabaje desde su oficina o en la casa. Que sean expuestos a internet y uno o varios dispositivos.

Como todos estamos laborando desde muchos sitios, se considera que no es requerido cerrar el ámbito a un grupo pequeño, cerrar el muestreo a un grupo cerrado es cegarse a la situación actual de muchas personas.

3.6 Instrumentos de recolección de datos

Los instrumentos de recolección de información permiten conseguir datos “crudos”, que deberán ser analizados, para fines de conteos y mediciones o bien para ser sujetos de un proceso de interpretación.

Uno de los medios de recolección se basa en encuestas generadas por medio de la plataforma *survey monkey* donde se van a publicar cinco preguntas muy específicas referidas a arquitecturas de cero confianza. En ella se aplicarán encuestas en dos idiomas, inglés y español para tener un mayor alcance de respuesta. Las encuestas serán publicadas en internet y por redes sociales, *whatsapp* entre otros. De este modo al ser preguntas abiertas y concisas cortas se espera obtener un mayor volumen en las respuestas.

Capítulo 4. Análisis del diagnóstico

Las tecnologías antiguas y nuevas no solo están cambiando la industria y el panorama de la seguridad informática, sino que a diario desafían la forma en que la sociedad opera de manera continua.

La convergencia de los sistemas de información con las tecnologías operativas, y los sistemas heredados, han provocado grandes desafíos en el ecosistema digital. La aparición de nuevas tecnologías y sus aplicaciones, tales como inteligencia artificial, *big data*, redes de quinta generación, computación en la nube, IoT y computación cuántica, cuestionan drásticamente nuestro pensamiento convencional sobre el futuro de la economía digital.

Por un lado, ofrecen inmensas oportunidades de eficiencia e innovación, pero también amplifican la superficie de ataque y pueden crear riesgos de seguridad y privacidad de datos todavía desconocidos. Por esta razón, las empresas y los gobiernos deben trabajar juntos para desarrollar una comprensión sólida de los riesgos emergentes de ciberseguridad relacionados desde una perspectiva de políticas, de los riesgos y de las operaciones.

4.1 Aplicación de los cuestionarios

A continuación, se presentan los análisis de los resultados del instrumento utilizado por el investigador, con el fin de conocer la situación actual del mercado. Dichos resultados fueron obtenidos de encuestados donde el enlace de la encuesta fue compartido mediante redes sociales y correos electrónicos.

Este análisis pretende demostrar las debilidades de la arquitectura de seguridad que presentan muchas empresas en cuanto a la seguridad de a información y dispositivos, así como saber cuanto saben los usuarios finales de seguridad en los dispositivos y acceso hacia las herramientas de la empresa. Con base en los resultados se podrá obtener un enfoque de la realidad que sucede hoy en día en muchas empresas, sabremos qué tan protegidas están o actualizadas en temas de seguridad bajo principios de cero confianza.

4.1.1 Aplicación de cuestionarios a usuarios de las empresas

A continuación, se estará explicando las resoluciones de las respuestas en las encuestas, en donde se estará evaluando aspectos relevantes de los usuarios como, por ejemplo, la cantidad de contraseñas que utiliza, ¿quién es el dueño del dispositivo?, ¿cómo se conecta a la organización?, ¿quién administra o gestiona el dispositivo?

Pregunta #1

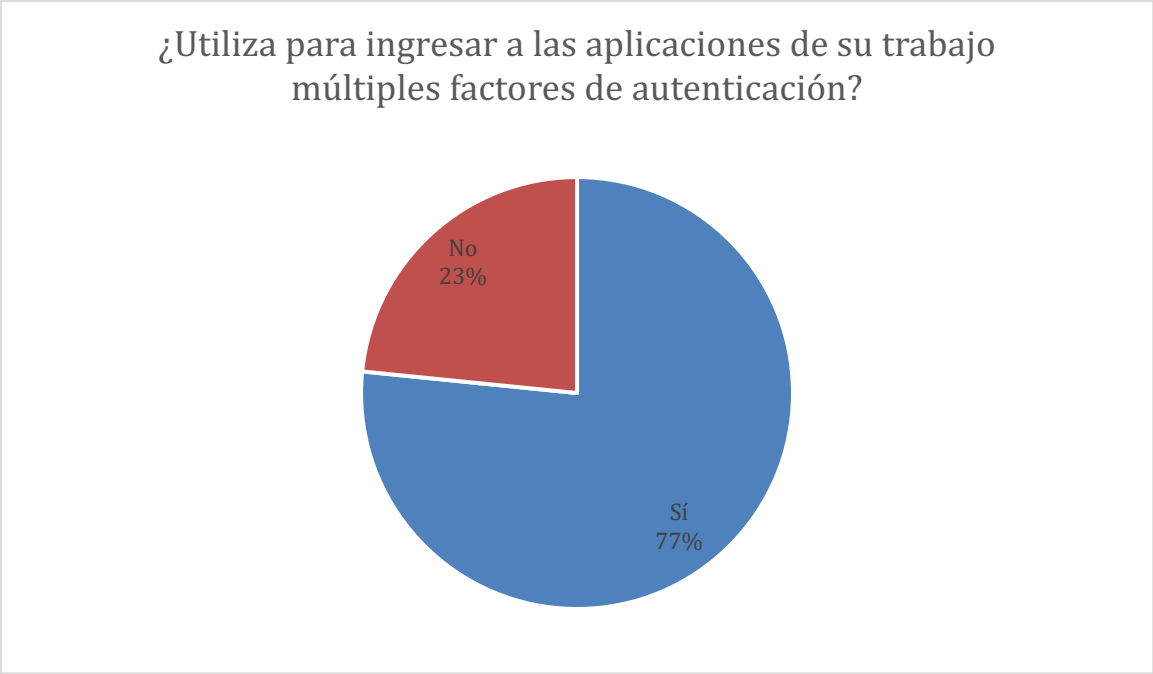


Gráfico 1. Fuente: elaboración propia

Como se puede apreciar, en el gráfico anterior, el 77 porciento de las personas encuestadas sí utilizan múltiples factores de autenticación para ingresar, contra un 23 porciento que pueden estar gravemente expuestas a un ataque. Sin embargo, la mayoría de las empresas ven el múltiple factor de autenticación, como el doble factor, es decir que emplean *token* y alguna otra herramienta. Hoy en día se recomienda por estándares como el PCI\DSS utilizar múltiple factor en vez de doble. Esto brinda mayor seguridad al usuario y para el atacante debe ser más difícil no solo obtener la contraseña, sino, también, dos factores de autenticación adicionales.

Pregunta #2

¿Utiliza una red privada virtual (VPN) para conectarse remotamente a su trabajo?

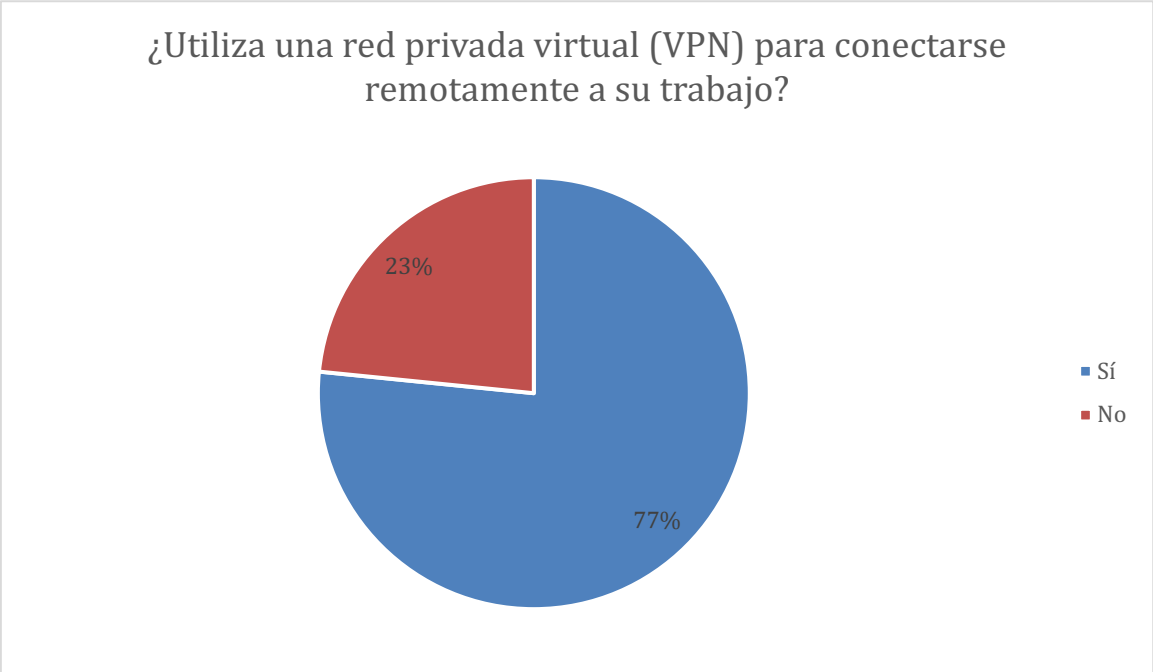


Gráfico 2. Fuente: elaboración propia

Al igual que en la pregunta anterior, el 77 porciento de los encuestados comenta que utilizan la red privada virtual para acceder a sus aplicaciones de trabajo, lo cual demuestra que muchas empresas aún no están preparadas para brindad a sus usuarios nuevas formas de conectividad hacia las aplicaciones corporativas, mas aún sabiendo que ahora muchas aplicaciones son SaaS.

Pregunta # 3

¿El dispositivo que utiliza para consumir aplicaciones de su empresa es propio o corporativo?

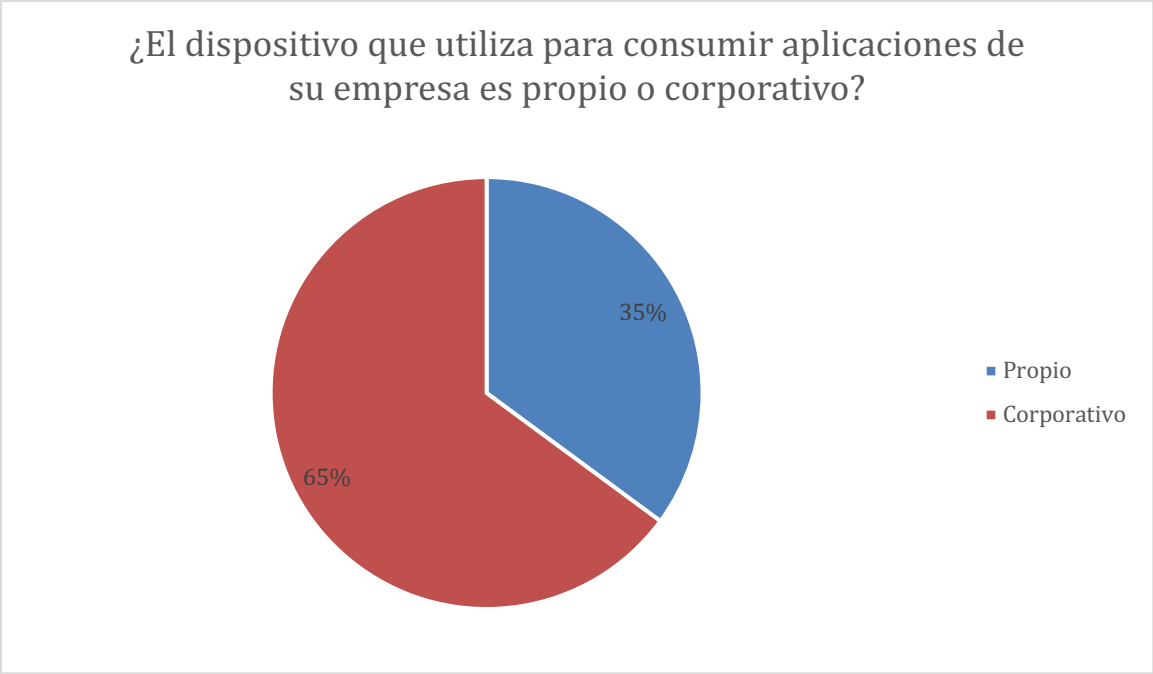


Gráfico 3: Fuente: elaboración propia

En el escenario anterior se evidencia que el 65 porciento de las empresas prefieren mantener el dispositivo corporativo como primera opción, aún así el 35 porciento han adoptado políticas como BYOD (traer su propio dispositivo). Esto significa que las empresas aún se encargan de la administración del dispositivo en su mayoría.

