TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Administración de la infraestructura de TIC, con Tp Link y Aruba Instant On para proteger la red de la empresa J&T EXPRESS (Conejo Corriendo S. de R.L. de C.V).

Titulación por estancias

Por obtener el título de

Ingeniería en Sistemas Computacionales

Con la Especialidad

Seguridad

Presenta:

Daniel Joel Mendoza Gonzalez

Coacalco de Berriozábal,03/ 2024

AGRADECIMIENTOS

Agradezco a mi asesor interno por mostrarme su tiempo, resolver mis dudas y darme la ayuda para poder tener mi proyecto en tiempo y forma.

Agradezco el tiempo, atención y apoyo brindado por la empresa, siendo parte de sus miembros, dedicación y responsabilidad en mis labores que concreto día con día.

RESUMEN

El presente trabajo está relacionado a los temas administración, configuración y monitoreo mediante Aruba. Principalmente el tema de la administración es importante, con la configuración y monitoreo permite tener en buen funcionamiento la infraestructura a la conectividad de la empresa. Como tema principal a diario está en continua marcha la administración en las redes, por lo cual este trabajo está enfocado en la configuración y el monitoreo por posibles fallas y el cómo poder restablecer el servicio brindado por nuestra área. El resguardo de las redes de cada punto desemboca varios temas que se tienen que tratar, dichos temas han sido mencionados anteriormente, por lo tanto, son las variantes que resultan estar presentes en la administración de las redes. El monitoreo es una de las actividades que se desempeñan en el ámbito del área T.I. para que la empresa haga diagnósticos oportunos que lleven a la corrección de fallas para el buen funcionamiento de los sistemas de información y servicios.

CONTENIDO

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

CAPÍTULO 1

GENERALIDADES DEL PROYECTO

INTRODUCCIÓN

La administración es una labor que se encarga de emplear de la mejor manera los recursos con lo que se cuentan, mediante las funciones de la organización y control. Una correcta administración es esencial para el desarrollo laboral, bien sea en el ámbito individual o en el entorno de una empresa con beneficios a los servicios brindados. Para este trabajo, la administración es fundamental para la manera en que se llevan los dispositivos Aruba dentro de la organización, puesto que es de primordial importancia saber en qué puntos se van a visualizar las redes.

La configuración es la serie de modificaciones que se realiza en cualquier tipo de situación, puede entenderse también como ajustes que se llevan de la mano del usuario. Para este trabajo se explica la manera en que se configura desde inicio hasta la forma en que se pueden dar de alta y configurar todo lo relacionado a los dispositivos en uso laboral. (Pérez, J. y Gardey, A., 2016).

El monitoreo consiste en la observación de algún proceso ya en marcha, el cual nos permite ver anomalías eventuales, cambios, fallas o actualizaciones en el proceso en continuidad. Solo ciertas personas dentro de un departamento tienen la autoridad de poder verificar lo anterior dicho con el propósito de tener estable el proceso. Para este trabajo el monitoreo es parte esencial, debido a que, en base al personal autorizado dentro de un departamento, son capaces de poder diagnosticar las eventualidades que presentan los dispositivos en el ámbito laboral. (Diario explorador, 2023).

La presentación de este proyecto surge de la principal característica la cual es el estabilidad, seguridad y mantenimiento dentro del ámbito laboral, está estabilidad viene de la problemática a las posibles fallas en su entorno, tales como problemas de conectividad, errores de software, servicios, energía, y ajustes en las configuraciones. El enfoque principal de este tema es mantener el concentrado de las redes a evaluar y verificar en los puntos, en este caso, centros de distribución y oficina principal. Gracias a la aplicación Aruba podemos consultar las redes. Primeramente, se tiene una adecuada estructura en los nombres de la red de cada sitio, lo que ayuda a la asignación correcta de recursos y clientes en la red. Lo anterior permite mantener a los departamentos conectados a su correspondiente red (o subred) con el monitoreo adecuado para la obtención de métricas de uso de la red (Ancho de banda, peticiones remotas, etc.). Así mismo, la aplicación permite la generación de alerta

en caso de fallos como la perdida de conectividad; como también el establecimiento de conexiones seguras hacia los sitios web y los servicios de correo.

El capítulo del marco teórico trata los temas de los antecedentes del trabajo, bases teóricas, bases conceptuales y la relación entre estas tres partes. Los antecedentes se referencian a las necesidades que la empresa está teniendo y en base a eso darle una solución mediante la configuración realizada mediante la infraestructura T.I. Las bases teóricas están de referencia a la base legal, donde entra la ley contra delitos informáticos, esta ley posee cuatro temas con sus respectivos artículos que infringen esa ley. Y como bases conceptuales están los conceptos más relevantes, explicados con su funcionalidad para este trabajo.

El capítulo de desarrollo se centra en explicar parte por parte toda la administración, configuración, y monitoreo, las tablas en la base de datos y su estructura. En la codificación se muestran capturas del sistema utilizado, las funciones que se pueden realizar con los dispositivos, la visualización de las redes, las secciones de bloqueos y desbloqueo de usuarios. La conclusión será la parte final donde se muestra la funcionalidad de todos los pasos que se muestran en la configuración.

El capítulo de resultados se muestran una gráfica, una de ellas muestra cómo se encuentran la conectividad correcta de cada red y cada cuando tiene falla.

El alcance del proyecto fue tener desarrollo en nuevas formas que ayudaran a comprender y obtener el resultado que se quería dentro del área T.I. En su totalidad fue un nuevo nivel de aprendizaje propio para tener el resultado querido. El cronograma se fue llevando de la mano con los requerimientos solicitados.

DESCRIPCIÓN DE LA EMPRESA

Nombre, razón social: CONEJO CORRIENDO S. DE R.L. DE C.V.

Ubicación: AV. PATRIOTISMO 229, TORRE 2, PISO 3. SAN PEDRO DE LOS PINOS, BENITO JUÁREZ, 03800, CDMX.

Organigrama:

Jefe directo: Lic. Luiggi Chek-Tong Martínez Wong.

Sector productivo de la empresa: Servicio logística.

Misión, Visión, Política de calidad

Misión: Orientada al cliente y basada en la eficiencia.

Visión: Ser una empresa sana y sustentable.

Valores: Compartir, servicio, responsabilidad y orientación a resultados.

Breve historia de la empresa.

Fundada en agosto del año 2015 con el nombre de J&T, es un proveedor global de servicios de logística con negocios líder en el negocio de entrega urgente en el Sudeste de Asia y China, los mercados más grandes y de más rápido crecimiento en el mundo.

Siguiendo su misión "orientada al cliente y basada en la eficiencia", J&T Express se compromete a proporcionar a sus clientes soluciones logísticas integradas a través de infraestructura inteligente y una red logística digital, como parte de su estrategia global para conectar al mundo con mayor eficiencia brindando beneficios logísticos a todos.

PROBLEMÁTICA POR RESOLVER

La problemática en el área, en su momento era que no existía el personal que pudiera implementar una infraestructura dentro de la red en corporativo, en puntos de venta y en centros de distribución. Antes de poner en funcionamiento el área de T.I. se manejaba una red básica de 50 mbps no simétrica, ningún dispositivo de red, ningún equipo de cctv o las consultas especializadas sobre adquisiciones de equipos. Una vez teniendo el personal especializado, se concluyó la manera en que hubiera conectividad dentro de los sitios mencionados. Como principal y primer lugar a resolver fue en el corporativo, ya que en este está todo el personal administrativo y gerencial. En cuanto a los puntos de venta, estos no generan tráfico significativo en la red, debido a que en estos puntos hay mínimo personal, sin embargo, se atacaron los puntos a resolver. En cuanto a las áreas con más problemáticas que resolver, los centros de distribución son los que presentaban un mayor número de incidencias.

Por lo tanto, una vez concluida la instalación requerida, resolver la forma adecuada de la instalación, administración y monitoreo de la infraestructura proporcionada por la empresa era de prioridad, debido a la inversión proporcionada al área T.I.

OBJETIVOS

Objetivo General.

Implementar la administración, configuración y monitoreo de la infraestructura mediante el área de T.I. para el correcto funcionamiento de los sistemas de información, servicios y conectividad de red.

Objetivos Específicos.

• Implementar una gestión de redes para la empresa.

• Explicación detallada de la administración de los sitios en red.

• Implementaciones generales al área de T.I.

JUSTIFICACIÓN

Los beneficios adquiridos de este proyecto constan de las configuraciones realizadas en los dispositivos utilizados, la muestra del seguimiento brindado por el área de T.I., incluyendo actualmente como se mantiene. Los aportes a la empresa son fundamentales en explicar, ya que, al ser solicitudes por la empresa va de la mano con la responsabilidad que se tiene al llevar el área y sean útiles para la misma.

Es fundamental el área de T.I. ya que es la encargada de proporcionar la administración de datos tecnológicos, una mayor productividad en la red, la toma de decisiones en donde se verifica el ahorro de costos, de mayor importancia ya que la empresa tuvo esa solicitud de prioridad. Personalmente el aprendizaje y la experiencia obtenida al realizar las actividades posteriores han sido de valor importante, debido a que todo lo nuevo por aprender siempre es satisfactorio para la persona que lo está realizando. La contribución personal fue la responsabilidad para poder realizar y poner en práctica las solicitudes de la empresa,

Ante la sociedad el área de T.I. impacta debido al desarrollo de nuevas herramientas y dispositivos, las cuales funcionan para la comunicación, organización, aprendizaje y evolución de estas.

A futuro esta explicación ayuda a comprender cual el siguiente paso en la evolución informática y la facilidad de poder administrar algo complejo. En base a tener paciencia, pero a la vez la determinación define a cada individuo y sus ambiciones, pero más que nada el saber qué planes siguen en la vida.

Estos temas ayudan a la empresa a tener una organización, seguridad y control en la red. La administración comienza con los sitios y asignaciones de redes de estos. Consiguiente, la configuración de los sitios y la forma de establecer ciertos bloqueos de cada red para los usuarios. Por último, el monitoreo toma pauta en que los usuarios pueden entrar a la red sin problema alguno, dependiendo de cada red y la restricción de cada una.

CAPÍTULO 2

MARCO TEÓRICO

Antecedentes de la investigación

Inicialmente en toda empresa hay requerimientos en los cuales se contrata al personal indicado con la profesionalidad correcta para poder solucionar y concretar las solicitudes de esta. Es este punto donde entra la parte de T.I. o sistemas computacionales, los cuales en esta empresa son punto clave en poder realizar una nueva implementación y así asegurar un nuevo mejoramiento para la misma. Todo parte desde la abertura de la empresa, se requiere un puesto de T.I. donde se levante un servicio de Internet mediante la instalación de un proveedor, enfocándose directamente en la red en los sitios como puntos de venta, cedis y cedis. Es importante mencionar que no existía ninguna configuración previa en la empresa, debido a que era nueva en su momento (Apellido y Apellido, 2000).

Los equipos manejables, son equipos de marca TP-link, proveedor global de productos para redes informáticas, con gran variedad de modelos y funciones ideales para un departamento de T.I. Firewall Fortinet, estos equipos son específicos en seguridad, ya que permiten mantener las redes seguras y proporcionan una seguridad amplia. Aruba, una compañía líder de la industria en soluciones de redes cableadas, inalámbricas y de seguridad para brindarle a las organizaciones una experiencia increíble con la mayor simplicidad. Existen diferentes modelos a manejar y con facilidad de configuración y uso doméstico.

Posteriormente, en cuanto a los dispositivos TP-link contienen su cable de corriente y cable ethernet para poder realizar la configuración, de igual forma el equipo Fortigate 80F, el cual contiene los mismos componentes. Como todo dispositivo tiene su cierto número de serie, el dispositivo AP11 puede tener su cable de corriente para brindarle energía en caso de que al dispositivo previo a este no sea PoE, en caso contrario, el dispositivo puede ser solamente conectado con un solo cable ethernet, sin necesidad de un cable de corriente, ya que el dispositivo AP11 si es PoE. Gracias a esta ventaja del dispositivo, es posible reducir tiempos para el área de compras, ya que en el área de T.I. se cuenta con la herramienta necesaria para poder ponchar cables de red sin problema alguno.

Los únicos con posibilidad de acceso a la plataforma de Aruba, es el área de T.I. los cuales son los responsables en dar de alta y bajas las redes de cada sitio, incluyendo el ingreso a las redes mediante las contraseñas. De igual forma dentro de la plataforma es posible realizar cambios básicos en las opciones de configuración del dispositivo, tales como poder modificar la red a un radio 2.4 o 5 GHz, localización de dispositivo, pruebas de la misma red, reinicio, conectividad por DHCP o estática (siendo esto con un dispositivo previo el cual permita realizar).

Bases teóricas.

Como principal concepto, un servicio de tecnologías de la información es el conjunto de actividades que buscan resolver las necesidades un corporativo o cliente, mediante soporte y soluciones tecnológicas usando procedimientos para lograr una eficiencia. Se presentará la base teórica que sustenta este trabajo sobre el uso adecuado de la infraestructura de T.I. en esta empresa. (Contreras, M., 2016).

Bases legales.

