Universidad de Valladolid

Escuela de Ingeniería Informática

TRABAJO FIN DE GRADO

Grado en Ingeniería Informática
Mención en Tecnologías de la Información

Zero Trust como Concepto de Seguridad

Autor: Gabriel Pérez Pérez

Universidad de Valladolid

Escuela de Ingeniería Informática

TRABAJO FIN DE GRADO

Grado en Ingeniería Informática
Mención en Tecnologías de la Información

Zero Trust como Concepto de Seguridad

Autor: Gabriel Pérez Pérez

Tutor: Valentín Cardeñoso Payo

Agradecimientos

En esta sección quiero aprovechar para agradecer la ayuda a todas las personas que me han ayudado en mayor o menor medida a poder finalizar este proyecto y con ello mi vida universitaria. En primer lugar a Gonzalo Perán, que fue uno de los precursores de la idea de hacer un proyecto de fin de grado estudiando en profundidad Zero Trust. Por otro lado, me gustaría agradecer el apoyo técnico a Darell Pérez y a Joan Regidor, dos técnicos de seguridad de altísimo nivel y que me han ayudado en más de un punto a lo largo del desarrollo. Por último, me gustaría agradecer a Valentín Cardeñoso varias cosas, y la primera es el haber sido tan flexible en la elección del tema del trabajo y en el desarrollo de este. Me ha guiado durante el camino pero también me ha dejado libre para que fuera yo quien explorara las opciones que tenía ante mi y pudiera ver si eran realmente válidas o no. Con un poco de ayuda de cada uno de ellos he podido terminar con éxito uno de los desafíos más grandes que he tenido en mi vida. Gracias.

Resumen

Para muchos, *Zero Trust* viene a solucionar gran parte de las grietas que tienen los modelos de seguridad informática actuales. Dando un nuevo enfoque y con políticas más estrictas, *Zero Trust* viene a revolucionar el mercado, o al menos así es como se está vendiendo actualmente. Desde aquí, haremos un repaso de manera estructurada al concepto en sí mismo, para estar seguros de como está planteado, y a todo lo que gira en torno a él, de la mano de las grandes tecnológicas y consultoras del mundo, para asegurarnos de si es tan potente como parece.

La primera cuestión que se va a plantear es qué es Zero Trust, puesto que hay quienes lo consideran una arquitectura, otros lo consideran un modelo de seguridad, y para muchos, es simplemente un concepto. A partir de ahí, se irán resolviendo las dudas y explicando cada uno de los conceptos que vayan apareciendo para terminar resolviendo la duda ya planteada *¿Qué es Zero Trust?*, y la que es aun más difícil que la primera, *¿Realmente Zero Trust va a revolucionar la seguridad informática?*.

Abstract

For many, *Zero Trust* comes to solve many of the cracks in the current information security models. With a new approach and stricter policies, *Zero Trust* will revolutionize the market, or at least that is how it is currently being sold. From here, we will make a structured review of the concept itself, and everything that revolves around it, from the hand of the major technology and consulting firms in the world to make sure if it is as powerful as it seems.

The first question that will be asked is what Zero Trust is, since there are those who consider it an architecture, others consider it a security model, and for many, it is simply a concept. From there, the doubts will be solved and each of the concepts that appear will be explained to end up solving the doubt already raised, *What is Zero Trust"*, and the one that is even more difficult than the first, *Is Zero Trust really going to revolutionize computer security?*.

Índice general

Índice de cuadros

Índice de figuras

Capítulo 1

Introducción

1.1 Introducción

En los últimos años, dentro de mundo de la seguridad informática hay un término que resuena más alto que el resto, un término que parece ser una nueva revolución y que viene a resolver muchos de los problemas que parecen tener las arquitecturas y modelos de seguridad actuales. Este término no es otro que *Zero Trust*.

En la práctica Zero Trust no es tan moderno como parece, y por mucho que se haya puesto de moda en los últimos años, sus orígenes reales se remontan a abril de 1994 cuando Stephen Paul Marsh[1] en su tesis doctoral [21] introduce este término, redefiniendo el concepto de confianza y dando una primera pincelada de lo que hoy se conoce como Zero Trust. A grandes rasgos, Stephen proponía que Zero Trust consiste en eliminar la confianza que se tiene por defecto en los usuarios de la red y define ésta como algo finito y sujeto a funciones matemáticas.

Desde esa primera mención, tuvieron que pasar más de 10 años para que Google hiciera una primera implementación en el año 2009 y un año más para que Zero Trust tuviera el que para muchos es su nacimiento, el momento en el que Jhon Kindervag[2] introduce ese concepto. A partir de ahí y en especial en los últimos años, Zero Trust ha crecido como la espuma, mostrándonos su potencial real pero sembrando a su vez una gran cantidad de dudas. En *Zero Trust Architecture* [1] el NIST[3] si que arroja gran cantidad de luz al problema, sobre todo en el momento en el que diferencia el concepto de *Zero Trust* de la *Zero Trust Architecture* dando dos definiciones que veremos más adelante. Además de esas dos importantes definiciones, dicho documento proporciona una gran cantidad de información sobre cómo implementar Zero Trust de manera práctica e incluso aporta algún ejemplo de cómo or-

[1] Stephen Paul Marsh trabajó como consejero nacional para el gobierno de Canadá y actualmente es profesor asociado de seguridad de sistemas en el Instituto tecnológico de Ontario, Canadá.

[2] Jhon Kindervag fue durante más de 8 años y medio investigador principal de Forrester Research, donde además también fue vicepresidente. Actualmente es CTO de PaloAlto Networks.

[3] El NIST, o NAtional Institute of Standards and Technology, es un organismo perteneciente al gobierno de los Estados Unidos que se encarga de generar estándares tecnológicos y publicarlos.

ganizar la arquitectura completa. Sin embargo, no vamos a quedarnos ahí y vamos a intentar ampliar esa información con los informes y artículos de las principales empresas de tecnología y consultoría del mundo para ver si nos pueden dar más información o si, incluso, hay algo de información contradictoria.

Dado el crecimiento y la transformación que están sufriendo las empresas, que cada vez son más dependientes de las Tecnologías de la Información, es necesario que la seguridad evolucione a la par. Con los modelos de negocio vistos hasta principios de los 2000, el modelo de seguridad perimetral seguía funcionando suficientemente bien, puesto que los límites de la red corporativa estaban relativamente claros puesto que muchas veces dependían de los propios dispositivos físicos. Hoy en día con la deslocalización, el teletrabajo y la gran cantidad de dispositivos móviles que se tienen, esa red es más compleja, llegando incluso a terminar en tu bolsillo.

Es por eso que se plantea un nuevo concepto o principio que debe cubrir esas nuevas necesidades y que esté preparado no sólo para la actualidad, sino para el futuro, con cada vez más servicios en cloud y el IoT[4] cada vez más de moda. Estas nuevas formas de hacer uso de la red traen nuevos desafíos tanto de conectividad como de seguridad y debemos estar preparados para evitar perder los miles de millones de dólares que se pierden cada año por los ataques informáticos. Esta cifra, concretamente, oscila entre los 375 y los 575 miles de millones de dólares según un estudio de CSIS y McAfee en 2014 [22].

Dada la precisión que requiere un documento de este tipo, tras la introducción se va a hacer un repaso de lo que es una arquitectura de seguridad, un modelo de seguridad, y qué ejemplos podemos encontrar en la actualidad de ambos términos. A continuación, se empecerá a hablar específicamente de Zero Trust, pudiendo hacer comparaciones con los modelos y arquitecturas vistos, facilitando así el flujo de información, para finalizar con un apartado dedicado a la implementación de Zero Trust en un entorno real, con los pasos a seguir, los principios que requiere y con una serie de ejemplos reales de cómo hoy en día las empresas aplican Zero Trust a las diferentes ramas de la informática, que como veremos, tienen diferencias significativas.

1.2 Motivación

Durante el último curso de mi grado en Ingeniería Informática, surgió la necesidad de decidir, dentro de los conocimientos adquiridos, a qué rama de la informática me quería dedicar. No fue una decisión fácil, pero con un poco de inspiración vi rápidamente que me quería dedicar a la seguridad informática. Y una vez dentro, la decisión de comenzar a adquirir conocimientos de *Blue Team*[5] fue bastante sencilla por diferentes motivos. Una vez en ese punto, y por recomendación de un amigo, leí

[4]El *Internet of Things* o Internet de las Cosas en español, es la agrupación e interconexión de dispositivos y objetos a través de una red (bien sea privada o Internet, la red de redes), dónde todos ellos podrían ser visibles e interaccionar. Respecto al tipo de objetos o dispositivos, podrían ser cualquiera, desde sensores y dispositivos mecánicos hasta objetos cotidianos como pueden ser el frigorífico, el calzado o la ropa.

[5]Dentro de la seguridad informática, se conoce como el *Blue Team* al grupo de gente que se dedica a investigar, desarrollar e implementar medidas defensivas para los sistemas y organizaciones.

por primera vez en el término Zero Trust en un artículo[28] de Xataka[6] que es un portal que suelo consultar de manera asidua. En él, hablaban, a grandes rasgos, de cómo las grandes tecnológicas del mundo estaban adoptando Zero Trust para mejorar su seguridad corporativa, y de que Zero Trust plantea como uno de los principales vectores para proveer seguridad a una red. Ese artículo me dejó con más dudas que respuestas, pero desató la curiosidad para empezar un TFG de este estilo.

Tras una muy breve investigación, vi que Zero Trust tenía conceptos muy interesantes, pero no terminaba de entender qué era y cómo funcionaba. La información era difusa y a veces un poco contradictoria. Por eso, y tras comentarlo con mi tutor y con profesionales del sector, decidí comenzar un TFG como este, puramente teórico, con la firme intención de entender que propone Zero Trust y lo más importante, como aplicar esos principios a una organización real de manera que mejore la seguridad de manera eficiente, barata y efectiva.

1.3 Objetivos

El objetivo de este documento es responder a todas las preguntas que me surgieron durante la investigación previa a la realización del TFG, entendiendo si Zero Trust es tan potente como se anuncia y si funciona para los diferentes campos de la seguridad informática. Averiguar si realmente lo que propone Zero Trust va a ser la próxima revolución en la seguridad informática y su adopción va a ser masiva en los próximos años. Además, complementará mi formación laboral como ingeniero de seguridad mejorando mis conceptos básicos de arquitectura de seguridad y de como esta se implementa en entornos empresariales, no solo desde el punto de vista técnico, sino también desde un punto de vista práctico.

Por último, se propondrá un caso de aplicación real con el propósito de ver las dificultades que tiene un despliegue de seguridad de tipo Zero Trust, para poder ver los desafíos reales, y hasta qué punto se puede implementar con garantías un cambio tan grande en la estructura de red y de seguridad de una empresa que ya está en funcionamiento.

1.3.1 Planificación

A continuación, se muestran las 3 fases principales del desarrollo del proyecto, y justo debajo la división del trabajo por semanas, a continuación, un pequeño análisis de los riesgos relevantes y, por último, una planificación presupuestaria.

1. **Documentación previa.** Lectura y documentación de material para empezar a generar la estructura del documento. Recopilación de documentación para el desarrollo de las diferentes secciones de este. 4 julio - 15 agosto

2. **Redacción teórica.** Desarrollo de los primeros capítulos de documento que son de carácter teórico y que deben servir de base para la implementación práctica. 15 agosto - 15 de octubre

[6]Xataka es una web español de noticias tecnológicas, fundada en 2004, que trata de llevar la tecnología a todos los públicos.

3. **Propuesta de implementación de un plan de seguridad.** Generación de un caso de estudio ficticio pero lo más aproximado a la realidad que sea posible. 15 de octubre - 1 de diciembre

La división del trabajo por semanas se puede ver en el cuadro 1.1. Es complicado realizar una planificación tan precisa a largo plazo, pero es una buena orientación de lo que considero como un correcto desarrollo del trabajo.

Semana	Fecha	Descripción
1-4	04/07-31/07	Búsqueda de enlaces y documentación
5-6	01/08-14/08	Resumen documental y estructuración del documento.
7-8	15/08-28/08	Capítulos 1 y 2
9-11	29/08-11/09	Capítulos 3 y 4
12-14	12/09-09/10	Capítulo 5
15-16	10/10-23/10	Propuesta del caso de estudio
17-21	24/10-27/11	Capítulo 6
22	28/11-04/12	Revisión Final

Cuadro 1.1: Desarrollo del proyecto por semanas

1.3.2 Riesgos

Puesto que se trata de un desarrollo teórico prácticamente en su totalidad, el riesgo principal son los retrasos por causas personales o de salud, aunque no son los únicos.

- **Retrasos por causas personales.** Es posible que durante los aproximadamente 6 meses del desarrollo del proyecto pueda haber lesiones o enfermedades que ralenticen el desarrollo del proyecto. Por otro lado, los problemas familiares o personales por causas ajenas a la salud también son un riesgo, aunque menos probable.

- **Retrasos por causas laborales.** La totalidad del proyecto se va a llevar a cabo durante el periodo de prácticas curriculares en empresa y posteriormente durante el desarrollo del trabajo ya en el mercado laboral. La falta de tiempo puede ser un riesgo realmente importante en este aspecto.

- **Retrasos en el asesoramiento.** Por un lado, parte del proyecto se va a llevar a cabo en verano, que es un periodo complejo para poder cuadrar sesiones y tutorías universitarias. Por otro lado, parte del asesoramiento se va a llevar a cabo por profesionales que están trabajando en empresas y que pueden no ser fácilmente accesibles. Será necesario disponer de amplios márgenes para la consulta de dudas.

1.3.3 Presupuesto

Por último, vamos a hablar del gasto previsto/supuesto para el desarrollo del proyecto. En primer lugar, en cuanto a gasto de material lo único destacable es la necesidad de un ordenador, con conexión a internet y su respectiva alimentación eléctrica. Estos gastos son difícilmente cuantificables porque en

el caso del ordenador, no ha habido uno específicamente utilizado para el desarrollo del proyecto; de igual manera ocurre con la conexión a internet, que es utilizada con otros fines. Sí es más fácilmente cuantificable el gasto eléctrico. Según un medidor de potencia del que dispongo, mi ordenador bajo una carga de trabajo normal consume 180W, o lo que es lo mismo 0,18KwH por cada hora que pase encendido. Si aproximadamente se han utilizado 300 horas que es lo que curricularmente se estipula para el desarrollo de un proyecto de este tipo, sale un total de 54 KWH. Con un precio promedio de 0,24 céntimos el KWh, se ha generado un gasto de 13€ en electricidad.

Por otro lado, el gasto personal, que también se calculará en base a las 300 horas empleadas. Vamos a suponer un precio por hora de trabajo de un becario de 4,5€, lo que genera un gasto de 1350€. Esto no sería realmente así, puesto que 100 de las horas se han realizado siendo becario, y 200 siendo ingeniero junior (técnico de nivel 1) con un precio por hora bastante superior, aunque dejaremos un precio final de 1.350€ para no complicar los cálculos.

No han sido necesarias licencias ni ningún material adicional, por lo que podemos cerrar el gasto del desarrollo del proyecto en 1.363€.

Capítulo 2

Modelos de Seguridad

Este es el primero de los dos términos importantes que van a ser analizados como preparación antes de entrar de lleno en Zero Trust. Habiendo hecho una investigación previa puedo saber que un modelo de seguridad es algo más específico que una arquitectura, por lo que empezaremos por aquí. Vamos a hacer un análisis de artículos y publicaciones de fuentes consideradas fiables para poder conformar nuestra propia definición de *Modelo de Seguridad*, que a partir de ese momento y en adelante, será la que se tome como definición de referencia. El capítulo terminará con una breve explicación de algunos modelos de seguridad utilizados en la actualidad para hacernos una idea clara de que opciones hay en el mercado antes de pasar a Zero Trust.

2.1 Definición de Modelo de Seguridad

La información al respecto no siempre es clara, por eso para dar respuesta a la pregunta vamos a apoyarnos en varias fuentes para ir cogiendo de cada una la información más relevante. Para responder esta pregunta vamos a proponer 5 definiciones de 5 fuentes diferentes, vamos a analizarlas por separado y por último, vamos a proponer una definición propia que recoja lo mejor de cada una. Las definiciones que no estén en español serán directamente traducidas.

1. **IGI-Global**[14]. Un modelo de seguridad es un modelo informático que se utiliza para identificar e imponer políticas de seguridad. No requiere ninguna formación previa, puede basarse en el modelo de derecho de acceso o en el modelo de distribución de la informática o del cálculo.

2. **IGI-Global**[14]. Un modelo de seguridad es un "sistema formalütilizado para especificar y razonar sobre la política de seguridad. Está destinado a abstraer la política de seguridad y manejar su complejidad; representar los estados seguros de un sistema, así como la forma en que el sistema puede evolucionar, verificar la coherencia de la política de seguridad y detectar y resolver posibles conflictos.

3. **Wikipedia**[5]. Un modelo de seguridad informática es un esquema para especificar y aplicar políticas de seguridad. Puede basarse en un modelo formal de derechos de acceso, en un modelo

de computación, en un modelo de computación distribuida o en ninguna base teórica en particular. Un modelo de seguridad informática se aplica a través de una política de seguridad informática.

4. **Pearson Certifications**[11]. Los modelos de control de seguridad se utilizan para determinar cómo se aplicará la seguridad, qué sujetos pueden acceder al sistema y a qué objetos tendrán acceso, es decir, son una forma de formalizar la política de seguridad. Los modelos de control de la seguridad suelen aplicarse aplicando controles de integridad, confidencialidad u otros.

5. **QuickStart**[26]. Un modelo de seguridad define los aspectos esenciales de la seguridad y su relación con el rendimiento del sistema operativo, proporcionando el nivel de comprensión necesario para una implementación exitosa y eficaz de los requisitos clave de protección. Los modelos de seguridad de la información son los procedimientos utilizados para validar las políticas de seguridad, ya que se proyectan para ofrecer un conjunto preciso de instrucciones que un ordenador puede seguir para aplicar los procesos, procedimientos y conceptos vitales de seguridad contenidos en un programa de seguridad.

Todas las definiciones tienen parecidos y diferencias, de manera que para empezar vamos a comparar los diferentes comienzos que tienen las 3 primeras definiciones. Tres definiciones que proponen, que un modelo de seguridad es tres cosas diferentes. Por un lado, un *modelo informático*, por otro un *sistema formal* y por último un *esquema*. Las tres propuestas hablan de cosas similares, pero como vemos no hay una definición cerrada. Por ello, no vamos a centrarnos en qué es un modelo de seguridad, si no en qué aporta, donde ya si vamos a empezar a ver más parecidos entre las definiciones.

El término que se repite en las 5 definiciones es *Políticas de Seguridad*, por lo que vamos a empezar por ahí. Como definición simple y concisa de qué es una política de seguridad podemos encontrar *Una política de seguridad es un documento que especifica como una organización planea proteger sus activos de las amenazas, tanto internas como externas, manteniendo la confidencialidad, integridad y disponibilidad de ellos, y cómo se van a afrontar las situaciones en las que ocurran ataques*[12][29][19]. Esta, es una definición propia formulada a partir de las fuentes mencionadas.

Un modelo de seguridad es, por lo tanto, y entre otras cosas, un sistema formal que se utiliza para aplicar y gestionar un conjunto de políticas de seguridad, especificando dónde y cómo estas deben ser aplicadas. Es importante hacer hincapié en que un modelo de seguridad debe forzar la aplicación de esas políticas de seguridad de manera adecuada. Podríamos entender así, que las políticas de seguridad son los requisitos que pone la organización a nivel de seguridad, y el modelo es el medio para aplicar esos requerimientos de manera adecuada.

Con el fin de complementar un poco más las definiciones encontradas, IBM como parte de su documentación oficial[8], no da una definición cerrada, pero si propone una serie de características que debe tener un modelo de seguridad, que son las siguientes:

- Debe verificar de la identidad de los usuarios, haciendo uso de sistemas de autenticación como contraseñas y otros factores.

- Permitir a los usuarios autorizados acceder a los recursos proporcionados por los sistemas de autorización. Estos, definen los procesos de autorización basándose en la solicitud y en la autenticación. Los recursos, por ejemplo, incluyen cuentas, servicios, información de usuario y aplicaciones. Un modelo de seguridad también requiere procesos adicionales de aprovisionamiento para seleccionar los recursos a los que los usuarios pueden acceder.
- Es necesario que administrar qué operaciones y permisos se conceden a las cuentas y a los usuarios.
- Un modelo de seguridad debe poder delegar actividades de un usuario a otros usuarios, en base a una solicitud o asignación.
- Proteger la información sensible, como las listas de usuarios, sus permisos, o los atributos de las cuentas.
- Asegurar la integridad de las comunicaciones y de los datos.

Ha sido necesario hacer ciertas modificaciones a las características, además de una traducción, para poder entender realmente lo que quieren decir. Una vez que vemos esas características, ya podemos por fin ver la amplitud del término *Modelo de Seguridad*, puesto que vemos qué debe hacer. Cada una de esas características, se lleva a cabo mediante la implementación de una o más políticas de seguridad. Por ejemplo, la verificación de identidad se llevará a cabo mediante diferentes mecanismos de autenticación aplicados en diferentes situaciones, es decir, mediante una política de autenticación de usuarios. Por lo tanto, podemos concluir que un modelo de seguridad está formado por un conjunto de políticas, este conjunto al completo proporciona las características de seguridad propias del modelo. Esto es así, puesto que de manera independiente no se puede aplicar una política de seguridad y considerar que se está generando seguridad.