Aunque la utilización de sus propios dispositivos para acceder a recursos de la empresa tiene ventajas, como que los empleados son más productivos, que se eleva la moral de estos, o que permite mayor flexibilidad a la hora de trabajar; también puede ser perjudicial, es necesario tener todo bien configurado para que no se produzcan fisuras por las que se pueda filtrar información confidencial o introducir aplicaciones maliciosas en la red.

Uno de los orígenes de la perdida de confidencialidad es el extravío o robo de alguno de los dispositivos personales. Si estos dispositivos no están debidamente protegidos, se puede comprometer información privada de la empresa. También se ha de tener en cuenta que si el empleado utiliza un dispositivo infectado, como puede ser disponer de una aplicación infectada, al conectarse a la red corporativa podría infectar todos los dispositivos conectados en esa misma red.

Otro factor a tener en cuenta es el uso de programas no permitidos por la política de aplicaciones permitidas, o incluso programas “crackeados” que podrían entrañar riesgos, como una infección o vulnerar las leyes de propiedad intelectual.
Además, hay que destacar que el uso de multitud de terminales diferentes conlleva el sobreesfuerzo de forma necesaria del personal de TI.

Pregunta # 4

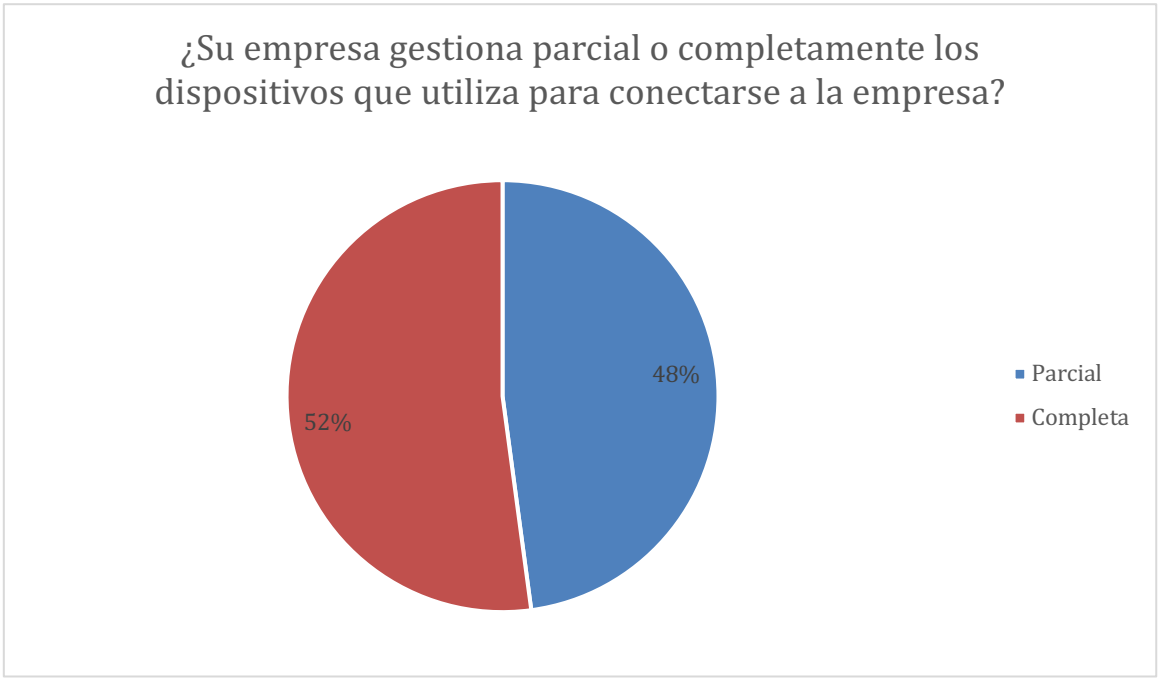


Gráfico 4. Fuente: elaboración propia

Como se observa en el grafico anterior, las empresas gestionan el dispositivo en su mayoría. Sin embargo, se ha demostrado que, aunque el dispositivo sea gestionado por la empresa, ya no es confiable, más aún si dicho dispositivo está fuera de la compañía, lo que provoca que las actualizaciones, auditoría entre otros sea más distante y le sea mas sencillo al atacante utilizar alguna puerta trasera.

Pregunta # 5

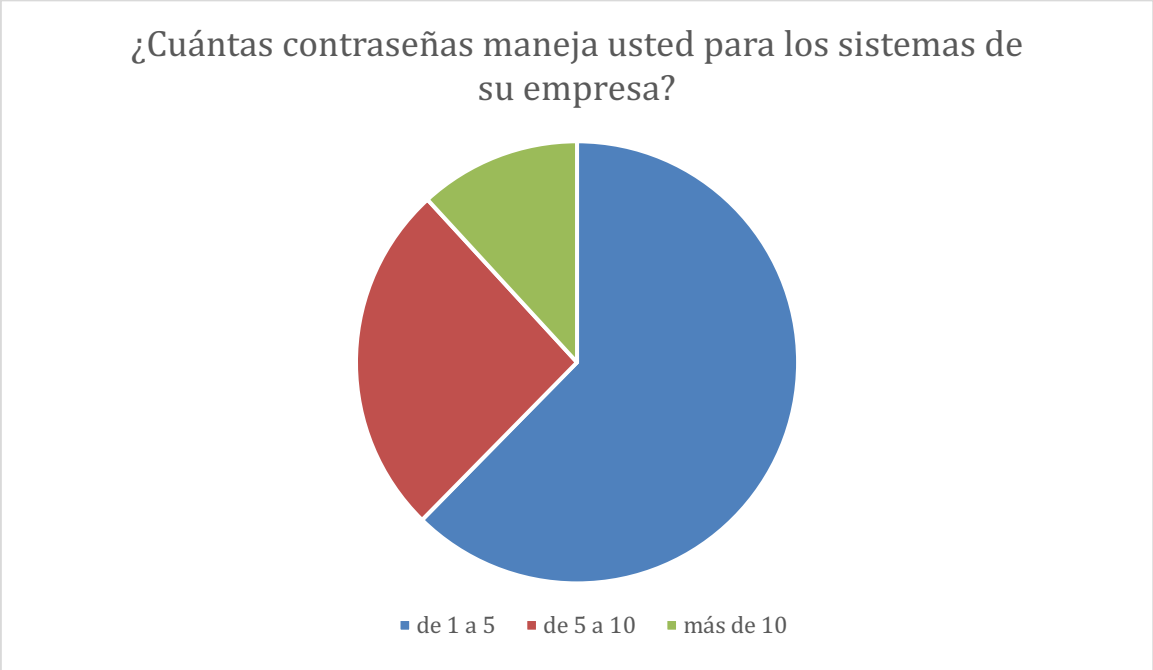


Gráfico 5. Fuente: elaboración propia

En la respuesta a esta pregunta se ve reflejado que existen personas que incluso tienen muchas contraseñas. Lo cual puede provocar errores humanos, mantenimiento de cuentas, llamadas a soporte para reiniciar contraseñas entre otros cargos operativos para una organización. A esto se le adiciona que la persona posiblemente no se recuerde de las distintas contraseñas y debe poner, las reglas, historial, vigencia, entre otros.

4.1.2 Conclusiones de los resultados

Con base en los análisis de las respuestas de la encuesta, se observa que hay carencia en la seguridad de los principios de cero confianza, muchas empresas brindan movilidad a sus trabajadores, sin embargo, están llenas de retos tecnológicos, operativos y sociales, los cuales han hecho que sean vulnerables desde muchas aristas. Se debe ser especialmente cuidadosos con el uso mixto corporativo-personal

que se hace de estos dispositivos, ya que es un riesgo añadido que se debe controlar. Para ello es fundamental involucrar y concienciar al usuario de estos dispositivos en su correcto uso.

Mas adelante se mostrará como se puede intentar reconocer deficiencias, mitigar, transferir o asumir el riesgo y atacar el problema.

Capítulo 5. Propuesta de solución

Durante muchas épocas las personas se han enfocado en crear marcos de arquitectura para brindar una solución a un problema, en este caso se puede ver que empresas o personas han creado arquitecturas empresariales para brindar modelos de referencia por seguir, algunos ejemplos son los siguientes:

- Zachman Entreprise Architecture Framework (ZIFA).
- The Open Group Architecture Framework (TOGAF).
- Extended Enterprose Architecture Framework (E2AF).
- Federal Entreprise Architecture Framework (FEAF).
- Enterprise Architecture Planing (EAP).
- ISO/IEC 14252.
- IEEE Std 1471-2000.

Lo que sucede en muchas ocasiones con los marcos, como los anteriormente mencionados, es que pocas organizaciones los siguen de como fueron establecidos. Implementar dichos marcos de referencia de arquitectura es bastante costoso, o incluso es difícil encontrar personas capacitadas para este fin, ante esta situación, en la mayoría de las organizaciones, por no decir todas, las implementaciones o diseños son distintos, por lo que la aplicación del marco difiere o es inexistente.

Según Gartner, en su documental “Prioridades principales para tecnologías de información” (2021), los arquitectos empresariales y los líderes en innovación tecnológica ahora se enfrentan a una oportunidad sin precedentes, para ayudar a sus

organizaciones a seleccionar, crear e implementar las plataformas empresariales y tecnológicas adecuadas para respaldar sus ecosistemas comerciales.

Debido a que existen muchos marcos de arquitectura, algunos de ellos privados, se explicará como debería realizarse una arquitectura cero confianza como propuesta de modernización en principios de seguridad.

Cuando se habla de este tema, lo que viene inmediatamente a la mente son las herramientas y aplicaciones de seguridad como *firewalls*, *software* antivirus, programas *antimalware* y similares. Sin embargo, una arquitectura de seguridad es la suma de todas esas cosas y más.

“Arquitectura de seguridad” es el término que se utiliza para definir el sistema general necesario para proteger la infraestructura de TI de una organización. Dicho sistema incluye las especificaciones, procesos y procedimientos operativos estándar involucrados en la prevención, mitigación e investigación de diferentes amenazas. Así como el diseño arquitectónico de un edificio instruye a los ingenieros sobre cómo construir una estructura, una arquitectura de seguridad define cómo el personal debe llevar a cabo los procesos de seguridad.

Así como el ciclo de vida del *software* o de los proyectos deben reinventarse mediante la mejora continua, mediante el aprendizaje y adopción, de igual manera debe darse en las arquitecturas de seguridad en principios de cero confianza. Para ello se definirán algunas fases para el entendimiento del lector de este documento.

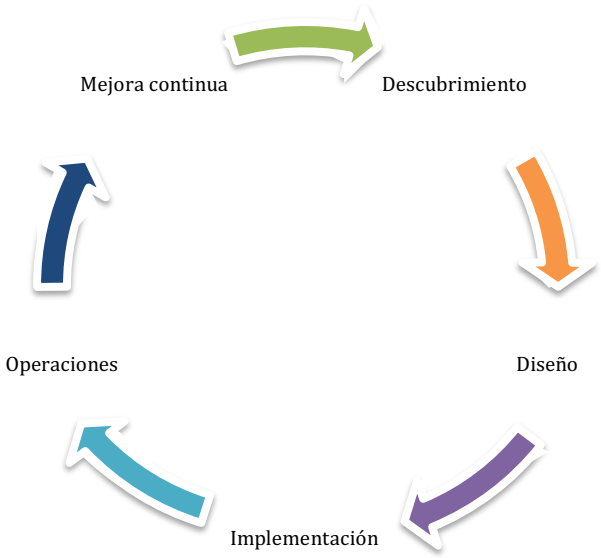


Ilustración 6. Ciclo del desarrollo de una arquitectura de seguridad basada en cero confianza

La presente propuesta de solución de modernización de accesos e identidades en principios de cero confianza se basan en cómo se debe llevar a cabo todo el desarrollo de una arquitectura, para posteriormente ponerla en marcha. Se desea que el lector de este documento comprenda que toda arquitectura no solamente son números y letras, o digitar teclas frente un enrutador o *firewall*. Una buena arquitectura posee fases de planeación y desarrollo antes de la implementación. Para ello se describe todo el ciclo de vida del proyecto como propuesta de solución, así la persona u organización que desee implementar una arquitectura de este tipo de complejidad tendrá una noción de lo que deben desarrollar.