DECRETO por el que se crea la Comisión Intersecretarial de Tecnologías de la Información y Comunicación, y de la Seguridad de la Información. La Comisión Intersecretarial de Tecnologías de la Información y Comunicación, y de la Seguridad de la Información, publicado en el Diario Oficial de la Federación (CITICSI) es un mecanismo de coordinación y conducción colegiada de acciones para la implementación de las políticas federales en materia de tecnologías de la información y comunicación, y de la seguridad de la información. Fue creada a partir del Decreto publicado el 10 de enero de 2023 en el Diario Oficial de la Federación.

De conformidad con el artículo 505 del Reglamento del Congreso de la Ciudad de México, el Instituto de Investigaciones Legislativas es un órgano administrativo del Congreso, cuyo objetivo es la investigación y difusión de temas relacionados con el estudio, historia, funciones y actividades legislativas. Además, se encarga de realizar actividades, investigaciones y estudios con la finalidad de fortalecer el quehacer legislativo y la practica parlamentaria; generando con ello, publicaciones de consulta bibliográfica útiles relativas a la Ciudad de México. Asimismo, nos encargamos de dar seguimiento puntual a las modificaciones que impactan el marco normativo de esta Ciudad, con la finalidad mantener actualizada la legislación local. En conjunto, generamos mecanismos de colaboración y coordinación con Instituciones Académicas y de Investigación para llevar a cabo el cumplimiento de nuestros objetivos e impartir cursos de capacitación en materias de técnica legislativa y práctica parlamentaria.

Gaceta del Senado. Martes 25 de septiembre de 2007 / LX/2PPO-121-396/13967

CAPITULO II. Acceso ilícito a sistemas y equipos de informática.

Artículo 211 bis 1.

"Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa." (Artículo adicionado DOF, 1996).

Artículo 211 bis 2.

"Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa." (Párrafo adicionado DOF, 2009).

Artículo 211 bis 3.

"Al que, estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. Al que, estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.". (Párrafo adicionado DOF, 2009, Artículo adicionado DOF, 1999).

Artículo 211 bis 4.

"Al que, sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que, sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.". (Artículo adicionado DOF,1999).

Artículo 211 bis 5.

Al que, estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que, estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. (Artículo adicionado DOF, 1999).

Normas y estándares.

En cuanto a la norma que se trata de apegar en la empresa surge la norma ISO 20000, la cuál es una norma internacional sobre Gestión de servicios de TI (ITSM), publicada por ISO (Organización Internacional de Normalización) e ICE (Comisión Electrotécnica Internacional). El objetivo de la norma ISO es ofrecer a las empresas una certificación que garantiza que la metodología y buenas prácticas están correctamente establecidas en sus procesos de gestión de la información. La cual se divide en 2 partes, sin embargo, actualmente se está haciendo enfoque en la primera parte.

Parte 1 - ISO 20000-1:2011

Recoge un conjunto de especificaciones para la gestión eficiente del suministro de servicios de tecnologías de la información. En esta parte se definen los requerimientos para ofrecer los servicios Ti con una calidad aceptable, el diseño y transición de los servicios y los siguientes procesos:

Procesos de servicios. Todos aquellos procesos que tienen que ver con la entrega del servicio como disponibilidad, capacidad, seguridad de la información y otros procesos de gestión de servicios.

Procesos de relaciones. Aquellos procesos relativos a las relaciones y comunicaciones tanto con el negocio como con los suministradores.

Procesos de resolución. Aquellos procesos de resolución de problemas, incidencias y petición de servicio.

Procesos de control. Todos los procesos relacionados con la configuración, cambios y entrega y despliegue de los servicios.

En la empresa, se hace enfoque a los procesos de servicios mediante el resguardo de la información de excolaboradores, en el área se tienen 3 discos duros externos, en donde el primero contiene una capacidad de 5 TB, posterior a este, se tienen 2 discos los cuales contienen la capacidad 1 TB cada uno. La información está disponible para los responsables de cada departamento siempre y cuando sea solicitada.

Los procesos de relaciones en la empresa se usan mediante la correlación con los otros departamentos mediante los procesos establecidos, los principales son las solicitudes de equipos, asignaciones de equipos, entregas de equipo, configuración de equipos, etc.

Los procesos de resolución en la empresa son enfocados en las solicitudes que se requieren para el área, es decir, la solicitud de un cambio o algún aviso de anomalía en la red, cotizaciones de equipos pc, laptops, cctv, inventarios, cambio de usuarios, mantenimientos preventivos a equipos, reparaciones, etc.

Por último, los procesos de control en la empresa están enfocados específicamente en los seguimientos e inventarios que se tienen en el área, sobre todo en los números de serie de los equipos, debido a que se encuentran ubicados en diferentes puntos de la ciudad. (Anzil, F., 2010).

Profesionalmente, se conocen normas y estándares que se pueden incluir como ciertas bases para poder tener un mejoramiento interno en el área tal como la Biblioteca de Infraestructura de Tecnologías de la Información (Information Technology Infrastructure Library). Es un marco simple y práctico que se enfoca en alinear sus servicios de tecnología de información, y se conforma de 5 etapas, estrategia, diseño, transición, operación, y mejor continua del servicio. El uso de la estrategia fue plasmado en la forma de trabajo que se iba a tener en el área, repartir las actividades de manera que se pueda concretar las solicitudes de la empresa, por parte del diseño se tenía que visualizar como iba a ser la infraestructura de los equipos que se utilizarían, es decir, una consistencia de las conexiones y de cómo iba a quedar bien acomodado en su debido site o lugar. Posteriormente en la transición se tenía el tiempo limitado, ya que la solicitud era buscar una solución de equipo y costo para poder realizar la función adecuada. De manera operacional, teniendo la instalación completada se fue verificando las modificaciones en la red, el objetivo era visualizar los usuarios que se fueran conectado, debido al límite de DHCP. Actualmente, la mejora de continua al servicio se sigue conformando por el monitoreo de las redes de cada sitio, los cuales de manera remota se pueden visualizar mediante la aplicación de puntos de acceso Aruba, de igual forma el soporte con el proveedor en caso de ser un error de tercero.

También el marco de trabajo de objetivos de control para la información y tecnología relacionada (COBIT), en donde se hizo enfoque en los objetivos de gestión en donde los cuatro dominios APO (Alinear, Planificar y Organizar), BAI (Construir, Adquirir e Implementar), DSS (Entregar, Dar Servicio y Soporte) y MEA (Monitorizar, Evaluar y Valorar) fueron utilizados similarmente a la ITIL. (Laoyan, S., 2022).

Finalmente, dentro de nuestros procesos, dentro de la normalización del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) aplica la 802, donde se centra en desarrollar estándares de redes de área local (LAN) y redes de área metropolitana (MAN), en el que el estándar 802.11 se enfoca en las normas inalámbricas y se usa dentro de la gestión del área T.I. (Wikipedia, 2024).

Se sabe que la ciberseguridad es la práctica de proteger equipos, datos, aplicaciones o datos personales, donde actualmente los programas malignos (malware) es un tema de importancia ya que son softwares malintencionados (virus) que están a la orden del día, actualmente mediante links por correos. En la empresa se cuenta con los dispositivos Fortigate 80F, el cual es un dispositivo firewall de seguridad de red, previniendo el filtrado de contenido, control de aplicaciones y servicios de red, seguridad entre correos, y una visibilidad completa de lo mencionado anteriormente. Gracias a este dispositivo es posible mantener una seguridad completa dentro de nuestras redes en la empresa.

Bases conceptuales.

PoE: (Power over Ethernet), alimentación a través de Ethernet, es una tecnología que permite enviar energía eléctrica a través de los cables de red Ethernet junto con los datos. Esta tecnología es especialmente útil en entornos donde se requiere alimentar dispositivos como cámaras de seguridad, puntos de acceso inalámbrico y teléfonos IP sin la necesidad de una toma de corriente cercana.

Implementación: Es una etapa totalmente operativa, depende en gran parte de la administración de los colaboradores del proyecto, de la optimización de los recursos y del buen manejo de los temas económicos, principalmente la implementación de un proyecto debe estar respaldada por la empresa y dirección de todos los colaboradores implicados.

Administración: La administración en el ámbito empresarial es la disciplina encargada de gestionar, organizar, dirigir y asignar recursos eficientemente, para lograr un objetivo determinado. Es primordial gestionar adecuadamente los pasos para alcanzar el objetivo que requiera la empresa.

Configuración: La configuración en el ámbito laboral conlleva a la alineación de los recursos internos de la empresa que contribuyen a la ventaja dentro de la competencia de cada uno de los negocios, sobre todo en el sector logístico. Siendo así una serie de modificaciones que realiza un área, ya sea junto con el fabricante o el usuario, para que un dispositivo presente las características que más se ajusten a las necesidades de la empresa.

Monitoreo: El monitoreo se realiza posteriormente a la ejecución del plan, con la finalidad de analizar y observar el curso que está tomando el proyecto planteado con anterioridad. Es importante mencionar la detección de fallas, comprobaciones de riesgo, proponer soluciones, identificar debilidades y realizar una medida preventiva ante dichas fallas.

Para obtener el resultado de lo que se necesitaba, se analizó el tipo de operación en donde internamente se tenía que atacar el problema. Primero, se generó la solicitud previa, la cual era la posibilidad de poder tener un servicio de internet para cada punto de cada centro de distribución, lo cual fue sencillo debido a que se contrató un servicio de internet simétrico. Por consiguiente, de manera interna en el área T.I. se configuraron varios dispositivos previos a los puntos de acceso Aruba. Siendo así el tema principal de los dispositivos de red, Aruba es el que nos permite realizar el monitoreo de las redes a través de su plataforma.

Después se dio una deducción de la problemática, la cual era visualizar fallas o bajas en el servicio de internet proporcionado por el proveedor, incluyendo también la prevención del mal uso de las redes, mediante la plataforma se puede atacar ese tipo de acciones, la acción principal es poder realizar algunos bloqueos mediante el apartado “Aplicaciones”, el cual consta de mostrar el tipo de aplicación en uso por el usuario o empleado. La idea en su momento era minimizar la visualización ya se por medio de la plataforma web o en su caso una existente aplicación en celular.

La innovación realizada por este tipo de aplicaciones es de mejoría a una forma que no se podía realizar con anterioridad, gracias a esto es posible tener varios sitios dentro de un solo perfil y dentro de cada sitio tener varias redes. La versión AP11 tiene como ventajas poder conectar hasta 50 dispositivos a la vez, en casos mayores 75, con una velocidad de datos 1167 Mbps, un peso ligero de 123 g, incluyendo radios de 2,4 GHz 802.11n (Wi-Fi 4); 5 GHz 802.11ac, y una de las principales características es que es un dispositivo PoE.

Ya teniendo forma y como finalidad tener un resultado con éxito, se ha replicado la misma situación en otros centros de distribución, los cuales actualmente son 5, incluyendo el corporativo los cuales se dividen en 2. Es de importancia recalcar nuevamente que los dispositivos envían una alerta en caso de tener un error con el servicio de internet del proveedor, de esta manera se tiene como responsabilidad restablecer el servicio por medio de comunicación por el soporte técnico del proveedor, siempre y cuando el caso salga de nuestras posibilidades internas en la empresa.

Como base teórica, se tiene la base legal, hablando específicamente de la ley especial contra delitos informáticos y conexos. Como su nombre mismo lo dice, se habla específicamente de la seguridad, la cual en esta implementación se visualiza en las redes hacia los colaboradores y como el departamento de T.I. tiene único acceso a las mismas. La administración esta empleada en la segregación de redes y monitoreo de esas mismas.

Tal parece que el método de la implementación es esencial en cualquier empresa, sobre todo en una donde te dan la oportunidad de implementar nuevas y mejores formas de llevar un departamento controlado. Las medidas de prevención son únicas para cada lugar laboral. Incluyendo los cuatro artículos específicos de la ley especial contra los delitos informáticos. La autoridad es la cabeza de todo un cuerpo, es decir, los altos mandos en este caso la gerencia general y administrativa son los encargados de ponerle un límite o sanción a cualquiera de los trabajadores que estén infringiendo esas leyes. Tal vez no todas las empresas están al tanto de este tipo de leyes, ya que como se puede observar en algunas empresas no están tan apegadas a esa forma de trabajo, cada empresa tiene sus leyes y sanciones a su criterio. El hecho de tener conflicto con cualquier colaborador que infrinja las leyes decretadas en la empresa, son medidas que se deben de tomar en cuenta junto con el departamento que lleve estas actividades.

CAPÍTULO 3

DESARROLLO

En base con la metodología waterfall (cascada), la cual en resumen es sencilla y práctica para la rápida implementación solicitada. Consta de los requisitos de la empresa, análisis interno, diseño, programación, pruebas y operaciones, se utilizó como forma básica para un buen proceso. (Laoyan, S., 2022).

Requisitos y planificación.

Como primer paso, con las herramientas proporcionadas por la empresa se planificaron los dispositivos requeridos para la infraestructura del corporativo, ya que este, fue el primer sitio a realizar. En la siguiente imagen se puede visualizar la ONT del proveedor (Servicio de 200 Mbps con simetría), un router capaz de administrar ips y configuraciones adicionales, 2 switches de 48 puertos PoE para poder sustentar dispositivos y nodos salientes de aproximadamente 100 nodos, un NVR de 16 cámaras, capaz de monitorear y visualizar al momento, por supuesto, los puntos de acceso Aruba, capaces de ser administrables e impresora ip. Principalmente todos los dispositivos tienen que ir conectados a la energía, por eso es importante tener un respaldo, en este caso, un UPS capaz de soportar apagones y puedan afectar a los dispositivos. Esto se llevó a cabo tal cual la imagen presentada.