2.1.1 Definición propia de modelo de seguridad

Para poder formular una definición completa, vamos no solo a hablar de qué es un modelo de seguridad, si no de qué funciones debe de cumplir, ayudándonos de la documentación de IBM mencionada. Empezando por el *Qué*, ya hemos visto que un modelo de seguridad parece ser muchas cosas. Personalmente no considero que sea un esquema como se propone en la Wikipedia, si no algo más específico. Se encarga de aplicar y controlar las políticas por lo que es más correcto decir que es, por ejemplo, un método, o un conjunto de instrucciones, que permite aplicar políticas de seguridad. Habiendo visto la información de la documentación de IBM, es interesante añadir a la definición ciertas características que debemos encontrar en un modelo de seguridad, por ejemplo, la gestión de usuarios y de accesos. Reuniendo todo esto podemos dar una definición para modelo de seguridad que es la siguiente:

Un modelo de seguridad es un sistema formal que se utiliza para aplicar y gestionar un conjunto concreto de políticas de seguridad, especificando dónde y cómo estas deben ser aplicadas de manera que se cumplan los requisitos de seguridad impuestos. Puede estar basado en otros modelos más genéricos, pero debe proporcionar el nivel de comprensión suficiente para poder gestionar la identidad

de los usuarios, autorizar los accesos, proteger la información sensible y asegurar la integridad de las comunicaciones.

2.2 Variantes de modelos de seguridad

En esta sección vamos a ver 3 modelos de seguridad existentes en la actualidad, de manera que podamos tener una base teórica suficiente para comparar cuando entre en escena Zero Trust. Por el momento, no serán introducidos conceptos ni comparaciones con Zero Trust, y los modelos de seguridad serán analizados de manera independiente a lo que será visto en próximos capítulos. Por otro lado, se evaluará la precisión de la definición propuesta en el apartado anterior para cada uno de los modelos vistos, con el fin de comprobar la rigurosidad de esta.

2.2.1 Modelo Bell-LaPadula

Este modelo recibe su nombre por sus creadores David Elliot Bell y Leonard LaPadula y fue creado en los años 70. Es utilizado mayoritariamente en entornos gubernamentales o militares, y pretende resolver los problemas relacionados con la protección de la información y se centra en controlar el acceso a esta (confidencialidad). Esto se consigue dividiendo el permiso de acceso de los sujetos a los objetos en función de etiquetas de seguridad.

Este modelo tiene 3 elementos principales.

- **Objetos.** Estos son aquellos elementos que actúan de forma pasiva al realizar un acceso. Pueden ser archivos, aplicaciones, maquinas o cualquier otro elemento que pueda ser accedido, como una base de datos, o el perfil de un usuario registrado en el sistema. Para ajustarnos más al modelo con el que estamos trabajando, un objeto es aquello a lo que se le pueda asignar una etiqueta de seguridad, las cuales veremos a continuación.
- **Sujetos.** Dentro del modelo Bell-LaPadula, un sujeto es todo aquello que tenga un determinado nivel de autorización dentro de la organización. Pueden ser usuarios o procesos, pero estos últimos hay que tratarlos con cuidado. Un proceso, cuando intenta acceder a un elemento es un sujeto, y por lo tanto deberá tener un determinado nivel de autorización, similar a un proceso ejecutado como administrador en Windows. A su vez, cuando el proceso es accedido por otro sujeto, entonces pasa a ser objeto, con su correspondiente etiqueta de seguridad.
- **Operaciones de Acceso.** Recoge las acciones que los sujetos pueden realizar sobre los objetos, y hay 4 dentro de este modelo
  - **Solo lectura.** Permite a un sujeto leer la información de un objeto.
  - **Añadir.** Permite a un sujeto añadir o modificar la información de un objeto, pero sin leer lo que hay en él.
  - **Ejecutar.** Permite a un sujeto ejecutar un objeto, pero no leer ni escribir información en él.

- **Lectura y escritura.** Permite a un sujeto leer y escribir en un objeto.

Además de estos tres elementos y como se ha comentado, la otra parte fundamental del modelo son las etiquetas que clasifican a los objetos y a los sujetos, que son Alto Secreto, Secreto, Confidencial y Desclasificado, siendo Alto Secreto el nivel más restrictivo. Como se puede ver es un modelo centrado principalmente en la confidencialidad, por lo que tiene ciertas carencias para lograr la seguridad. Tiene dos principios sobre los que se fundamenta la estructura de accesos, que son los siguientes:

- **Read Down.** El primer objetivo del modelo de seguridad de Bell-La Padula es evitar que los usuarios accedan a información por encima de su habilitación de seguridad. En otras palabras, un usuario con acceso Çlasificado"(una habilitación de bajo nivel) no debería poder leer los archivos marcados como .Alto Secreto"(un nivel más alto de secreto), pero alguien con .Acceso Alto Secreto"sí. Esto se denominó *Propiedad de Seguridad Simple* puesto que en muchos casos no es suficiente para garantizar la seguridad. Por otro lado, y puesto que solo se pueden leer objetos con clasificación igual o inferior a la del sujeto, se denomino a esta propiedad *Read Down* o en español *Leer hacia abajo*.

- **Write Up.** Por otro lado, los desarrolladores se dieron cuenta un problema en la Propiedad de Seguridad Simple, puesto que a la hora de proteger un documento con clasificación por ejemplo Alto Secreto, nada impedía a un usuario o proceso con esa clasificación filtrar información a niveles inferiores leyéndola y pegándola en un documento con clasificación inferior. Por esto se decidió que un usuario no puede escribir ni generar documentos con una clasificación inferior a la suya. Esto se denominó principio de *Write Up* o en español *Escribir hacia arriba*.

Comparando directamente lo visto aquí con nuestra definición de Modelo de Seguridad, vemos que cumple, pero solo en parte. Es un sistema formal, que se utiliza para la implementación de políticas de seguridad. Especifica estas políticas e indica además que son un grupo cerrado por lo que no podrán ser añadidas ninguna más. Sí proporciona un nivel de comprensión suficiente sobre su funcionamiento y sobre la gestión de permisos que hace, pero no cumple con la mayoría de los requisitos que impone IBM para poder considerar a un Modelo de Seguridad como tal. Además de que solo se centra en uno de los 3 aspectos básicos de la seguridad de la información. Podemos decir por lo tanto que cumple a medias la definición.

2.2.2 Modelo Biba

El modelo de integridad Biba[33] fue desarrolla en 1975 por Kenneth J. Biba, que se centra como su propio nombre indica en la integridad de los datos. Es un sistema formal de transición de estados diseñado para expresar un conjunto de reglas de control de acceso con el fin de garantizar la integridad de los datos. Los datos y los sujetos se ordenan por sus niveles de integridad en grupos, y el modelo está diseñado para que un sujeto no pueda corromper los datos de un nivel superior al del sujeto y para restringir la corrupción de los datos de un nivel inferior al del sujeto.

Vamos a recordar brevemente cuales son los objetivos de la integridad de los datos para ver así cuales son los objetivos de este modelo:

- Evitar que los datos sean modificados por fuentes no autorizadas.
- Mantener el estado de los datos, desde que se almacenan hasta que se accede a ellos.
- Recuperar los datos una vez que estos han sido corrompidos.

Biba también estipula unos principios básicos de funcionamiento que son tres:

1. El *Principio Simple de la Integridad* propone que un usuario con un determinado nivel de integridad no pueda leer datos de un nivel de integridad inferior. Esto se hace para asegurar que una persona que se considera integra a nivel de seguridad, lo sigue siendo, evitando que la lectura de archivos potencialmente no íntegros haga disminuir su nivel de integridad. Esto se conoce como *No Read Down.*
2. El ** Principio de Seguridad* propone que un sujeto con un determinado nivel de integridad no escribe datos en un nivel de integridad superior. Esto tiene mucho sentido si lo que queremos es asegurar que la información que lee un sujeto con un determinado nivel de seguridad tiene al menos un nivel de integridad igual al suyo. Esto se conoce como *No Wirte Up.*
3. La **Propiedad de invocación**, estipula que un sujeto no puede invocar un proceso y solicitar un objeto de un nivel superior de integridad.

Como se puede ver, el modelo de integridad Biba se parece bastante al modelo Bell LaPadula, y esto es porque Biba se publicó en Mitre un año después que Bell LaPadula. Cuando Biba se dio cuenta de que las políticas que proponía Bell Lapadula no ofrecían protección contra el caso en el que un usuario de nivel X escribe información de nivel Y cuando X era un nivel de seguridad inferior a Y. En ese momento se vio que un usuario sin la autorización suficiente podría escribir documentos altamente clasificados.

Biba eligió la dualidad matemática de las políticas de Bell LaPadula, en el que hay un conjunto de niveles de integridad, una relación entre ellos y dos reglas que, si se aplican correctamente, se ha demostrado matemáticamente que impiden que la información de cualquier nivel de integridad pase a un nivel de integridad superior. Esto es muy interesante, porque propone una manera de comprobar a nivel teórico la fiabilidad del modelo que se propone. Los niveles de integridad típicos son "no fiable", "ligeramente fiable", "fiable", "muy fiablez "tan fiable que no necesitamos un nivel de confianza superior", etc.

Una robustez tan grande trae consigo problemas, como la dificultad para implementar este modelo en un sistema compartido moderno con diferentes tipos de usuarios, o por los problemas de usabilidad que conlleva aplicar tantas restricciones.

Vamos, por último, a analizar si se cumple o no con la definición propuesta. Al igual que el modelo Bell LaPadula, solo se centra en uno de los aspectos de la seguridad de la información. De la misma manera, también es un sistema formal que aplica un conjunto cerrado de políticas y que proporciona un nivel suficiente de comprensión. Por otro lado, demuestra de manera matemática la ausencia de

grietas en el modelo por lo que añade un plus de rigurosidad. Sin embargo, tampoco cumple con las características mencionadas por IBM. Incluso se queda corto cumpliendo el principio de integridad, puesto que solo propone medidas activas, pero ninguna reactiva, es decir, en caso de que se quisiera comprobar de manera efectiva si la integridad ha sido corrompida no se podría; por no hablar de que no hay ningún mecanismo para recuperar datos en caso de que estos se vean corrompidos. Podemos decir de nuevo, que cumple a medias la definición propuesta.

2.2.3 Modelo Clark Wilson

El modelo Clark-Wilson se considera un modelo de integridad, más que un modelo de seguridad como tal, y provee fundamentos para especificar y analizar una política de integridad para un sistema informático. Apareció por primera vez en 1987 en un *paper*[1] llamado *Comparision of Commercial and Military Computer Security Policies*, obra de David D. Clark y David R. Wilson. El documento desarrolla el modelo como una forma de formalizar la noción de integridad de la información, al compararlo con los requerimientos del *Sistema de Seguridad Multinivel*, o por sus siglas en inglés, MLS, descrito en el *Orange Book*[6].

La integridad de la información se mantiene impidiendo la corrupción de los datos en un sistema, debido a un error o a una intención maliciosa. Esto se logra mediante políticas de integridad. Una política de integridad describe cómo los elementos del sistema deben mantenerse íntegros entre un estado del sistema y el siguiente. El modelo utiliza etiquetas de seguridad para conceder acceso a los objetos mediante procedimientos de transformación y un modelo de interfaz restringido. El modelo de Clark-Wilson utiliza un enfoque polifacético para reforzar la integridad de los datos. El modelo define elementos en función de los datos y permite las modificaciones de estos a través de un pequeño conjunto de programas. El modelo utiliza una relación tripartita de sujeto/programa/objeto conocida como triple de control de acceso. Dentro de esta relación, los sujetos no tienen acceso directo a los objetos, si no que para acceder a estos lo hacen a través de programas.

Para realizar este acceso a los objetos, se proponen una serie de reglas de aplicación y certificación del modelo que definen los elementos de datos (objetos) y las políticas de integridad que son la base para la realización de las transacciones. Las transacciones son el núcleo del modelo y son cada una de las operaciones que realizan los programas que acceden a los datos. Entendemos por "transacción bien formada.[a] una serie de operaciones que hacen pasar a un sistema de un estado consistente a otro estado consistente. En este modelo, la política de integridad se ocupa de la integridad de las transacciones, y lo hace mediante el *Principio de Separación de Funciones*, que exige que el certificador de una transacción y el ejecutor sean entidades diferentes.

El modelo se basa por otro lado en dos conjuntos de reglas, las reglas de certificación (C) y las reglas de aplicación (A). Es necesario explicar 3 conceptos básicos antes de empezar. Los CDR o Con-

[1] Un *paper* o artículo científico es un trabajo de investigación o comunicación científica que sigue un proceso riguroso y que publicado en alguna revista especializada. También se le llama documento científico, o simplemente artículo o publicación.

junto de Datos Restringidos, son los elementos básicos dentro del modelo Clark-Wilson y son cada uno de los elementos accesibles en el sistema. Un PVI o Proceso de Verificación de la Integridad, es un proceso que verifica que un CDR es válido, es decir, que aún conserva su integridad. Por último, los PT o Procedimientos de Transformación, convierten un conjunto de datos sin restricciones como, por ejemplo, la entrada de datos de un usuario, en un CDR, garantizando que esta conversión se hace con el mayor nivel de integridad posible.

Empezamos por las reglas de certificación.

- **C1.** Cuando un PVI se ejecuta, este debe asegurarse de que los CDR son válidos.
- **C2.** Para un conjunto de CDRs asociados, un PT debe transformar estos de un estado válido a otro. Dado que debemos asegurarnos de que estos PT están certificados para operar sobre un CDR en particular, se deben cumplir E1 y E2.
- **C3.** Las relaciones permitidas deben cumplir el Principio de Separación de Funciones, y es necesaria la autenticación de las partes implicadas para poder llevar un registro.
- **C4.** Todos los PTs deben generar un registro suficientemente preciso como para reconstruir la operación. Esto es necesario porque cuando la información entra en el sistema no tiene por qué ser de confianza ni estar restringida.
- **C5.** Cualquier PT que tome un conjunto de datos como entrada sólo podrá realizar operaciones válidas para todos los posibles valores del conjunto de datos. Sería el equivalente a asegurar que para dos números enteros que se proponen como entrada, el PT solo puede realizar operaciones definidas para el conjunto de números enteros. El PT convertir o no el conjunto de datos en un CDR.

Por otro lado, tenemos las Reglas de Aplicación:

- **E1.** El sistema debe mantener una lista de relaciones certificadas que son las únicas que pueden operar en el sistema. Además, debe asegurar que sólo los PTs que han sido autorizados para funcionar en un CDR cambian ese CDR.
- **E2.** El sistema debe asociar un usuario con cada PT y conjunto de CDRs. El PT puede acceder al CDR en nombre del usuario si este ha sido previamente autorizado.
- **E3.** El sistema debe autenticar la identidad de cada usuario que intente ejecutar un PT. Esto requiere llevar un registro de triples (usuario, PT, CDIs) llamados relaciones permitidas". Esto es un usuario, un Procedimiento de Transformación asociado, y el conjunto de datos sobre el que este puede actuar.
- **0**E4. Sólo el certificador de un PT puede cambiar la lista de entidades asociadas a ese PT. No se especifica lo que es un certificador por lo que intuyo será el administrador del sistema.

Por último, vamos a comprobar cuanto se parece a la definición de Modelo de seguridad propuesta. De los tres modelos vistos parece el más riguroso y a la vez el más flexible, con una política de comunicaciones entre elementos más detallada y con reglas como la C4, que habla de reconstruir operaciones, lo cual es algo que hasta el momento no habíamos visto. Podemos decir por lo tanto que es un sistema formal, que aplica una serie cerrada de políticas de seguridad, y definitivamente si ofrece un nivel de comprensión suficiente sobre cómo deben organizarse los sujetos, los objetos y las comunicaciones entre estos. Además, comenta por encima la gestión de usuarios, y la integridad de las comunicaciones, aunque a un nivel muy muy alto.

Capítulo 3

Arquitecturas de Seguridad

El término *Arquitectura de Seguridad* es ampliamente mencionado en entornos TI, incluso ya ha sido mencionado en este documento, por lo que entenderlo en profundidad va a conformar este quinto capítulo. Además, será necesario tener una definición rigurosa para poder después entender y catalogar Zero Trust debidamente, similar a lo visto en el capítulo anterior. Por llevar un orden, vamos a empezar desde lo más simple a lo más complejo, añadiendo por último ejemplos de arquitecturas de seguridad en uso actualmente. Un comienzo simple podría ser consultar en Google *What is a security architecture* y analizar los resultados propuestos. Esta búsqueda genera 178.000 resultados; y tras empezar por el primer resultado que se nos proporciona, saltando los anuncios, iremos refinando y sumergiéndonos en búsquedas y definiciones más complejas para ver si podemos completar esa primera definición que seguro, va a estar incompleta.

3.1 Concepto: aproximación

En mi caso el primer resultado arrojado tras la búsqueda es de *Digital* cuyo artículo se llama *What is Security Architecture, and What do you need to know?*[7]; no tiene autor y a priori no parece una fuente demasiado fiable, aunque era algo previsible. Una vez traducida del inglés, nos da una definición dice que *Una arquitectura de seguridad es un conjunto de principios, métodos y modelos de seguridad diseñados para alinearse en sus objetivos y ayudar a mantener una organización a salvo de las ciberamenazas. Una arquitectura de seguridad traduce los requisitos empresariales en requisitos de seguridad ejecutables.* Esta primera definición parece bastante rigurosa, pero analicémosla por partes. Comienza hablando de principios, métodos y modelos por lo que vamos a empezar por ahí. Como en el capítulo anterior ya hemos visto en profundidad lo que es un modelo de seguridad, vamos a pasar directamente a buscar una definición para los otros dos términos. Con el fin de ser un poco más concisos, vamos a dar directamente las definiciones más apropiadas para cada término.

- **Principio de seguridad.** Cada una de las características que debe tener un dato para considerar que está asegurado. Los principios básicos de seguridad son la *Confidencialidad*, la *Disponibilidad*

y la *Integridad*. Hay quien añade también la *Autenticidad*.

- **Principio de seguridad, 2.** Según la publicación *The Protection of Information in Computer Systems*[23] de 1975, los principios de seguridad son un conjunto de 7 características que debe de tener todo sistema informático para ser considerado seguro.

- **Método de seguridad.** Es cada uno de los procedimientos o acciones que añade seguridad a un sistema. Por ejemplo, la necesidad de contraseña de acceso es un método de seguridad, pero también lo es el doble factor de autenticación.

Aunque esta definición ha permitido el repaso de varios conceptos interesantes, no profundiza suficiente en terminología y utilidad.

Por otro lado, Minitool[1] propone como definición básica de arquitectura de seguridad [24]*"Método sistemático para mejorar la seguridad de la red y reducir los riesgos."* Esta, es una definición realmente pobre, pero habla de *"método sistemático"* lo que añade bastante valor respecto a la definición anterior. Esto quiere decir que estamos ante algo estructurado y que es replicable en múltiples organizaciones mediante un procedimiento. Por otro lado, añaden que *Una arquitectura de seguridad hace referencia a los sistemas, procesos y herramientas que se utilizan para proteger la organización y mitigar los ataques.* Esto amplía aún más el alcance de la definición, puesto que no solo consiste en trazar un plan, si no en decidir qué componentes (tanto software como hardware) van a ser utilizados en cada uno de los segmentos.

Otra posible definición es la siguiente[9]: *Una arquitectura de seguridad es un marco que especifica la estructura organizativa, los estándares, las políticas y el comportamiento funcional de una red informática junto a sus características y seguridad.* Es decir, una arquitectura es algo muy amplio que engloba prácticamente todas las partes de la estructura de información de una organización, y que se asegura de que estas estén diseñadas e implementadas siguiendo una misma dirección.

En las definiciones mencionadas hemos visto que hablan de los sistemas, procesos, herramientas, estándares, políticas, comportamiento funcional e incluso de la estructura organizativa. En ese mismo enlace, también se comenta que una arquitectura de seguridad eficaz consta de personas, procesos y herramientas. Visto esto, podemos afirmar que una arquitectura de seguridad es el conjunto de elementos lógicos y físicos que forman una red y que, además, para poder implementar con garantías una arquitectura de seguridad, la base sobre la que se monta debe también ser correcta. Esto quiere decir, que la manera en la que la empresa divide sus departamentos, organiza sus oficinas, asigna privilegios, coordina a sus empleados y distribuye los recursos es importante, y esto es algo que veremos en más detalle en la última sección del documento.

[1]Minitool es una empresa especializada en el desarrollo de software para gestión de particiones, copias de seguridad y recuperación de archivos con más de 60 millones de usuarios

Hemos visto que una arquitectura de red es todo el conjunto de cosas que hay que tener en cuenta para que una red sea segura. Abarca desde el diseño y la estructura organizativa, hasta la decisión del hardware utilizado, pasando por todas las decisiones que hay que tomar para engranar cada una de las partes. Además, es algo que tiene que ser sistemático y que debe estar documentado para que pueda ser replicado. Debe cumplir los principios básicos de seguridad y haciendo uso de tantos métodos de seguridad como sea necesario para conseguirlo. Puede englobar varios modelos de seguridad, permitiendo que cada uno se encargue de una parte de la estructura lógica de seguridad. Viendo la información recopilada podemos dar nuestra propia definición de arquitectura de seguridad, y es la siguiente:

Una arquitectura de seguridad es un procedimiento sistemático de diseño, implementación y mantenimiento de la seguridad de una red que debe estar correctamente documentado y ser replicable en un entorno que posea características similares. Debe satisfacer los principios básicos de seguridad coordinando herramientas, personas, procedimientos y estándares mediante tantos modelos y métodos de seguridad como sean necesarios para conseguir una red segura, robusta y eficiente.

3.2 Cybersecurity Mesh Architecture, CSMA

Según el analista de Gartner[2], Felix Gaehtgens, la malla de seguridad (*CyberSecurity Mesh*) se parece más a una estrategia que a una arquitectura de seguridad definida, pero lo que está claro es que el concepto alinea mejor las organizaciones con la protección frente a amenazas. *Gartner* propone esta arquitectura, pero además dice que *Las organizaciones que adopten una arquitectura de malla de ciberseguridad para integrar herramientas de seguridad para trabajar como un ecosistema cooperativo reducirán el impacto financiero de los incidentes de seguridad individuales en un promedio del 90 %.*

Ya hemos visto el concepto de MDR, o *Manage, Detection and Response*, pero *Gartner* aquí habla de XDR o *Extended Detection and Response*, que son productos que hoy en día ya están en el mercado por ejemplo de la mano de Trend Micro. Estos son una manera en la que los proveedores de seguridad pueden vincular diferentes productor a una plataforma unificada. En este caso, el XDR simplemente agrega valor a la capa de análisis de inteligencia, igual que lo hacen los SIEM, *Security Information and Event Management* o los SOAR, *Security Organization, Automation and Response*. Aquí se recomienda que la organización construya su estructura de seguridad por capas, que son las siguientes.