La propuesta, o solución de modernización, de accesos basados en principios de cero confianza consta de las siguientes fases:

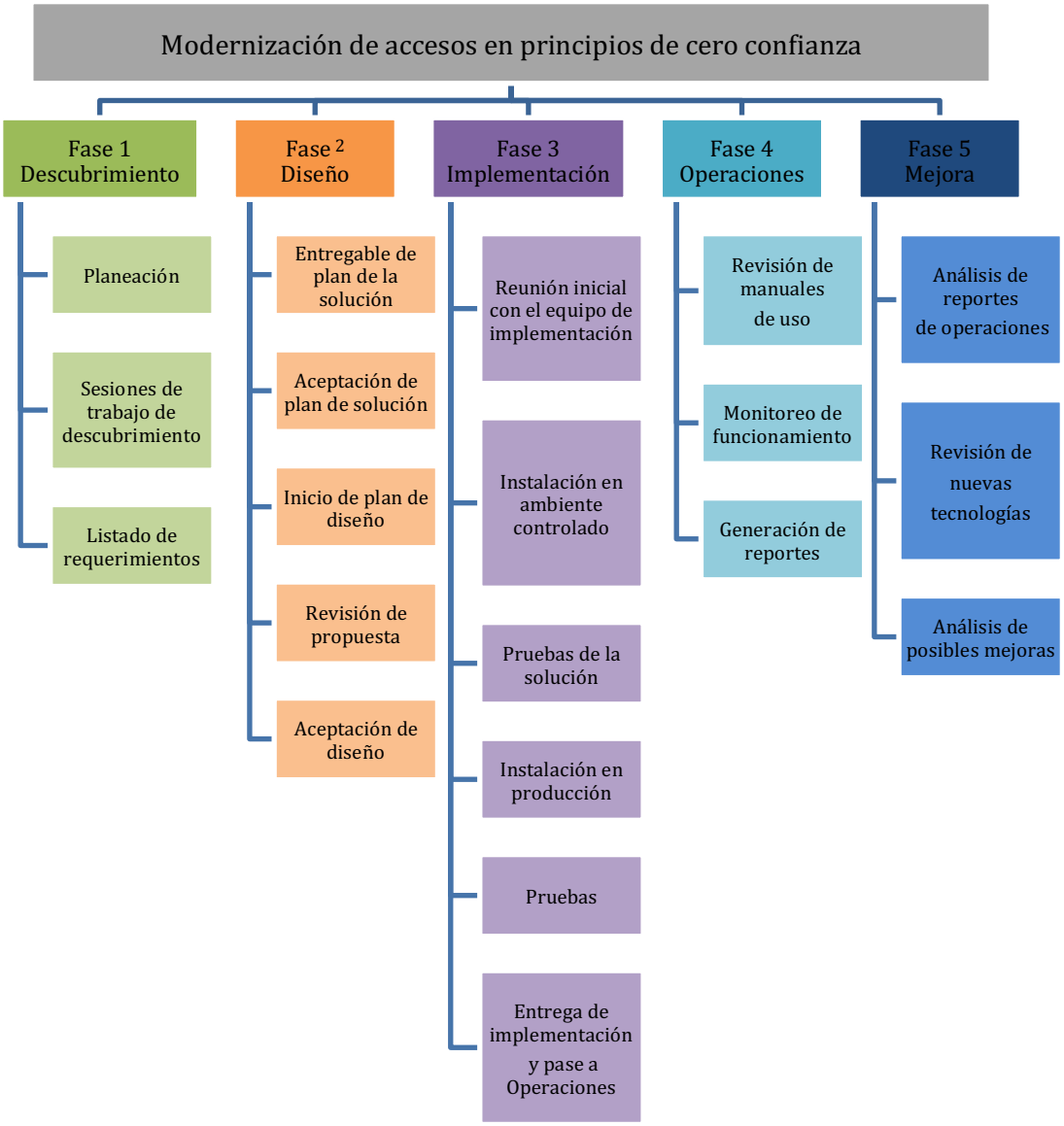


Gráfico 6. Fases de la propuesta de modernización de acceso en principios de cero confianza. Fuente: elaboración propia

Debido a que muchas literaturas mencionan, dependiendo del marco de trabajo, cómo será una arquitectura y con base en la experiencia del escritor de este contenido se propone como solución las fases que se detallarán mas adelante.

5.1 Descubrimiento

En esta fase se sugiere que se pueda trabajar en recolectar toda aquella información que sea esencial para el desarrollo de una arquitectura. Un arquitecto de seguridad que quiera trabajar en principios de cero confianza debe conocer el estado actual de la empresa, cuáles son sus necesidades, los riesgos que se desea mitigar, traspasar y asumir, entre otros.

Gráfico 7. Fase 1 Descubrimiento. Fuente: elaboración propia

Mas adelante, se presentará un ejemplo de plantilla, la cual será necesaria para recolectar información

En la situación se capturan las ideas o problemas actuales como, por ejemplo: actualmente las empresas no poseen un sistema de segundo factor de autenticación o bien otro ejemplo sería: Hoy en día la información de la empresa no se encuentra cifrada o controlada dentro de un dispositivo móvil.

5.1.1 Generación de documentos y evidencia

Para obtener información, registrarla, llevar control y presentación de informes, se deben tener plantillas que permitan manejar las reuniones de una forma ordenada. Una minuta es un buen ejemplo de cómo documentar la información de las reuniones y así llevar control de los temas tratados.

¿Qué es una minuta?

Viene del latín *minutus* que significa pequeño, o *minuta* que significa borrador. Existen varios tipos de minuta, es de acuerdo con el contexto como se puede saber. La minuta de reunión es el resumen de su contenido, desde los asistentes y desarrollo hasta sus conclusiones.

Una estructura básica de una minuta debe contener la siguiente información:

1. Datos de la reunión como fecha, hora, lugar y asistentes requeridos, así como quién es la persona que dirigió o modero la junta y la persona que lleva a cabo la minuta.
2. Agenda del día: son los puntos que centrales que se deben tratar y por lo cual fue convocada la reunión.
3. Temas discutidos y los que no pudieron ser discutidos (aun cuando estaban en la agenda) y por qué (falta de tiempo, ausencia de alguien, etc.) Aquí se puede agregar los acuerdos a los que se llegaron y cómo fueron logrados (si por voto, debate, consenso, etc.).
4. Acciones por tomar. Es aquí donde debemos poner que acciones, responsables y tiempo necesario para terminar una actividad.
5. Firma de asistencia.

La siguiente plantilla demostrará un ejemplo de una minuta de reunión de captura de requerimientos para facilitar al arquitecto en la recolección de información.

MINUTA DE REUNIÓN

Fecha		Hora inicio	
Lugar		Hora fin	
OBJETIVO			

ASISTENTES

ASISTENTES			
Nombre	Puesto	Asistencia	Firma o motivo

ASUNTOS TRATADOS

1. Asunto con prioridad.

……
.....

2. Asunto secundario o menos importantes.

……
……

COMPROMISOS ASUMIDOS

N.º	TAREA	RESPONSABLE	FECHA DE ENTREGA

Tabla 1. Ejemplo de minuta de reunión. Fuente: elaboración propia

5.1.2 Planeación

Durante la planeación el arquitecto debe hacer un orden de ideas, que consiste en pensar cómo debe abordar el problema o requerimiento del negocio.

Gráfico 8. Fase de planeación. Fuente: elaboración propia

Si se desea atraer la atención de los ejecutivos, los cuales poseen poco tiempo o tienen muchas responsabilidades, se debe abordar el tema de una forma menos técnica y con un enfoque mayor hacia el negocio. Por lo que un arquitecto debe capturar las ideas principales y trabajarlas para cumplir. A la alta gerencia no se le debe conversar con tecnicismos, se debe hablar de temas genéricos que sean flexibles y entendibles para todos. Cuando ya se tiene la atención de los ejecutivos, es cuando se debe indicar una propuesta. La cual va a llevar beneficios y soluciones a sus desafíos empresariales. La siguiente imagen es un abordaje de dos situaciones que se presentaron durante la toma de información mediante las encuestas.

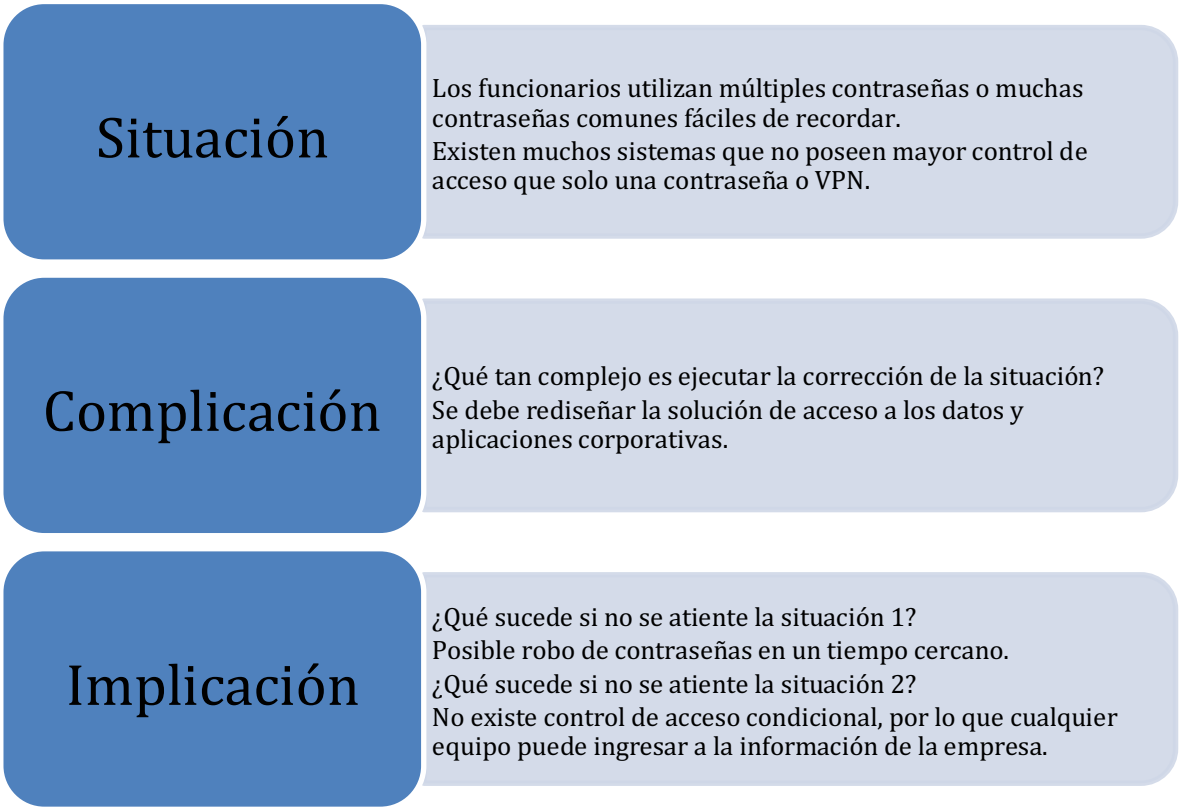


Ilustración 7. Resumen de la situación actual de la empresa. Fuente: elaboración propia

En la imagen anterior se evidencian dos situaciones particulares que surgieron durante la fase de recolección de información, en las encuestas. Muchas empresas utilizan redes VPN para conectarse a los sistemas o algunos funcionarios manejan 10 contraseñas o más para ingresar a los sistemas.

Para darle valor a alguna situación, se debe conversar y averiguar qué tan complejo es implementar o solucionar la situación, y con mayor razón demostrar cuáles serían las consecuencias o implicaciones a corto o mediano plazo, si no se normaliza la situación.

5.1.3 Sesiones de trabajo

Gráfico 9. Fase de sesiones de trabajo. Fuente: elaboración propia

Durante la primeras reuniones un arquitecto no debe esperar que todas las informaciones van a estar presentes. Por lo cual se recomienda como mínimo llevar un cuestionario de preguntas generales. Inicialmente se debe reunir el arquitecto con personal técnico para obtener información de cuales proyectos están a futuro en la organización y para presentar una pre-propuesta de casos de uso que la empresa debe mejorar hoy en día.