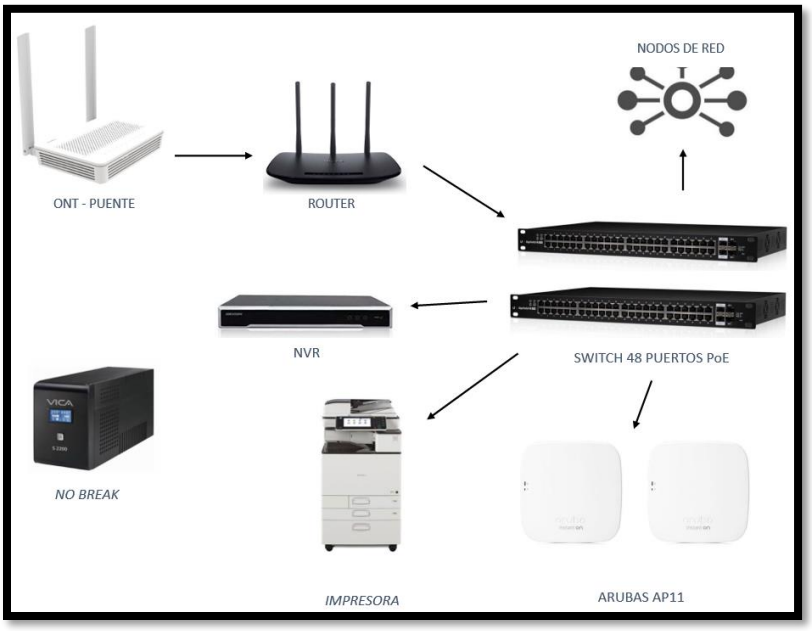


Imagen 1: Red corporativa. Fuente: Autoría propia.

Después, para los centros de distribución se debía tener otra infraestructura, no tan simple. de igual manera al corporativo, tenemos la ONT del proveedor (Servicio de 200 Mbps con simetría), un Router capaz de administrar IP's y configuraciones adicionales, 1 switch de 8 puertos PoE, este rango de puertos es debido a que no se requirieron nodos para equipos PC ya que en su lugar se suplantaron adaptadores de antenas USB – Wifi, de igual forma tenemos el NVR de 16 cámaras, una impresora ip, y un punto de acceso Aruba. De igual manera se tiene un UPS en caso de fallas de energía.

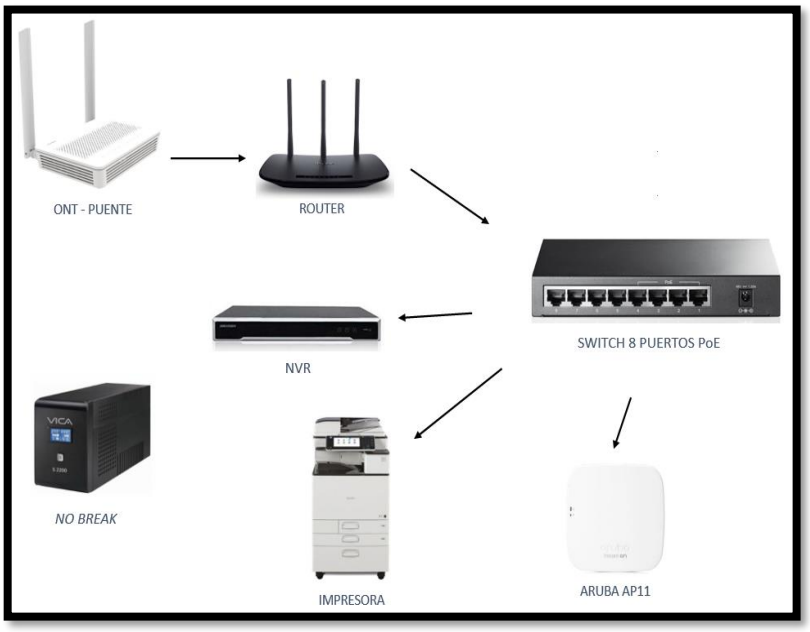


Imagen 2: Red en centro de distribución. Fuente: Autoría propia.

Las fallas en cualquier situación son de presencia de una u otra forma, sin embargo, siendo clientes preferentes de nuestro proveedor de internet, se tiene una atención inmediata en caso de errores o conexiones erróneas en la red. Afortunadamente, con los puntos de acceso Aruba, se tiene la capacidad de identificar cuando es el error de nuestro lado o por parte del proveedor, sin embargo, ya sea mediante el monitoreo remoto es más rápido el saber de qué se trata la afectación. Es importante mencionar que se manejan actualmente 5 centros de distribución alrededor de la CDMX, los cuales se manejan con la misma infraestructura y se han mantenido correctamente.

Por último, se visualiza la infraestructura que se tiene en un punto de venta, primeramente, la ONT del proveedor (Servicio de 40 Mbps con simetría) conectado directamente a un switch PoE, proporcionando red directa al NVR con 4 cámaras, 2 PC. Por supuesto, se cuenta con un UPS capaz de sustentar la energía en caso de fallas.

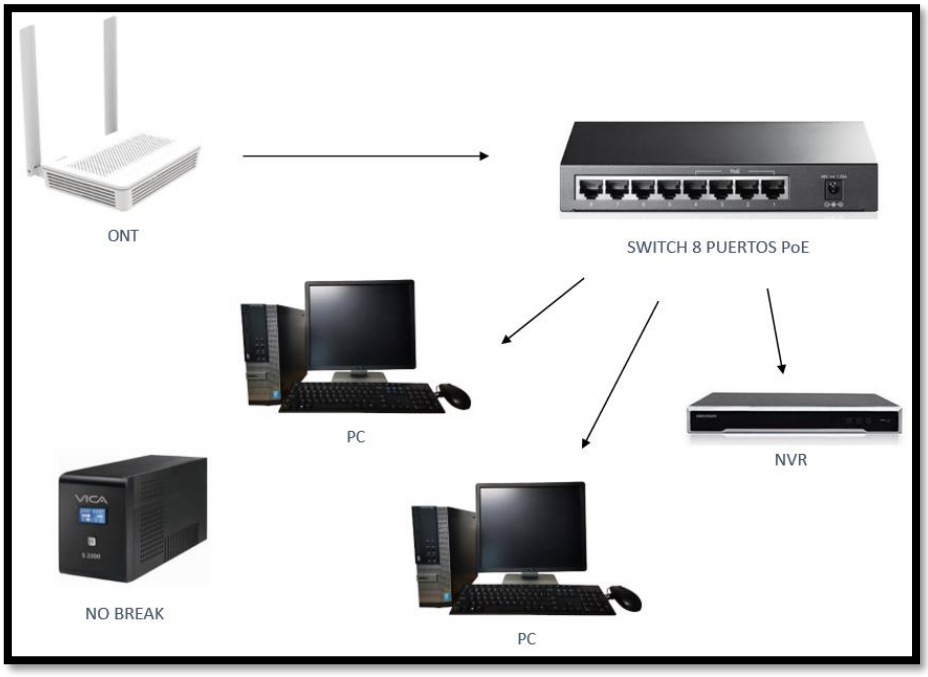


Imagen 3: Red en punto de venta. Fuente: Autoría propia.

Actualmente se manejan 20 puntos de venta alrededor de la CDMX, en los cuales de igual forma se utiliza la misma infraestructura y se mantienen de manera correcta.

Las herramientas que se utilizaron para realizar el requerimiento solicitado por parte de la empresa fue, una vez teniendo la instalación del servicio de internet del proveedor, verificar por parte interna del departamento T.I. la manera de poder brindar una red mediante wifi y los colaboradores dentro del centro de distribución pudiesen conectarse de manera inalámbrica para poder realizar sus actividades, algunos vía dispositivo laptop o pc, otros celular, y otros con la principal herramienta que es una PDA. Fue importante llevar una serie de pasos, en este caso, una metodología rápida, la cual fue waterfall. Con esta metodología se puede dar pauta a los requisitos que necesitaba la empresa en los sitios, analizando los problemas como las desconexiones, errores en la red, etc, se analizó como poder contrarrestar esas problemáticas, en la parte del diseño, se tomó en cuenta que tipo de dispositivo era el que se iba a utilizar para poder llegar al objetivo principal, como tal la programación fue seguir la serie de pasos para la configuración del equipo Aruba, en el cual

se llevaron a cabo las pruebas de conectividad y todas la demás características incluidas en el dispositivos para poder alcanzar la parte operacional sin problemas.

Los conocimientos obtenidos para poder realizar la implementación fueron las pruebas realizadas durante el periodo mencionado, durante la estancia corta en el proceso de pruebas, se pudo percatar de la mayoría de las ventajas que se podían realizar con esos dispositivos, las cuales se mencionan nuevamente como: poder modificar la red a un radio 2.4 o 5 GHz, localización de dispositivo, pruebas de la misma red, reinicio, conectividad por DHCP o estática (siendo esto con un dispositivo previo el cual permita realizar), entre otras más.

Implementación y gestión de dispositivos de red.

De manera inicial fue importante tener el servicio de internet mediante un proveedor, en la elección se tuvo como primera opción al proveedor Totalplay, ya que fue accesible el precio y el servicio que ofrecían. Por lo tanto, se comienza teniendo como primer dispositivo la ONT del proveedor, el cual nos brinda los Mbps contratados dependiendo el punto a instalar.

Imagen 4: ONT de proveedor. Extraído de: https://realfirmware.net/producto/firmware-reestablecimiento-para-modem-roteador-ont-huawei-hg8245h-epon-gpon-ou-xpon/

Después se tiene el Router, la elección fue tener un Router que se pudiera configurar en un entorno grafico amigable para los usuarios que lo fueran a manejar. Es importante este comienzo ya que de aquí se parte para la configuración de IPs DHCP o estáticas, las redes LAN, o bien, simple como un medio para poder administrar otros dentro del entorno y punto a instalar.

Imagen 5: Router empresarial TP-Link. Extraído de: https://www.tp-link.com/vn/home-networking/wifi-router/tl-wr940n/

Como todo dispositivo, se conecta a energía y se deja que encienda, es importante tener el dispositivo ya conectado a la red del proveedor, verificando las especificaciones que vienen detrás del dispositivo, se puede anclar a él mediante una contraseña especificada del dispositivo, mediante una IP que viene en la información del dispositivo se entra en red y posteriormente, iniciar sesión de manera inicial.

En esta sección se explicará cómo se usa el Router de marca TP-Link AC600.

Imagen 6: Login inicial TP-Link. Fuente: Autoría propia.

Cuando se inicia sesión, aparecen las opciones generales del lado izquierdo, las cuales servirán para poder configurar el dispositivo y en el centro de la información dentro de ese panel. Solo se visualizan algunos paneles principales que hacen un correcto funcionamiento dentro de la empresa.

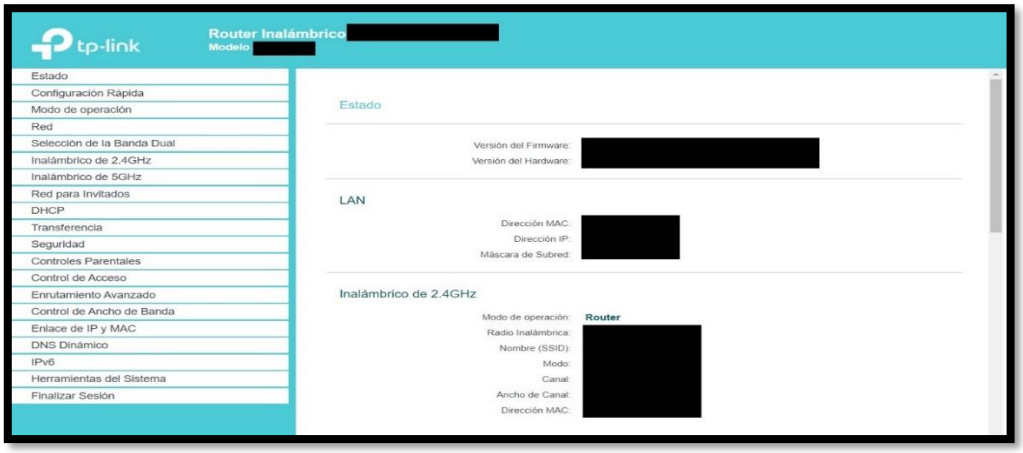


Imagen 7: Centro inicial de TP-Link. Fuente: Autoría propia.

En el panel de configuración rápida como indica, se ejecuta de una acción rápida en configuración, la configuración de internet. La cual no puede ser, ya que se tienen datos específicos del proveedor que configurar.