- **Análisis e inteligencia de ciberseguridad.** Ya hemos visto que CSMA pretende llevar a cabo una administración centralizada, lo que significa que se pueden recopilar, consolidar y analizar grandes cantidades de datos en tiempo real en una ubicación central. Esto mejora sus capacidades de análisis de riesgos, análisis de patrones, el tiempo de respuesta a amenazas y la mitigación de ataques. CSMA combina los datos y los resultados que ofrece la inteligencia de amenazas para proporcionar un análisis de amenazas mejorado y desencadenar las respuestas apropiadas.

[2]Gartner Inc. es una empresa consultora y de investigación de las tecnologías de la información con sede en Stamford, Connecticut, Estados Unidos. La empresa se concentra en la investigación, programas ejecutivos, consultas y eventos, y entre sus clientes están algunas de las más grandes empresas, agencias de gobierno, empresas tecnológicas y fondos de inversión del mundo.

- **Tejido de identidad distribuido.** Esta capa proporciona capacidades como acceso adaptable, gestión de identidad descentralizada, servicios de directorio, gestión de accesos y pruebas de identidad. La gestión de la identidad para la posterior autenticación de usuarios es un punto fundamental de toda arquitectura de seguridad.

- **Gestión Consolidada de Políticas.** CSMA puede traducir una política central, definida de manera genérica, en una configuración nativa para cada herramienta de seguridad que esté integrada, lo que garantiza que los equipos de TI puedan identificar de manera más efectiva los riesgos de cumplimiento y los problemas de configuración. Puede parecernos una capa más banal, pero el *compliance*[3] y *hardening*[4] de los sistemas, es un punto prioritario en nuestra estrategia de ciberseguridad, tan importante como la gestión de la identidad.

- **Dashboards consolidados.** CSMA ofrece una visibilidad clara del ecosistema de ciberseguridad mediante la generación de *dashboards*, lo que permite a los equipos de seguridad detectar eventos de una forma más eficientemente y desplegar las respuestas apropiadas. Es posible visualizar de manera conjunta la información de todas las fuentes de información integradas, gracias a que estas están centralizadas.

[3]El *compliance* o cumplimiento corporativo es definido por la *World Compliance Association* como "el conjunto de procedimientos y buenas prácticas adoptadas por organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control, y reacción frente a los mismos".

[4]El *hardening* consiste en el endurecimiento del sistema, con el fin de reducir y evitar las amenazas y los peligros de este.

Capítulo 4

Zero Trust. Aproximación general.

El término ya se introdujo al inicio del documento, y en este capítulo se va a hacer un repaso más profundo de lo que es Zero Trust y de si realmente supone una revolución en el mundo de la seguridad informática. Únicamente se va a abordar la parte teórica, siguiendo la información que proporcionan las mayores empresas de seguridad, tecnología y consultoría tecnológica del mundo. Por otro lado, vamos a mantener como referencia el documento *NIST Special Publication 800-207*[1] que proporciona el NIST[31] y que por el momento proporciona la mayor cantidad de precisión y rigurosidad encontrada en cuanto a Zero Trust.

Por otro lado, y habiendo dado ya una definición suficientemente específica de los términos *Arquitectura de Seguridad* y *Modelo de Seguridad* nos apoyaremos en sus definiciones y en la información encontrada para complementar la explicación de que es Zero Trust, y así de paso, ver si Zero Trust puede ser considerado una arquitectura, un modelo o ninguna de las dos cosas.

4.1 ¿Qué es Zero Trust?

Tras analizar la información encontrada la mejor respuesta que puedo dar por el momento es que Zero Trust es un **cambio de paradigma**. Principalmente Zero Trust propone eliminar la existencia de zonas seguras dentro de una red corporativa, proponiendo que toda red y todo dispositivo es vulnerable por defecto, y que por lo tanto no se debe dar por hecho la existencia de zonas totalmente seguras, o de dispositivos o usuarios totalmente confiables. Es importante tener en cuenta que esta propuesta no se debe aplicar de manera totalmente radical, incrementando los controles de seguridad hasta el infinito y eliminando por completo lo que se conoce como *Zona implícita de seguridad*, si no reduciendo esta zona segura todo lo posible, y acercándola todo lo posible al activo que se quiere proteger.

Es por esto por lo que vamos a decir que este cambio de paradigma propone eliminar parcialmente la seguridad perimetral, mejorando los controles y reduciendo el tamaño de las áreas de seguridad, de manera que cuando estés dentro de un perímetro considerado seguro, este será lo más pequeño posible

y englobará la menor cantidad de activos que se pueda. Esto supone aumentar la granularidad, que es un concepto que detallaremos más adelante, para llevar a otro nivel la segmentación de la seguridad.

Además de esta, que es mi visión en base a la documentación encontrada y referida en este documento, otras fuentes muy fiables que se detallarán a lo largo de esta sección, proponen ideas complementarias que enriquecen el término y lo dotan de mayor rigurosidad.

Es importante hacer esta aclaración, porque en ocasiones se tiende a pensar que Zero Trust propone eliminar los perímetros de seguridad y convertir a todo el mundo, tanto el que esta autentificado como el que no, en usuarios iguales, y eso no es así. Un usuario autentificado debe generar más confianza que uno que no lo está, pero Zero Trust sugiere que incluso para esos usuarios debemos seguir aplicando restricciones y limitando el acceso.

4.1.1 Zero Trust según Kaspersky

El primer artículo que vamos a analizar es de **Kaspersky**[1], *Desconfía y verifica siempre: el modelo de seguridad Zero Trust*[10] donde ya desde el título podemos ver una de las mutaciones del proverbio ruso *Confía, pero verifica* que se hizo famoso a finales de los años 80 cuando Ronald Reagan lo utilizó. Desde entonces, su aplicación se ha convertido para muchos en garantía de seguridad, aunque como vamos a ver, en un ecosistema de seguridad de redes moderno se ha quedado anticuado. Zero Trust viene a sustituirlo por algo como lo que propone Kaspersky en este artículo, *Desconfía y verifica siempre.*

Kaspersky propone a Zero Trust como concepto – de seguridad –, que fue introducido por John Kindervag en 2010. Por lo tanto, vemos que, al menos en sus orígenes, Zero Trust de planteaba como una idea y no tanto como una arquitectura, y esto tiene mucho sentido, ahora que tenemos una buena idea de lo que es una arquitectura de seguridad, y que hemos visto su amplitud.

Sin embargo, el artículo habla de cosas muy interesantes, como por ejemplo, de la existencia de múltiples maneras de aplicar Zero Trust por lo que no estamos ante un único procedimiento estandarizado ni mucho menos y debemos tomar el documento del NIST[1] como una de las posibles implementaciones.

Por otro lado, habla de otros dos conceptos realmente interesantes como son los de *Superficie de Protección* y *Superficie de Ataque*. Estos conceptos hablan de la cantidad de elementos que en una organización deben ser protegidos, y de la cantidad de recursos que pueden ser atacados, respectivamente. Ambas superficies no son iguales, y en este caso se hace hincapié en la superficie de protección, centrando así los recursos físicos y económicos solo en aquellos activos que son importantes para la organización. También se introduce por primera vez el término micro-segmentación, que separa la red

[1]Kaspersky es una empresa multinacional con sede central en Reino Unido que desarrolla y distribuye servicios de seguridad y antivirus a nivel personal y corporativo con 25 años de experiencia y 400 millones de usuarios. Es un referente mundial en la investigación de soluciones de seguridad informática[17].

en trozos pequeños, del cual hablaremos en profundidad más adelante; del principio de los menores privilegios, que no es algo específico de Zero Trust; y de la necesidad de controlar de manera total los dispositivos corporativos, y poder conocer sus movimientos, que es un punto que comparte con el NIST.

4.1.2 Zero Trust según Malwarebytes

Por otro lado, **Malwarebytes**footnoteMalwarebytes Inc es una empresa multinacional estadounidense dedicada a la ciberseguridad, que desarrolla productos software de seguridad para ordenadores domésticos, teléfonos móviles y equipos empresariales. Dispone de un gran abanico de productos como software anti-ransomware, anti-exploits, análisis de amenazas en tiempo real etc. para adaptarse a las diferentes necesidades en su artículo *Explained: the strengths and weaknesses of the Zero Trust model*[3] también habla del "concepto introducido por John Kindervag" que coincide con lo propuesto por Kaspersky. Por otro lado, también se habla de que Zero Trust es considerado un Framework[2] que provee de visibilidad y de los controles IT necesarios para asegurar, administrar y monitorizar todos los dispositivos, usuarios, aplicaciones y redes que pertenecen o son utilizadas por los empleados de la empresa, o por terceros relacionados con ella.

En palabras de *Malwarebytes*, Zero Trust un *framework* totalmente desarrollado que proporciona un montón de características de seguridad de alto interés para la empresas, sin embargo no explica cómo hacerlo ni aporta información relevante en este sentido más allá de un par de consejos genéricos. Por otro lado, habla de que Zero Trust ayuda a la empresas a reducir su superficie de ataque, lo cual es curioso porque con la información encontrada hasta ahora, en lo que se debe de centrar Zero Trust no es en la superficie de ataque, si no en la superficie de defensa, haciendo esta más robusta y sin limitarse a generar seguridad perimetral como se ha hecho hasta ahora.

Por último, se proponen 4 pilares clave para entender e implementar Zero Trust, que son los siguientes:

- **Identificación de usuarios y accesos.** Forzando el uso del doble factor de autenticación, o con aplicaciones que implementen IDaaS, *Identity as a Service*. Mantener una correcta auditoría de qué usuarios están dados de alta en la organización y qué permisos tienen.
- **Segmentación de la red.** Que permita separar esta en trozos cuanto más pequeños mejor para poder controlarlos de manera independiente, asignando accesos y permisos en base a lo que cada segmento necesita.
- **Seguridad de los datos.** Incluso manteniendo unos estrictos controles de seguridad puede haber pérdida o filtración de datos. Se deben mantener los datos encriptados, tanto de manera local como cuando estos viajan a través de la red; y además se debe de tener una revisada política de copias de seguridad.

[2]Un "Software Framework"[25] es una herramienta que recopila herramientas, automatiza procesos y mantiene el proyecto ordenado, de manera que los programadores puedan ser más rápidos y eficientes en el desarrollo de software.

- **Orquestación de la seguridad.** La propuesta de seguridad corporativa de ser unánime y cada elemento de esta debe trabajar en conjunto con el resto. Se deben evitar los elementos redundantes tanto software como hardware.

4.1.3 Zero Trust según ESET

Por su parte **ESET**[3] en *¿Qué es el modelo de seguridad Zero Trust y por qué está creciendo su implementación?*[27], ya desde el título, trata Zero Trust como un modelo de seguridad, en el que las organizaciones no deben confiar en ninguna entidad, tanto interna como externa, de manera predeterminada. Sigue el principio *Nunca confíes, verifica siempre* que ya hemos visto, y además propone generar seguridad en torno a cada uno de los activos que se quiere proteger, muy en la linea de lo visto hasta el momento.

Por otro lado, se proponen 3 áreas principales sobre las que trabajar si se quiere implementar Zero Trust con éxito.

- **Visibilidad.** Consiste en identificar los recursos y dispositivos que se quieren proteger.
- **Políticas.** Es decir, establecer controles que solo permitan a personas específicas acceder a cada recurso.
- **Automatización.** Es necesario automatizar los procesos para garantizar una correcta aplicación de las políticas.

Por último, ESET da una definición de Zero Trust como modelo de seguridad, que es la siguiente:

Zero Trust es un modelo de seguridad que construye defensas alrededor de los datos, las redes, los dispositivos, la carga de trabajo y las personas.

Una definición muy poco específica pero que deja claro que aquí Zero Trust es un modelo y no una arquitectura, dando unos principios muy vagos de lo que hay realmente detrás de Zero Trust y de cómo implementar este modelo en una organización.

4.1.4 Zero Trust según IBM

Antes de continuar con nuestro documento de referencia, vamos a hacer una última parada para revisar si **IBM**[4] puede aportar algo más de información. En primer lugar, habla de Zero Trust como *framework* y como modelo, y con su implementación promete una protección efectiva de los activos

[3]ESET es una compañía de software eslovaca centrada en la ciberseguridad. Pioneros a nivel europeo en el desarrollo de este tipo de software y con más de 110 millones de clientes es una de las gigantes del sector.

[4]International Business Machines Corporation[30], también conocida como IBM, es una empresa multinacional estadounidense de tecnología y consultoría que fabrica y comercializa hardware y software para computadoras, y ofrece servicios de infraestructura, alojamiento de Internet, y consultoría en una amplia gama de áreas relacionadas con la informática, desde computadoras centrales hasta nanotecnología.

más valiosos de la organización[13].

Siguiendo esta línea, una red de confianza cero (Zero Trust Network o ZTN de ahora en adelante) debe guardar e inspeccionar todo el tráfico de red corporativo; limitar y controlar el acceso a la red; y verificar y asegurar los recursos de red. En este caso añade un matiz interesante a todo lo visto hasta el momento, y es que no solo no se debe confiar por defecto, si no que los recursos de la red no deben ser accesibles por defecto. Este matiz va acorde a la idea de otorgar los menores privilegios posibles, de manera que, si no necesitas un recurso, no vas a tener acceso a él. También es necesario proteger los accesos máquina-maquina, que muchas veces se pierden de vista y que son igualmente peligrosos, prestando especial atención a los accesos por API[5].

IBM además propone unos requerimientos mínimos en cuanto a capacidades y experiencia para poder integrar Zero Trust en una red corporativa, y puesto que hasta el momento es la única compañía que lo ha hecho, vamos a detenernos aquí.

- **Identidad.** Es necesario definir y aplicar las políticas de acceso de todos los usuarios y cuentas privilegiadas con SSO(Single Sign-on)[6], autenticación multifactor y gestión del ciclo de vida.
- **Datos.** Se deben descubrir, controlar y administrar los accesos a todos los datos de la organización.
- **Dispositivos y carga de trabajo.** Es necesario contar con dispositivos y aplicaciones que estén diseñados para poder ser monitorizados, de manera que sea más rápida y eficiente la extracción y monitorización de información.
- **Análisis y visibilidad.** Se debe poder conocer y analizar el comportamiento de los usuarios, los dispositivos y las conexiones.
- **Automatización y orquestación.** La automatización permite la aplicación de políticas dinámicas de manera mucho más efectiva que se puedan ir modificando según las necesidades de la organización.
- **Redes y endpoints.** Es necesario proteger la red física y los dispositivos.

Por otro lado, IBM introduce el término *contexto* para realizar una correcta planificación de la red. Que cada red es diferente es algo evidente, pero en este caso y con el nivel de granularidad que se propone en Zero Trust es aún más importante hacer un diseño a medida. Se debe de conocer el funcionamiento de la organización, sus flujos de trabajo, sus grupos de usuarios con sus necesidades específicas, tanto de hardware como de software, la infraestructura que se tiene y el nivel de criticidad de cada parte de la organización para poder repartir los recursos de manera más eficiente. A todo esto, es a lo que IBM se refiere con *contexto* y es una de las claves en el diseño de redes seguras a medida.

[5]Una API o *Interfaz de Programación de aplicaciones* es un conjunto de definiciones y protocolos que se utiliza para comunicar dos aplicaciones sin necesidad de conocer como están implementadas

[6]Single Sign-on es un mecanismo de autenticación que permite a un usuario introducir sus credenciales una única vez y que estas se utilicen en múltiples aplicaciones.

4.2 La normalización del Zero Trust

Por último, vamos a analizar la *NIST Special Publication 800-207*[1] que proporciona el NIST. Este documento tiene un carácter radicalmente diferente al resto de los propuestos en este análisis, puesto que no es un documento divulgativo, si no el comienzo de un estándar desarrollado por una organización que específicamente se dedica a ello. Nos centraremos únicamente en el carácter teórico del documento, dejando la parte práctica para el siguiente capítulo.

Para mí, una de las características más curiosas de este documento es que dualidad que genera en torno al concepto Zero Trust; por un lado, propone una definición genérica para Zero Trust, y por otro propone Zero Trust como arquitectura de seguridad. Puesto que ya tenemos claramente definidos los conceptos *Modelo de Seguridad* y *Arquitectura de Seguridad* podemos ver con facilidad que aunque no lo dice de manera explícita, la primera definición que aporta es entendiendo Zero Trust como modelo de seguridad, y es la siguiente:

Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

Por otro lado para Zero Trust como arquitectura se aporta esta otra definición:

Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.

Ahora si podemos ver que, el planteamiento de Zero Trust como modelo o como arquitectura es realmente diferente, manteniendo las bases, pero con una implementación aplicada a niveles totalmente distintos. Se mantiene la introducción del término recurso, que sustituirá de ahora en adelante a usuarios, dispositivos, maquinas e información, como ya se sugería en puntos anteriores.

De manera inicial se destacan dos grandes puntos a tratar que se extraen de las definiciones propuestas y de los primeros párrafos:

- Prevenir el acceso no autorizado a datos y servicios, no solo por parte de los usuarios sino también por parte de las máquinas que intercambian información.
- Generar políticas de acceso tan granulares como sea posible, es decir, generar seguridad especializada para cada caso concreto, ajustándose a las necesidades que tiene cada recurso.

Sin embargo, más adelante se concreta más en lo que denomina principios básicos de Zero Trust:

1. **Todos los datos y servicios de computación son considerados recursos.** Puesto que una red está compuesta por muchos tipos de dispositivos y usuarios, y sabiendo que todos ellos necesitan ser protegidos, un concepto común ayuda a entender que se debe tener visibilidad sobre el conjunto completo de la organización.

2. **Todas las comunicaciones deben ser protegidas independientemente de la localización.** La confianza no se debe proporcionar basándose únicamente en la procedencia del dispositivo, e incluso las comunicaciones internas de la organización deben ser realizadas de la manera más segura posible.

3. **El acceso a los recursos individuales de la empresa debe hacerse por sesión.** La confianza de un dispositivo o de un usuario se debe evaluar en el momento de la petición, esto quiere decir que no se debe proporcionar acceso por defecto al iniciar sesión. Además, este acceso debe ser concedido con la menor cantidad de privilegios posible.

4. **El acceso a los recursos debe generarse por políticas dinámicas.** La confianza que se tiene en un dispositivo o usuario no debe ser proporcionada de manera estática y continua a lo largo del tiempo. Esta confianza debe evaluarse *in-situ* y dependerá de las condiciones en las que se encuentra el dispositivo/usuario en el momento de acceder al recurso. Teniendo en cuenta su historial de seguridad, su historial de comportamiento, su localización actual, el nivel de autenticación que ha proporcionado, etc.

5. **Se deben monitorizar la integridad y el estado de la seguridad de todos los activos de la organización.** Una organización que implemente una ZTA deberá tener un sistema de diagnóstico y mitigación continuos (por sus siglas en inglés CDM) o similar para monitorizar el estado de los dispositivos y aplicaciones y deberá aplicar parches si es necesario.

6. **La autenticación y autorización de todos los recursos debe ser dinámica y estrictamente verificada antes de conceder el acceso al recurso.** Aquí se genera un ciclo constante de obtención de acceso, escaneo y evaluación de riesgos, adaptación, y reevaluación de la confianza en la comunicación que se está llevando a cabo.

7. **La organización debe recopilar tanta información como pueda acerca del estado actual de los activos, la infraestructura de red y las comunicaciones.** Esa información será almacenada y analizada con el fin de mejorar la seguridad de los procesos y comunicaciones.

Además de estos aspectos representativos de un modelo de seguridad Zero Trust, a continuación, se enumeran los aspectos de lo que desde el NIST llaman *A Zero Trust View of a Network* que viene a explicar cómo se plantea una red informática bajo el amparo de un modelo de seguridad Zero Trust.

- La red corporativa privada no será considerada segura por defecto.

- Los dispositivos que se utilizan pueden no ser propiedad de la organización o pueden no estar configurados por esta.

- Ningún recurso deberá ser considerado seguro, y se deberán aplicar políticas más estrictas a los recursos que no sean propiedad de la empresa.
- No todos los recursos de la organización se encuentran física y lógicamente en el interior de la organización.
- Los sujetos y objetos que se conecten a la red corporativa desde el exterior de esta no deberán confiar en sus redes locales.
- Los activos y flujos de trabajo que se muevan entre infraestructura de la empresa e infraestructura externa deberán estar bajo una estricta y consistente política de seguridad.

4.2.1 Una revisión a la propuesta del NIST

Como hemos visto el NIST hace una presentación bastante clara y amplia de lo que significa Zero Trust, sin embargo en *Zero Trust: The What, How, Why and When*[20] estos 7 elementos básicos son complementados de la siguiente manera.

En primer lugar, se plantea la posibilidad de que los recursos no sean utilizados por personas físicas, si no por máquinas, que es algo de lo que ya hemos hablado en este documento pero que el NIST pasa un poco por alto. La protección frente a este tipo de accesos debe realizarse de la misma manera que se haría respecto de las personas físicas, teniendo muy en cuenta las diferencias intrínsecas que hay entre el acceso y la autenticación que lleva a cabo una persona (haciendo uso de escáneres biométricos por ejemplo) que la que puede realizar un servidor.

Por otro lado, se propone llevar un paso más allá la microsegmentación, aislando cada elemento de manera individual, y generando seguridad en torno a él de manera específica. Esta microsegmentación es un aspecto de Zero Trust sea relevante, pero en la práctica es realmente difícil llevar a cabo por la cantidad de recursos que conlleva. Por otro lado, no todos los recursos son iguales y hay algunos en los que es muy difícil implementar seguridad, o al menos, aplicarla al nivel que se propone. El nivel de microsegmentación que se puede alcanzar y el coste asociado se verá en detalle más adelante.