Para lo tanto se elaboraron las siguientes preguntas como ejemplo para el arquitecto de seguridad para conocer el negocio:

Cuestionario de captura de información

<table>
<tr><td>1</td><td>¿Qué principios de Confianza Cero son más convincentes para usted y su organización?
<table>
<tr><td>□ Autenticación continua, autorización</td><td>□ Sin distinción de confianza entre red interna o externa</td></tr>
<tr><td>□ Confianza obtenida a través de la verificación de la entidad (por ejemplo, usuario, dispositivo, infraestructura)</td><td>□ Visibilidad y auditoría de acceso de un extremo a otro</td></tr>
<tr><td>□ Segregación de recursos.</td><td>□ Facilitar el acceso con privilegios mínimos.</td></tr>
<tr><td>□ Protección de datos (por ejemplo, conexión segura).</td><td>□ Política de acceso granular y centralizada.</td></tr>
</table></td></tr>
<tr><td>2</td><td>¿Qué tan seguro está para aplicar el modelo / principios de confianza cero en su arquitectura de acceso seguro?</td></tr>
<tr><td>3</td><td>¿Cuáles son los factores clave para que su organización inicie / aumente un programa de gestión de acceso a la identidad / cero confianza?
<table>
<tr><td>□ Prevención de infracciones.</td><td>□ Abordar los problemas de seguridad de TI híbrida.</td></tr>
<tr><td>□ Cumplimiento normativo / de la industria (por ejemplo, HIPAA, GDRP, PCI DSS).</td><td>□ Seguridad / protección de datos.</td></tr>
<tr><td>□ Cumplimiento interno.</td><td>□ Respuesta a una auditoría o incidente de seguridad.</td></tr>
<tr><td>□ Eficiencia operacional.</td><td>□ Reducir las amenazas internas.</td></tr>
<tr><td colspan="2">□ Reducir las amenazas a la seguridad de endpoints e IoT.</td></tr>
</table></td></tr>
</table>

<table>
<tr><td>4</td><td>¿Cuál de los siguientes controles de acceso a la identidad / confianza cero prioriza para la inversión en su organización en los próximos 12 meses?
<table>
<tr><td>□ Defensa contra amenazas móviles.</td><td>□ Autenticación multifactor.</td></tr>
<tr><td>□ Gestión de acceso privilegiado.</td><td>□ Anti-Phishing.</td></tr>
<tr><td>□ Agente de seguridad de acceso a la nube.</td><td>□ Microsegmentación.</td></tr>
<tr><td>□ Gestión y gobernanza de la identidad.</td><td>□ Cortafuegos de aplicaciones web.</td></tr>
<tr><td>□ Control total sobre el acceso de la red cero confianza.</td><td>□ Perímetro definido por software.</td></tr>
<tr><td>□ Inicio de sesión único.</td><td>□ Gestión móvil empresarial.</td></tr>
<tr><td>□ Redes privadas virtuales.</td><td>□ Servicios de directorio empresarial.</td></tr>
<tr><td>□ Analítica de identidad.</td><td>□ Control de acceso a la red.</td></tr>
</table></td></tr>
<tr><td>5</td><td>¿Cuáles son las prioridades de acceso seguro de su organización para los próximos 1-2 años?</td></tr>
<tr><td>6</td><td>Zero Trust Access será toda una aventura, ¿qué escenarios describen mejor el viaje de su organización?
□ La solución ZTNA funcionará junto con VPN sirviendo diferentes casos de uso en los próximos años.
□ Cambiando a los usuarios gradualmente de la solución VPN a la ZTNA, pero siempre mantendremos la VPN para el conjunto principal de usuarios.
□ Migre todos los usuarios a una solución ZTNA.</td></tr>
<tr><td>7</td><td>¿Cuál de los siguientes enfoques es más probable para su organización en evolución a SASE?</td></tr>
</table>

	□ Permanezca con los proveedores existentes, consolide según sea necesario. □ Busque proveedores que puedan proporcionar una solución SASE completa. □ Adoptar el mejor enfoque de su clase para seleccionar los proveedores que sean más apropiados para las necesidades de mi organización.
8	**La implementación de Zero Trust es un proceso gradual, ¿cómo planea implementar Zero Trust en su entorno extendido?** □ Nos estamos asociando con múltiples proveedores de seguridad para construir una hoja de ruta práctica y pragmática para implementar la confianza cero. □ Hemos realizado grandes inversiones en diferentes tecnologías y no estamos seguros de por dónde empezar debido a las complejidades operativas. □ Ya hemos comenzado a implementar la confianza cero con un enfoque principal en la identificación de nuestros activos críticos. □ Todavía no estamos listos para implementar la confianza cero debido a la falta de recursos y habilidades necesarias
9	**¿Cuáles son los principales desafíos a los que se enfrenta su organización cuando se trata de asegurar el acceso a aplicaciones y recursos? (seleccione todas las que correspondan)** □ Dispositivos en riesgo que acceden a los recursos de la red (puntos finales desconocidos, no autorizados, que no cumplen). □ Los procesos manuales son complejos y ralentizan la capacidad de reaccionar rápidamente. □ Sobre el acceso privilegiado de los empleados. □ Dispositivos móviles vulnerables, con ***jailbreak*** o perdidos que acceden a recursos. □ Ataques cibernéticos (por ejemplo, denegación de servicio, secuencias de comandos entre sitios, intermediarios, ***phishing***). □ Socios que acceden de forma insegura a aplicaciones y recursos. □ TI en la sombra.

<table>
<tr><td>10</td><td>¿Hasta qué punto cree que los usuarios de su organización tienen privilegios de acceso más allá de los que requieren?</td></tr>
<tr><td>11</td><td>¿Qué planes tiene para adoptar un modelo de acceso Zero Trust dentro de su empresa?</td></tr>
<tr><td>12</td><td>Durante los próximos 18 meses, ¿en qué medida planean usted y su organización trasladar las capacidades de Zero Trust Access a SaaS?</td></tr>
<tr><td>13</td><td>¿Cuáles son las prioridades de seguridad actuales de su organización?
<table>
<tr><td>□ Aumento o reemplazo de las herramientas de acceso remoto existentes (por ejemplo, VDI, VPN, RDP).</td><td>□ Realizar una inspección profunda de SSL (por ejemplo, descifrado de sesión seguro para escaneo de malware y filtrado web / correo electrónico).</td></tr>
<tr><td>□ Mejorar la corrección de vulnerabilidades (por ejemplo, gestión de vulnerabilidades, gestión de parches).</td><td>□ Prevención de pérdida de datos (DLP).</td></tr>
<tr><td>□ Mejorar la gestión de identidades y accesos.</td><td>□ Habilitar administración de dispositivo móvil (EMM) / BYOD (por ejemplo, usuarios, dispositivos).</td></tr>
<tr><td>□ Garantizar el acceso seguro a las aplicaciones alojadas en proveedores de servicios en la nube (por ejemplo, Microsoft, Amazon, Google).</td><td>□ Proporcionar una mejor protección contra amenazas móviles (Defensa contra ataques móviles o anti-phishing).</td></tr>
<tr><td>□ Simplificar la entrega de acceso seguro (por ejemplo, experiencia del usuario, administración).</td><td>□ Mejorar las funciones de seguridad de SD-WAN.</td></tr>
</table></td></tr>
</table>

	□ Suplemento de detección y respuesta de puntos finales.	□ Ninguna de las anteriores.
14	**¿Cuál de los siguientes escenarios ha encontrado al proporcionar acceso seguro a aplicaciones de nube pública para usuarios móviles o remotos?** □ No puedo implementar mi dispositivo VPN remoto preferido en entornos de nube pública. □ Me veo obligado a "fijar" a los usuarios remotos a través de mi (s) centro (s) de datos para acceder a las aplicaciones en la nube pública	

	□ Tengo que exponer públicamente mis aplicaciones privadas en la nube pública para proporcionar acceso

Tabla 2. Cuestionario de abordaje a empresas en principios de cero confianza. Fuente: elaboración propia

5.1.4 Listado de requerimientos

Gráfico 10. Listado de requerimientos. Fuente: elaboración propia

Una vez hechos los cuestionarios de información hacia la empresa se deben tener requerimientos establecidos. Los cuales, de acuerdo a los resultados de las encuestas, se utilizarán de ejemplo los siguientes, pero queda abierto a que cualquier empresa decida agregar o eliminar requerimientos basado en la gestión de riesgos que se maneja como política corporativa.

Basado en la revisión de las encuestas se determina que hay cinco posibles requerimientos que pueden ser tomados en la mejora de accesos e identidades del presente documento:

- Requerimiento #1: se debe mejorar la experiencia del usuario al ingresar a sus aplicaciones de una forma segura y eficiente.
- Requerimiento #2: los dispositivos permitidos para conectarse a la organización deben estar autorizados previamente.
- Requerimiento #3: los usuarios no pueden utilizar una única contraseña y se debe valorar en todo momento su ingreso.

- Requerimiento # 4: se debe tener la posibilidad de abrir aplicaciones sin necesidad de manejar múltiples inicios de sesión.
- Requerimiento # 5: los accesos a la red deben estar condicionados al tipo de conexión o entorno.

5.2 Diseño

Gráfico 11. Fase de diseño. Fuente: elaboración propia

Durante la fase de diseño se deben tener reuniones para capturar aspectos técnicos que no fueron capturados durante las sesiones iniciales, en estos ejercicios, permitirán definir los alcances del proyecto. Estas reuniones y mesas de trabajo colaborarán a generar una mejor arquitectura.

Es imperativo documentar los requerimientos de la fase 1 para poder ordenarlos de acuerdo a las prioridades. Durante la fase de diseño se define una arquitectura en principios de cero confianza basado en la situación actual y requerimientos capturados.

5.2.1 Propuesta de alto nivel

Es recomendable entregar a la organización una propuesta de alto nivel o *High level Design* (HLD, por sus siglas en idioma inglés), donde se diagrama parte de los procesos recabados, que serían las acciones de mejora y los beneficios. En la siguiente imagen se dará un ejemplo, para mayor claridad, donde se brindan cierto

inicio de ideas para que el arquitecto pueda llevar las reuniones con la alta gerencia y hacerles saber la importancia de que la organización asuma los consejos y los pasos por seguir durante la presentación de la propuesta.

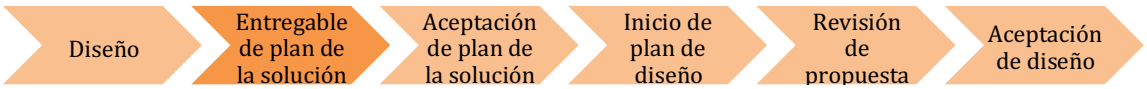


Gráfico 12. Fase de creación de propuesta de alto nivel. Fuente: elaboración propia

En la siguiente imagen se describe como ejemplo de manera ilustrativa cómo debería entregarse una propuesta de alto nivel. Dicho diseño de alto nivel como mínimo debe presentar una propuesta, el plan de acción (lo que se debe realizar) y los beneficios al realizar la ejecución de la propuesta.

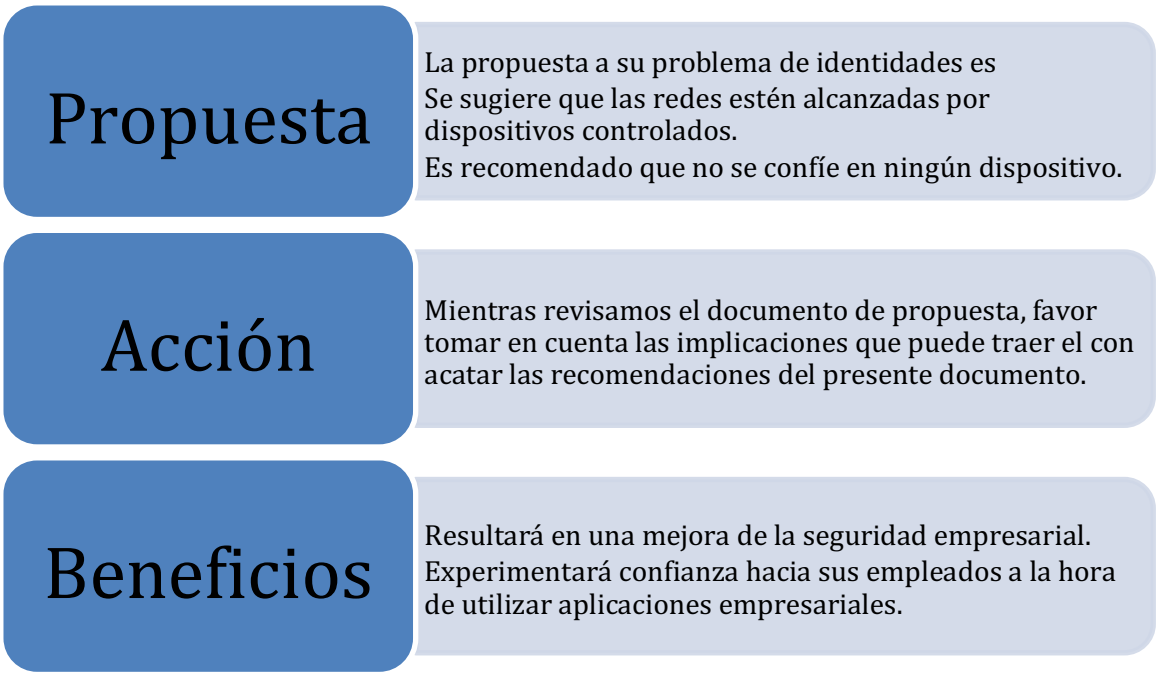


Ilustración 8. Resumen de propuesta hacia la gerencia. Fuente: elaboración propia

Una vez que ya se tiene claridad y hay acuerdos entre las partes, arquitecto empresarial y el negocio, es cuando se procede a trabajar en un documento de bajo nivel que explique cómo debe implementarse los principios de cero confianza en la organización.