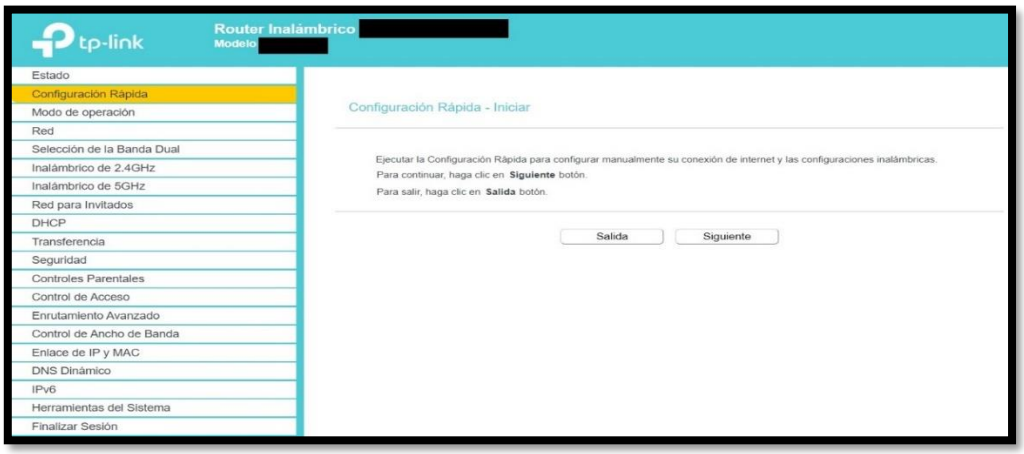


Imagen 8: Configuración rápida de dispositivo TP-Link. Fuente: Autoría propia.

Se continua con el modo de operación del dispositivo, en donde se puede elegir el tipo de modo que va a estar haciendo función el dispositivo, se elige modo router ya que se manejan diferentes direcciones IP.

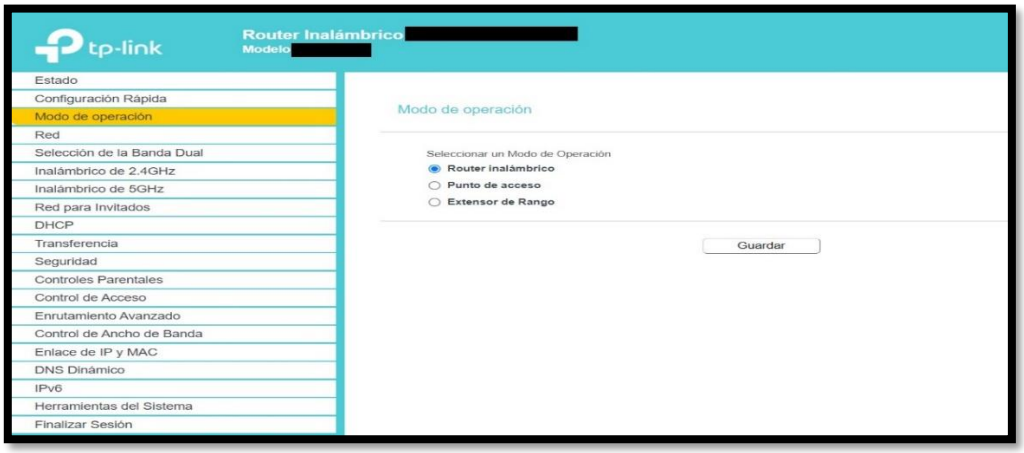


Imagen 9: Modo de operación de dispositivo TP-Link. Fuente: Autoría propia.

Una vez elegido el modo de operación del dispositivo, se puede visualizar la red a configurar, la cual será dependiendo del servicio del proveedor. Dentro de la red WAN se tienen dos modalidades, dinámica o estática. En los servicios se tiene un servicio estático, ya que se tiene una ip fija estática por parte del proveedor, esto para no perder ninguna configuración de los dispositivos posteriores. Se cuenta por parte del proveedor con la dirección IP asignada, la máscara de subred, la puerta de enlace, y nuestros DNS. Una vez configurado correctamente los datos de red del proveedor, se procede a guardar los cambios y el dispositivo se reiniciará automáticamente tomando los cambios que se asignaron. Se hace mención sobre la ip estática ya que, en caso de no haber energía por algún problema de terceros o internos, el dispositivo no va a guardar la ip.

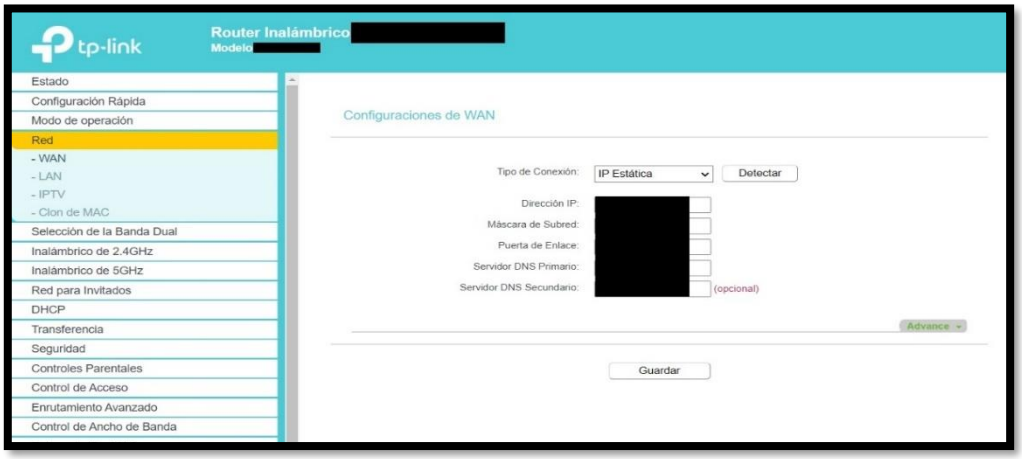


Imagen 10: Configuración de la red WAN. Fuente: Autoría propia.

Dentro de la configuración de la red, se encuentra la configuración LAN, en donde se puede configurar la puerta de enlace predeterminada propia, es decir, desde donde va a comenzar el segmento. De igual forma se va a poder configurar la máscara de subred. Es importante esta parte, ya que de aquí se pueden configurar las IP's estáticas al modo de uso laboral.

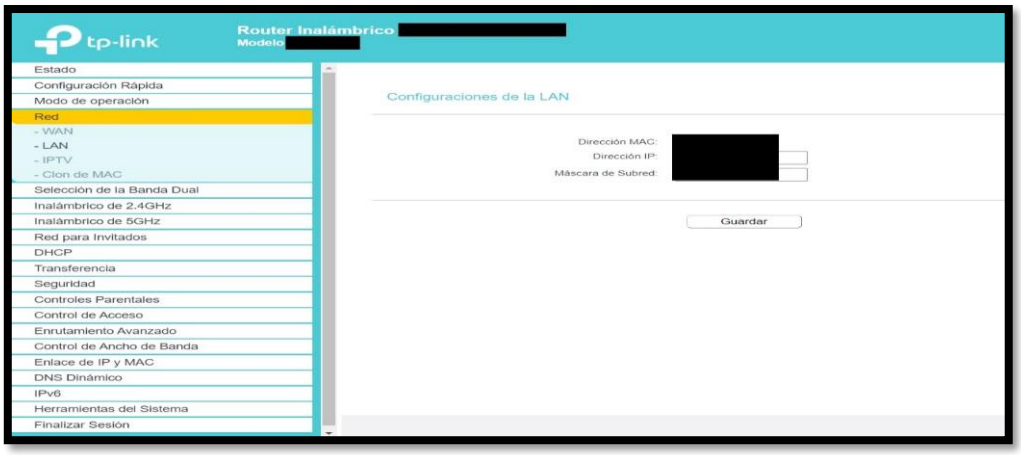


Imagen 11: Configuración de la red LAN. Fuente: Autoría propia.

La banda dual permite codificar y decodificar las ondas de radio en las frecuencias 2.4GHz y 5GHz. En el dispositivo Router da 2 opciones en dejar habilitada la frecuencia que se quiere utilizar. El 2.4G significa 2.4 Gigahercios (GHz), mientras que el 5G significa 5 Gigahercio (GHz). En el radio 5GHz se tiene más velocidad, menos interferencias, pero un menor rango de alcance para conexiones inalámbricas. En cuanto al radio 2.4 GHz se tiene menos velocidad, más interferencias, pero con un mayor rango de alcance. Sin embargo, este apartado es útil cuando no se cuenta con algún punto de acceso, lo cual estos apartados no son de uso, ya que, en las configuraciones específicas de cada radio se puede deshabilitar el SSID (Service Set Identifier), en caso contrario no son útiles ya que se manejan puntos de acceso Aruba, los cuales brindan la misma configuración de las ondas de radio.

Imagen 12: Selección de Banda Dual. Fuente: Autoría propia.

La configuración de ambas ondas de radio es utilizable en caso de que no haya puntos de acceso, se puede observar en la configuración la posibilidad de habilitar o deshabilitar la onda, el nombre de la red, región, y lo más importante el visualizador SSID, que viene siendo la red para poderla visualizar en los dispositivos.

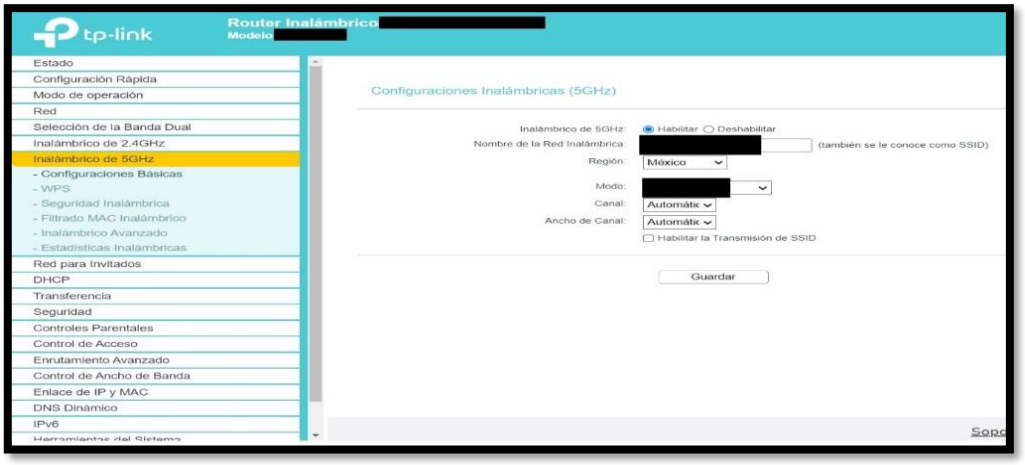


Imagen 13: Configuración de radio 5GHz. Fuente: Autoría propia.

La seguridad inalámbrica del radio 5GHz se encuentra básicamente la contraseña a configurar del radio seleccionado.

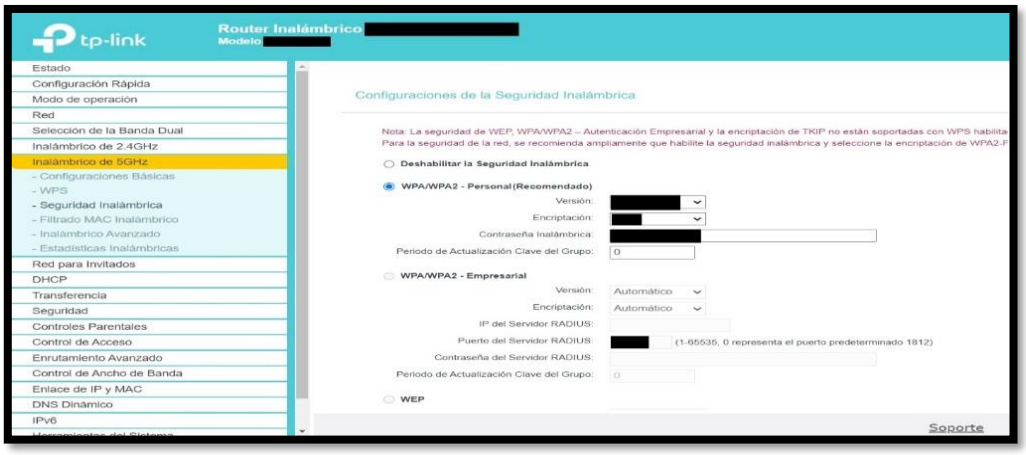


Imagen 14: Configuración de contraseña de radio 5GHz. Fuente: Autoría propia.

Continuando con las configuraciones DHCP, las cuales, si son fundamentales, ya que del Router se va designa el rango de IP's a tomar por dispositivo, es decir, tener 100 dispositivos PC o Laptops, 50 dispositivos celulares, NVR, etc. El tiempo de arrendamiento funciona para configurar el tiempo de liberación de IP's, lo que significa tener que, si se conecta un dispositivo y esta toma un ip, se libera en cierto tiempo configurado, es importante este cambio, debido a que hay varios dispositivos que se conectan en los centros de distribución, de esta manera se evita conflictos de IP's. Cada dispositivo tomara una ip, estos conectan directamente con los puntos de acceso que son los que van a brindar la conexión inalámbrica. De igual forma se configura la puerta de enlace predeterminada, junto con los DNS primario y secundario. Para finalizar se guarda la configuración y el dispositivo tomara el cambio realizado.

Imagen 15: Configuración DHCP del dispositivo. Fuente: Autoría propia.

En la lista de clientes DHCP se visualizan los clientes conectados, esta herramienta de igual forma ayuda a visualizar quienes se han conectado a la red, de igual forma está acción puede visualizarse en los dispositivos de punto de acceso Aruba.