Por último, sugiere el uso de inteligencia artificial[7] para llevar a cabo la evaluación de la confianza de los usuarios y de los *end-points*[8]. Esto no se aborda de manera directa en el documento del NIST puesto que es una de muchas maneras en las que se pueden generar las políticas de seguridad. La implementación de este tipo de motores de políticas conlleva problemas, no solo de costes y desarrollo, sino también de implementación, por la dificultad que conlleva generar un software que puede generar una política a cada activo, y asegurarse de que el software lo está haciendo correctamente. Una implementación más sencilla puede ser generar las políticas manualmente, y que la inteligencia artificial sea

[7] En este contexto, se entiende por inteligencia artificial a un software basado en algún modelo de aprendizaje supervisado que es capaz de tomar una decisión en base a un conjunto de casos de entrada que han sido validados por un humano.

[8] En end-point, en este caso, es cada uno de los elementos finales desde los que se realiza, por ejemplo, una petición de autenticación, o la comprobación de alguna política.

la encarga de identificar para cada tipo de usuario y activo, cuáles son las políticas más apropiadas. En cualquier caso, esto se discutirá en la sección de implementación.

Capítulo 5

Zero Trust. Características

Hasta ahora, y según el modelo de seguridad perimetral, se diferencian dos claras zonas en cuanto a una red se refiere. El exterior de la red, es decir, la parte de la red que no pertenece a la red de la organización, también conocida como internet, que es donde están los usuarios que aún no se han autenticado; y la parte interna de la red, donde se encuentran los recursos y los equipos corporativos, y todos los usuarios que están autenticados, y que por lo tanto son considerados confiable. Eso ya lo conocemos puesto que ya hemos indagado a lo largo de este documento.

Como ya hemos visto, Zero Trust trae consigo un cambio de paradigma que promete mejorar las soluciones de seguridad actuales y adaptarlas mejor a la descentralización y a unas redes corporativas con límites cada vez más difusos. Ya hemos hecho un repaso a la parte teórica de Zero Trust desde diferentes puntos de vista, y ahora vamos a profundizar en la parte puramente práctica, aportando ejemplos, para finalizar el documento con un ejemplo de implementación. Igual que hasta ahora mantendremos la *NIST Special Publication 800-207*[1] como documento de referencia, que será complementado con otras publicaciones según sea necesario.

5.1 Los tenets de Zero Trust

Conociendo todas las bondades de una arquitectura Zero Trust, es necesario llevar eso a la práctica, y eso conlleva una serie de problemas dada la amplia variedad de redes corporativas desplegadas a lo largo del mundo. El problema viene cuando debemos implementar los principales *tenets* de Zero Trust en ese dispar mundo de arquitecturas de red; esos 4 *tenets* son *Identificación de usuarios y accesos, Segmentación, Seguridad de los datos* y *Coordinación de la seguridad*. Vamos a ver cada uno de ellos detenidamente.

5.1.1 Identificación de usuarios y accesos

Seguramente este sea el punto más complicado de llevar a cabo. En primer lugar, es necesario saber qué usuarios hay registrados en la organización, pero ¿Que entendemos por la organización? Podemos

dar por hecho que se dispondrá de un sistema de *Microsoft Active Directory*[1], de ahora en adelante AD, pero eso no tiene por qué ser siempre así. Además, incluso disponiendo de él, el AD no cubre todas las necesidades de trabajo de los usuarios, que necesitan, correo electrónico, mensajería instantánea, servicios de videoconferencia, calendario corporativo, acceso a aplicaciones de trabajo, algunas propiedad de la organización y otras externas; acceso físico a la organización que deberá ser controlado y auditado; deberán de tener asignados dispositivos corporativos de trabajo, que no necesariamente harán uso de un sistema operativo Microsoft Windows; acceso a la red inalámbrica corporativa para los dispositivos portátiles, etc.

Por lo tanto, podemos ver que cuando hablamos de identificar a usuarios, debemos hacerlo de manera prácticamente independiente para cada aplicación o servicio que se les proporciona; y esto tiene mucho sentido, porque no todos los usuarios tienen acceso a las mismas aplicaciones, por lo que será necesario poder limitar el acceso a cada aplicación o servicio de manera independiente.

Suponiendo que se tiene resuelta la identificación y administración de aplicaciones, llegamos a otro punto complejo, como es la identificación de dispositivos. Aquí será necesario diferenciar, entre los dispositivos corporativos y los dispositivos personales, que probablemente estén mezclados.

- **Dispositivos Corporativos.** Muy seguramente, a los trabajadores se les proporcione un dispositivo de trabajo personal, ya sea portátil o de sobremesa, que estará çontrolado"por la empresa. La clave está en qué entendemos por Çontrolado por la empresa". Hay ciertas cosas que se pueden monitorizar y otras que no, veámoslo detenidamente. El dispositivo estará plataformado por la organización, es decir, llevará un sistema operativo, que en este caso será Microsoft Windows, elegido por la empresa, cuyos usuarios serán creados por los técnicos y registrados en el AD de la organización, y las aplicaciones que tendrá instaladas serán elegidas junto con sus respectivas versiones también por los técnicos. Para ello se habrá creado al trabajador un correo electrónico corporativo siguiendo la nomenclatura que la empresa considere oportuna, habitualmente *nombre.apellidos@empresa.com* como ha hecho la Universidad de Valladolid habitualmente, o haciendo uso de la primera letra del nombre *letraApellidos@empresa.com*.

  La empresa dispondrá muy seguramente de alguna *suite* de aplicaciones para trabajo corporativo de ofimática, las más habituales son la suite de *Office*, propiedad de Microsoft, y la *Google Workspace*. Con ello también quedan definidas cuales son las aplicaciones oficiales para el trabajo de ofimática, como Word, Excel, PowerPoint, etc. en Microsoft o, Documentos, Hojas de Cálculo, Presentaciones de Google, etc; para el correo electrónico *Outlook* o *GMail*; para mensajería instantánea y videoconferencias *Microsoft Teams* o *Google Meets*; y para el calendario *Calendario de Microsoft* o *Google Calendar*.

[1] Active Directory o también llamado AD o Directorio Activo, proporciona servicios de directorio normalmente en una red LAN, creando objetos como usuarios, equipos o grupos para administrar las credencias durante el inicio de sesión de los equipos que se conectan a una red.

Pero una vez están definidas que aplicaciones debe usar cada usuario, ¿Hasta qué punto se puede o se debe monitorizar el tráfico de red o los documentos que estas generan?, ¿Se pueden seguir monitorizando estas aplicaciones fuera de la red corporativa?, ¿Podrá iniciar sesión el ordenador sin estar en la red corporativa?, ¿Están monitorizados la introducción o extracción de documentos a través de dispositivos de almacenamiento extraíbles?

Es posible que además de ordenador de empresa, también se disponga de teléfono de empresa para todos o para una parte de la plantilla. De ser así, este también deberá estar monitorizado por la empresa, aunque no es sencillo. En EE.UU. por ejemplo, todos los datos almacenados en un dispositivo móvil corporativo pertenecen a la empresa, incluyendo llamadas, mensajes y correos, aunque esto no es así en todo el mundo. Hay ciertos tecnicismos que hay que tener en cuenta en este sentido, pero no vamos a profundizar en ellos. Otra opción es utilizar una tarjeta SIM de empresa dentro de un dispositivo móvil personal, lo cual complica aún más la situación. La manera más segura es proporcionar a los trabajadores que lo necesiten dispositivos móviles corporativos y monitorizarlos de la manera más estricta que permita la legislación local. Para ello hay aplicaciones como *InterGuard* o *Coscopy* que son capaces de recoger una gran cantidad de información.

- **Dispositivos no Corporativos.** Los problemas continúan y se incrementan cuando hablamos de dispositivos que no están controlados por la empresa, como ordenadores personales o dispositivos móviles. En el punto anterior se ha hablado de dispositivos corporativos fuera de la empresa, pero ¿Qué ocurre si hay dispositivos no corporativos dentro de la empresa? Esto es un problema que a su vez se divide en dos, dispositivos personales que se utilizan para trabajo corporativo, ya sea por falta de medios, de presupuesto o por cualquier otro motivo; y dispositivos personales que no se utilizan para trabajo corporativo, pero están dentro de la organización como parte de los objetos personales de los trabajadores, el caso más evidente, dispositivos móviles personales.

  Dispositivos de trabajo no corporativos. Estos pueden ser ordenadores, teléfonos móviles, tabletas inteligentes, impresoras, dispositivos de almacenamiento, etc. Es poco habitual que se utilicen ordenadores personales para el trabajo, pero podría suceder, por ejemplo, durante el teletrabajo. Es importante que se pueda identificar desde qué dispositivo se está conectando cada usuario, porque el uso de estos dispositivos no corporativos puede ser conocido por la empresa, en cuyo caso se habrá tomado alguna medida, o no. Las recomendaciones mínimas en estos casos son las mismas que las que vemos para dispositivos corporativos, como el uso de VPN, el uso de un gestor de contraseñas, evitar la instalación de software que no haya sido proporcionado por la empresa, etc. El uso de teléfonos móviles no corporativos para el trabajo es mucho más habitual. Para intercambiar llamadas, mensajería instantánea (WhatsApp, Telegram, etc.), responder correos electrónicos, etc. Aquí el peligro es mayor, sobre todo por la mala gestión de este tipo de dispositivos que hace la gente sin conocimientos técnicos. La solución más sencilla es restringir el uso del teléfono no corporativo para tareas de trabajo, puesto que la ley en

cuanto a la monitorización de dispositivos personales para uso corporativo complica la situación. Sin embargo, si la empresa no dispone de recursos para proporcionar dispositivos de trabajo y dispositivos móviles corporativos a todos los trabajadores, en un caso en el que suponemos es necesario el uso de ambos, la mejor solución es concienciar y formar a los trabajadores, para que conozcan los peligros. Aun así, esta solución es muy pobre y está totalmente desaconsejado el uso de dispositivos personales no corporativos para el trabajo.

Dispositivos personales en el trabajo. La solución fácil es prohibirlos, puesto que en esta categoría estamos tratando dispositivos que no se van a utilizar para trabajar, pero van a estar en el entorno de trabajo como, por ejemplo, un ordenador portátil personal en una mochila. La situación no es tan clara cuando se trata de los teléfonos móviles, puesto que hoy en día se convertido en imprescindible llevar nuestro teléfono móvil a todos los sitios. En cualquier caso, se debe limitar su uso, y si es posible, limitar su acceso a lugares que estén altamente restringidos. De esta manera evitas la toma de fotografías y vídeos, la grabación de audio, y toda una larga serie de peligros relacionados con la conexión a redes corporativas, la suplantación de redes, la monitorización de dispositivos, el mapeo de red, ataques de descubrimiento, etc.

Una vez tenemos a los activos identificados y se han generado accesos para todos los recursos necesarios, es momento de preparar una sólida política de autenticación que asegure que esos usuarios son efectivamente quienes dicen ser. El método más habitual es mediante contraseñas, las cuales han demostrado ser un método relativamente efectivo, pero tienen carencias que será necesario suplir, por ejemplo, con el doble factor de autenticación.

- **Contraseñas.** Por un lado, estas deben ser robustas, idealmente, deberían ser una combinación aleatoria de números, letras mayúsculas y minúsculas, y símbolos. En caso de que usemos contraseñas que no estén generadas aleatoriamente, estas deberán ser lo más aleatorias que sea posible, no contener palabras y tener al menos 10 caracteres. Por otro lado, se deberá modificar la contraseña, idealmente cada 3 meses, pero una modificación cada 6 meses tampoco pone en peligro el activo que la contraseña está protegiendo. *Kee Pass* es un gestor de contraseñas de código libre que se plantea como una gran opción para la gestión de contraseñas, generando una base de datos cifrada que permite evitar las alternativas que ofrecen los navegadores para introducir automáticamente los datos de autenticación.

- **Doble factor de autenticación.** Deberá ser también imprescindible el tener activado en todos los mecanismos de autenticación que lo permitan el doble factor de autenticación. Típicamente, esto se consigue haciendo uso de alguna herramienta externa de autenticación como *Google Authenticator* o *Microsoft Authenticator*, que normalmente se instalan en el teléfono móvil, mediante el correo electrónico, o mediante SMS.

- **Escáneres biométricos.** Es una manera cada vez más utilizada de autenticar a los usuarios. Si bien es bastante fiable, sigue teniendo falsos positivos y es una tecnología cara de implementar. Por suerte hoy en día prácticamente todos los teléfonos tienen escáneres biométricos de huellas dactilares lo que facilita su implementación. La tasa de falsos negativos, es decir, de veces que

a un usuario legitimo no es capaz de autenticarle con éxito, es relativamente alta, entre un 5 y un 30 por ciento según *LockStep*[32]. La tasa de falsos positivos, es decir, cuando a un usuario ilegitimo se le autentica erróneamente que, por cierto, es mucho más peligrosa, es mucho menor.

- **Single Sign-on.** Voy a introducir *Singles Sign-On* como uno de los nuevos sistemas de autenticación que están entrando en uso actualmente. *Single Sign-On* permite que un usuario que intenta acceder a una web, se autentique, no contra esa web, si no contra una entidad de autenticación de identidad, y que mediante el acuerdo de confianza entre la web y la entidad de autenticación, al usuario se le conceda permiso para acceder. La mejor parte, es que ese proceso de autenticación del usuario contra la entidad de autenticación, solo se tiene que hacer cada un determinado tiempo o al variar unas determinadas condiciones, mientras tanto, el usuario podrá autenticarse en tantos sitios como quiera sin tener físicamente que volver a autenticarse. Se considera que *Single Sign-On* es un método de autenticación bastante fiable, pero como todo sistema que está centralizado, tiene sus inconvenientes.

5.1.2 Segmentación

Otro de los puntos importantes es por supuesto la segmentación de la red, que ya se ha comentado hasta ahora, pero no se han planteado las complicaciones que tiene. Al igual que en el punto anterior identificamos usuarios y activos, ahora hay que identificar la red corporativa y definirla a nivel lógico. Identificar la red física es "sencillo", porque basta con tener claro que dispositivos tienes, como están conectados y cuál es su función. Por supuesto, si la red es muy grande y está deslocalizada en diferentes sedes o centros de producción, o dispone de muchos dispositivos móviles que cambian de localización, la cosa se complica. Pero aún se complica más cuando tratamos la red lógica, porque en ella, muchas veces no es sencillo encontrar el límite entre lo que es tuyo y lo que pertenece a los servicios proporcionados por otras empresas, como por ejemplo los servicios en cloud, los servicios del proveedor de seguridad, el proveedor de red, conexiones con otras empresas o *partners*, etc.

Aquí no se van a plantear todas las casuísticas posibles, pero si vamos a ver unas cuantas que son relevantes.

Conexión con el ISP. El ISP o por sus siglas en inglés *Internet Service Provider* (Proveedor de Servicios de Internet), es la empresa encargada de proporcionarnos conexión con internet. Es la entidad encargada de gestionar el punto en el que se encuentra el puente entre la red interna de la empresa y el exterior. Hay varios puntos que hay que tener en cuenta así que vamos uno por uno.

- **Localización de la infraestructura.** Esta decisión no pertenece a este punto, pero es importante saber que antes de elegir la conexiones con el exterior es necesario saber cómo se van a distribuir los activos físicamente en la organización, y decidir cuáles de ellos estarán alojados en local y cuales en cloud. Según esta distribución, serán necesarias más o menos enlaces con el ISP.

- **Ancho de banda necesario.** Este cálculo es realmente complejo y no es más que una estimación de lo que se prevé que se va a necesitar. Si el ISP ofrece flexibilidad, no será un problema cometer

pequeños o medianos errores de cálculo, puesto que se podrá rectificar. La cantidad de ancho de banda va a depender de diferentes factores, vamos a comentar alguno. El número de trabajadores de la empresa y el gasto promedio por trabajador son en principio uno de los mayores consumos de ancho de banda. Hay que tener en cuenta si los recursos están alojados en local o están en cloud; y hay que tener en cuenta también que, aunque todos los recursos estén almacenados de manera local en la organización, físicamente puede que no estén en todos los centros de producción de la empresa, por lo que siendo más precisos, habría que saber el número de trabajadores que va a necesitar acceder de manera remota a datos de la empresa. Por otro lado, el consumo de internet "público"que van a tener estos trabajadores, que dependerá totalmente del tipo de trabajo que desempeñen. Y por último dentro del consumo de los trabajadores, las conexiones VPN de trabajadores en remoto. Estas pueden estar configuradas para redirigir todo el tráfico del usuario a la red corporativa, o para redirigir solo el tráfico imprescindible. Esto dependerá de las necesidades de la organización. Se verán casos con necesidades específicas en el siguiente capítulo. Típicamente podemos estar hablando de velocidades entre los 500Mbps y los 10Gbps por cada enlace. De todos modos, no todos los enlaces deben tener la misma velocidad necesariamente.

Por otro lado, el ancho de banda dependerá de las conexiones máquina-máquina que se hagan. Estas pueden ser entre servidores de diferentes sucursales, o entre servidores y el cloud. Según el tipo de organización estas pueden suponer la mayor cantidad de ancho de banda. No hay una cifra especifica de ancho de banda recomendado en estos casos, dependerá del volumen de transacciones.

- **Número de conexiones necesarias.** Evidentemente, para cada oficina o grupo de oficinas que estén físicamente separadas unas de otras será necesario un enlace con internet. Típicamente, utilizar más de 1 conexiones a internet en organizaciones medianas o pequeñas se hace para obtener una buena redundancia, no por necesidades de ancho de banda, puesto que en España se pueden obtener sin demasiado problema velocidades de 10Gbps. Para organizaciones grandes si puede llegar a ser una restricción, por ejemplo, a partir de 500 dispositivos de trabajo conectados en simultaneo puede haber problemas; esto serian .ªproximadamente"20Mbps por puesto de trabajo, que es en mi opinión, el mínimo que se debe tener para poder trabajar con fluidez en prácticamente todo tipo de puestos. Por último, es necesario tener en cuenta la diferencia entre las necesidades de ancho de banda de subida y de ancho de banda de bajada. Según el modelo de trabajo puede que se requiera más velocidad de subida, de bajada, o ambas por igual.

Visto desde la perspectiva de la disponibilidad, sí que es recomendable disponer de un segundo enlace que disponga de características similares. Realmente este enlace podría tener prestaciones inferiores, puesto que su función sería la de seguir proporcionando internet a la organización en caso de que el principal no esté operativo, y su nivel de servicio no tendría que ser necesariamente el mismo. Por otro lado, es importante que este segundo enlace sea de un proveedor

diferente, y no solo eso, sino que se debe asegurar que la infraestructura física sea diferente. En España por ejemplo, la infraestructura de *O2* es de *Movistar*, por lo que no tendría sentido tener un enlace principal con *O2* y uno secundario con *Movistar* puesto que todo va por el mismo cable.

- **Elección del proveedor.** De esta manera llegamos justo al último punto, para el que deberemos tener muy en cuenta lo visto en el caso anterior. Resumiendo, para necesidades muy grandes de ancho de banda será necesario disponer de varios enlaces de internet. Estos enlaces podrán tener el mismo ancho de banda o ser diferentes. En cualquier caso, será necesario disponer de un balanceador de carga, que lo veremos en el siguiente capítulo. Estos enlaces con el propósito de incrementar el ancho de banda pueden ser provistos por el mismo ISP; sin embargo, para los enlaces cuyo objetivo sea generar redundancia, es imprescindible contar con al menos 2 ISP que dispongan de infraestructura física separada.

  Los proveedores deberán ofrecer un nivel de servicio superior al que se ofrece para enlaces domésticos, proporcionando una disponibilidad superior y un ancho de banda mínimo lo más cercano posible al ancho de banda máximo.

Localización de los activos. Aquí se van a detectar cuales son cada uno de los dispositivos o grupos de dispositivos que forman la red. Partiendo de una red ya desplegada, en esta parte se deben identificar todos los firewalls (tanto hardware como software), routers, switches, servidores y demás elementos que forman la red, como puntos de accesos o impresoras. Se debe saber qué marca, modelo y versión de software utiliza cada uno, y en que parte física de la organización se encuentra. También es necesario localizar los end-points, tanto los fijos como los portátiles, para tener así una idea real del tamaño y distribución de la red. Toda esta información debe estar documentada detalladamente.

División en subredes. Esto es más subjetivo y depende mucho de la experiencia del arquitecto de red y de la estructura de la empresa. Vamos a proponer un ejemplo simple para ejemplificar las dos maneras generales en las que se puede aproximar esto. Partimos de la base de que tenemos como cliente una cadena de supermercados, que tiene diferentes supermercados en diferentes ciudades, y en cada uno de ellos tiene una serie de departamentos o, mejor dicho, grupos de trabajo, que es más general. Suponiendo que todos estén dentro de la misma red, que es algo que no tiene por qué ser así necesariamente, podemos organizar las subredes por departamentos o por supermercados.

- **Por departamentos.** Ya hemos dicho que cada supermercado tiene una serie de grupos de trabajo, 3 en este caso (A, B y C). Podemos hacer que todos los departamentos A de todos los supermercados compartan subred, que a su vez estarán divididos en subredes, para cada uno de los supermercados específicos, Aa, Ab y Ac. El problema de este modelo es que en una misma subred estarán sistemas de localizaciones muy diferentes. Sin embargo, puede ser necesario que esté configurado de esa manera para que el intercambio de información y el acceso a los recursos compartidos sea más sencillo.

- **Por localización.** La manera más sencilla de organizar subredes en este caso es por localización. A cada supermercado se le asigna una subred, y a su vez a cada departamento se le asigna una subred. Esto sigue una topología de árbol bastante sencilla de entender e implementar, y es la manera que utilizaremos en la propuesta de implementación del siguiente capítulo.

Zero Trust propone implementar una segmentación lo más granular posible, es decir, aislar a nivel de red los activos todo lo que se pueda, generando tantas subredes como sean necesarias. Hasta ahora hemos hablado de la segmentación de los equipos de trabajo, pero se debe de implementar algo similar con los servidores, Firewalls, Routers, etc.

Por otro lado, es importante la gestión de las WLANs. Estas deben estar en una subred propia, y lo mismo tiene que ocurrir con las WLANs de invitados, que además de estar separadas, deberán de tener una gran cantidad de restricciones aplicadas.