5.2.2 Aceptación de propuesta de solución

Gráfico 13. Aceptación de plan de la solución. Fuente: elaboración propia

Es de suma importancia que la organización tenga claro el trabajo qué se va a diseñar, en este documento se debe demostrar como una guía de trabajo. Se debe tener el visto bueno por parte del negocio, que se capturaron los requerimientos correctos y se procederá con el inicio del diseño en la siguiente fase. En donde se aprobaron los recursos de personal, dinero, tiempo y demás. Con esta aceptación se da por enterado que la organización apoyará los requerimientos del proyecto y se iniciará la fase de desarrollo.

Esta aceptación es importante, porque iniciar un proyecto sin aceptación del negocio puede terminar en un proyecto fallido.

5.2.3 Diseño

Gráfico 14. Sub-fase de inicio de diseño. Fuente: elaboración propia

A partir de este momento se acaban los temas técnicos, donde se enfocan los principios de cero confianza. Durante las encuestas del capítulo 3 se observaron múltiples problemas técnicos, que deben ser solucionados, para ello luego de haber tenido una solución de alto nivel como se explica en el paso 5.2.1, se procederá a abarcar la problemática durante el diseño.

Según múltiples autores como Forester (2018), la arquitectura de cero confianza tiene ocho principios que se explicarán a continuación:

1- Conocer la arquitectura, incluidos usuarios, dispositivos, servicios y datos:

Para obtener los beneficios de la confianza cero, se necesita conocer cada componente de la arquitectura. Esto permitirá identificar dónde se encuentran sus recursos clave, los principales riesgos para su arquitectura y también evitar los obstáculos en la etapa tardía, al integrar servicios heredados que no admiten la confianza cero.

Bajo este principio el arquitecto de la empresa debe realizar cuestionarios similares al cuestionario de la tabla 2, apartado 5.2.1 donde se realizan consultas tan técnicas que prácticamente es conocer el diagrama de la red de la empresa.

De acuerdo a la Agencia central de inteligencia (Central Ingeligency Agency CIA, por sus siglas en inglés), referentes a la seguridad de la información, los datos deben cumplir tres características:

- **Confidencialidad:** los datos sensibles deben ser marcados, no puede haber información por la red, sin ser marcada como secreta, personal, pública entre otros
- **Integridad:** se debe mantener la información íntegra, es decir que no cambie de manera no autorizada, por ejemplo, se puede utilizar encriptación para que la integridad del dato se mantenga.
- **Disponibilidad:** para mantener la disponibilidad de la información, se recomienda que las organizaciones deben tener alta disponibilidad, servidores a pruebas de fallos, o herramientas de denegación del servicio. Por ejemplo, en un centro de datos se debe tener doble sistema de *firewall*. En caso de falla en algún componente, que exista otro que le permita continuar al servicio.

Es necesario obtener los diagramas generales de la red, los servicios que se proveen por la red como protocolos, puertos, saber si la información es video, voz, administración, o tráfico de producción.

Se debe obtener un mapa de comunicación para entender los servicios que existen sobre la red, quienes lo consumen y quienes están autorizados. Es necesario saber los dispositivos por cantidades y tipos de servicio, así como los datos, se debe realizar un análisis de riesgos.

Una vez que se conoce la arquitectura se pueden determinar los riesgos para su nueva arquitectura de destino y asegurarse de que se mitiguen.

Después de la etapa de descubrimiento de activos sería sensato comenzar con una evaluación de riesgos, incluido el modelado de amenazas de su enfoque hacia la confianza cero. Esta evaluación se puede utilizar para ayudarlo a comprender si los componentes de confianza cero en consideración mitigarán - protegerán contra - todos sus riesgos.

El grado de mitigación del riesgo puede depender de la criticidad de los activos y su apetito por el riesgo. Por lo tanto, es imperativo evaluar la importancia de los activos y brindarles las salvaguardas adecuadas.

La siguiente tabla es un de ejemplo de riesgos, para que el arquitecto en conjunto con el negocio y las personas de TI puedan llevar a cabo una evaluación detallada de riesgos.

En la tabla se puede valorar algunos tipos de riesgos para un negocio, cuáles serían sus vulnerabilidades, amenazas, la probabilidad y el impago. Una vez que se tiene la probabilidad y el impacto con un número asignado de 1 a 5 (donde 1 es menos riesgoso y 5 es muy riesgoso) se puede ver la severidad y el tipo de cuadro de calor. Luego en la columna de controles se adiciona qué controles se pueden designar al riesgo y volver a valorar el impacto luego de aplicar el control. Con ello la severidad debe de bajar, si no baja es que el control no es eficiente. La tabla en un formato más grade se puede valorar en la sección de anexo 1.

Riesgo	Vulnerabilidad	Amenaza	Probabilidad	Impacto	Severidad	Controles	Probabilidad	Impacto	Severidad
Robo de información de clientes	Falta de controles de seguridad	Hacker	2	3	8	Firewall	1	3	7
Falla en ERP	Falta de actualización de antivirus	Virus	2	3	8	EDR/XDR/EPP	1	3	7
Fallas de hardware	Falta de sistemas de respaldo	Corto Circuito	2	2	6	UPS	1	2	5
Falla del CRM	Falta de controles de seguridad	Injección de SQL	3	3	9	WAF	1	3	7
No entrega de productions a clientes	Inventario	Proveedor	2	2	6	SLA	1	2	5
Falla del servicio de correo	Caida de plataforma tercerizada	Proveedor	1	3	7	SLA	1	3	7
Falla sistema relaciones con clientes	Servicios de nube no disponible	Proveedor	1	3	7	SLA	1	3	7
Caida de servicio de Internet	Falla de enlaces empresa	Proveedor	2	3	8	Redundancy/SLA	1	3	7
Incapacidad usuario conectarse desde casa	Falla de enlaces domestico	Proveedor	3	1	5	Ir a Oficina	2	1	4

Tabla 3. Tabla de ejemplo de riesgos, vulnerabilidades y amenazas. Fuente: elaboración propia

La siguiente tabla, es un cuadro de calor. Donde basado en la probabilidad y el impacto del riesgo considerado por el negocio se aprecia qué tan grave puede ser un riesgo para la organización.

Impacto								
	Catastrófico	Mayor	5	Media	Media	Alta	Alta	Alta
			4	Media	Media	Media	Alta	Alta
	Moderado	Menor	3	Baja	Media	Media	Media	Alta
			2	Baja	Baja	Media	Media	Media
	Insignificante		1	Baja	Baja	Baja	Baja	Media
				1	2	3	4	5

Simbología
Procedimientos de rutina
Medidas a corto plazo
Acciones Inmediatas

Ilustración 9. Cuadro de calor de los riesgos. Fuente: elaboración propia

Si no se pueden mitigar todos los riesgos con un enfoque de confianza cero, los controles de seguridad existentes de su arquitectura de red actual deberán permanecer en su lugar.

2- Conocer las identidades de usuario, servicio y dispositivo

Una identidad puede ser un usuario, una cuenta de servicio (proceso de *software*) o un dispositivo. Cada uno debe ser identificable de forma única en una arquitectura de cero confianza. Este es uno de los factores más importantes para decidir si alguien o algo debe tener acceso a datos o servicios.

La organización debe usar un directorio de usuarios definitivo, creando cuentas que estén vinculadas a individuos. Esto podría venir en forma de un directorio virtual o sincronización de directorios, para dar la apariencia de un directorio de un solo usuario.

Cada identidad debe asignarse a un rol y este debe configurarse como “privilegio mínimo”, de modo que un usuario solo tenga acceso a lo que necesita para llevar a cabo su rol. De hecho, estos privilegios a menudo se derivan de la función laboral del usuario dentro de una organización.

La siguiente lista son servicios idóneos que una organización debe de tener:

- Crear grupos de seguridad:

Los grupos se usan para recopilar cuentas de usuario, cuentas de equipo y otros grupos en unidades administrables. Trabajar con grupos en lugar de usuarios individuales, esto ayuda a simplificar el mantenimiento y la administración de la red.

- Definir roles que se han configurado para tener privilegios mínimos:

La asignación de permisos que puede tener un usuario sobre un sistema o la información es una práctica de seguridad que se aplica de forma continua. Por ejemplo, los sistemas operativos son desarrollados con diferentes roles (y por

supuesto privilegios), pensados para distintos perfiles de usuarios, de acuerdo con sus actividades y responsabilidades.

Operar bajo el principio del menor privilegio, tal como su nombre lo indica, parte de la premisa de otorgar los permisos necesarios y suficientes a un usuario para desempeñar sus actividades, por un tiempo limitado, y con el mínimo de derechos necesarios para sus tareas. Una práctica que se puede implementar en cuanto al uso de la tecnología, con el objetivo de procurar la seguridad de la información, así como la privacidad.

- Admite métodos de autenticación sólidos y modernos, como la autenticación multifactorial o sin contraseña:

Debido a que las contraseñas hacen al usuario mas vulnerable, la autenticación multifactor provee beneficios a las organizaciones, agregando una capa de protección adicional al iniciar sesión y verificar la identidad una vez más.

En el caso de usuarios sin contraseña, provee múltiples capas de seguridad, ya que no se digita la contraseña y se solicitan otros factores, como códigos, certificados entre otros.

- Que proporcione credenciales a los usuarios de forma segura: los usuarios no deberían recibir su contraseña por un correo electrónico. Eso implica una falta a la seguridad, incluso cuando una persona de TI se la brinda a otro usuario. Esto porque son dos personas que saben la misma contraseña. Por ello es recomendable que los sistemas envíen un *link* de recuperación, y tras validarse la identidad con un multifactor se permita el cambio de credenciales.
- Se debe habilitar la autenticación federada para los servicios (por ejemplo, SAML 2.0, OAuth 2.0 u OpenID Connect). Es muy común utilizar autenticación

federada, donde un sistema confía que el usuario que consulta la aplicación ya se autenticó previamente en un sistema de identidad. Por ejemplo: los sistemas de *Office* 365 utilizan federación de *Azure Active directory*. Esto ayuda que el usuario tenga un portal único de inicio de sesión, se evitan múltiples pantallas, existe centralización del usuario, se pueden reforzar las políticas de seguridad, ya que este sistema de inicio de sesión puede solicitar cumplimientos de políticas adicionales que un sistema tradicional no admite, y brinda una experiencia unificada al tener todas las aplicaciones del usuario en un solo portal.

- Gestionar identidades de usuario en servicios externos, cuando corresponda. Permite un manejo de usuarios centralizado y automático. De dicha forma, la información del usuario se mantiene uniforme en el resto de las aplicaciones.

Las organizaciones deben considerar cómo las personas van a acceder desde fuera de la empresa. Si los servicios son federados con proveedores de identidad externo permitirían el acceso externo con usuarios previamente autenticados.

Identidad del servicio:

Un *software* que brinde un servicio debe tener su propia identidad, así como, mantener los privilegios mínimos necesarios para conservar su operación, por ejemplo, se debe restringir la comunicación mínima requerida para operar, conservar la lista permitida de conexiones basados en la identidad del servicio. Se puede incluir un certificado único a cada servicio. Esto para brindar identidad al servicio que se conectan los usuarios.

El *software* debe de actualizarse constantemente, aplicando los parches de seguridad de forma regular. Adicionalmente, se deben reforzar las políticas de seguridad, así

como mantener un *firewall* dentro definido por *software* para impedir comunicaciones extrañas hacia el servicio.