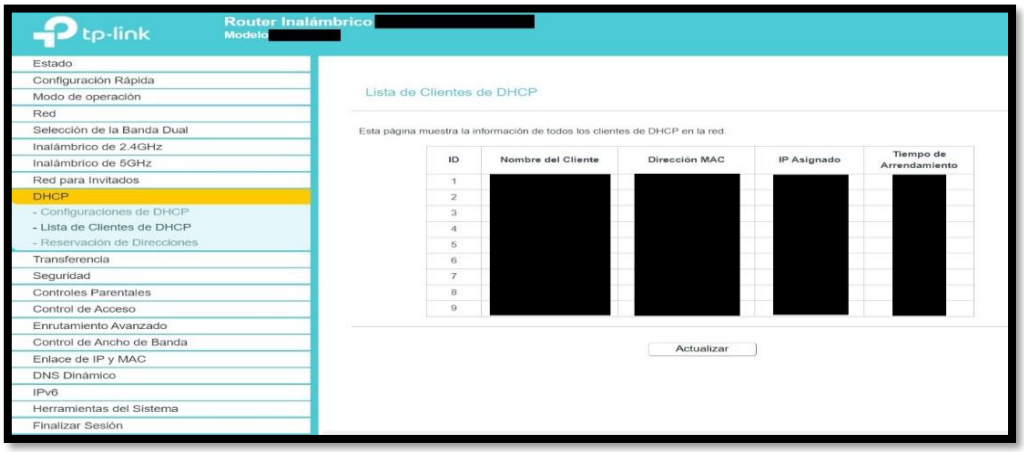


Imagen 16: Lista de dispositivos DHCP. Fuente: Autoría propia.

Como segundo plano y el cual también se tiene la configuración, se explicará la configuración realizada a la par del dispositivo Fortigate 80F de la marca Fortinet, al igual que sus aparatados, el equipo Fortigate se tiene actualmente en corporativo.

Imagen 17: Equipo Fortigate 80F. Extraído de: https://www.avfirewalls.com/FortiGate-80F.asp

De primera instancia se tiene el apartado de Dashboard – Panel / Status – Estado, el cual permite visualizar la información del sistema, incluyendo el hostname, el número de serie, firmware, modo, tiempo de sistema, uptime y la wan ip. De igual manera se visualiza las licencias, la nube y la seguridad de fábrica.

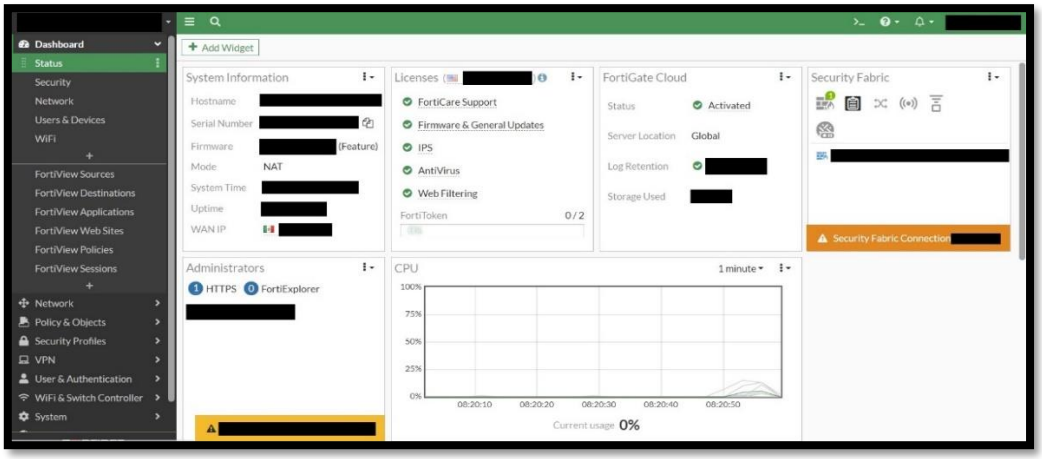


Imagen 18: Dashboard - Status. Fuente: Autoría propia.

Continuando con el aparatado de seguridad del Dashboard, se puede visualizar principalmente el tipo de amenaza con su respectivo nivel, este es un apartado previo a lo más gráfico.

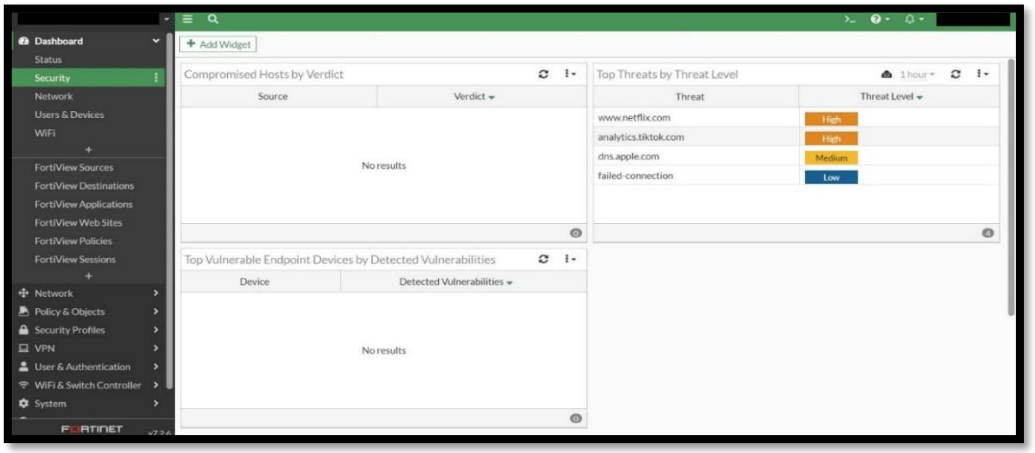


Imagen 19: Dashboard - Security. Fuente: Autoría propia.

En la parte de Network – Red, se visualiza de manera gráfica los dispositivos que están conectados en el momento, incluyendo el ruteo.

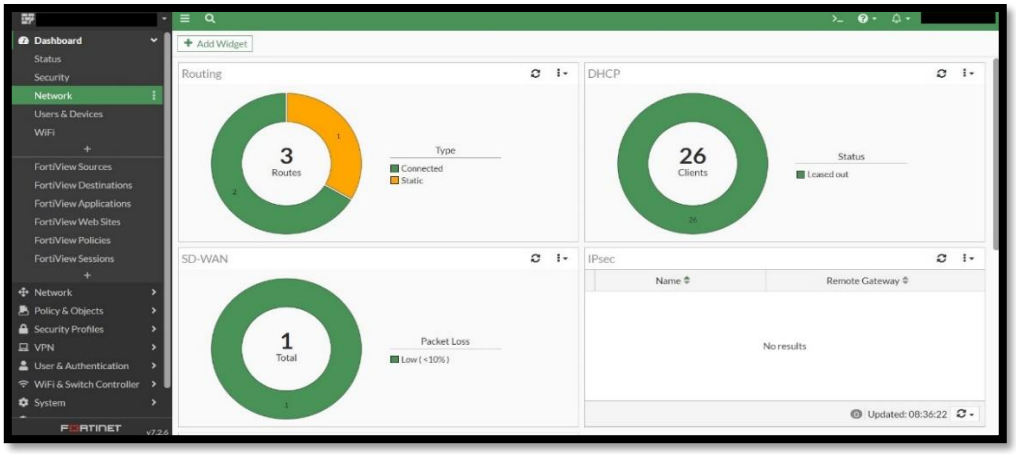


Imagen 20: Dashboard - Network. Fuente: Autoría propia.

En el siguiente apartado se visualizan los dispositivos que han sido conectados al dispositivo Fortigate, se muestra por marca y número de dispositivos conectados alguna vez.

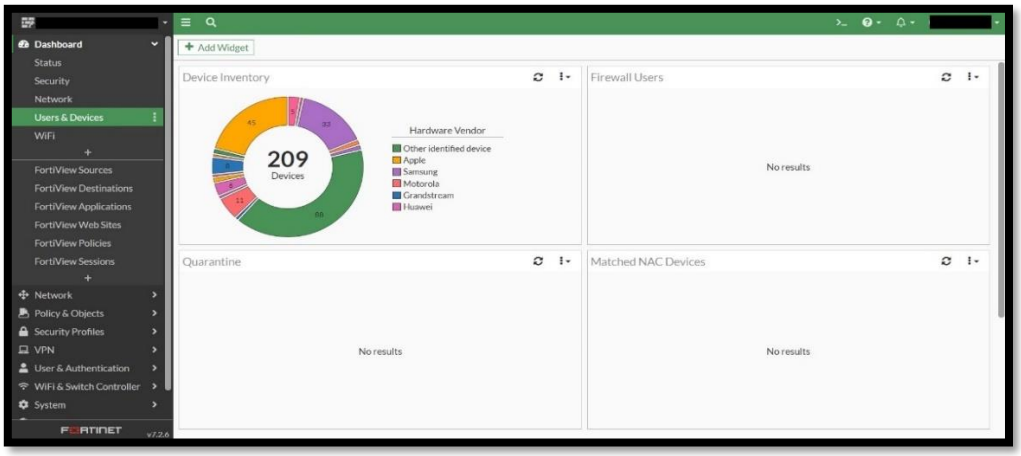


Imagen 21: Dashboard – Users & Devices. Fuente: Autoría propia.

Después, se puede visualizar el apartado de FortView Sources, el cual muestra los dispositivos una vez ya conectados a la red en donde se observan las ip's que toman, incluyendo los bytes consumibles.

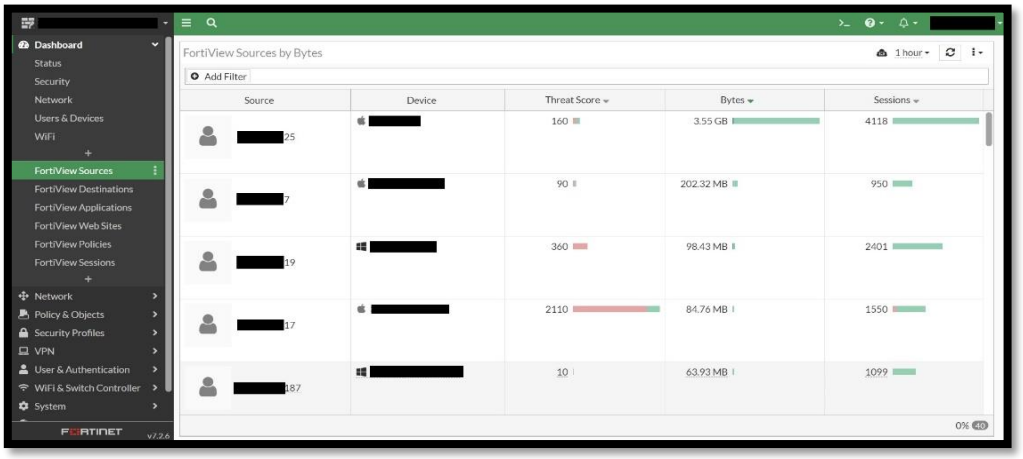


Imagen 22: Dashboard – FortView Soucers. Fuente: Autoría propia.

Continuando con el apartado FortiView Destinations, en donde se muestra de nueva cuenta los dispositivos conectados a la red junto con la aplicación y los en consumo.

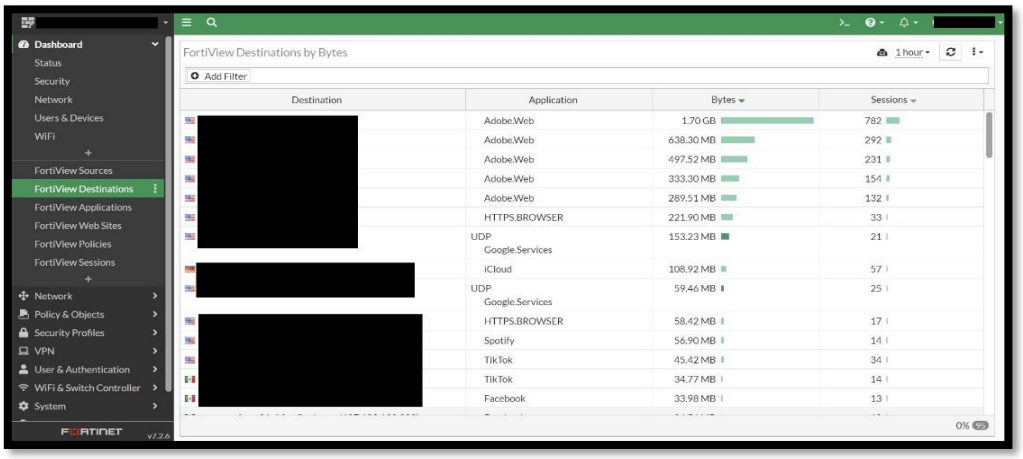


Imagen 23: Dashboard – FortView Destinations. Fuente: Autoría propia.

Se tiene la parte de FortiView Applications, de nueva cuenta fija los clientes conectados a la red con la diferencia que se visualiza la categoría aplicada en el dispositivo Fortigate.