Identificación de dispositivos. Realmente la identificación no pertenece a la segmentación, pero es relevante comentarlo. Normalmente esto se hace sabiendo la IP del dispositivo, su MAC y su nombre. Pero si queremos ir un paso más allá hay que aplicar otro enfoque. La dirección IP no es realmente relevante salvo para aquellos dispositivos con IP estática, el resto, irán cambiando de IP según al dispositivo al que se conecten. Las IP estáticas normalmente solo se asignan a servidores o dispositivos que van a ser accedidos habitualmente por otros usuarios o dispositivos. La dirección MAC tampoco aporta demasiado puesto que, aunque es única en el mundo originalmente, se puede cambiar. Por último, el nombre del dispositivo, que no aporta mucho valor, aunque, como el equipo ha sido configurado por la organización y el usuario no tiene permiso para cambiar ese tipo de información, podría en cierto sentido ser suficiente para la identificación de los dispositivos.

5.1.3 Seguridad de los datos

Consiste en proporcionar confidencialidad, integridad y disponibilidad a los datos que posee la organización. A grandes rasgos, los datos pueden estar almacenados, o en movimiento a través de la red. Los peligros a los que se enfrentan los datos en cada uno de esos dos estados son diferentes por lo que conviene hablar de cada uno por separado.

- **Datos almacenados.** Este es sin duda el estado más seguro en el que pueden estar los datos, cuando están almacenados en algún medio de almacenamiento. No entra dentro del alcance de este documento analizar los diferentes medios de almacenamiento disponibles, pero si nos vamos a detener en la manera en la que los datos deben estar dentro de dichos medios. Cada uno de los 3 aspectos claves mencionados se consigue de diferentes maneras por lo que vamos a ir uno a uno.

    - **Confidencialidad.** Consiste en mantener oculta la información. Esto se consigue mediante métodos de cifrado, dentro de los cuales tampoco vamos a profundizar porque no entra dentro del alcance del documento. Si merece la pena comentar que se puede realizar encriptación

por software o por hardware, siendo la encriptación por hardware la más interesante en este caso. *Bitlocker* es una herramienta de Windows que permite de manera nativa encriptar discos duros por hardware, mediante el algoritmo AES[2] con clave de 128 bits. Sí hay que tener en cuenta, que cifrar y descifrar datos es un proceso costoso, sobre todo dependiendo del algoritmo, y que se debe hacer con cuidado según la cantidad de accesos que vayan a recibir los datos.

- **Integridad.** Es la característica que hace que los datos se mantengan inmutables desde el momento en el que son almacenados hasta el momento en el que son accedidos. No solo se debe procurar proporcionar integridad, sino que también se deben preparar mecanismos para recuperar los datos que hayan sido corrompidos, aunque esta última parte se verá con más detalle en el punto de la disponibilidad. Para asegurar la integridad de los datos, no basta con protegerlos, sino que también es necesario proporcionar un mecanismo que permita comprobar que esos datos siguen siendo íntegros. Para lograrlo podemos encontrar como las *Funciones Hashs*[3] o los *Códigos de Redundancia Cíclica*[4] o CRC. Estas dos herramientas funcionan de maneras diferentes. En el caso de las funciones *Hash*, será necesario generarlas cuando los datos sean almacenados, y volverlas a generar cuando se quiera comprobar si los datos siguen siendo íntegros, lo cual se hará comprobando que los resultados obtenidos coinciden. Por otro lado, los CRC van integrados dentro de los propios datos, por lo que no es necesario volver a hacer los cálculos; por otro lado, los CRC pueden arreglar ciertos tipos de errores de integridad que podamos encontrar en los datos.

  El segundo gran mecanismo mediante el cual se logra integridad es mediante copias de seguridad. Una copia de seguridad consiste en tener los datos almacenados varias veces, de manera que, si una de las copias deja de ser funcional por el motivo que sea, podemos utilizar otra. Hay copias de seguridad de varios tipos, por ejemplo, en bases de datos las hay parciales y totales, y en un sistema operativo la manera más habitual de hacer copias de seguridad es mediante puntos de control, que permiten generar una instancia del sistema operativo para que en caso de detectar corrupción podamos devolver este a un estado conocido e íntegro. Por otro lado, si únicamente se quiere hacer una copia de seguridad de los archivos, estas siguen una estructura similar a la que siguen las bases de datos.

- **Disponibilidad.** Esta es una de las partes más importantes de manera que voy a simplificarla en la medida de lo posible para poder profundizar adecuadamente. La manera más

[2]The Advanced Encryption Standard (AES), en español *Encriptación Avanzada Estándar* es el método de cifrado estándar estipulado por el NIST en EEUU. Tiene un tamaño de bloque de 128 bits y claves de 128, 192 y 256 bits

[3]Las funciones *Hash* son un conjunto de operaciones matemáticas que se aplican sobre un conjunto de datos de tamaño indefinido que generan un código resultante, cuya longitud depende el algoritmo utilizado, que es único en el mundo. Una modificación en los datos hará que el resultado obtenido sea diferente. Este tipo de funciones dispone de otras funcionalidades muy interesantes que no serán estudiadas aquí.

[4]Los Códigos de Redundancia Cíclicas o CRC consisten en un proceso matemático que aplica en bucle una serie de operaciones que permite obtener un resultado en base a un conjunto de datos de entrada denominado trama. Comprobando la varían en este CRC se puede saber que los datos han sido alterados y en que parte lo han sido. Se aplica sobre datos en bloque de un tamaño fijo.

común de proporcionar disponibilidad es mediante redundancia, que consiste en replicar la información en diferentes lugares físicos para intentar que este siempre disponible en al menos uno de ellos. Adicionalmente se podrían hacer copias de seguridad en otras particiones de un mismo disco, lo cual no es óptimo, pero si puede ser funcional en ciertos casos. Estas copias de seguridad las podemos generar y almacenar nosotros o se pueden contratar como servicio en la nube, eligiendo también el nivel de replicación que queremos.

Otro aspecto relevante de la disponibilidad es la accesibilidad. No solo es necesario que los datos estén disponibles, sino además se tiene que poder acceder a ellos bajo unos determinados requisitos, como, por ejemplo, que estén accesibles en la nube (no únicamente en un ordenador), o que se disponga de un determinado ancho de banda para el acceso. La política de distribución y replicación de la información debe cubrir estas necesidades de negocio. No sirve de nada tener un conjunto de datos almacenados y replicados correctamente, si necesitas acceder a ellos desde el exterior de la organización y no puedes; o puedes hacerlo, pero la velocidad de acceso no es suficientemente rápida.

- **Datos en movimiento.** Los datos en movimiento suponen un riesgo extra. En primer lugar, porque al pasar por varios dispositivos estás dando mayor visibilidad de estos; cuantos más dispositivos vean los datos mayor probabilidad de que alguno de ellos esté comprometido. Pero además, es posible que los datos estén en movimiento por el exterior de la red corporativa, lo cual hace que el número de dispositivos crezca, a la vez que disminuye el control que se tiene sobre ellos. Viajar a través de dispositivos y redes externas supone un riesgo extra que se debe tener en cuenta a la hora de configurar la seguridad de los datos. Igual que se ha hecho en el punto anterior, vamos a analizar una a una las características que deben tener los datos para ser considerados seguros.

  - **Confidencialidad.** El concepto es el mismo que para los datos almacenados, pero la manera de lograrlo difiere un poco. Nos tendremos que apoyar de nuevo en la encriptación, pero esta va a tener que ser mucho más dinámica, y mucho más eficiente, puesto que se encriptarán los datos al inicio de la transmisión y se desencriptarán al final. Esto se puede lograr haciendo uso de túneles VPN, que son una herramienta muy común pero que se pueden configurar de maneras muy dispares. En su defecto, se deberá forzar el uso de protocolos cifrados como SSH, SFTF o HTTPS. Estos protocolos aplican su propia capa de encriptación basada en SSL o TLS que, haciendo uso de las versiones más actualizadas, es protección suficiente. Se debe por lo tanto evitar el cifrado múltiple siempre que no sea estrictamente necesario, sobre todo para la transmisión de grandes cantidades de datos.
  - **Integridad.** Este es el segundo aspecto importante de la seguridad de los datos en movimiento. Consiste en asegurar que los datos que se reciben sean los mismos que se enviaron, pero centrándonos principalmente en las modificaciones que puedan sufrir los datos por obra de un intruso. Esto quiere decir que no se va a tener en cuenta los errores de inte-

gridad producidos por el medio de transmisión por lo que no se hablara de los protocolos de corrección de errores de la red, como los que encontramos en TCP por ejemplo. Dicho esto, las técnicas que se pueden utilizar para lograr esto son similares a las vistas para los datos almacenados. Es muy habitual, por ejemplo, al ir a descargar software de internet, que este esté publicado junto con algunas de sus funciones Hash, para que así el usuario pueda asegurar que el software que descarga sea el que efectivamente se publicó.

- **Disponibilidad.** En este caso la disponibilidad pasa a un segundo plano. Con los datos en movimiento no se puede hablar de disponibilidad, en todo caso podríamos plantear dudas sobre la fiabilidad del método de transporte, lo cual pertenece al tipo de protocolo utilizado y no entra dentro del estudio de este documento. Aquí la disponibilidad depende principalmente de dos factores; el primero es la disponibilidad de los datos almacenados, es decir, tener una fuente activa y fiable de la que coger datos, lo cual ya se ha visto en el apartado anterior; y por otro lado, se debe asegurar la disponibilidad de la red o método de transmisión, lo cual habitualmente está fuera de nuestro alcance, o en todo caso, depende de la propia disponibilidad de la red, que no vamos a tratar en este documento.

5.1.4 Coordinación de la seguridad

Consiste en asegurar que todas las medidas y políticas implementadas trabajen al unísono. Habiendo hablado de encriptación en el apartado anterior, un error de coordinación de seguridad sería utilizar VPN cuando se utilicen aplicaciones que apliquen su propia encriptación. La coordinación de la seguridad hará la red corporativa más eficiente pero también más segura, por ejemplo, generando una correcta política de replicación de los servidores, o una política de copias de seguridad acorde a las necesidades reales de la empresa.

Este es un punto mucho más relevante de lo que parece a simple vista, sobre todo cuando se trata de una red basada en Zero Trust. Cuando se aplica Zero Trust, se está tratando de proporcionar seguridad específica para cada parte de la red y para cada recurso de manera prácticamente independiente. Es necesario por lo tanto que la empresa cuente con un CISO[5] formado y capacitado para coordinar las necesidades de seguridad de la empresa. Este, deberá tener formación técnica para poder entender el funcionamiento y la de seguridad que necesita la red, pero también formación administrativa, puesto que debe ser capaz de coordinar a los técnicos de la organización. Por otro lado, será el encargado de subcontratar si es necesario los servicios que la empresa no se pueda proporcionar por sí misma, como el proveedor de servicios de internet, los proveedores de hardware de seguridad, los proveedores de servicios en la nube, o los proveedores de los servicios de seguridad gestionados que se requieran. Además, deberá de supervisar el trabajo que estos realizan y asegurarse de que se cumplen con los estándares de calidad y seguridad que impone la organización.

[5] *Chief Information Security Officer*[15] o en español, Jefe de Seguridad de la Información, es un rol desempeñado a nivel ejecutivo y su función principal es la de alinear la seguridad de la información con los objetivos de negocio.

5.1.5 Formación

En la mayoría de los documentos consultados no se propone como característica necesaria para proporcionar seguridad, pero la formación del personal es algo absolutamente necesario. En una red de tipo Zero Trust en la que vas a imponer una desconfianza por defecto, debemos empezar por los propios miembros de la organización, puesto que, si vamos a seguir centrándonos únicamente en la desconfianza sobre los agentes externos, no es necesario generar una estructura de seguridad tan compleja como la que se propone en Zero Trust. Una cadena es tan fuerte como su eslabón más débil, y cuando intentamos defendernos de ciberdelincuentes hay que tener claro que, si tenemos un eslabón débil, lo van a encontrar. La formación de los administradores de red es algo que se da por supuesto y que además se exige que exista, acreditándolo con certificaciones del mayor prestigio posible. Sin embargo, los administradores de red y de seguridad de la información suelen ser una parte muy pequeña del personal que utiliza la red. Dado el rápido avance que han sufrido las tecnologías de la información en los últimos años, debemos asegurar que los empleados de las organizaciones tienen conocimientos suficientes en materia de seguridad.

Se trata de asegurar que los trabajadores conocen lo que es un *phising* y como detectarlo, el peligro que tiene conectar dispositivos de almacenamiento extraíbles a máquinas corporativas, el peligro que corren conectados a según qué tipo de redes Wi-Fi, como hacer una correcta gestión de las contraseñas, qué es y cómo activar el doble factor de autenticación, saber identificar una página web que no dispone de certificados o que no hace uso de HTTPS, y un largo etcétera de aspectos de seguridad básicos que son necesarios para garantizar la seguridad. Por todo ello la formación se convierte en un aspecto fundamental, en el que se debe invertir tiempo y dinero para evitar que de manera accidental los trabajadores comprometan la seguridad de la organización.

Por otro lado, la formación no se puede aplicar de manera igualitaria a todos los miembros de la organización, y aunque podría ser apropiado segmentar estos grupos para dar formación más específica, con el fin de no complicar en exceso la sección vamos a dividir al personal en dos grupos, que se ven a continuación.

- **Para el personal técnico.** Entendemos personal técnico como aquel encargado del soporte y mantenimiento de la red, y al personal de dirección encargado de tomar decisiones relevantes para el funcionamiento de la red, de los equipos, y de las aplicaciones que se utilizan. La manera más popular de adquirir conocimiento técnico certificable es mediante las conocidas certificaciones. Pueden ser ofrecidas por organismos públicos o por empresas privadas. Las certificaciones más prestigiosas suelen ser proporcionadas por empresas privadas y suelen tener un coste elevado, de ahí la necesidad de inversión por parte de la empresa que busca formar a sus trabajadores. Algunas de las más prestigiosas en cuanto a redes son ofrecidas por Cisco[6], como por ejemplo *Cisco CCIE* o *Cisco CCNP*, que son dos certificaciones para técnicos avanzados. En la misma

[6]Cisco Systems es una empresa de tecnología estadounidense que opera en todo el mundo y que es mejor conocida por sus productos de redes informáticas y de telecomunicaciones. Actualmente es una de las compañías más grandes del mundo en ese sector, y proporciona hardware y software del más alto nivel que existe.

rama pero más básicas podemos encontrar *CompTIA Network+* o *Cisco CCNA* que son para niveles más bajos, ideales para los técnicos de Nivel 1 (N1) o Nivel 2 (N2). Según los servicios que tenga la empresa contratados pueden ser necesarias certificaciones más específicas como *AWS Certified Advanced Networking* para el trabajo con servicios en cloud con AWS[7], o *VMware VCP-NV* dedicada a la virtualización de equipos mediante VMware. A nivel de hardware también se ofrecen una gran cantidad de opciones como las de *Fortinet* que ofrece 7 niveles de certificación desde NSE1 hasta NSE8, siendo algunos de ellos gratuitos. *Palo Alto Networks* por su parte, también tiene un buen abanico de opciones desde las más básicas como la PCCSA hasta las más avanzadas como la PCNSE.

- **Para el resto del personal.** La formación para este grupo de gente, que seguramente formen cerca del 90 % de la organización, se complica. El personal técnico está acostumbrado a trabajar con certificaciones y a tener que sacarlas y renovarlas regularmente"para estar a la altura de los estándares que se exigen, sin embargo, para el resto del personal esto no es así. La manera más fácil en mi opinión es utilizar semanalmente un par de horas del horario laboral para que el personal técnico de la empresa intente concienciar a los trabajadores sobre que se debe y que no se debe hacer. Se hablará de un completo programa de formación en el próximo capítulo.

5.2 Una posible arquitectura para Zero Trust

La arquitectura basada en Zero Trust mejor detallada es la propuesta en el documento del NIST ya mencionado, motivo por el cual es el documento de referencia, de manera que vamos a pasar a explicar qué se plantea y cuáles son las partes de esta arquitectura de seguridad.

La estructura lógica propuesta tiene 3 elementos principales, que primero se van a tratar de manera teórica pero que en el próximo capítulo veremos opciones de implementación reales.

- **Policy Engine (PE).** En español significa motor de políticas, y en última instancia y en base a la información que haya podido recopilar, es la parte del sistema encargada de proporcionar, denegar o revocar el acceso a un recurso. La decisión final será tomada por el administrador de las políticas, pero el PE es lo que asigna o deniega los accesos, es decir, que ejecuta las acciones.

- **Policy Administrator (PA),** o en español, administrador de políticas, es la parte encargada de generar comunicación entre un objeto y un sujeto. Una vez que se ha autorizado la comunicación por el PE, la PA configura la comunicación, o PEP.

- **Policy Enforcement Point (PEP),** que en español significa punto de aplicación de la política, se encarga de generar, monitorizar y si es necesario terminar la comunicación entre el objeto y el sujeto. Puede ser un único elemento o se puede dividir en dos partes, una en el lado del objeto y otra en el lado del sujeto.

[7] Amazon Web Services es una colección de servicios de computación en la nube pública que en conjunto forman una plataforma de computación en la nube, ofrecidas a través de Internet por Amazon.com.

En ocasiones PE y PA se consideran un único sistema que recoge todas las funciones de la gestión de las políticas, llamado *Policy Decision Point*, que configura el PEP, que sigue siendo el elemento que genera la comunicación real entre objeto y sujeto.

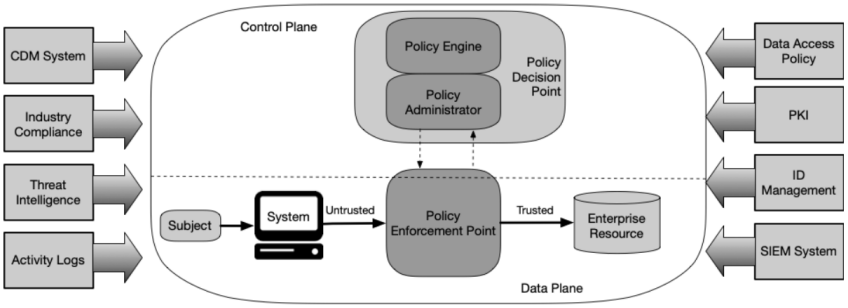

Figura 5.1: Modelo de comunicación entre PE-PA y PEP, NIST[1]

El proceso por el cual el PE administra las políticas y asigna o deniega accesos puede realizarse por un humano tomando decisión en función de sus capacidades, o por una máquina que automatice el proceso en función de la información de la que dispone. La manera óptima y más segura es que el proceso se realice de manera automática es mediante un sistema que recoja información de diferentes fuentes, la procese y genere una decisión. Estas fuentes de información pueden ser propias de la organización, y estar alojadas tanto en local como en cloud, o externas, subcontratando servicios que provean la información que se requiera. Las fuentes de información que considera el NIST más relevantes son las siguientes.

- **Sistema de mitigación y diagnostico continuo, CDM** recoge información del estado actual de los dispositivos de la organización, las peticiones realizadas, los eventos de sistema operativo y la presencia de dispositivos anómalos, entre otros.
- **Industry Compliance System.** Su traducción literal es un poco fea y quiere decir *Sistema de cumplimiento de la industria*. Se refiere a aquellos sistemas encargados de monitorizar a una organización para asegurar el cumplimiento de alguna normativa concreta, como por ejemplo, el RGPD[8]. Es habitual en los sistemas sanitarios o bancarios.
- **Threat Intelligence.** Proporciona información, basada en el conocimiento y la experiencia previa almacenada sobre la ocurrencia y evaluación de amenazas físicas y lógicas con el objetivo ayudar a mitigar, pero sobre todo prevenir, posibles ataques y eventos dañinos que puedan ocurrir.
- **Ficheros log de red y de sistema.** Son los eventos que generan los dispositivos de red y los sistemas operativos de los dispositivos, en los que almacenan la información de cada una de las acciones que ocurren en ellos y que ayuda a monitorizarlos. Permiten obtener información en tiempo real del estado de un dispositivo, pero también se pueden analizar los pasados para obtener patrones de comportamiento o un historial.

[8]El Reglamento General de Protección de Datos es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos.

- **Políticas de acceso a datos.** De aquí es de donde el PE obtiene las políticas que están en cada momento en funcionamiento. Es importante que se consulte de manera periódica, y además en este caso externa, para que este actualizada en todo momento. Estas políticas también pueden permitir obtener conocimiento sobre los accesos que tienen habilitados los usuarios, o sobre posibles restricciones que estén impuestas.

- **Infraestructura de clave pública.** Fundamental para poder hace uso de encriptación mediante el uso de clave pública y clave privada. Este sistema es el encargado de generar y gestionar los certificados y las claves de cifrado que utiliza la organización. Su criticidad es máxima y debe ser una prioridad proporcionar seguridad a esta fuente.

- **Sistema de gestión de la identidad.** Se encarga de crear, almacenar y administrar las cuentas de usuario y los registros de identidad. LDAP es un ejemplo de este tipo de sistema, donde se almacena la información relevante de un trabajador, además de su información en relación con la empresa, como su rol, sus credenciales internas, elementos asignados, etc.

- **Security Information and Event Management (SIEM) system.** En español significa sistema de gestión de información y eventos de seguridad, se encarga de recolectar la información de seguridad para su posterior análisis. Podríamos decir que aplica una primera capa de procesamiento a los eventos de seguridad para su posterior envío.

Esta información se recoge, se almacena y cuando es necesario se procesa en tiempo real para decidir si se concede un acceso o no. Esta parte es realmente relevante, y es que es imprescindible el procesado en tiempo real. La confianza no se garantiza por defecto, y aunque se hagan comprobaciones para evaluar esta, la situación del usuario que intenta acceder (sujeto a partir de ahora) a un objeto, cambia. Es necesario tener en cuenta la situación actual en la que se encuentra el sujeto y esto solo se puede conseguir analizando la información en tiempo real. Este análisis, que utilizará tantos factores como sean necesarios en cada caso, lo lleva a cabo un software que se conoce como **Trust Algorithm**, o algoritmo de confianza, que determinará el nivel de confianza que se tiene sobre un sujeto en un momento concreto. Con esa información, el PE (Policy Engine) otorgará o no, el visto bueno para el acceso a la información.