El uso de un sistema criptográfico bien implementado permitiría dar seguridad e identidad a los sistemas hasta para que sea comprometido en 5000 años con la tecnología de hoy en día.

Identidad del dispositivo:

Hoy en día, todos los dispositivos como teléfonos inteligentes, tabletas, computadoras; pueden ser utilizados para conectarse a la red corporativa, para producir, consumir o compartir información.

Todos los dispositivos deben de manejar una identidad única. Habilitando un manejo eficiente de los dispositivos brindando claridad y visibilidad de quienes acceden al servicio o al dato.

Existen múltiples plataformas que brindan identidad al dispositivo dependiendo del tipo, plataforma o *hardware*. Dichas plataformas permiten tener acceso al dispositivo de manera remota, administrarlo, asegurarlo, actualizarlo, ver los registros de seguridad, entre otros. Se necesita que el *software* sea capaz de instalar el antivirus, anti *malware*, encripte el dispositivo, aplique estándares de seguridad entre otros.

En la actualidad, algunos dispositivos manejan un criptoprocesador que permite controlar el cambio de llaves y brindar identidad al dispositivo. De esta forma, una

plataforma de administración de dispositivos puede sacar ventaja para cifrar la información confidencial del dispositivo o identificarlo.

3- Evaluar el comportamiento de sus usuarios, el estado de los dispositivos y los servicios

El comportamiento del usuario y el estado del servicio o del dispositivo son indicadores importantes cuando se busca establecer confianza en la seguridad de sus sistemas, lo que los convierte en señales importantes para los motores de políticas. Por lo tanto, tener la capacidad de medir el comportamiento del usuario, el estado del dispositivo y del servicio es clave en una arquitectura de confianza cero.

Se debe tener la confianza de que los dispositivos que acceden a sus servicios y datos están en buen estado. El estado de estos dispositivos representa algunas de las señales más importantes que se utilizan para controlar el acceso a sus datos y servicios. El estado del dispositivo consiste en el cumplimiento de las políticas de configuración del dispositivo y el estado del dispositivo.

Primero, definir políticas de configuración que impongan una línea de base segura para los dispositivos. La guía de seguridad del dispositivo del NCSC puede ayudar con esto, mediante un servicio de administración de dispositivos, aplicando estas políticas a los dispositivos y haciéndolas cumplir. Luego, verificando continuamente que los dispositivos sean compatibles.

El estado del dispositivo se puede determinar a partir del estado de las funciones de seguridad en la plataforma. Por ejemplo, ¿está habilitado el arranque seguro? ¿Están

instaladas las últimas actualizaciones del sistema operativo? ¿Está habilitada la seguridad basada en virtualización o la protección de la integridad del sistema?

asimismo, se podría determinar el estado subyacente del *firmware* de un dispositivo, el proceso de arranque, la *suite* de seguridad del punto final y el *kernel* del sistema operativo, son señales fuertes que ayudan a determinar el estado general del dispositivo. La atestación es una forma de lograr esto, tomando una instantánea del estado de un dispositivo, con afirmaciones sobre diferentes componentes del *hardware* y del sistema operativo. Algunas *suites* de seguridad para terminales pueden proporcionar señales que pueden ayudar a determinar si un dispositivo es confiable.

Debe asegurarse que los usuarios legítimos tengan un camino definido y claro para llevar sus dispositivos a una buena salud cibernética, y si accidentalmente ha caído por debajo del estándar requerido. Se podría bloquear el acceso de un usuario legítimo a un servicio o datos si un dispositivo no ha realizado algún mantenimiento de rutina.

Por ejemplo, si un dispositivo ha estado fuera de línea durante un período de tiempo y no ha recibido un parche del sistema operativo, el usuario debe tener la capacidad y el soporte necesario para actualizar su dispositivo, de modo que pueda considerarse compatible.

4- Utilizar políticas para autorizar solicitudes

Cada solicitud de datos o servicios debe autorizarse según una política. El poder de una arquitectura de confianza cero proviene de las políticas de acceso que defina. Las políticas también pueden ayudar a facilitar el intercambio de datos o servicios gestionados por riesgos con usuarios invitados u organizaciones asociadas.

El motor de políticas es un componente clave de la arquitectura de cero confianza, utiliza múltiples señales y proporciona un mecanismo de control de acceso flexible y seguro que se adapta a los recursos que se solicitan.

Estas políticas pueden incluir configuraciones de seguridad básicas, como requerir un código de acceso y hacer cumplir ciertas precauciones, incluida la seguridad del código de acceso, denegar la lista de ciertas aplicaciones y requerir intervalos de registro del dispositivo.

Una vez que se determina que los dispositivos están fuera de cumplimiento, el motor de cumplimiento advierte a los usuarios que aborden los errores de cumplimiento para evitar acciones disciplinarias en el dispositivo. Por ejemplo, el motor de cumplimiento puede activar un mensaje, para notificar al usuario que su dispositivo no cumple con los requisitos.

Además, los dispositivos que no cumplen no pueden tener perfiles de dispositivo asignados y no pueden tener aplicaciones instaladas en el dispositivo. Si no se realizan correcciones en el tiempo especificado, el dispositivo pierde el acceso a ciertos contenidos y funciones que usted defina. Las políticas y acciones de cumplimiento disponibles varían según la plataforma.

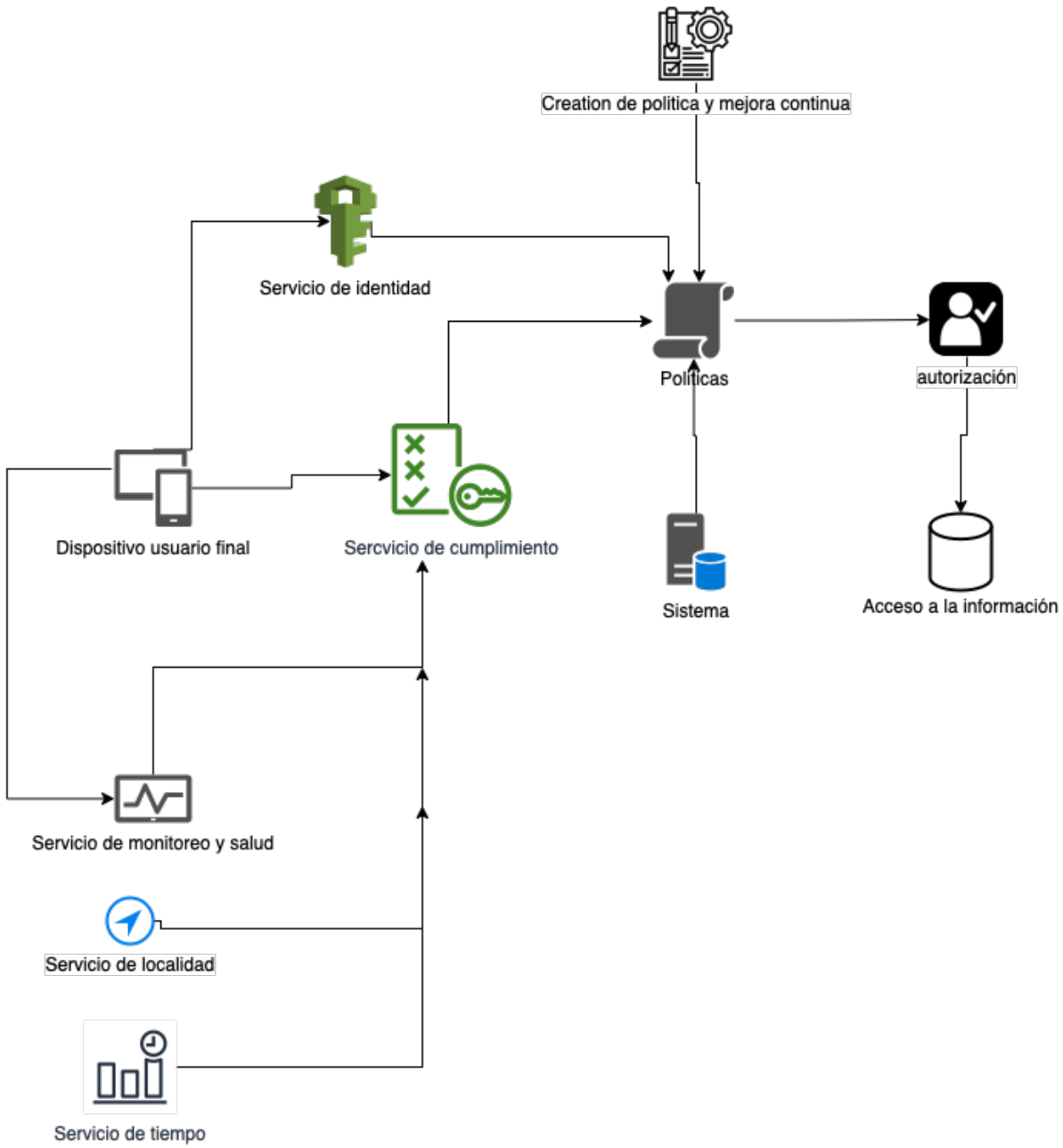


Ilustración 10. Diagrama de gestión de políticas cero confianza. Fuente: elaboración propia

En la imagen anterior, se observa como un dispositivo que desea ingresar a algún sistema debe atravesar múltiples condicionales, como por ejemplo la localidad debe ser válida, el horario mediante servicio de tiempo debe ser en horario hábil, la salud del dispositivo debe estar correcta, no se permiten teléfonos con *root* o alterados. Si el motor de cumplimiento valida las condiciones anteriores, se procede a pasar la información al servicio de identidad. Esta valorará que el usuario esté correcto y se le

gestionará con políticas, que nuevamente validan el dispositivo, la fecha y hora de solicitud, así como el sistema tiene políticas para el usuario que se autentica. Todas estas políticas deben ser aprobadas y mejoradas continuamente. Por último, si la información es correcta, se procede con la autorización y el acceso.

5- Autenticar y autorizar en todas partes

Las decisiones de autenticación y autorización deben considerar múltiples señales, como la ubicación del dispositivo, el estado del dispositivo, la identidad del usuario y el estado para evaluar el riesgo asociado con la solicitud de acceso. se hace esto porque se asume que la red es hostil y se desea asegurar que todas las conexiones que acceden a sus datos o servicios estén autenticadas y autorizadas. Se puede implementar autenticación sin contraseñas. Que brinda una seguridad robusta y excelente solución de experiencia para el usuario.

6- Enfoque su monitoreo en usuarios, dispositivos y servicios

En una arquitectura de confianza cero, es muy probable que su estrategia de supervisión cambie para centrarse en los usuarios, los dispositivos y los servicios. El monitoreo de estos dispositivos, servicios y comportamientos de los usuarios lo ayudará a establecer su salud. El monitoreo debe vincularse a las políticas que ha establecido para obtener seguridad en su configuración.

Aunque no se confía en la red, y se supone que es hostil, la supervisión de la red sigue siendo importante para garantizar un buen rendimiento y la higiene cibernética.

El monitoreo debe llevarse a cabo en sus redes para medir el rendimiento, identificar todos los dispositivos conectados a su red, detectar dispositivos no autorizados y actividad maliciosa. Esto es especialmente cierto si está alojando servicios en las instalaciones.

Junto con el monitoreo de dispositivos, el monitoreo de la red puede ayudar a mejorar la visibilidad y la correlación. Por ejemplo, puede rastrear las conexiones de red hasta el proceso en un dispositivo que las generó.

7- No confiar en ninguna red, incluida la de la empresa propia

No confíe en ninguna red entre el dispositivo y el servicio al que accede, incluida la red local. Las comunicaciones a través de una red, para acceder a datos o servicios, deben utilizar un protocolo de transporte seguro para tener la seguridad de que su tráfico está protegido en tránsito y menos susceptible a amenazas.

Una arquitectura de cero confianza cambian la forma en que se implementan las protecciones de usuario tradicionales, como el filtrado de sitios web maliciosos y la protección contra el *phishing*, que pueden necesitar ser proporcionadas por diferentes soluciones en su arquitectura de confianza cero.

8- Se recomienda elegir servicios diseñados para la confianza cero

Es posible que los servicios no admitan la confianza cero y, por lo tanto, pueden requerir recursos adicionales para integrarse y aumentar la sobrecarga de soporte. En estos escenarios, puede ser prudente considerar productos y servicios alternativos que se hayan diseñado teniendo en cuenta la confianza cero.

El uso de productos que utilizan tecnologías basadas en estándares permite una integración e interoperabilidad más fáciles entre los servicios y los proveedores de identidad.