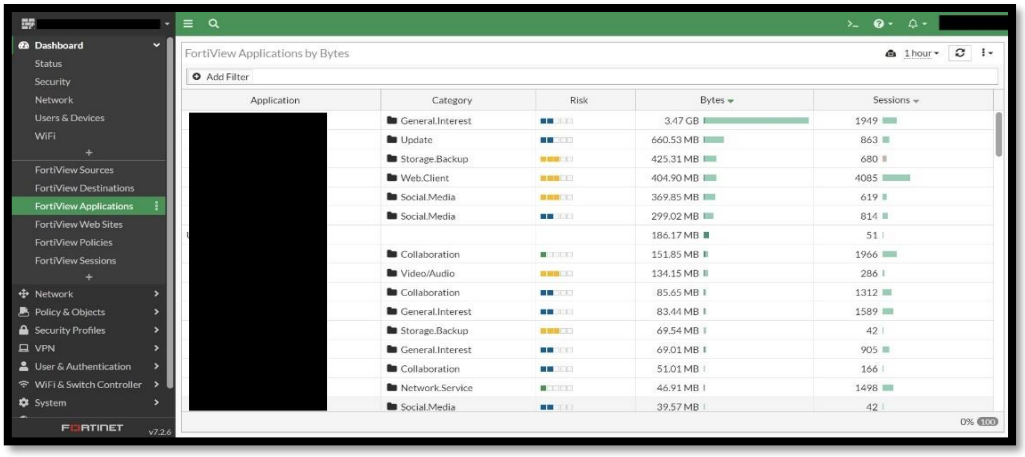


Imagen 24: Dashboard – FortView Applications. Fuente: Autoría propia.

Se tiene el aparatado FortiView Policies, en donde se puede observar la política fijada en el equipo Fortigate junto con la entrada física configurada, fuente y destino, incluyendo los bytes y las sesiones.

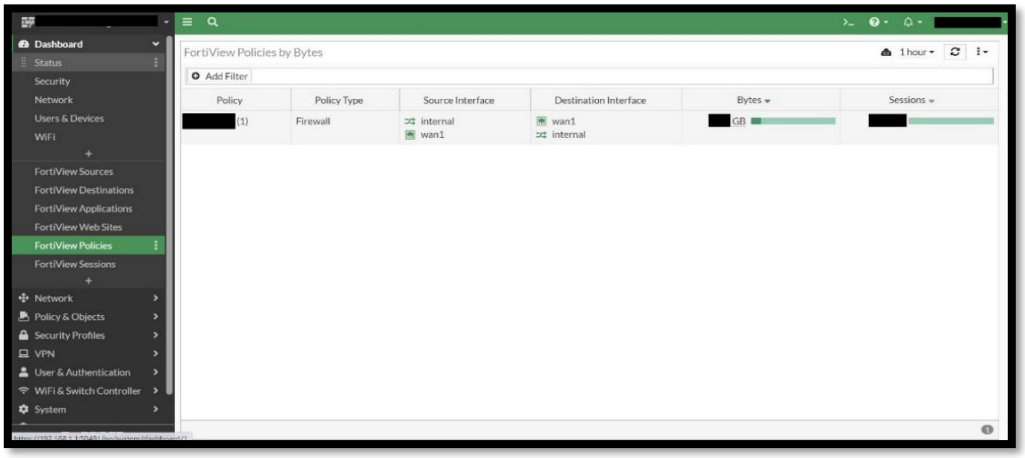


Imagen 25: Dashboard – FortView Policies. Fuente: Autoría propia.

En el apartado de FortiView Sessions se puede visualizar de manera específica la fuente (ip), dispositivo, destino, aplicación, tipo de protocolo, fuente y bytes de los clientes conectados a la red.

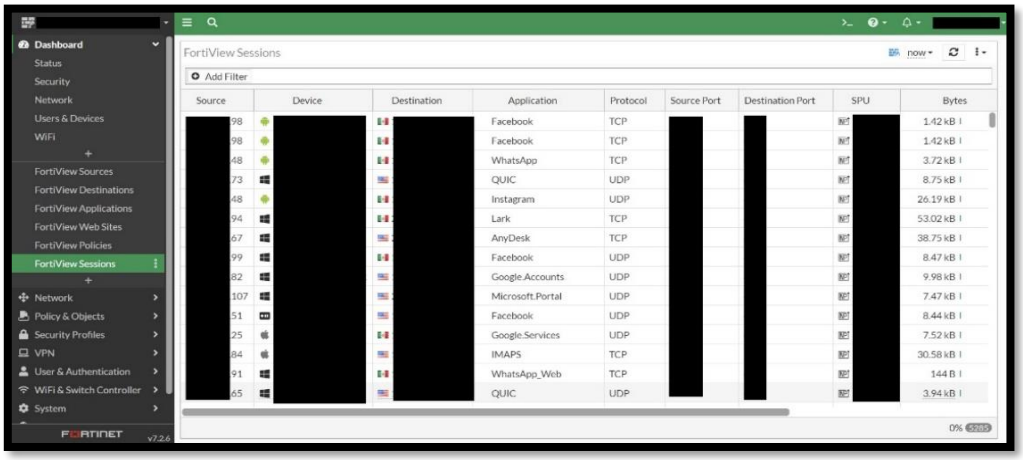


Imagen 26: Dashboard – FortView Sessions. Fuente: Autoría propia.

Pasando a otro apartado que es más específico en la red de las interfaces, en donde se visualiza gráficamente en puerto de enlace predeterminado, visualizando la asignación de los puertos del switch incluidos en el dispositivo Fortigate.

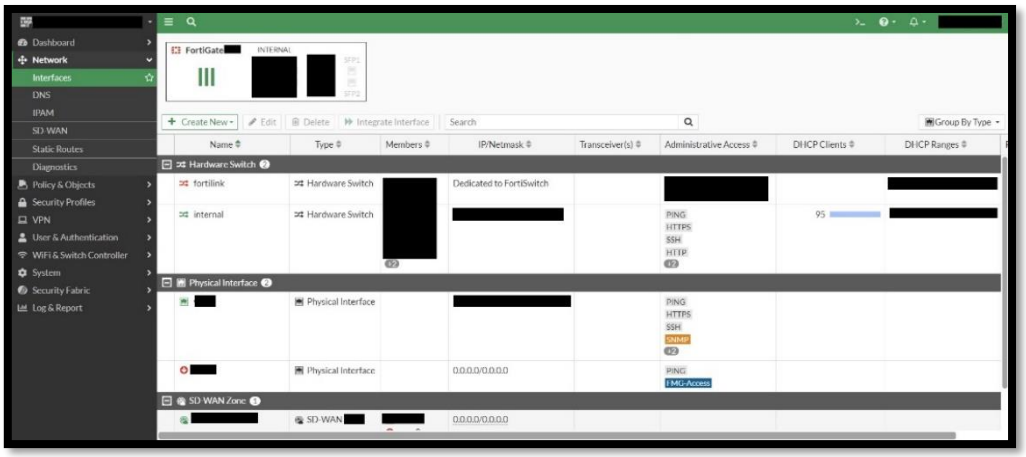


Imagen 27: Network – Interfaces principal. Fuente: Autoría propia.

Dentro de las interfaces, se puede visualizar la ip del dispositivo, las puertas de enlace y la segmentación DHCP que repartirá el equipo Fortigate, incluyendo los tipos de acceso.

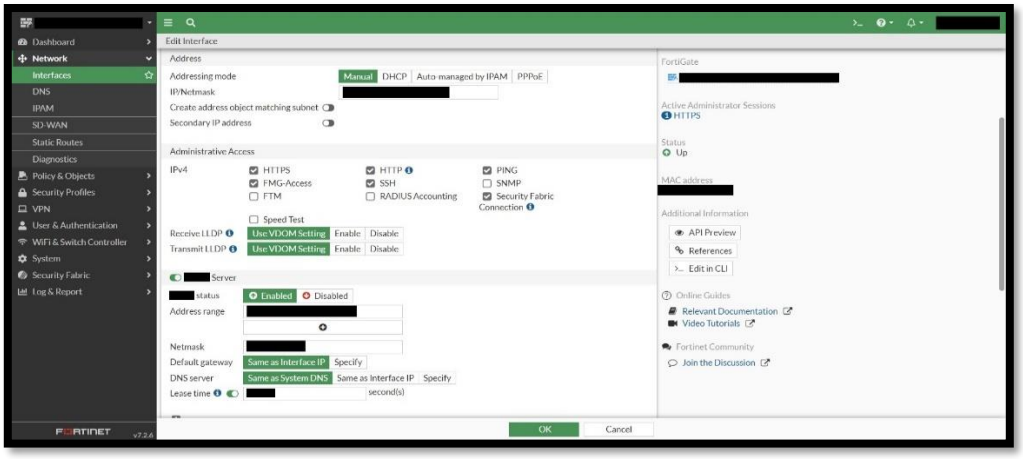


Imagen 28: Network – Interfaces editar. Fuente: Autoría propia.

En el apartado Security Profiles, se visualiza en la parte Web Filter, las páginas bloqueadas junto con el tipo de amenazas que de igual forma pueden separarse en tres tipos, Warning de aviso, Block de bloqueado y Enable de acceso.

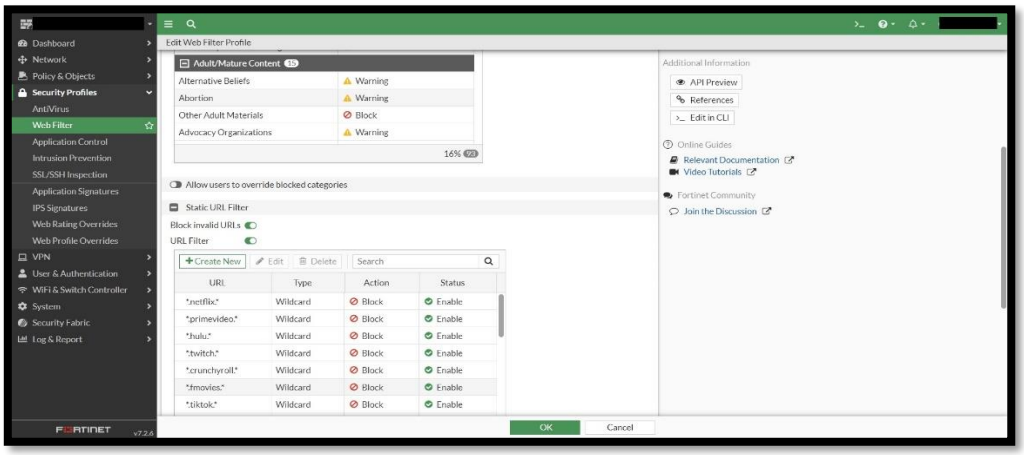


Imagen 29: Security Profiles – Web Filter. Fuente: Autoría propia.

En el apartado User & Authentication - User Definition se visualiza el usuario habilitado en uso, el cual muestra el tipo y el estatus en que se encuentra.

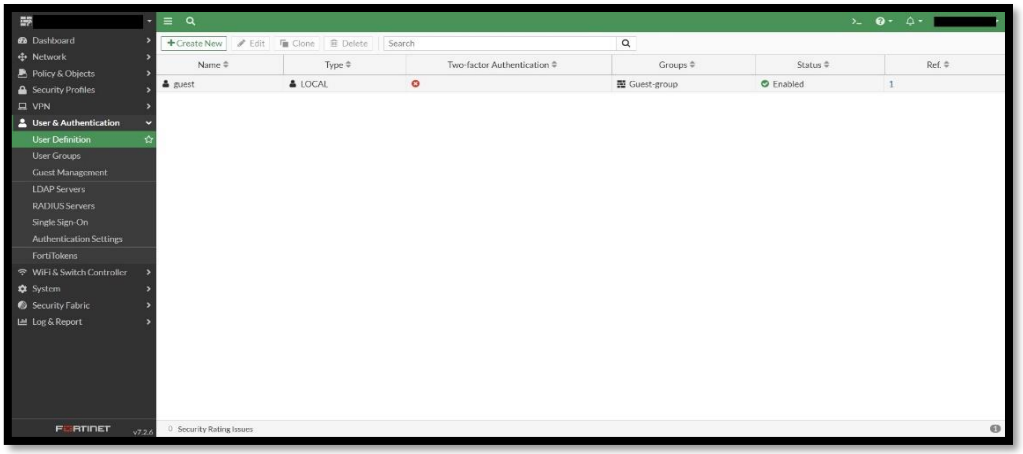


Imagen 30: User & Authentication en Fortigate. Fuente: Autoría propia.

En el apartado System - Settings, se puede visualizar el nombre del dispositivo, incluyendo los puertos HTTPS.

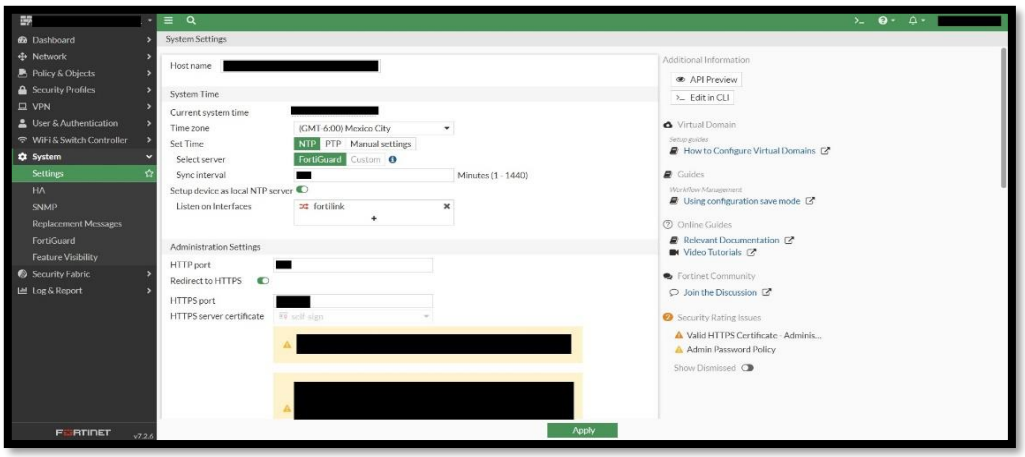


Imagen 31: Systems – Settings. Fuente: Autoría propia.