Ese procesamiento se puede lograr de varias maneras y obtener resultados que utilicen diferentes métricas. Es importante que el algoritmo que procese los datos trabaje en consonancia con el resto de los elementos. Se verá una ligera idea de implementación de un algoritmo de este tipo en el próximo capítulo.

Una vez que un determinado sujeto tiene permiso para acceder a un determinado objeto, la PA genera un PEP para habilitar la comunicación. Este también puede generar la comunicación en base a diferentes métodos, pero el que yo considero más apropiado es el método de generación de sesiones. El PEP generará un .ºbjeto de sistema"llamado sesión, que recoge el sujeto que tiene acceso, el objeto al que tiene acceso y las restricciones o requisitos que se deben tener en cuenta durante la comunicación.

Estos requisitos son por ejemplo, la necesidad de reevaluación de la capacidad de acceso, las condiciones en las que puede acceder (solo lectura o lectura y escritura), el tiempo durante el que el objeto estará disponible, etc.

Por otro lado, se proponen ciertas posibles modificaciones al flujo de información que se propone en la5.1. Concretamente se proponen 4 variantes, de las cuales vamos a revisar las 2 que a mi juicio son las más útiles.

- **Device Agent/Gateway-Based Deployment.** Propone dividir el PEP en dos partes, una alojada en el sujeto, y otra en el objeto (no es necesario que esté en cada objeto, puede estar gobernando un grupo de objetos o una base de datos). Ahora es más sencillo de entender lo que es el PEP, puesto que, aunque ya no recibe ese nombre, es la comunicación que se generará entre el agente instalado en el sujeto (Agent) y el agente instalado en el objeto (Gateway(, que sigue siendo configurado por el *Policy Administrator (PA)*. Esto se puede ver detalladamente en la figura5.2.

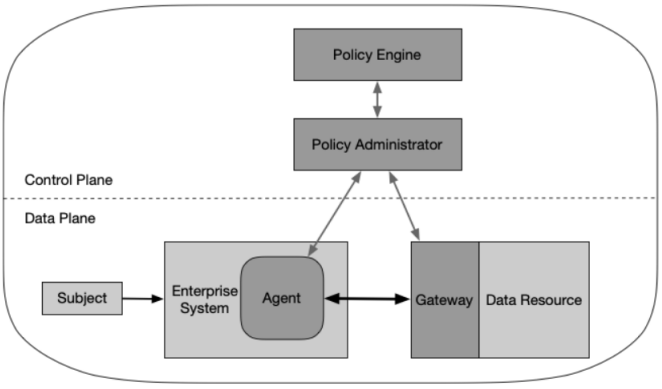

Figura 5.2: Device Agent/Gateway Variation, NIST[1]

- **Resource Portal-Based Deployment.** Aquí volvemos a tener el PEP unificado en un único elemento, pero en este caso haciendo de intermediario. A nivel lógico es prácticamente idéntico al modelo original, pero tiene la ventaja de que no es necesario instalar software en ninguna de las partes y que, además, el *gateway*, o lo que conocemos nosotros como PEP se puede externalizar, cuando por ejemplo, hacemos uso de servicios en cloud. En la práctica este sistema es un poco más complejo que el método de identificación y autenticación que se utiliza en un cliente web de un proveedor de servicios en cloud, pero la base es la misma.

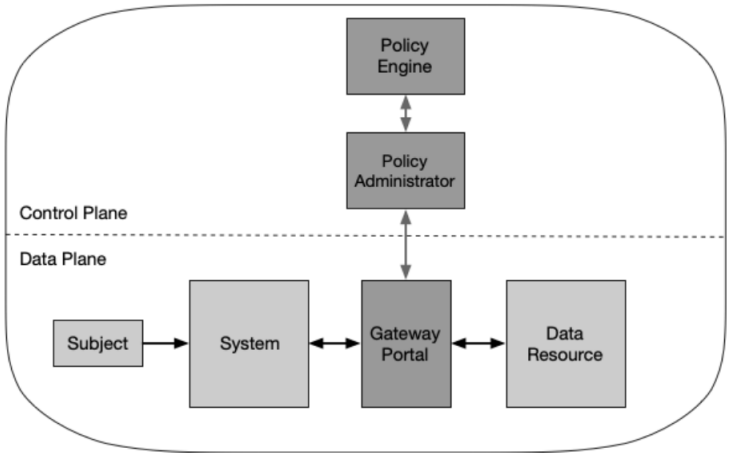

Figura 5.3: Portal Variation, NIST[1]

5.2.1 Zona implícita de seguridad

Este es uno de los puntos candentes de toda arquitectura de seguridad, es decir, en qué momento consideramos que un usuario está suficientemente autenticado como para dar por hecho que es él, y por lo tanto permitir el acceso a los recursos que tiene asignados. Lo único que se ha dicho al respecto hasta ahora es que esa zona debe ser lo más pequeña posible, y tratándose de una arquitectura de tipo Zero Trust, esta debe de estar lo más cerca posible del activo. Además, hay que tener en cuenta la fuerte segmentación que hemos hecho, por lo que podemos decir que la zona de implícita de seguridad es únicamente el propio activo o grupo de activos.

Esto quiere decir, que en el momento en el que el PA verifique mediante el PE la identidad del usuario, y genera el PEP, podremos decir que el usuario está autorizado a acceder al objeto. Recordar también el uso de las sesiones, las cuales generan las restricciones propias de esa conexión, como es por ejemplo, la duración de la misma. Por otro lado, el usuario habrá sido autorizado a acceder a un objeto o grupo concreto de objetos, que debe ser lo más pequeño posible, y sobre el que se le deben asignar la menor cantidad de privilegios que sean necesarios para que el usuario pueda cumplir su labor.

5.3 Dificultades de Implementación

Plantearemos como dificultades el impacto económico, la degradación de la experiencia de usuario y la necesidad de formación del personal. No se van a plantear complicaciones técnicas puesto que estas dependen de cada implementación concreta. Las dificultades específicas de implementación se verán en el próximo capítulo.

5.3.1 El Impacto Económico

Como ya hemos visto Zero Trust nos da unas guías de actuación, pero la implementación queda a cargo de cada empresa por lo que cada una puede variar sus métodos. Aun así, hay cosas que son

tan caras como imprescindibles, como la monitorización, las auditorías o las copias de seguridad. Este punto es realmente difícil de analizar de manera específica, por lo que vamos a ir haciendo ciertas suposiciones para simplificarlo.

Acabamos de hablar de las copias de seguridad por lo que vamos a empezar por ahí. Hoy en día podemos decir que gran parte de la información de las empresas está en cloud[9] por lo que los precios disminuyen, y además simplifica mucho el proceso, eliminando la parte física de la arquitectura, como la elección de los discos, las configuraciones RAID[10]etc. Aun así, una copia de seguridad consiste en duplicar toda tu información por si acaso la pierdes, por lo que para 1GB de datos válidos, necesitas al menos 2GB físicos. Esto no es necesariamente así según los sistemas utilizados para algunos tipos de copias de seguridad, pero no vamos a sumergirnos tanto en las posibles configuraciones que hay. Continuando con nuestra suposición de que para N GB de datos necesitamos 2N GB de almacenamiento, debemos tener en cuenta que esa copia de seguridad tiene que estar lo más separada posible de la copia original, tanto física como lógicamente. Además de que, si realmente queremos llevar la seguridad un paso más allá, deberíamos tener múltiples copias de seguridad realizadas a lo largo del tiempo almacenadas de manera simultánea, como ya se comentó en la primera parte de este capítulo.

Continuando con el impacto económico, vamos a hablar de los túneles VPN[18]. Lo suyo seria que cada persona que no esté físicamente en la organización, para poder acceder a los recursos empresariales este conectada a través de una VPN. No vamos a detallar las ventajas del uso de una VPN pero sí que esta redirección del tráfico de red es costosa. Al igual que en el resto de los casos, no puedo aportar cifras concretas, pero proporcionar servicios siempre conlleva un gasto.

Específicamente de la formación ya hemos hablado, al inicio del capítulo de su utilidad, y al final de este sobre los problemas que conlleva. Aquí por otro lado vamos a hablar brevemente del gasto económico, y es que hay certificaciones que superan ampliamente los 1000€. Por supuesto las hay mucho más baratas, e incluso gratuitas, pero la formación siempre va a requerir de un despliegue de medios y de personas que costará dinero, ya sea de manera directa o indirecta.

Las licencias son otro de los puntos caros en una implementación de este tipo. Prácticamente todas las herramientas corporativas requieren una licencia que es de pago. Estas licencias muchas veces se pagan por usuario y son anuales, de manera que es un gasto que viene para quedarse. Aquí entran las herramientas de trabajo, las herramientas de gestión y las herramientas de monitorización. Y por otro lado aparecen las licencias de fabricantes como las de *Trend Micro*, *Netskope*, *Imperva*, *Fortinet*, *Check-Point*, etc. que proporcionan herramientas o hardware para el funcionamiento de la red. El problema que conlleva un desembolso de este tipo es que estas pagando por un servicio y no por un activo, y eso para una empresa es un problema a nivel contable, porque se puede parecer más a un gasto que a una

[9] A grandes rasgos, el cloud o los servicios en cloud[16], consiste en externalizar elementos de la red tanto hardware como software, contratándolos a terceros que permiten realizar acciones de manera remota a través de internet.

[10] RAID es un acrónimo del inglés que significa *Redundant Array of Independent Disks*, literalmente «matriz de discos independientes redundantes», aunque no todos los sistemas RAID proporcionan redundancia. Según el tipo de RAID utilizado se puede conseguir redundancia de la información o mayor velocidad de acceso.[2]

inversión, aunque no vamos a profundizar más en el tema.

También serán necesarios la contratación de ciertos servicios como ya se ha comentado. Servicios de auditoría, que no son baratos, pero son muy necesarios por el estatus que te proporcionan; servicios de asesoramiento, a nivel financiero, técnico, legal, etc. que van a ser necesarios para asegurar que, llegado el caso, se cumple con la normativa vigente, o con cualesquiera que son los requerimientos impuestos; y servicios de seguridad, que proporcionen servicio 24x7 y asistencia en tiempo real en caso de sufrir un ataque; entre otros.

Y por último el punto más importante, que es el diseño, despliegue y mantenimiento de la red basada en una arquitectura de tipo Zero Trust. Se verá más en detalle en el próximo capítulo del documento, pero vamos brevemente a hablar de ello. Será necesario una planificación, una propuesta, una implementación con su correspondiente despliegue, la generación de un plan de pruebas para probar la correcta implementación que se ha hecho, y la generación de una documentación para el mantenimiento. Todo ello conlleva a un gran número de personas altamente cualificadas, y además, la interrupción, ralentización o interferencia del normal funcionamiento de la red durante el proceso de despliegue de la nueva solución que previsiblemente puede afectar al normal funcionamiento de la empresa, causando potenciales costes económicos.

5.3.2 Degradación de la experiencia de usuario

Este punto, junto con la formación, es lo que más va a afectar a los trabajadores. En este caso, lo va a hacer de dos maneras, de manera directa, mediante el incremento de los controles de seguridad; y de manera indirecta, mediante la ralentización del sistema.

Degradación directa de la experiencia de usuario. El número de controles de seguridad se va a incrementar y eso va a hacer que el usuario/trabajador deba pasar más tiempo pasando estos. Esta sería la diferencia entre los controles de seguridad que hay en una estación de autobuses, y los que hay en un aeropuerto. Los controles físicos de la organización puede que se vean incrementados, por lo que la libre circulación de personas en la organización será restringida. Habrá un mayor número de controles para controlar el movimiento de gente entre diferentes partes del edificio por la compartimentación que va a tener este, aunque como este no es el propósito de este documento, no vamos a entrar en detalles con ellos. Los controles software para utilizar el equipo corporativo si son más relevantes.

Se ha hablado ya de los controles de seguridad por lo que aquí hablaremos únicamente de como estos degradan la experiencia de usuario. Una estricta política de contraseñas hará que los usuarios deban tener almacenadas una gran cantidad de contraseñas, y además se verán obligados a cambiarla regularmente. Por otro lado, el doble factor de autenticación para iniciar sesión en las aplicaciones será un dolor de cabeza que se deberá afrontar. El número de sitios en los que se solicita la contraseña dentro del entorno corporativo se verá incrementado, a la vez que se reduce la duración de las sesiones por lo que los usuarios verán como estas se cierran automáticamente, aumentando aún más el número

de veces que será necesario autenticarse.

Por otro lado, la fuerte restricción del uso de dispositivos personales, y de aplicaciones no corporativas tampoco hará gracia a los usuarios. Es cierto que, en un principio, en horario laboral no se deberían de utilizar ni dispositivos personales (salvo excepciones), ni aplicaciones no corporativas en los ordenadores o dispositivos de la empresa; el problema es que sí que se utilizan, y su restricción no va a sentar bien a nadie. No sería la primera vez que se abre un ticket al soporte informático alegando problemas en el uso de aplicaciones como *Youtube*, *Facebook* o *TikTok* después de que estas fueran restringidas. Los usuarios no solo no podrán utilizar aplicaciones recreativas, si no que las aplicaciones que deberán usar en el trabajo estarán fuertemente restringidas, limitando la capacidad de cada usuario de elegir por ejemplo, si prefiere el cliente de *Gmail* o el de *Outlook* para su correo electrónico.

Degradación indirecta de la experiencia de usuario. Aquí nos referimos a la ralentización del sistema debido a la monitorización que se hace de él. Empezando por la necesidad del uso de VPN para poder trabajar desde fuera de la organización. Esta no hará las comunicaciones radicalmente más lentas, pero si añade un cierto retardo y una cierta complicación para quien es ajeno al mundo de las tecnologías. A nivel interno, al análisis en tiempo real del tráfico también ralentiza el funcionamiento de la red; los paquetes de red serán analizados por diferentes capas de software y pasarán seguramente por múltiples firewalls y al igual que en el caso anterior, el retardo introducido por cada dispositivo o tecnología de manera individual no es demasiado, pero el conjunto se nota.

5.3.3 Necesidad de formación

También hemos hablado largo y tendido de la formación durante este capítulo, de manera que la explicación será breve y concisa. Conseguir que la gente esté concienciada de los peligros que acarrea el uso incorrecto de los dispositivos electrónicos es complicado, pero el objetivo va aún más allá, y es conseguir que la gente este suficientemente concienciada como para que busque formación por su cuenta y así evitar ponerse en riesgo a sí mismos o a la organización para la que trabajan. Esta tarea para gente en puesto lejos del mundo de la informática es prácticamente imposible, y más cuando hablamos de personas de más de 50 años.

Por eso las empresas deben encontrar la manera de conseguir que la gente este correctamente formada, y eso conlleva tiempo y dinero. En primer lugar, por ofrecer la formación, y pagar los cursos, los profesores y los exámenes, pero por otro lado, esta formación muy seguramente se deba desarrollar en horario laboral, sobre todo si quiere implantarse de manera obligatoria. Perder horas productivas conlleva una gran pérdida económica, pero eso es algo que la empresa debe prever en su plan económico. Esta formación puede ser teórica, sobre conceptos relevantes, o práctica, para enseñar a utilizar nuevas herramientas propuestas por la implementación de Zero Trust como, por ejemplo, el doble factor de autenticación.

Además, sería interesante que una empresa que esté interesada en tener y mantener unos trabaja-

dores formados, ofreciera ciertos beneficios a la gente con una mejor formación, como posibilidad de teletrabajo o flexibilidad de horarios y de vacaciones; o incentivos económicos, como un aumento de sueldo, un aumento en los días de vacaciones, una mejora en las condiciones laborales, etc. De nuevo, prácticamente todos los incentivos posibles conllevan un gasto económico por lo que, al igual que lo mencionado al principio del capítulo, todo se reduce a la gestión económica de la empresa.

Capítulo 6

Implementación de Zero Trust

Aquí comienza la fase más práctica de este documento, que consiste en proponer un caso lo más parecido a la realidad que sea posible, en el que se tratará de implementar de la manera más rigurosa que se pueda una *Zero Trust Network Architecture*. La mayor parte de la información se ha obtenido de *ZeroTrustRoadMap*[4] que es una web propiedad de *Cloudflare* específicamente dedicada explicar los pasos de implementación de una propuesta de este tipo. Por otro lado, se pondrán en práctica en mayor o menor medida todos los conceptos teóricos vistos hasta ahora, aportando el mayor grado de precisión que sea posible.

6.1 Propuesta del caso de estudio

La implementación de la ZTNA se hará sobre un escenario ficticio lo más parecido a la realidad que sea posible. Se realizarán las simplificaciones que sean necesarias para facilitar el desarrollo y la explicación de los conceptos.

La empresa del caso de estudio es una cadena de supermercados llamada ACME. Dicha empresa dispone de supermercados en 3 ciudades y en cada ciudad dispone de 3 supermercados. En una de esas ciudades tiene además las oficinas centrales y en otra de ellas el almacén principal, es decir, 9 supermercados, un almacén y unas oficinas. Dispone a su vez de 5 departamentos que son recursos humanos, contabilidad, logística, servicio y mantenimiento.

- **Recursos humanos.** Se encarga de la gestión legal del personal. Únicamente opera en las oficinas.
- **Contabilidad.** Se encarga de la gestión monetaria. Opera en las oficinas y en los supermercados.
- **Logística.** Se encarga del movimiento de material y de su almacenamiento. Opera en el almacén y en cada uno de los supermercados.

- **Servicio.** El personal que trabaja en los supermercados y que realizan en ellos la mayoría de las labores. Opera únicamente en los supermercados.
- **Mantenimiento.** Están agrupados aquí el servicio de limpieza y el servicio que se encarga propiamente del mantenimiento. Operan en todos los lugares de la empresa.

Adicionalmente se dispone de dos técnicos de TI para el mantenimiento de la infraestructura de red. Estos dos técnicos son los administradores, y cada uno dispone de un ordenador portátil proporcionado por la empresa.

Cada supermercado tiene 32 personas de servicio, 6 de logística, 1 de contabilidad y 2 de mantenimiento. Es decir, en los supermercados trabajan 288 personas de servicio, 54 personas de logística, 9 personas de contabilidad y 18 personas de mantenimiento. En el almacén principal trabajan 8 personas de servicio, 23 de logística, 1 de contabilidad y 6 de mantenimiento. Por último, en las oficinas centrales trabajan 4 personas de recursos humanos, 5 de contabilidad y 1 de mantenimiento. Por lo tanto, el número total de trabajadores en la empresa es de 417. Es decir, 4 personas en recursos humanos, 15 personas en contabilidad, 77 personas en logística, 296 en servicio y 25 personas en mantenimiento.

Estos trabajadores hacen uso además de una serie de dispositivos que utilizan la red de la empresa, que son los siguientes:

- Teléfonos de empresa. Teléfonos proporcionados por el departamento de TI y monitorizados por ellos. Los teléfonos son de diferentes marcas, todos con sistema operativo Android, pero con diferentes versiones. Solo los departamentos de Recursos humanos, contabilidad y los repartidores a domicilio del departamento de logística disponen de uno de ellos. En total la empresa tiene desplegados 59 teléfonos de empresa.
- Ordenadores. Ordenadores de trabajo personales y compartidos proporcionados y monitorizados por la empresa. Algunos son ordenadores portátiles y otros de escritorio, de diferentes años y generaciones, algunos con Windows 7 y otros con Windows 10. Algunos de los ordenadores están conectados por cable y otros por Wi-Fi. Solo los departamentos de recursos humanos y contabilidad dispondrán de ordenadores de trabajo. En total son 59 ordenadores personales lo que la empresa tiene bajo control, más los dos ordenadores de los administradores de la red.
- Cajas registradoras digitales. Cada supermercado tiene en producción 7 cajas registradoras conectadas por cable RJ45 a la red de la empresa. En total son 63 cajas registradoras.
- Terminales de control. Son aquellos dispositivos que permiten comprobar el inventario, modificarlo, consultar precios, etc. Son terminales inalámbricos, y cada miembro tanto del departamento de servicio como del de logística posee uno.
- Elementos del sistema de seguridad. Como alarmas sonoras, sensores (de movimiento, temperatura, humedad, humo), cerraduras de puertas, rastreo de camiones de reparto, cámaras de seguridad, etc.

La organización dispone de varios dominios web que proporcionan varios servicios, permitiendo la realización de compras por internet para los usuarios registrados en la aplicación.

Para simplificar el caso de estudio vamos a suponer que no se dispone de infraestructura previa, de manera que no se va a detallar el despliegue antiguo para posteriormente sobre el montar el nuevo; únicamente se hablará de como desplegar una ZTNA sobre una organización como la que se plantea.

Por otro, tampoco se va a detallar el presupuesto del despliegue ni el coste de las soluciones hardware y software propuestas, puesto que en la mayoría de los casos no son accesibles por la gente ajena al mundo de las arquitecturas de seguridad desde un punto de vista profesional.

6.2 Despliegue de la ZTNA

Como ya se ha dicho, en un principio y mientras lo considere oportuno, vamos a seguir la propuesta de despliegue detallada en la página web *zerotrustroadmap*.

6.2.1 Usuarios

Aquí dentro se incluyen los trabajadores, el personal subcontratado y los clientes. Se debe saber quién es quién, y qué permisos tiene.

La identificación de los trabajadores se divide en dos. Por un lado, la identificación software dentro del sistema, que se llevará a cabo mediante un sistema *Microsoft Active Directory*, AD de ahora en adelante; y la identificación física, mediante contraseñas para abrir las puertas, huellas dactilares, tarjetas de identificación, etc.

Cada usuario tendrá un usuario dentro del dominio local, que será ACME.local. Los usuarios se generarán concatenando la primera letra del nombre con el apellido. Si esto generara usuarios repetidos, se haría concatenando la primera letra del nombre, la primera letra del primer apellido y el segundo apellido. Por su parte los administradores deberán tener dos cuentas, un usuario normal sin privilegios para realizar la mayoría de las funciones corporativas, el cual deberá utilizar la misma nomenclatura que la del resto de usuarios; y un usuario administrador que solamente utilizarán cuando sea estrictamente necesario. Cada uno dispondrá de su propio usuario administrador del dominio para que sea más sencillo saber qué administrador hace qué. Estos usuarios serán del tipo *amartinez.admin*.