Se recomienda seguir estándares, como *Open* ID Connect, OAuth 2.0 y SAML, es decir no se requiere inventar infraestructuras que van a traer alto costo y complejidad, cuando el mercado ya posee tecnologías avanzadas y asumidas por muchas empresas.

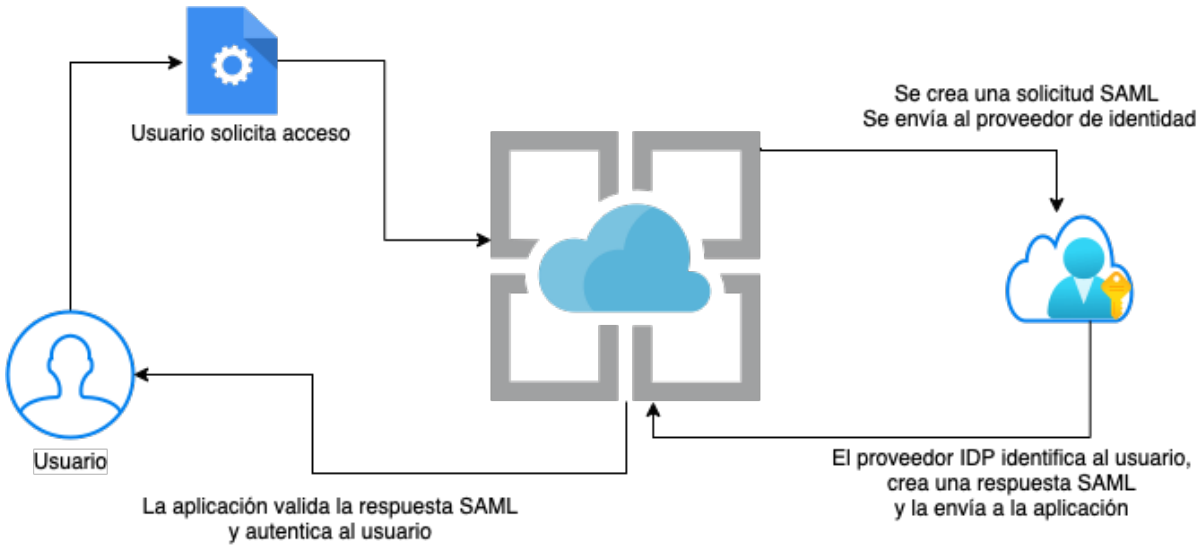


Ilustración 11. Autenticación SAML. Fuente: elaboración propia

5.2.4 Revisión del diseño

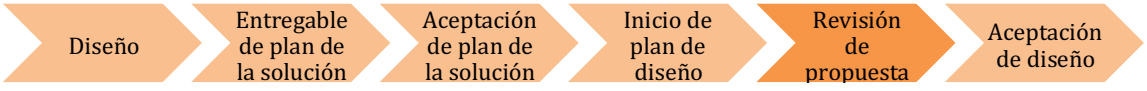


Gráfico 15. Sub-fase de revisión de propuesta de diseño

Todo arquitecto debe realizar una presentación del diseño a la organización. Con ello se deben definir roles y responsabilidades dentro de la empresa, para que se pueda

valorar la forma de cómo se va a colaborar dentro de proyecto de modernización de accesos e identidades en la empresa.

A este punto la organización ya debe tener claro los conceptos básicos de alto nivel de una arquitectura de cero confianza y cómo se van a manejar los accesos y cómo se van a modernizar, queda esperar que se autorice el diseño y se asigne el presupuesto para la posible compra de servicios o de equipo según sea el caso y las necesidades individuales de cada organización.

5.2.5 Aceptación diseño

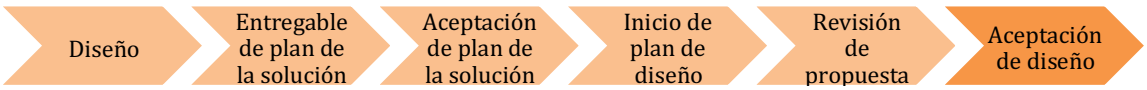


Gráfico 16. Sub-fase de aceptación de diseño

Previo a la puesta en marcha o implementación, un buen arquitecto que presente una propuesta de solución de modernización de accesos basados en principios de cero confianza debe asegurarse que el negocio acepta la propuesta, como se mostró en la fase de diseño, donde indicaron todas las funciones que se deben asegurar, en cómo se debe manejar el ingreso de los usuarios, y asegurar los dispositivos, entre otros.

La aceptación del diseño da por un hecho que se implementarán los productos, pero no quiere decir que el proyecto no sufra modificaciones en el futuro o bien, algún cambio de producto o requerimiento.

5.3 Implementación

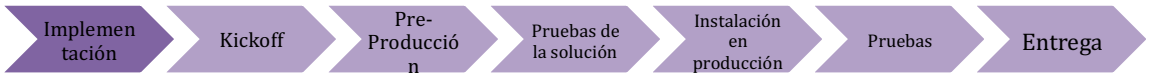


Gráfico 17. Fase de implementación. Fuente: elaboración propia

Una vez que el diseño ha sido generado, aceptado por la organización y aprobado, el paso consecuente es la implementación. El diseño previamente generado es de gran relevancia, donde las personas que lo van a implementar se guían sobre cómo trabajarán y cuáles parámetros deben utilizar. Se considera que la implementación y la adopción es la parte más compleja de muchos proyectos, donde una adopción puede tardar meses como en muchos casos, ya que se depende de factores externos.

Se considera que la fase de implementación debe estar dividida en 6 sub-fases:

5.3.1 Reunión inicial del proyecto

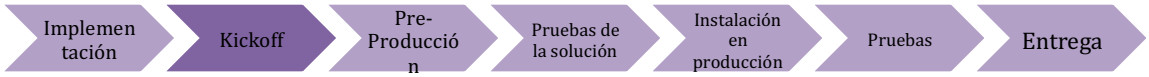


Gráfico 18. Sub-Fase de reunión inicial de proyecto. Fuente: elaboración propia

La reunión inicial del proyecto o *kickoff* para un proyecto de modernización de accesos e identidades, basado en principios de cero confianza, es donde se debe explicar al equipo técnico y del proyecto, además de cómo debe quedar implementada la solución, ahí se debe aclarar cualquier duda técnica y validar las deficiencias del

equipo para intentar complementarlas con capacitaciones o bien personal externo experto en el tema.

5.3.2 Implementación de pre-producción

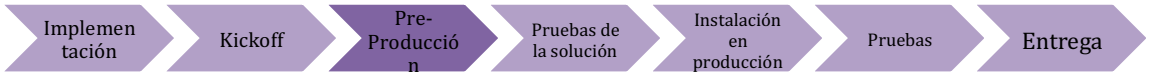


Gráfico 19. Sub-Fase: implementación de pre-producción. Fuente: elaboración propia

En esa etapa se considera que la organización debería de tener un entorno aislado, que permita ejecutar cambios sin afectar a otros. Posiblemente se requiera comprar nuevo *hardware* y *software* si es que el ambiente no existe, o no está disponible para este proyecto. Es recomendable hacer pruebas de la implementación en un ambiente controlado.

5.3.3 Pruebas de la solución

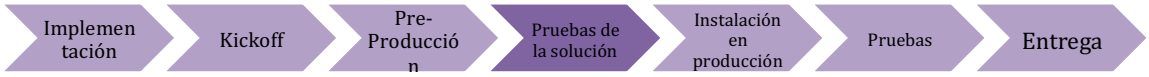


Gráfico 20. Sub-Fase pruebas de solución en ambiente de pruebas y desarrollo

Acompaña a la etapa anterior de desarrollo en un entorno no productivo. Su objetivo es encontrar y eliminar los problemas mayores, configuraciones restantes de funcionalidad entre otros. Es muy común devolverse a la etapa anterior para realizar cambios necesarios y, ocasionalmente, se puede devolver a la fase de diseño para realizar ajustes mayores.

5.3.4 Fase de implementación en producción

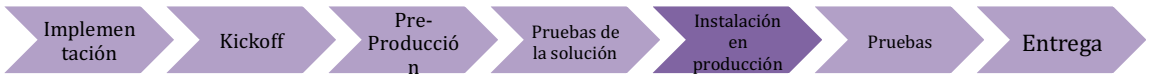
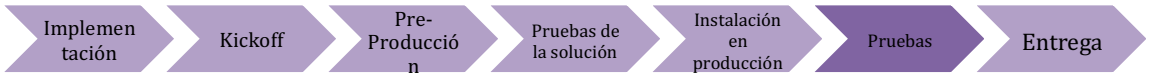


Gráfico 21. Sub-fase de implementación en producción. Fuente: elaboración propia

Luego de satisfacer todos los pre-requisitos del negocio o del proyecto, se puede mover la implementación a una etapa de análisis de calidad, posiblemente se deba repetir las etapas de desarrollo e implementación en conjunto con la fase de pruebas, hasta que el entorno quede con las expectativas deseadas para ser trasladado a producción.

En esta etapa ya los componentes comprados o desarrollados para la organización fueron adquiridos y están listos en producción para ser utilizado, ahora se pasará a una fase de piloto donde se agregarán nuevos usuarios a la modernización de los accesos y así recibir retroalimentación.

5.3.5 Pruebas en ambiente de producción



Durante esta fase, lo idóneo es que ya no existan errores, ya las pruebas se realizaron en pre-producción y la organización está preparada para asumir la producción, se considera un tiempo prudencial que se pueda tomar como plan piloto para que las personas tengan aceptación y uso de las herramientas, provean una retroalimentación y permitan al equipo pensar una futura fase de mejora continua.

5.3.6 Entrega a operaciones

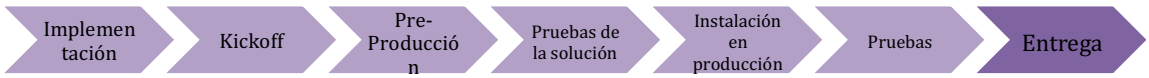


Gráfico 22. Sub-fase de entrega a operaciones. Fuente: elaboración propia

El pase a operaciones luego de una implementación es de suma importancia. Usualmente este tipo de pase de operaciones se da cuando ya existió una prueba piloto que acompañó y demostró el éxito del proyecto. Usualmente es dar el control o responsabilidad a otros, este paso forma parte del ciclo de vida de los proyectos donde existió un alcance, tiempo, costo, entregables, expectativas entre otros.

Un proyecto de cero confianza normalmente arrancan para satisfacer las necesidades de una organización, una vez construido ese producto final se debe transferir a la empresa para que lo utilice. Lo que se describe con anterioridad se centra en el pase a operaciones de la organización. Pero no sólo existe esa transferencia de responsabilidades, ya que normalmente en los proyectos existe la transferencia hacia otra área más.

Como se menciona en la fase anterior, se debe documentar como sería la operación de la arquitectura, manuales de uso, matrices de responsabilidad.

Es importante asegurar que después de la aceptación del resultado final del producto hay un sistema establecido de escalado y de comunicación de incidencias, y otros asuntos, es decir, quién es responsable de qué y con quién tiene que contactar el cliente cuando pasa algo.

5.4 Operaciones

Gráfico 23. Fase de operaciones. Fuente: elaboración propia

El día a día de las organizaciones debe estar establecido, planeado y con un plan pre-meditado. Es necesario que las personas que asuman una arquitectura, modernización de accesos en principios de cero confianza, se encuentren capacitadas y sepan cómo es el plan de estalación en casos de falla, quienes toman las decisiones, y cmo se debe informar en caso de una falla y cuáles son los procesos de toma de evidencia, entre otros.

5.4.1 Manuales de uso

Gráfico 24. Sub-fase de manuales de uso. Fuente elaboración propia

En esta fase se tienen las guías de implementación, los diagramas funcionales y de alto nivel. Es necesario que el producto posea documentación de cómo funciona la plataforma, así como la documentación de cómo se debe operar. Saber cómo actuar en caso de falla o bien en momento de alguna actualización saber cómo deben iniciarse la plataforma. Por ello es importante tener manuales de operación que permitan incluso evaluar si la plataforma se encuentra estable y saludable.

5.4.2 Monitoreo de funcionamiento

Gráfico 25. Sub-Fase monitoreo de funcionamiento. Fuente: elaboración propia

Establecer un control de monitoreo de la plataforma es una mejor práctica que se desarrolla incluso en manuales como la NIST-800. Donde se debe tener monitoreo continuo, para visualizar posibles amenazas y fallas en el funcionamiento de los sistemas. Como controles se deben tener consolas que alerten en caso de falla. Revisión constante de la plataforma y captura de logs en caso de errores.