Brevemente, se termina con la configuración rápida de nuestro dispositivo Router TP-Link o Fortigate 80F, una vez realizado este paso, se continua con el dispositivo Switch PoE administrable, de igual forma se utiliza una versión básica para los centros de distribución y puntos de venta. Switch PoE de 8 puertos.

Imagen 32: Switch TP-Link PoE. Extraído de: https://www.dipol.com.pl/switch_poe_tp-link_tl-sg3210xhp-m2_8_x_2_5gbit-s_8_x_poe_2x_sfp_240w_802_3af-at_N30223.htm

Se necesitaba un dispositivo de estética y diseño básico, no eran tan demandante que tuviera algo relevante en esta cuestión, sin embargo, el dispositivo AP11 tiene un diseño compacto y fácil de instalar. El empaque del dispositivo contiene el punto de acceso AP11, soporte de montaje para pared y techo para evitar alguna caída o afectación estética.

Imagen 33: Aruba parte frontal. Extraído de: https://www.abasteo.mx/Redes/Access-Points/Access-Point-Aruba-de-Banda-Dual-Instant-On-AP11-867Mbit-s-1x-RJ-45-2-4-5GHz-Antena-de-5-8dBi.html?gad_source=1&gclid=CjwKCAiAzc2tBhA6EiwArv

Imagen 34: Aruba parte trasera. Extraído de: https://www.abasteo.mx/Redes/Access-Points/Access-Point-Aruba-de-Banda-Dual-Instant-On-AP11-867Mbit-s-1x-RJ-45-2-4-5GHz-Antena-de-5-8dBi.html?gad_source=1&gclid=CjwKCAiAzc2tBhA6

De manera en medidas métricas, consta de 34 x 152 x 152 mm. En caso de no tener predecesoramente un dispositivo PoE es necesario comprar un eliminador para que pueda tener energía.

Para la parte programable del dispositivo, se visualizan 2 focos leds los cuales nos ayudaran a saber el proceso en que se encuentra el dispositivo, la serie de arranques con las luces led son las siguientes.

Tabla 1: Luces Led Aruba Ap11. Colores led de dispositivo.

LUZ LED	COLOR/ESTADO		SIGNIFICADO
Sistema	Ninguna luz		El dispositivo no tiene corriente eléctrica.
	Verde Intermitente		El dispositivo se está iniciando.
	Verde/Ámbar - Alternativo		El dispositivo está listo para configurar.
	Verde - Fijo		El dispositivo está listo.
	Ámbar - Fijo		El dispositivo ha detectado un problema.
	Rojo - Fijo		El dispositivo tiene un problema; se requiere acción inmediata.
Radio	Ninguna luz		El wi-fi no está listo, los clientes inalámbricos no se pueden conectar.
	Verde - Fijo		El wi-fi está listo, los clientes inalámbricos se pueden conectar.

Para poder configurar del equipo es necesario, una cuenta en la plataforma de Aruba. En la cual se deben de dar de alta los dispositivos, la configuración puede ser por medio web o aplicación de PlayStore. Una vez teniendo ya conectado el dispositivo a la red con los leds en color verde/ámbar, es posible comenzar con la activación, se muestra como tal la configuración del dispositivo Aruba, como primera vez en instalación.

- Se ingresa a la opción configurar un nuevo sitio y se da en continuar.

Imagen 35: Configuración de nuevo sitio. Fuente: Autoría propia.

- Elegimos la opción de punto de acceso, ya que esta va a ser la funcionalidad que va a tener el punto de acceso.

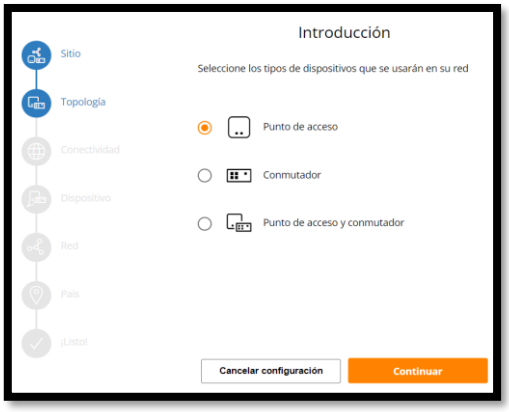


Imagen 36: Introducción para configurar dispositivo Aruba. Fuente: Autoría propia.

- Se elige la primera opción debido a que viene directo de un servicio de internet.

Imagen 37: Conectividad a elegir del dispositivo Aruba. Fuente: Autoría propia.

- Nos muestra que se debe tener el equipo ya conectado a la red con el cable UTP ponchado con un rj45, junto con el color ámbar verde y naranja para poder activar, se ingresa el número de serie del dispositivo para encontrarlo en red y así poder agregarlo.

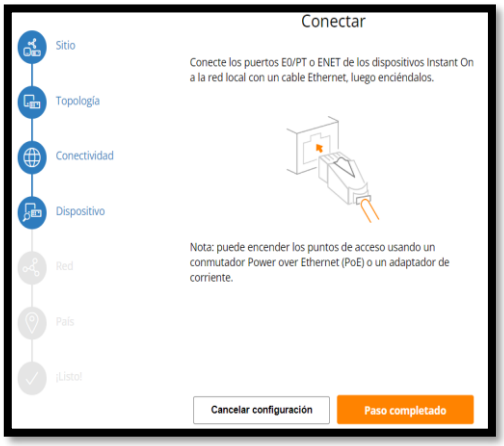


Imagen 38: Conectar el dispositivo directo a un cable de red. Fuente: Autoría propia.

Imagen 39: Muestra del modo de espera de dispositivo Aruba. Fuente: Autoría propia.

Imagen 40: Agregar por nombre el nuevo dispositivo en red. Fuente: Autoría propia.

Explicación de la administración de dispositivos de red.

Entrando a la parte de las pruebas y la operación de proporción del equipo, se puede visualizar todo el apartado con configuración de los sitio y redes. Se puede ver la parte de los apartados de redes, clientes, aplicaciones e inventario. Es de gran importancia hacer mención que, al momento realizar las pruebas, fueron de manera exitosa, ya que hasta la fecha operacionalmente los dispositivos Aruba en una palabra resumida “excelente”, ya que no se ha tenido ninguna baja de ningún dispositivo adquirido por proveedor en cuestión de hardware y software. A continuación, se muestran los apartados específicos, los cuales dan a mostrar lo que puede realizarse con esta plataforma, vía web y aplicación.

Se menciona la importancia de la conexión al servicio de internet, debido a que el dispositivo cuenta con su ranura con entrada rj45 para poder tener los datos del servicio, por medio de un cable ethernet.

Web.

- En la parte de red, nos muestra que nombre se quiere dar al sitio. El cual se muestra en algunas ya establecidos.

Imagen 41: Sitios a visualizar en cuenta. Fuente: Autoría propia.

Una vez dado de alta el dispositivo se puede visualizar de la siguiente forma. Dentro de este apartado se muestra lo que se puede modificar y crear dentro de cada uno, en estos apartados se puede modificar las redes, clientes, aplicaciones e inventario.

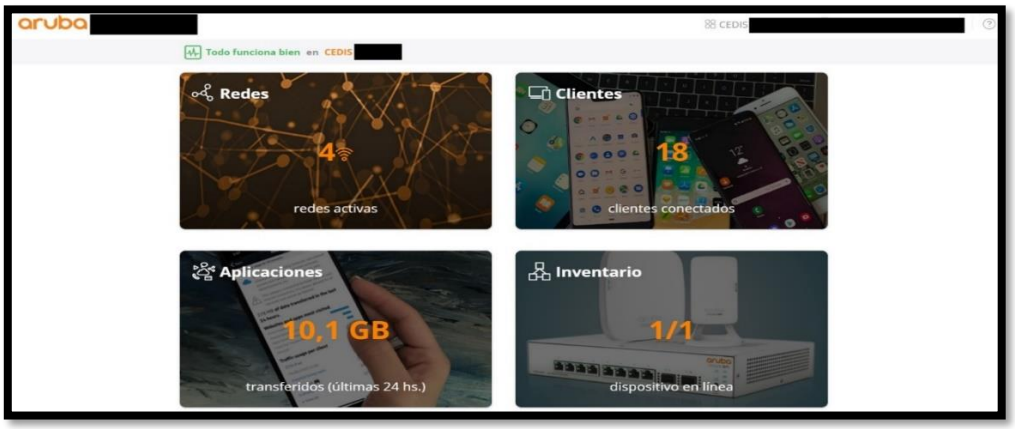


Imagen 42: Visualización general de plataforma Aruba. Fuente: Autoría propia.

En la parte de Redes se puede visualizar lo siguiente.

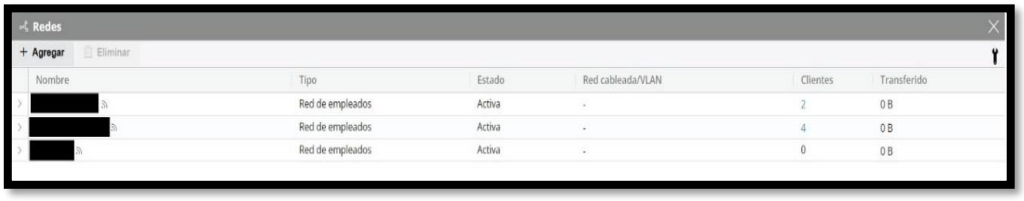


Imagen 43: Redes ya en línea. Fuente: Autoría propia.

- La parte de Identificación de la red, SSID y contraseña de la red.

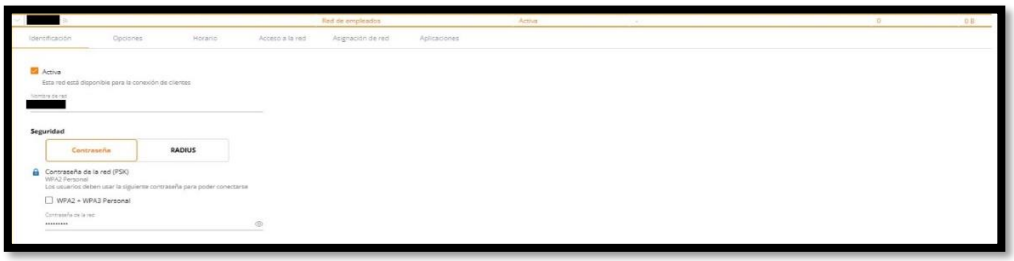


Imagen 44: Nombre de la red y contraseña en dispositivo Aruba. Fuente: Autoría propia.

- En la parte de opción vienen varias, como principales el mostrar la red, poder amarrar una IP estática, elegir el radio del dispositivo y la elección del radio del dispositivo, se deja por automático 2.4HGz y 5GHz.

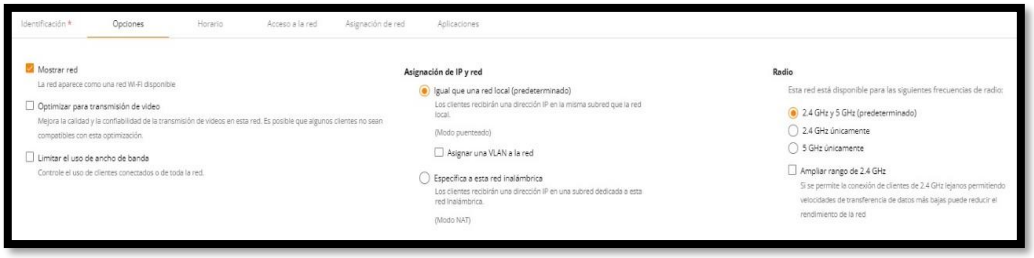


Imagen 45: Asignación de red y radio de dispositivo Aruba. Fuente: Autoría propia.

- Es posible habilitar el dispositivo con horarios.

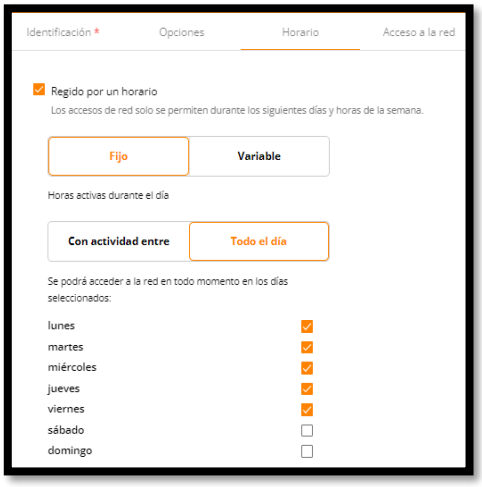


Imagen 46: Configuración de horarios de dispositivo Aruba. Fuente: Autoría propia.

- Se puede bloquear acceso a dispositivos mediante la IP.

Imagen 47: Acceso y bloqueo a dispositivos a la red. Fuente: Autoría propia.

- Asignación de una red en el dispositivo.