Solo los trabajadores disponen de una cuenta de dominio, que además servirá para iniciar sesión dentro de la red inalámbrica corporativa. Esto se llevara a cabo mediante una SAM[1] que permite llevar a cabo autenticaciones de usuarios directamente contra el directorio activo. Por otro lado, se dispondrá de

[1]El administrador de cuentas de seguridad o SAM es una base de datos almacenada como un fichero del registro en Windows NT, Windows 2000, y versiones posteriores de Microsoft Windows. Almacena las contraseñas de los usuarios en un formato con *hash*.

una red Wi-Fi de invitados para usuarios que quieran acceder a internet sin necesidad de autenticación.

Para poder hacer uso del doble factor de autenticación hay varias opciones disponibles. Una de las más comunes es mediante *Google Authenticator* o similares, que generan una OTP (*One Time Password*) en el teléfono móvil, la cual se debe de introducir en el ordenador. Por otro lado, y más habitual en este tipo de entornos, es el uso de lectores de tarjetas físicas. Para poder iniciar sesión mediante una tarjeta, será necesario configurar correctamente el controlador de dominio, y firmar las tarjetas de manera que sean consideras seguras en el proceso de autenticación. En nuestro caso y siempre que sea posible, se utilizará un doble factor de autenticación mediante la generación de OTP por aplicaciones externas como *Google Authenticator* o *Microsoft Authenticator*, que cada usuario deberá tener instalado en su teléfono móvil.

Por supuesto la contraseña deberá cambiarse en el primer inicio de sesión, y adicionalmente deberíamos forzar a un cambio de contraseña cada 6 meses. Se recomienda un cambio cada 3 meses, pero considero que 6 meses sigue aportando un buen nivel de seguridad. Por otro lado, y según las restricciones impuestas por Microsoft para Azure Active Directory, la contraseña debe tener un mínimo de 8 caracteres y un máximo de 256 caracteres y se requiere que cumpla al menos tres de los cuatro requisitos siguientes:

- Contener caracteres en minúsculas.
- Contener caracteres en mayúsculas.
- Contener números (0-9).
- Contener un símbolo.

6.2.2 Endpoints y dispositivos

Esta sección incluye la identificación de todos los dispositivos, APIs, software y servicios de los que dispone la organización por lo que iremos por partes. Vamos a empezar con la identificación de teléfonos móviles y ordenadores de trabajo.

Ordenadores de trabajo y dispositivos móviles. En este caso vamos a mantenemos alejados de la corriente BYOD, *Bring Your Own Device*, puesto que genera ciertos problemas de seguridad que no merece la pena asumir. Proporcionados por la empresa y como se comentó en el apartado anterior, encontramos 59 teléfonos móviles de empresa y 59 + 2 ordenadores de trabajo corporativos. Para los teléfonos móviles será necesario instalar una aplicación de gestión de dispositivos móviles que en nuestro caso será *Scalefusion*. Es un software barato de monitorización de dispositivos móviles, muy potente, y que permite generar entornos de tipo quiosco[2], ideales para los terminales del equipo de reparto a domicilio. En el caso del resto de trabajadores servirá para cifrar los datos y monitorizar el

[2]Un entorno de tipo quiosco permite generar una interfaz de usuario altamente restringida que no permite el acceso a ningún tipo de configuración y en el que únicamente están permitidas una serie de aplicaciones concretas.

estado de los dispositivos. Tiene un precio de 4$ al mes por dispositivo para la versión empresarial y ofrece una alta capacidad de monitorización. Por otro lado, se auditará la dirección MAC de la tarjeta de red del dispositivo, el número de serie y el numero IMEI[3]. Todos los dispositivos deberán además tener una versión de Android igual o superior a la 10, para seguir recibiendo actualizaciones de seguridad.

Para los ordenadores se utilizará un sistema operativo Windows 10 o Windows 11 actualizado a la última versión disponible en cada caso. Serán configurados totalmente por los técnicos e introducidos en el controlador de dominio de la empresa. Se recogerá su número de serie y la dirección de su tarjeta MAC. Además, todos los ordenadores deberán tener el disco duro cifrado mediante *bitLocker*. En cuanto al antivirus, además de tener *Windows Defender* y el *Windows Firewall* siempre activos, se instalará un software de protección extra que cubrirá de manera más específica estas necesidades. Se utilizara el *Netskope* como proxy web y CASB para monitorización de accesos a recursos corporativos, tanto en cloud como en local. Por último como EDR haremos uso de *ApexOne* que es la solución de Trend Micro para esta situación. SentinelOne tal vez ofrezca un mejor desempeño como EDR en relación calidad/precio pero de esta manera tendremos todas las soluciones de seguridad activas centralizadas dentro de la misma aplicación, *Trend Micro Vision One*, lo que facilitará la gestión y la monitorización. *Crowdstrike* es una opción mucho más avanzada para esta labor pero es mucho más cara y las características extra que aporta no son realmente necesarias.

Software y APIs. Este caso no es tan problemático porque no es una empresa que tenga una gran cantidad de software en propiedad. Aun así, sí que dispone de cierto material software relevante como es su página web (con todo el contenido que esta tiene), su versión personalizada de CRM, la aplicación de comercio electrónico (realmente podría ser considerado un módulo de la página web) y una aplicación de gestión de inventario interna, propiedad de ACME pero desarrollada por equipos externos subcontratados.

6.2.3 Trafico de internet

En este punto se va a realizar el diseño de la arquitectura de red utilizada, especificando en la medida de lo posible el hardware y el software que se utilizará en cada caso. No se va a detallar la configuración de las redes LAN ni VLAN ni tampoco las conexiones VPN que se establecen entre las diferentes sedes de la empresa.

Aunque todos los supermercados pertenecen a la misma red, cada uno es una entidad independiente muy separada geográficamente del resto, por lo que habrá que tener cuidado. En primer lugar, cada sede necesita su propia conexión a internet, en principio sin necesidad de redundancia. Siempre es beneficioso tener varias líneas contratadas como se vio en apartados anteriores, pero en este caso no será necesario. Si será necesario disponer de un pequeño router para cada sede, que permita además

[3]IMEI significa *International Mobile Equipment Identity*, y es un identificador único que tiene cada teléfono móvil. Esto quiere decir que el número IMEI de cada teléfono es único en el mundo, y sirve para identificar dispositivos en las comunicaciones que este realiza.

generar túneles VPN *site-to-site*[4] de manera que no sea necesaria la compra de un dispositivo específico para ello.

Firewalls. Hay muchas marcas de firewalls de alto rendimiento como *Fortinet*, *Cisco*, *Palo Alto*, *CheckPoint*, *SonicWall* o *WatchWard* entre otros. Ofrecen soluciones físicas y virtualizadas, siendo en nuestro caso las físicas las más interesantes. Elegiremos el modelo PA-820 de *Palo Alto Networks*, que es un modelo profesional pero de gama de entrada, ideal para el volumen de tráfico que se va a generar. Aun siendo de gama de entrada, hay margen para que cada sede de la empresa pueda ampliarse y crecer puesto que no son equipos que van justos en potencia. Palo Alto lo vende además como el primer cortafuegos de nueva generación con aprendizaje automático para prevenir ataques sin firma en línea. Por otro lado, realiza un análisis de capa 7 basado en aplicación y no en el puerto por lo que en principio podría no ser necesaria la instalación de software de análisis de capa 7 como Netskope o ZScaler. En cualquier caso, esto se discutirá más adelante. Otra característica interesante es el control del uso de protocolos TLS obsoletos. Su precio oscila entre aproximadamente los 4000 y los 9000 dólares según el paquete contratado. Además este firewall también servirá como concentrador VPN y dispone de modulo IPS[5] que es ideal en un despliegue de tipo Zero Trust

Únicamente será necesario un firewall en la red de la organización, que se encargará de establecer los túneles VPN punto a punto, y de filtrar todo el tráfico exterior de la organización. El esquema lógico de cómo está conectado dicho firewall se puede ver en la figura 6.1. Las conexiones entre sedes se realizan a través de internet mediante túneles VPN*site-to-site* configurados directamente entre el router de cada una de las sedes y el firewall. Por otro lado, vemos la conexión con la terminal de administración de Azure. De nuevo, es una VPN *site-to-site* configurada desde dicho portal para que únicamente admita conexiones desde dispositivos que se encuentren en la LAN de administración, que es la 10.1.0.0/16 a la cual se accede introduciendo las credenciales correctas en el cliente de escritorio de la VPN de palo-alto. Eso permite que un ordenador con una dirección IP cualquiera pueda ser identificado como un ordenador que pertenece a la red 10.1.0.0/16 si se dan las condiciones necesarias. La configuración y autenticación de los accesos a la VPN es de nuevo realizada a través de una SAM directamente contra el controlador de dominio, que en este caso está alojado en Azure. Además, este firewall también está conectado a la red de la oficina central, que es donde físicamente se encuentra, a través de un router para poder separar entre diferentes redes como veremos más adelante. Además, en este caso no es necesaria VPN porque están conectados físicamente de manera directa.

Por último, la conexión a internet. Todos los accesos a internet de toda la empresa se realizan a través del mismo punto a mediante un ISP. Concretamente se realizan a través de dos conexiones con dos ISP diferentes. En este caso no es necesario introducir un balanceador de carga porque las

[4]Las VPN site-to-site son aquellas en las que dos máquinas con IPs estáticas se conectan la una a la otra sin posibilidad de modificación. No es necesaria la autenticación y aumenta la seguridad por no requerir inicios de sesión.

[5]Un IPS o *Intrusion Prevention System* es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. El IPS podría ser considerado como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.

necesidades de conectividad que se requieren no son demasiado altas. Hay un enlace principal que es el que se utiliza habitualmente y uno secundario que se utiliza como *backup*. Esto solo ocurre en las oficinas centrales, en el resto de los casos la conexión con el ISP es única.

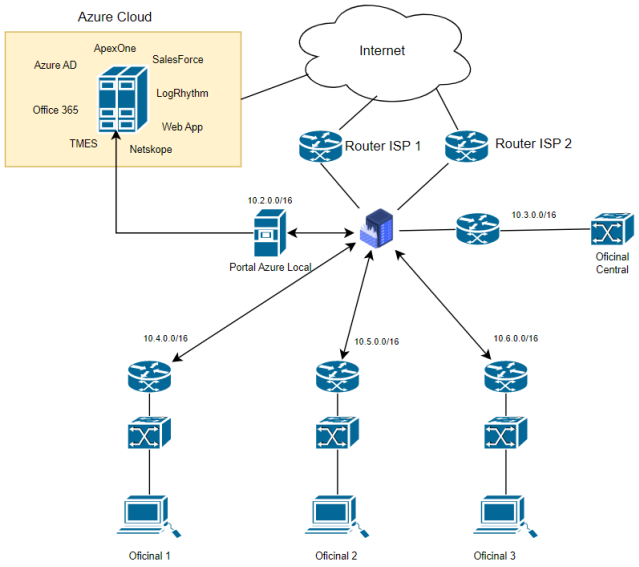

Figura 6.1: Esquema principal de la red

Routers. Usaremos los *Cisco Meraki MX75*, que según cisco soportan hasta 200 usuarios y el software propietario de cisco para la generación y administración de SD-WAN (*Software Defined Wide Area Network*), que en esta implementación no será necesario porque utilizaremos túneles VPN para la extensión geográfica de la red, pero que podría ser interesante en un futuro para poder gestionar de manera unificada la red entera. Además permite hasta 500Mbps de tráfico *VPN site-to-site* que es ideal para poder montar los túneles con el otro extremo, en el que estará el *PaloAlto PA-820*. Por otro lado, dispone de puertos RJ-45 que soportan Ethernet a 10Gbps en LAN, que es una característica que de momento no es necesaria pero podría ser una mejora muy interesante para ampliar la red en un futuro. Por supuesto, soporta todos los protocolos propietarios de Cisco. Su precio es de algo menos de 2000€ y será necesaria la instalación de uno de estos en cada sede, para gestionar el tráfico entre diferentes subredes y poder encaminarlo correctamente.

Switches. Aquí nos vamos a decantar de nuevo por la marca Cisco, concretamente por su gama centrada en la gestión de redes LAN de empresas de tamaño mediano. Esta es la gama *Bussines* concretamente la serie 250, que sería una especia de gama media. El modelo elegido es el *CBS250-24T-4G* como *switch* de distribución, que tienen un precio de unos 330€ y características suficientes para el desempeño que buscamos. Será necesario uno de estos switches para cada sede, que en muchos casos actuaran como switches centrales, haciendo uso de sus puertos de 4 Gbps. Para los switches de acceso (los que conectan directamente hosts) usaremos otros más asequibles que son los *CBS110-16PP*, un modelo de *switch* no gestionable con 16 entradas que soporta PoE[6] lo cual es una característica

[6] *Power-over-Ethernet* es el mecanismo que permite la transmisión de energía eléctrica a dispositivos compatibles.

interesante para, llegado el caso, poder conectar por ejemplo cámaras de seguridad o sensores entre otras cosas. Estos dispositivos tienen un precio de unos 200€, aunque depende del distribuidor.

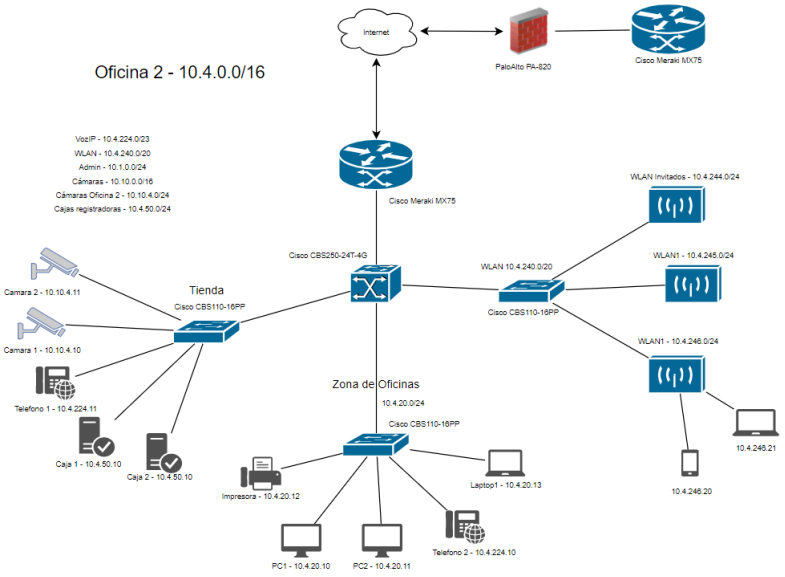

Figura 6.2: Diagrama de red de la sede 1

6.2.4 Redes

Aquí vamos a explicar brevemente cómo están distribuidas las redes y las subredes en el conjunto de la red corporativa. Cada una de las oficinas físicas tendrá asignada una red de tipo 10.X.0.0/16 tal y como se puede ver en la figura6.2. Por otro lado, la terminal de administración de los *routers* y *switches* tendrá asignada una dirección de la red 10.1.0.0/24. En la figura6.2 se puede ver cómo están distribuidas el resto de subredes.

En cuanto a la administración, será necesario habilitar la opción de *UDP forwarding* en los switches, para que cada router haga de servidor DHCP centralizado dentro de cada una de las sedes. Por otro lado, y dado que los equipos de Cisco lo permiten, convertiremos la red en una SND o por sus siglas en español en una *Red Definida por Software*, que permite la centralización de la administración de dispositivos para que la toma de decisiones sea central. De la misma manera, se utilizará OSPF, *Open Shortest Path First* como protocolo de encaminamiento, que es propietario de Cisco. Por el contrario, será necesario desactivar todo el filtrado y análisis de paquetes de capa 7 que se hace en los *routers*, puesto que ralentiza el flujo de información y además es redundante, puesto que Netskope se encarga de esa función de una manera más precisa.

No vamos a detallar la creación de ACLs, *Access Control Lists*, porque no entra dentro del alcance del proyecto, pero si es importante remarcar su importancia y la necesidad de una buena configuración de seguridad en los *routers*.

Esto es posible mediante el mismo cable de red que permite la conexión a las redes de área local.

6.2.5 Aplicaciones

Aquí se deben tomar un buen número de decisiones importantes de cara a la experiencia de usuario que puedan recibir los trabajadores. Se les debe proporcionar un entorno de trabajo cómodo y eficiente que les permita desarrollar su trabajo de manera eficiente.

Ofimática. Aquí vamos a hacer uso de Microsoft 365 por el simple hecho de que incorpora un buen número de aplicaciones que ya son conocidas por la mayoría de trabajadores, como son *Word*, *Excel* o *PowerPoint* entre otras. Además de ser ya conocidas, estas aplicaciones son muy versátiles y potentes para la realización de una gran cantidad de tareas, desde la gestión contable hasta la realización de documentos legales, o presentaciones corporativas. Ofrece un precio por usuario relativamente asequible.

Correo electrónico. De la misma manera que para aplicaciones de ofimática en mi opinión es mejor Microsoft, para el cliente de correo electrónico es mejor Google. Los correos serán corporativos y se dispondrá de un servidor propio de correo electrónico, pero para la visualización y el trabajo diario se utilizará por defecto *Gmail*. Ya es utilizado por la mayoría de los usuarios por lo que no requiere formación ni periodo de adaptación.

Mensajería instantánea y videoconferencias. La decisión aquí no se toma en base a la experiencia previa que tengan los usuarios en el uso de las aplicaciones, puesto que tanto Microsoft Teams como *Google Meets* son dos aplicaciones rara vez utilizadas fuera del entorno corporativo. En este caso nos decantaremos por Microsoft Teams sin ninguna duda. La opción de Google está dividida realmente en 2 aplicaciones que son *Google Meets* y *Google Chat*, una para las videoconferencias y otra para la mensajería instantánea lo cual complica el uso habitual de estas herramientas. Tras haber utilizado ambas, considero que *Google Meets* es un poco superior en experiencia de usuario a Microsoft Teams, pero esta integra más opciones que son necesarias en un entorno corporativo de este tipo. Además, Teams puede cerrarse a usuarios externos de manera que no se pueda haber contacto con personal del exterior de la organización. Los archivos compartidos se guardan directamente en el *Sharepoint* corporativo y tiene buena integración con *Netskope*, que lo veremos más adelante.

Por otro lado en ocasiones surge la necesidad de utilizar otro tipo de aplicaciones de mensajería como *WhattsApp* o *Telegram*, sobre todo para el contacto corporativo con personal ajeno a la empresa. En este caso, se permite el uso de ambas siempre y cuando se haga desde teléfonos corporativos, y no se permite el inicio de sesión web en ordenadores que no sean corporativos, especialmente para el uso de *Telegram*, que por la gestión de las sesiones de usuario que tiene hace que sea un poco más vulnerable.

CRM. También conocido como *Customer Relationship Management* es la aplicación encargada de gestionar el contacto con tus clientes y proveedores. Además, proporciona y gestiona la información del funcionamiento de estas relaciones y permite conectar tu organización otras intercambiando información o servicios. En el caso propuesto es la aplicación encargada del contacto con los proveedores y de proveedor datos para la venta online de artículos. Una de las opciones más utilizadas es *SAP*, que ofrece un CRM caro pero altamente personalízale para ajustar a cada modelo de negocio; otra opción

es SalesForce, una solución Cloud menos modificable pero más potente en cuanto a la descentralización; *Odoo* también ofrece una solución según dicen ellos más centrada en el cliente, lo cual para nosotros no es relevante puesto que nosotros el CRM lo necesitamos para el contacto con proveedores, cuyo número es más limitado. Elegiremos por la tanto la opción con SalesForce puesto que ofrece una gran integración con plataformas de todo tipo, por ejemplo con *Azure* y *AWS*, con plataformas de *ticketing* como *ServiceNow* o con plataformas de monitorización como *Varonis*. Dispone también de *APIs* muy potentes en varios lenguajes para la extracción de datos, muy útil para nuestra aplicación de comercio electrónico y para la aplicación de gestión de inventario. Aun así, SalesForce también permite un buen nivel de personalización en sus opciones más caras. Para nuestro caso concreto será necesario hacer uso de la versión *Professional* o de la versión *Enterprise* que tienen un precio de 75 y 150 dólares por usuario al mes respectivamente.

Gestión de inventario. Esta es una aplicación simple, desarrollada ad-hoc para el tipo de negocio. Es una aplicación que apenas permite personalización, muy restrictiva, muy sólida a nivel de seguridad, y con actualización no demasiado regulares, pero si eficaces. Básicamente se encarga de tener organizados los precios de los productos, la cantidad de productos disponible en cada sede y de generar gráficos para hacer predicciones simples de los consumos de productos en base a los datos recogidos en el pasado. Esta aplicación está diseñada para ser accesible desde los dispositivos empotrados de gestión que hay en los almacenes y por los lectores de códigos de barras que tienen los trabajadores. Almacena la información en una base de datos SQL alojada en *Azure* para poder tenerla accesible por toda la organización.

Monitorización de tráfico. Estas aplicaciones son aquellas que se utilizan para conocer el tipo de tráfico que circula por la red, y las aplicaciones que se utilizan. Vamos a utilizar 3 tipos de aplicaciones para lograrlo. Un EDR para la seguridad de los *endpoints* se comentó que utilizaríamos *Trend Micro*, un CASB[7] para la monitorización del tráfico de red y de los *endpoint* (*Netskope*, *Trend Micro*, *ForcePoint*, *ZScaler*...) y un *antispam* de correo para el filtrado automático previo al filtro aplicado en el propio *exchange* de correo.