Se deben implementar mecanismo de protección, comprobación de la integridad para verificar que el *software*, *hardware* y *firmware* estén dando información integra. Así como tener una base de referencia operacional (punto de esta tesis 5.4.1) para ver los flujos de los datos esperados de acuerdo a los inicios de sesión, comunicación, flujos de información entre otros.

Es importante determinar el impacto de los eventos. Establecer umbrales de alerta de incidentes. Esto permitirá la mejora continua en un futuro o evitará una eventual catástrofe.

5.4.3 Generación de reportes

Gráfico 26. Sub-fase: generación de reportes. Fuente: elaboración propia

La presentación de informes es importante, con ello se demuestra a la gerencia la importancia del gasto o esfuerzo que se realizó como compañía. El hecho de modernizar accesos en principios de cero confianza, debe traer un beneficio para la organización que se debe notar en el corto plazo. Con ello las empresas tendrán seguridad que han adquirido productos y servicios que son de calidad y han sido funcionales. No solamente un producto más, que sea revisado como un gasto.

Por ejemplo, se pueden generar reportes de accesos, horarios, aplicaciones que poseen los dispositivos corporativos, estado de salud del dispositivo, actualizaciones entre otros.

Todos estos reportes pueden ser de importancia para la organización en cuanto el manejo de dispositivos autorizados a conectarse a la red empresarial.

5.5 Mejora continua

Gráfico 27. Fase de mejora continua. Fuente: elaboración propia

Toda arquitectura de cero confianza debe tener un proceso de actualización y mejora continua. Como ser observó en la ilustración 10, el manejo de políticas de seguridad debe mantenerse actualizadas y en constante mejora.

En arquitecturas de cero confianza, la evaluación continua está respaldada por el monitoreo de señales de usuarios y dispositivos y su evaluación continua. Si la confianza en la seguridad se degrada, la re-autenticación puede activarse dinámicamente, antes de autorizar el acceso continuo a los servicios y datos.

Independientemente de cómo diseñe la arquitectura de confianza cero, el motor de políticas, o cualquier componente que haga cumplir la política, solo debe permitir conexiones si se cumplen las políticas estrictas que defina.

5.5.1 Análisis de reporte de operaciones

Gráfico 28. Sub-fase de análisis de reportes operaciones. Fuente: elaboración propia

Las decisiones de políticas deben considerar varias señales, tomadas de información histórica e información de conexión en tiempo real. Juntos, estos le permiten crear contexto, por lo que puede decidir si una solicitud de acceso puede ser lo suficientemente confiable como para continuar. Estas señales se envían a un motor de políticas para que pueda tomar una decisión de acceso informada.

Es importante utilizar varias señales para ganar confianza en una solicitud de acceso, ya que esto brindará más información para analizar y brindará una mayor confianza en que el solicitante es genuino y que su dispositivo se encuentra en buen estado de salud cibernética.

Gráfico 29. Sub-fase de revisión de nuevas tecnologías. Fuente: elaboración propia

El rápido avance de las tecnologías digitales apoya los descubrimientos e innovaciones de nuevas tecnologías, pero con ello crea nuevas vulnerabilidades a un paso más acelerado de lo que se pueden atender. Las empresas modernizan sus accesos y formas de trabajo, sin embargo, no es suficiente con sostener un proyecto en el tiempo sin darle los recursos necesarios para mantenerse al día con las nuevas tecnologías.

Hasta la fecha, el desequilibrio entre el tiempo de comercialización y el “tiempo de seguridad” sigue siendo una cuestión predominante, debido a la presión de las fuerzas del mercado en favor de los productos de nuevas tecnologías, sin incentivos para priorizar los elementos de seguridad desde el inicio del ciclo de vida del producto. Tanto las antiguas como las nuevas tecnologías no solo están reestructurando la industria y el panorama de la ciberseguridad, sino que desafían más ampliamente las formas tradicionales de operación de la sociedad.

Gráfico 30. Sub-Fase análisis de posibles mejoras. Fuente: elaboración propia

Como todo fundamento de arquitectura empresarial la mejora continua permite que los líderes de seguridad de TI aumenten la seguridad empresarial y se mantengan en el tiempo de una forma segura permitiéndoles trabajar de manera eficiente.

Dicho esto, el negocio se permitirá mantener balanceado con las prioridades de TI, donde solo se debe concentrar en proyectos futuros y la posible actualización o mantenimiento.

Mantener un análisis de posibles mejoras permite que el Departamento de TI se vuelva más responsable con los resultados de TI y los arquitectos de TI deben de ser capaces de prosperar con sus proyectos dentro de las restricciones, presupuesto, cronogramas y hasta escasez de habilidades.

Capítulo 6. Conclusiones y recomendaciones

6.1 Conclusiones

Actualmente, la confianza cero no es más que una filosofía en cuanto a la ciberseguridad que muy pocos están en condiciones de adoptar. Sin embargo, a medida que sigan debilitándose los perímetros de seguridad, la necesidad de implementarla será cada vez más frecuente. Los ciberdelincuentes no dejan de innovar, y las defensas tienen dificultades para seguirles el ritmo. El modelo de confianza cero representa una forma de minimizar realmente las amenazas al tiempo que se establecen nuevos estándares en los protocolos de ciberseguridad.

Aunque cada vez existe mayor demanda, la seguridad de la información sigue siendo un terreno por explorar, y en la que todavía no existen una gran diversidad de especialistas en el tema, al contrario, es un campo limitado.

Es probable que en el futuro esto cambie y que se convierta en un área cada vez más importante para el sector empresarial, sin embargo, a día de hoy, representa un reto y problema.

Existen muchas amenazas que enfrentan las empresas, y sin duda esta es una de ellas, más aún si consideramos el rumbo hacia la digitalización que está tomando el mundo y la cada vez más preponderante influencia de las tecnologías de la información.

Esto es más importante aún para las personas que aspiran o poseen un puesto directivo en las empresas, ya que deben estar atentos y pendientes ante este tipo de problemas.

Las amenazas nos se limitan al acceso a los sistemas de la empresa, existen muchas formas en que es vulnerable la información de la empresa.

Desde la información que se comparte a través de plataformas de mensajería, los ataques a la privacidad en espacios de trabajo, hasta simplemente las personas a nuestro alrededor que pueden escuchar cierta información que no debían.

Son muchas las amenazas, así como la necesidad de atenderlas. Por eso es importante la implementación de protocolos y reglamentaciones que prevengan la filtración; pero que también blinden y protejan a las empresas en caso de que sucedan agresiones a su seguridad.

A nadie le gusta sentir el miedo de ser vulnerable, y por eso es importante que la amenaza que representa la seguridad de la información sea atendida de manera eficiente y consistente, pero invisible para los usuarios y los clientes, para evitar levantar alarmas.

Conocer e implementar medidas de seguridad de la información permitirá ofrecer tranquilidad a los usuarios acerca de los datos que ellos mismos proporcionan, ofrece seguridad al interior y da certeza de que los procesos no tendrán problema con la información para funcionar adecuadamente.

6.2 Recomendaciones

Las siguientes recomendaciones pueden ser utilizadas para abordar las arquitecturas de cero confianza e implementarse en las organizaciones según su arquitecto.

Puede ser que muchos usuarios y empresas ya sean conscientes de las amenazas de seguridad que existen hoy en día, sin embargo, es necesaria una mayor concientización de los riesgos que pueden derivarse desde todas las aristas de posibles ataques a la organización, llámese redes, dispositivos finales, usuarios, servidores, aplicaciones, etc.

- Las empresas y sus funcionarios deben saber de forma anticipada que es una arquitectura de cero confianza. Se debe investigar los fabricantes y qué funcionalidades posee cada producto. Ya que existen muchos en el mercado y no todos ofrecen la misma gama de seguridad.
- La adopción a principios de cero confianza, puede ser frustrante para el usuario final al punto que puede optar por rechazarla. Para ello una política de información y de conocimiento hacia el usuario final puede ser importante para el éxito de una implementación de este tipo de soluciones.
- Todas las arquitecturas revisadas por los fabricantes tienen funciones similares y son atacadas bajo un mismo principio. Se recomienda analizarlas y ver cuál herramienta es la que mejor se adapta a la organización
- Así como en muchas normas no existe la receta con la mejor práctica, en arquitectura de cero confianza sucede que cada fabricante en base a los mismos principios utiliza su mejor práctica.

- Se recomienda hacer el uso de esta guía o marco de referencia para el desarrollo de una herramienta para el desarrollo de una arquitectura basa en principios de cero confianza, modernizando los accesos y visualizando todo el ciclo de vida del proyecto y vinculado con los objetivos o propósitos estratégicos de la organización relacionado al acceso de la información sensible del negocio.

Referencias bibliográficas

- UNICEF. (2021). Alfabetización digital en Costa Rica.
  - https://www.unicef.org/costarica/comunicados-prensa/alfabetizacion-digital-para-garantizar-el-presente-y-el-futuro-de-la-generacion

- Presidencia de Costa Rica (2019). Teletrabajo en Costa Rica.
  - https://www.presidencia.go.cr/comunicados/2019/09/teletrabajo-es-ley-de-la-republica/
- Procuraduría General de la República de Costa Rica. (20199. Decreto ejecutivo 42083.
  - http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=90342&nValor3=118927&strTipM=TC
- MICIT. (2021). Estrategia de transformación digital de Costa Rica 2018-2022.
  - https://www.micit.go.cr/sites/default/files/estrategia-tdhcrb.pdf
- La República. (2021). Costa Rica escala en índice de ciberseguridad.
  - https://www.larepublica.net/noticia/costa-rica-escalo-39-puestos-en-indice-global-de-ciberseguridad
- ITU. (2020). Global Cybersecurity Index 2020.
  - https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020
- IBM. (2021). Data Breach
  - https://www.ibm.com/security/data-breach
- Security Intelligence. (2020). Cost of a data breach report.
  - https://securityintelligence.com/posts/whats-new-2020-cost-of-a-data-breach-report/
- Palo Alto Networks. (2021). What is a zero trust architecture.
  - https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture
- National Institute of Standards and Technology. (2021). Zero Trust Architecture 800-207.
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
- Zscaler. (2020). What is zero trust?
  - https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust
- Microsoft. (2021). Zero trust adoption Report.
  - https://www.microsoft.com/en-ww/security/business/zero-trust
- Cloudflare. (2021). What is a zero trust network.

- https://www.cloudflare.com/en-ca/learning/security/glossary/what-is-zero-trust/
- Gartner. (2017). Zero trust vendors.
- https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/Qi-An-Xin/Qi-An-Xin-1-1OKONUN2.pdf
- Kindervag, J. (2010). Build security into your network's dna: The zero trust network architecture. Forrester Research Inc, 1-26.
- http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf
- Rose, S. W., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture.
- https://www.nist.gov/publications/zero-trust-architecture?TB_iframe=true&width=921.6&height=921.6

Apéndices

Anexo 1. Tabla de riesgos, vulnerabilidades y amenazas

ID	Riesgo	Vulnerabilidad	Amenaza	Probabilidad	Impacto	Severidad	Controles	Probabilidad	Impacto	Severidad
1	Robo de información de clientes.	Falta de controles de seguridad.	*Hacker*	2	3	8	*Firewall*	1	3	7
2	Falla en ERP.	Falta de actualización de antivirus.	Virus	2	3	8	EDR/XDR/EPP	1	3	7
3	Fallas de *hardware.*	Falta de sistemas de respaldo.	Corto circuito	2	2	6	UPS	1	2	5
4	Falla del CRM.	Falta de controles de seguridad.	Injección de SQL	3	3	9	WAF	1	3	7
5	No entrega de *productions* a clientes.	Inventario.	Proveedor	2	2	6	SLA	1	2	5
6	Falla del servicio de correo.	Caída de plataforma tercerizada.	Proveedor	1	3	7	SLA	1	3	7
7	Falla sistema relaciones con clientes.	Servicios de nube no disponible.	Proveedor	1	3	7	SLA	1	3	7
8	Caída de servicio de internet.	Falla de enlaces empresa.	Proveedor	2	3	8	*Redundancy*/SLA	1	3	7
9	Incapacidad usuario conectarse desde casa.	Falla de enlaces doméstico.	Proveedor	3	1	5	Ir a Oficina	2	1	4
10						0				0