- **EDR.** Podría utilizarse un antivirus en lugar de un EDR, pero dada la cantidad de tráfico cloud que tenemos, y que se almacenará una gran cantidad de información de usuarios (incluyendo sus tarjetas de crédito) es mejor optar por una opción un poco más robusta. Comenzamos por aquí porque es donde se proporciona la seguridad a nivel de *endpoint*. A diferencia del resto de herramientas que veremos a continuación, un EDR funciona incluso cuando el dispositivo no esté conectado a la red corporativa, cuando se esté accediendo a recursos no corporativos, e incluso cuando el ordenador este sin conexiones a internet. Utilizaremos *ApexOne* de *Trend Micro*, para centralizar un poco su administración en *ApexCentral* (junto con TMES que lo veremos más adelante). En cierto modo es una aplicación cloud, puesto que el núcleo principal esta centralizado en cloud, desde donde se generan las políticas, donde están las firmas de ataques, y donde se

[7]Un agente de seguridad de acceso a la nube, abreviado como CASB, es un punto de cumplimiento de directiva de seguridad que se posiciona entre los usuarios de la empresa y los proveedores de servicio en la nube.

monitorizan los equipos. Sin embargo, a su vez, es estrictamente necesaria la instalación de un cliente software en cada ordenador. *Crowdstrike* es seguramente el ejemplo más famoso de EDR. La principal ventaja de un software de este tipo es que puede aplicar remediación manual o automática, permitiendo incluso aislar a un equipo de la red en caso de que se detecte que puede estar comprometido. No vamos a detallar políticas de implementación específicas.

- **CASB.** En nuestra organización vamos a utilizar *Netskope*, que es una aplicación cloud que tiene una consola central alojada en el cloud, que recibe las conexiones de las aplicaciones de escritorio instaladas en los ordenadores de los trabajadores. Esto permite mucho control y un gran abanico de opciones, entre ellas la utilización de estas aplicaciones como proxy de navegación y como CASB (*Netskope* ofrece otros servicios además del de CASB). Como proxy de navegación, permite añadir reglas para no permitir el tráfico hacia un cierto tipo de direcciones, como pornografía o páginas de apuestas online, puedes cortar el tráfico hacia direcciones específicas como *Facebook* o *Youtube*, y lo puedes hacer tan granular como sea necesario. Por ejemplo, se puede permitir el acceso a Youtube solo en horario de comida, por ejemplo, de 2 a 4. Por otro lado, puede optar por no bloquearlo, pero si controlarlo, para saber qué hacen los usuarios durante la jornada laboral.

  Para su uso como CASB tiene una integración total con *Office365* y concretamente con *Microsoft Sharepoint*, que es la nube común que utiliza *Office365* para sincronizar todas sus aplicaciones, como OneDrive o Teams, entre otras. Esto permite que puedas controlar la subida y bajada de archivos, y además puedas leerlos, para generar reglas no solo en base a la ubicación, el nombre o el tamaño del archivo, sino también en función de su contenido. Estas políticas se pueden aplicar individualmente e igual que en el caso del proxy de navegación pueden ser tan granulares como se quiera, filtrando por directorios, por horarios, por tamaños de archivos, por cantidad de archivos, por la acción que se está realizando (subida o bajada), etc. Esto no sustituye la configuración de OneDrive donde también se deben aplicar restricciones, pero más centradas en los accesos y no en la monitorización.

- **AntiSpam.** El *antispam* perimetral filtrará todo el tráfico de correo dirigido al servidor de correo corporativo ANTES de que este sea entregado, por lo que la remediación que se puede aplicar es previa a que el correo entre en *Office365*, por lo que los usuarios no entran en contacto con el correo. Además de *TMES* que es la opción elegida también hay otras opciones como *Cisco* con su *CES* (Cloud Email Security). No vamos a especificar las políticas que se deben implementar pero si es importante mencionar que la granularidad y la precisión del filtrado que ofrecen estas aplicaciones es muy superior a la que ofrece *Office365* de manera nativa. *TMES* es una solución cloud que automáticamente filtra el correo electrónico dirigido al servidor de correo redirigiendo el tráfico, y una vez que se ha analizado el correo este es entregado al *exchange*.

6.2.6 Prevención de pérdida de datos

Aquí podemos encontrar dos variantes principales que son, por un lado, los datos y archivos que generan los trabajadores para poder realizar sus funciones; y por otro lado los datos que generan las

aplicaciones para su correcto funcionamiento, como por ejemplo el historial de precios de un producto, las actualizaciones del inventario, o la información de los clientes que realizan compras online.

Datos de usuarios. Puesto que estamos utilizando la suite de aplicaciones de Microsoft, podemos hacer uso de *OneDrive*[8] que además tiene una integración realmente buena con Microsoft Windows. Todos los archivos de todos los usuarios deberán estar subidos a sus respectivas cuentas de *OneDrive*, y quedará prohibido el trabajo en archivos fuera de línea. Esto no quiere decir que no se permite editar archivos locales con las aplicaciones de escritorio, tanto de Microsoft como de otros proveedores, si no que los archivos deberán ser cogidos directamente de *OneDrive* y actualizados de nuevo al guardar. Esto deberá hacerse por defecto y de manera automática. También se deberá sincronizar la carpeta de Descargas, la de Escritorio y la de Documentos para evitarla pérdida de información por posibles despistes. *OneDrive* ya permite de manera nativa recuperar archivos perdidos mediante una papelera virtual que almacena los archivos durante un determinado periodo, 90 días para la versión corporativa de la aplicación. Además, los archivos compartidos se sincronizan directamente con *SharePoint*, desde donde se deberá hacer el seguimiento de quien tiene acceso a esos datos.

Datos de la organización. De manera similar a los datos de los usuarios, aquí será necesario hacer copias de seguridad de toda la información corporativa. La integración entre SalesForce y *OneDrive* es realmente buena por lo que en ese aspecto no tendremos problema, es cuestión de realizar una buena configuración desde la terminal de administración de SalesForce para que periódicamente haga copias de seguridad en *OneDrive*. Por otro lado la aplicación de gestión de inventario guarda la información en una base de datos *SQL*, que proporciona de manera nativa la generación y almacenaje de copias de seguridad. Únicamente será necesario en ese caso almacenar las copias de seguridad fuera del gestor de bases de datos, y llevarlas a *OneDrive*, para aplicar así un nivel extra de seguridad, que es el que proporciona Microsoft con ese servicio.

6.2.7 Estabilización del despliegue

Esta sección a mi juicio se divide en tres partes, que son la realización de un *Penetration Test*[9], la contratación de un *SIEM* y la documentación del despliegue que se ha realizado. Vayamos por lo tanto uno a uno.

PenTest. No nos vamos a detener demasiado aquí con el propósito de no extralimitarnos, pero una vez realizada la configuración es necesario que un equipo de profesionales especialistas en encontrar agujeros de seguridad compruebe que efectivamente el despliegue se ha elaborado correctamente. Comprobaran las vulnerabilidades de los equipos instalados, comprobaran la seguridad de la configuración de los equipos, y de los protocolos utilizados, y aseguraran que la infraestructura es robusta

[8] OneDrive es el servicio de almacenamiento en la nube de Microsoft que permite conectarte a todos los archivos. Te permite almacenar y proteger tus archivos, compartirlos con otros usuarios y acceder a ellos desde cualquier lugar en todos tus dispositivos.

[9] Una prueba de penetración, o *pentest*, es un ataque a un sistema informático con la intención de encontrar las debilidades de seguridad y todo lo que podría tener acceso a ella, su funcionalidad y datos.

a ataques tanto externos como internos. Tras hacer la prueba, proporcionarán un informe de lo que hayan descubierto y permitirá realizar los cambios necesarios. Ninguna empresa de este tipo permite obtener información de precios ni alcance de la prueba sin solicitar una consulta formal. Empresas como *Fortra* o *Dolbuck* tienen buena reputación en este campo.

Contratación de un SIEM. Para la monitorización en tiempo real de los eventos ocurridos en la empresa es necesario contratar de nuevos los servicios de una empresa que se dedique a ello. Para ello normalmente es necesario contratar los servicios de una empresa de servicios de seguridad gestionados que ofrezca entre otras cosas servicio de *SIEM*, ya sea propietario o subcontratado. Es decir, las empresas de servicios de seguridad no tienen por qué ser propietarias del producto que ofrecen. Ejemplos de *SIEM* son *Splunk*, *Qradar* o *LogRhythm*. En nuestro caso utilizaremos *LogRhythm* sin *appliance*[10] físico que es lo más habitual. Precisamente una de las ventajas de *LogRhythm* es que permite el despliegue en cloud, en máquinas virtuales o mediante *apliance* físico por lo que es una solución interesante. Además, el software está muy trabajado y permite detectar un gran número de eventos de seguridad de manera conjunta. Por otro lado, *LogRhythm* solo ofrece el software por lo que es necesario contratar a una empresa con *SOC*[11] propio para que de el servicio. Una de las empresas que despliega este tipo de soluciones es *Exclusive Networks*, una empresa francesa no demasiado grande, con sede en España que es ideal para nuestras necesidades.

Generación de la documentación. Es necesario dejar correctamente documentado el funcionamiento de la red, el funcionamiento de las aplicaciones, los manuales de las aplicaciones, la configuración que se ha realizado en los dispositivos, los diagramas de red tanto físicos como lógicos y la matriz de escalado de incidencias. Los manuales de uso y la documentación de la configuración realizada ayudarán a futuros técnicos y usuarios a entender rápidamente cual es el despliegue específico que se ha hecho en la organización. Por otro lado, la matriz de escalado es sumamente importante para saber con quién contactar ante según qué tipo de incidencia, y en caso de que esa persona no tenga capacidad o autorización para solucionar el problema, con quien debe contactar para lograrlo. En este caso la documentación más relevante es la siguiente:

- **Documentación de fabricantes.** Muy importante para poder conocer las características de los equipos instalados y el funcionamiento de los dispositivos y aplicaciones. En este caso será necesario disponer de los manuales técnicos de los *firewalls*, *routers* y *switches*, y de los manuales del software que está en uso como es *Office365*, *Azure AD*, *Netskope*, *TMES*, etc. Es importante que esta documentación sea oficial y esté actualizada en base a las versiones del software que se esté utilizando.
- **Configuraciones.** Toda aplicación que tenga una configuración que no sea la que viene de fábrica deberá tener un documento propio e interno que especifique qué se ha hecho y el motivo del

[10] Un *appliance* es un dispositivo empotrado físico, en el que se instala un software. En muchos casos el dispositivo está diseñado parcial o totalmente para cubrir de la manera más eficiente posible las funcionalidades del software que contiene.

[11] *Security Operation Center*, o Centro de Operaciones de Seguridad es el lugar y a la vez el conjunto de personas encargados de gestionar en tiempo real la seguridad de las empresas y los incidentes que estas tienen.

cambio, para que futuros técnicos o usuarios puedan operar cómodamente. Para la configuración de los dispositivos se deberá realizar un documento para cada uno. En caso de que todos tengan la misma configuración puede haber un único documento genérico. Será necesario por lo tanto la generación de estos documentos para los *firewalls*, los *routers* y los switches, y también para las aplicaciones que se han desplegado como son *OneDrive*, *Netskope*, *Office365*, *Azure AD*, *ApexOne*, etc.

- **Diagramas de red.** En este caso los diagramas ya ha sido mostrados en las figuras 6.1 y 6.2 y ya se ha hablado de su importancia en anteriores capítulos por lo que no vamos a profundizar mucho más. Sí es importante añadir que estos diagramas se deberán actualizar a medida que la red evolucione.

- **Matriz de escalado.** Este es un documento simple, habitualmente realizado en una hoja de cálculo o en un documento *Word* en el que debe figurar para cada incidencia o tipo de incidencia a quien se debe avisar. En caso de que esa primera persona de contacto sea, por ejemplo, un técnico de bajo nivel, se debe especificar también con quien debe contactar ese técnico en caso de que no tenga capacidad para resolver la incidencia. Un ejemplo simple de matriz de escalado es el que se muestra en la tabla 6.1.

	Tipo de incidencia		
	Red	**Sistemas**	**Seguridad**
Horario de Oficina	email: cau@acme.com	cau@acme.com	cau@acme.com
No Horario de Oficina	email: cau @acme.com	cau@acme.com	cau@acme.com
Urgencias 24x7	Técnico 1: 646 34 43 00	Técnico 1: 646 34 43 00	Técnico2: 722 41 20 17

Cuadro 6.1: Matriz de escalado de incidencias

6.2.8 Observaciones

Aquí vamos a hacer un breve repaso de que ideas, conceptos o partes de la arquitectura hemos cogido de Zero Trust para realizar el despliegue. No ha sido posible implementar una arquitectura de red basada en Zero Trust de manera pura, o al menos tal y como la proponía el NIST, pero sí que hemos utilizado técnicas y herramientas relevantes.

En cuanto a la centralización de la toma de decisiones para la autorización de usuarios, no se ha podido hacer de manera total, pero si una buena parte de las aplicaciones están sincronizadas con el directorio activo. Por ejemplo, el acceso a la red inalámbrica, el acceso al cliente VPN y las cuentas de Microsoft 365 para el acceso a las aplicaciones de ofimática y al correo electrónico. También se ha centralizado en la medida de lo posible la administración de los dispositivos de red, mediante el software para redes definidas por software que proporciona Cisco de manera nativa.

Por otro lado, se han añadido varias capas de seguridad, además de las *ACLs* de los *firewalls* (tanto del *PaloAlto* como de los *firewalls software* de cada equipo), la instalación de un EDR, la instalación

de un CASB y el uso de las terminales de administración que ofrecen, por ejemplo, *OneDrive* para la gestión de archivos o *Gmail* para la gestión de correos. El uso de Netskope, TMES y ApexOne no anula, pero si refuerza las políticas que el resto de las aplicaciones pueda implementar. De esta manera se pueden hacer políticas mucho más granulares y específicas y tener mayor visibilidad de lo que está pasando en la organización.

La contratación de un *SIEM* también es un paso adelante en la dirección de Zero Trust, proporcionando monitorización en tiempo real y respuesta a incidentes las 24 horas del día. Además, según los servicios que ofrezca la empresa que realiza el despliegue, se puede contratar soporte, auditorías de seguridad, pruebas de penetración, ayuda en la configuración, etc.

Por último, el despliegue de la solución ha quedado correctamente documentado, lo que permitirá la intervención de técnicos ajenos a la organización cuando sea necesario. Esa documentación también permitirá sacar un mayor partido a los elementos de seguridad que se han incorporado en la red. También será más fácil que, llegado el caso, una auditora revise el correcto funcionamiento de la red de manera más rápida.

Capítulo 7

Conclusiones

Si bien es cierto que Zero Trust está más avanzado y desarrollado de lo que podría parecer en un principio, su integración en el flujo de datos de una organización es complicado, al menos con el estado actual de las tecnologías de que disponemos. Hay una parte que, sí que se puede abordar, de hecho: aplicar sus principios e ideas, que considero es una práctica necesaria. Sin embargo, desarrollar una arquitectura de red basada en Zero Trust tal y como propone el NIST es complicado. Centralizar todos los accesos a todas las aplicaciones y archivos en un único punto, y generar "pasarelas"de comunicación temporales entre ellos, no es imposible, pero es difícil. La consecuencia que considero más relevante y que podemos sacar en claro es la idea de reducir la zona implícita de seguridad, añadiendo controles intermedios y proporcionando acceso a la menor cantidad de información posible.

Bibliografía

[1] Scott Rose (NIST) Oliver Borchert (NIST) Stu Mitchell (Stu2Labs) Sean Connelly (DHS). *Zero Trust Architecture*. 11 de nov. de 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-207/final (visitado 19-08-2022).

[2] Rodrigo Alonso. *¿Qué es un sistema RAID de discos duros y que tipos hay?* 18 de jul. de 2022. URL: https://hardzone.es/tutoriales/montaje/raid-discos-duros/ (visitado 23-08-2022).

[3] Pieter Arntz. *Explained: the strengths and weaknesses of the Zero Trust model*. 28 de ene. de 2020. URL: https://www.malwarebytes.com/blog/news/2020/01/explained-the-strengths-and-weaknesses-of-the-zero-trust-model (visitado 22-08-2022).

[4] Cloudflare. *A Roadmap to Zero Trust Architecture*. 17 de dic. de 2022. URL: https://zerotrustroadmap.org/ (visitado 17-12-2022).

[5] *Computer Security Model*. URL: https://en.wikipedia.org/wiki/Computer_security_model (visitado 19-10-2022).

[6] Department of Defense of the EEUU. *Department of Defense Trusted Computer System Evaluation Criteria*. URL: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf (visitado 20-10-2022).

[7] dig8ital. *What is Security Architecture, and what do you need to know?* URL: https://www.dig8ital.com/post/what-is-security-architecture-and-what-do-you-need-to-know (visitado 22-08-2022).

[8] IBM docs. *Security Model Characteristics*. URL: https://www.ibm.com/docs/en/sim/7.0.1?topic=overview-security-model-characteristics (visitado 19-10-2022).

[9] DocuSign. *¿Qué es la arquitectura de seguridad de la información y por qué es relevante para las PYMES?* 18 de mayo de 2021. URL: https://www.docusign.mx/blog/arquitectura-de-seguridad%5C#:%5C~:text=La%5C%20arquitectura%5C%20de%5C%20seguridad%5C%20%5C%E2%5C%80%5C%94tambi%5C%C3%5C%A9n,a%5C%20sus%5C%20caracter%5C%C3%5C%ADsticas%5C%20y%5C%20seguridad. (visitado 23-08-2022).

[10] Sergey Golubev. *Desconfía y verifica siempre: el modelo de seguridad Zero Trust*. 28 de jun. de 2022. URL: https://www.kaspersky.es/blog/zero-trust-security/23550/ (visitado 23-08-2022).

[11] Michael Gregg. *CISSP Exam Cram: Security Architecture and Models.* URL: https://www.pearsonitcertification.com/articles/article.aspx?p=1998558&seqNum=4 (visitado 19-10-2022).

[12] Robert Grimmick. *What is a Security Policy? Definition, Elements and Examples.* URL: https://www.varonis.com/blog/what-is-a-security-policy (visitado 19-10-2022).

[13] IBM. *What is Zero Trust?* URL: https://www.ibm.com/topics/zero-trust#:~:text=Zero%5C%20trust%5C%20is%5C%20a%5C%20framework,approach%5C%20to%5C%20counter%5C%20those%5C%20threats. (visitado 22-08-2022).

[14] IGI-Global. *What is a Security Model?* URL: https://www.igi-global.com/dictionary/security-model/26110 (visitado 19-10-2022).

[15] Incibe. *CEO, CISO, CIO... ¿Roles en ciberseguridad?* URL: https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad (visitado 19-10-2022).

[16] IONOS. *¿Qué es el cloud? Introducción al cloud computing.* 25 de ago. de 2020. URL: https://www.ionos.es/digitalguide/servidores/know-how/que-es-el-cloud/ (visitado 23-08-2022).

[17] Kaspersky. *About Kaspersky.* URL: https://www.kaspersky.es/about (visitado 23-08-2022).

[18] Charlotte Empey & Nica Latto. *What is a VPN?* 22 de ago. de 2022. URL: https://www.avast.com/es-es/c-what-is-a-vpn (visitado 23-08-2022).

[19] Ben Lutkevich. *Security Policy.* URL: https://www.techtarget.com/searchsecurity/definition/security-policy (visitado 19-10-2022).

[20] Sherali Zeadally y Astha Keshariya Malcolm Shore. *Zero Trust: The What, How, Why, and When.* 11 de nov. de 2021. URL: https://ieeexplore.ieee.org/document/9585170 (visitado 12-12-2022).

[21] Stephen Paul Marsh. *Formalising Trust as a Computational Concept.* Abr. de 1994. URL: https://scholar.google.co.uk/citations?view_op=view_citation%5C&hl=en%5C&user=Qz73wh4AAAAJ%5C&citation_for_view=Qz73wh4AAAAJ:u5HHmVD_uO8C (visitado 26-08-2022).

[22] CSIS & McAfee. *Net Losses: Estimating the Global Cost of Cybercrime.* URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf (visitado 15-10-2022).

[23] Jerome H. Saltzer y Michael D. Schroeder. *The Protection of Information in Computer Systems.* Sep. de 1975. URL: https://web.mit.edu/Saltzer/www/publications/protection/ (visitado 12-12-2022).

[24] MiniTool. *What Is Security Architecture and How to Establish It?* URL: https://www.minitool.com/lib/security-architecture.html (visitado 23-08-2022).

[25] Tiago Monteiro. *What is a software framework?* 13 de jul. de 2022. URL: https://www.freecodecamp.org/news/what-is-a-software-framework/ (visitado 22-08-2022).

[26] Abdul Mujeeb. *What are Information Security Models?* URL: https://www.infosecacademy.io/blog/information-security-models/ (visitado 19-10-2022).

[27] Nicolas Raggi. *¿Qué es el modelo de seguridad Zero Trust y por qué está creciendo su implementación?* 7 de jul. de 2021. URL: https://www.eset.com/py/empresas/compania/que-es-el-modelo-de-seguridad-zero-trust-y-por-que-esta-creciendo-su-implementacion/#:~:text=Zero%5C%20Trust%5C%20promueve%5C%20el%5C%20concepto,por%5C%20fin%5C%20est%5C%C3%5C%A1%5C%20cobrando%5C%20fuerza. (visitado 23-08-2022).

[28] Pablo Rodriguez. URL: https://www.xataka.com/pro/que-sistema-zero-trust-que-microsoft-google-cisco-consideran-futuro-ciberseguridad-empresarial (visitado 22-08-2022).

[29] Technopedia. *Security Policy.* URL: https://www.techopedia.com/definition/4099/security-policy (visitado 19-10-2022).

[30] Wikipedia. *IBM.* 11 de mayo de 2022. URL: https://es.wikipedia.org/wiki/IBM (visitado 22-08-2022).

[31] Wikipedia. *Instituto Nacional de Estándares y Tecnología.* 6 de mayo de 2022. URL: https://es.wikipedia.org/wiki/Instituto_Nacional_de_Est%5C%C3%5C%A1ndares_y_Tecnolog%5C%C3%5C%ADa (visitado 19-08-2022).

[32] Stephen Wilson. *Understanding biometrics and their necessary fallibility.* URL: https://lockstep.com.au/understanding-biometrics-and-their-necessary-fallibility/#:~:text=A%20%E2%80%9CFalse%20Positive%E2%80%9D%20is%20when,or%20from%20site%20to%20site. (visitado 31-10-2022).

[33] Craig Wright. *Biba Model.* URL: https://www.sciencedirect.com/topics/computer-science/biba-model#:~:text=The%20Biba%20Model%20or%20Biba,integrity%20into%20groups%20or%20arrangements. (visitado 20-10-2022).