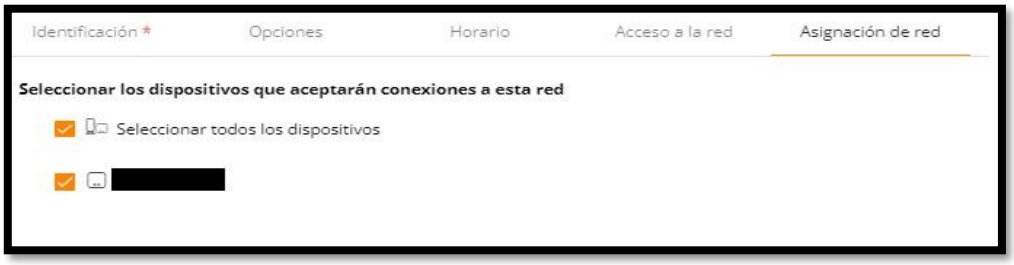


Imagen 48: Asignación de red a dispositivo. Fuente: Autoría propia.

- Las aplicaciones que se pueden bloquear para el uso correcto de cada área, se puede visualizar cada categoría a bloquear en la red a elegir del dispositivo.

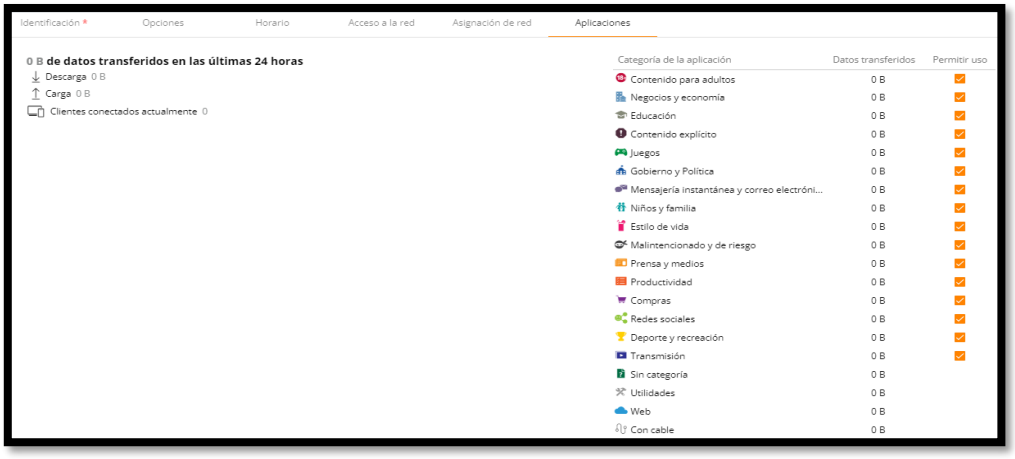


Imagen 49: Aplicaciones específicas a habilitar o bloquear. Fuente: Autoría propia.

En la parte de clientes se puede visualizar, los dispositivos que están conectados, en que red y en que se está consumiendo. Incluso en este apartado es posible bloquear dispositivos en caso de mal uso, así poder cerciorarse de que colaborador se trata.

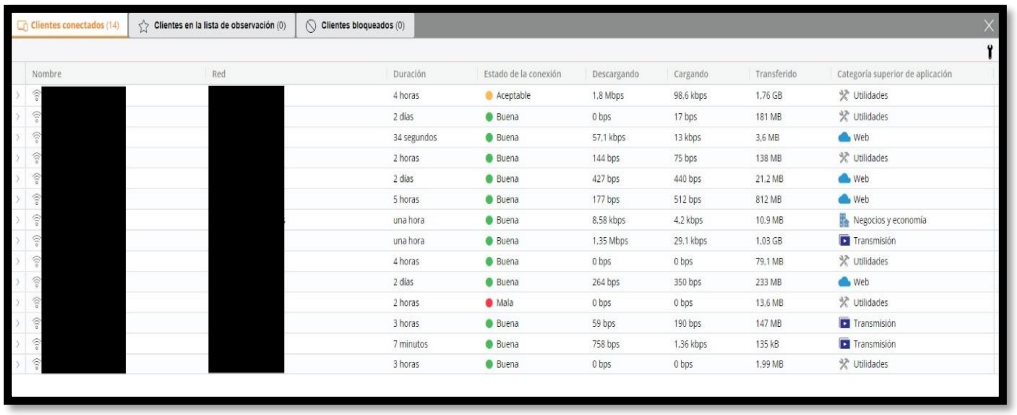


Imagen 50: Clientes conectados al dispositivo Aruba. Fuente: Autoría propia.

- En caso más específico es posible visualizar el dispositivo a fondo, ya sea para ver los consumibles durante días, que tipo de dispositivo es, que IP tiene, porcentaje de consumo, entre otros.

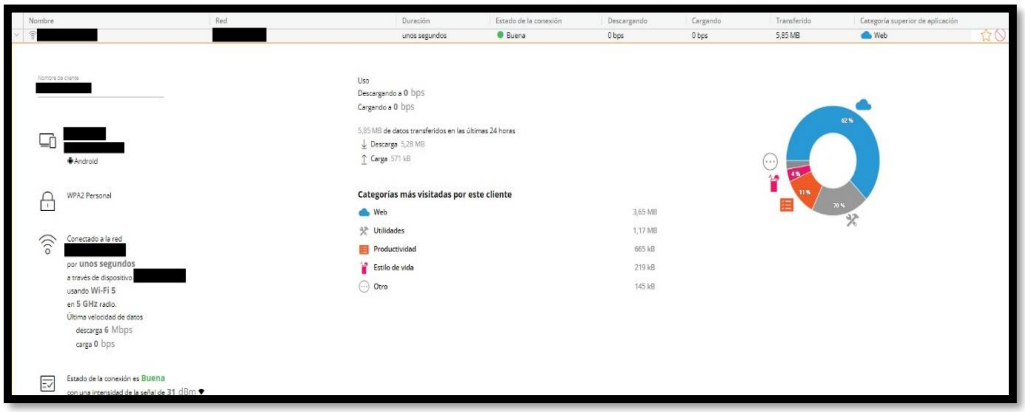


Imagen 51: Cliente específico en dispositivo Aruba. Fuente: Autoría propia.

En el apartado de aplicaciones, es posible verificar de igual forma de manera más específica quienes se conectan a la red y cuál es el dispositivo con más consumo de cada parte.

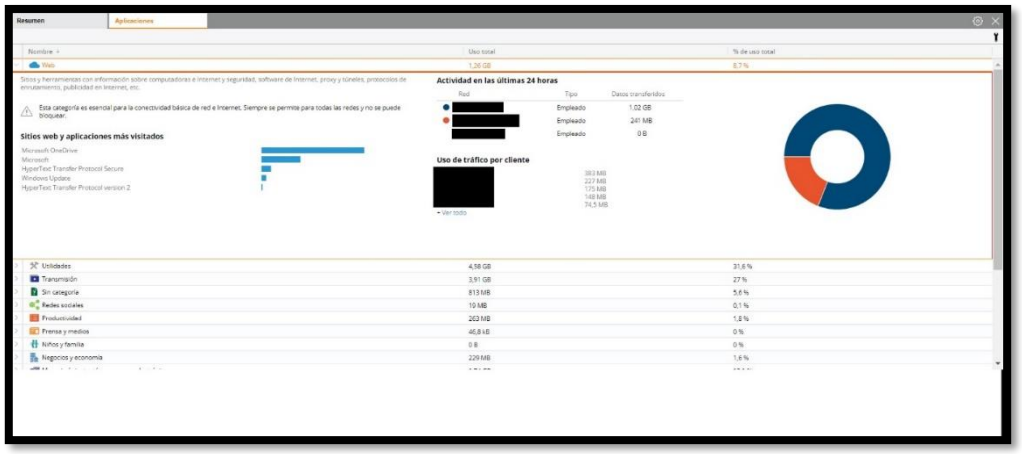


Imagen 52: Apartado de aplicaciones en dispositivo Aruba. Fuente: Autoría propia.

En el apartado de inventario es posible visualizar los dispositivos que están conectados.

- Se visualiza el nombre del dispositivo, información básica del mismo, los clientes conectados en qué tipo de radio.

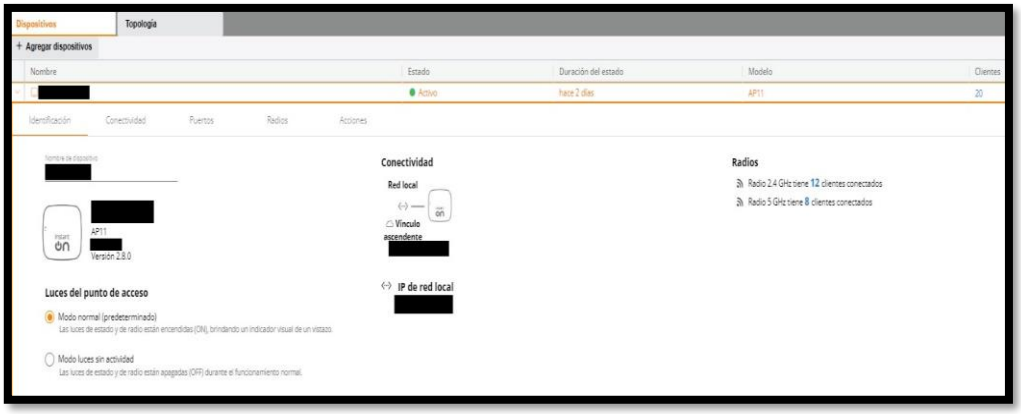


Imagen 53: Apartado del inventario en plataforma Aruba. Fuente: Autoría propia.

- La conectividad del dispositivo, en la cual estáticamente puede agregarse una IP específica para el mismo.

Imagen 54: Conectividad mediante IP LAN. Fuente: Autoría propia.

- El tipo de puertos del dispositivo Aruba en plataforma.

Imagen 55: Puertos en dispositivo Aruba. Fuente: Autoría

- El apartado más específico de los radios del dispositivo, en uso a elegir 2.4GHz o 5GHz, sin embargo, en modo predeterminado puede hacer uso de los 2.

Imagen 56: Radios específicos de dispositivo Aruba. Fuente: Autoría propia.

- Las acciones del dispositivo, en el cual se puede encontrar el dispositivo, realizar una prueba de red, el reinicio del dispositivo o desvincular el dispositivo. Cabe recalcar que todo se puede hacer remotamente desde la aplicación del celular.

Imagen 57: Acciones de dispositivo Aruba. Fuente: Autoría propia.

- Por último, en la topología se visualizan cuantos clientes hay en cada dispositivo, dependiendo el sitio, se pueden tener varios dispositivos Aruba conectados, dependiendo el switch que se tenga.

Imagen 58: Topología en red Aruba. Fuente: Autoría propia.

La plataforma avisa mediante alertas, alguna desconexión de dispositivos vista en versión Web.

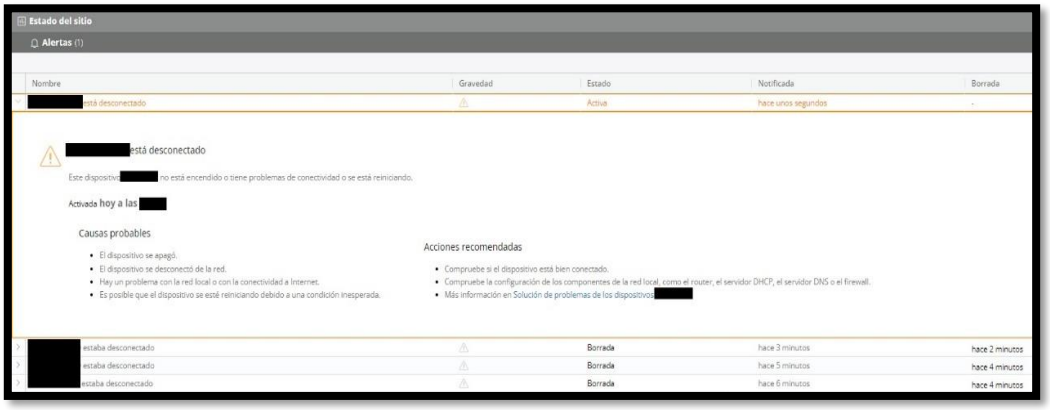


Imagen 59: Alertas de dispositivo Aruba. Fuente: Autoría propia.

De igual forma se tiene un apartado que da el soporte de poder realizar algún cambio interno, contraseña, notificaciones, en las cuales se pueden tener diferentes tipos de alertas. La conectividad del dispositivo avisa cuando el equipo se encuentra activo, el problema de dispositivo es la parte de la alerta con el problema de conectividad con el servicio de internet, de igual forma la capacidad de dispositivos que pueden estar conectados al punto de acceso, una actualización de software en donde se da la oportunidad de programar la actualización, por último, una regla infringida por algún dispositivo. La alerta puede ser vía móvil por medio de la aplicación y correo electrónico. De cierta manera es importante tener la App instalada para tener las notificaciones activas o bien activar el correo electrónico.

Imagen 60: Configuración de dispositivo. Fuente: Autoría propia.

App Aruba.

Básicamente, la versión de la aplicación de celular funciona de la misma forma con entorno grafico un poco diferente, pero se puede realizar exactamente lo mismo, una ventaja más de esta forma o manera de manejar Aruba es que se puede también dar de alta algún sitio desde el celular. En la actualidad tener este tipo de ventajas es importante para poder tener una reducción de tiempo en instalación y proporción en cualquier empresa.

- En entorno de aplicación, de igual forma se visualizan las redes.

Imagen 61: Sitios en aplicación Aruba. Fuente: Autoría propia.

- Podemos visualizar en un sitio las opciones generales como en la versión web.

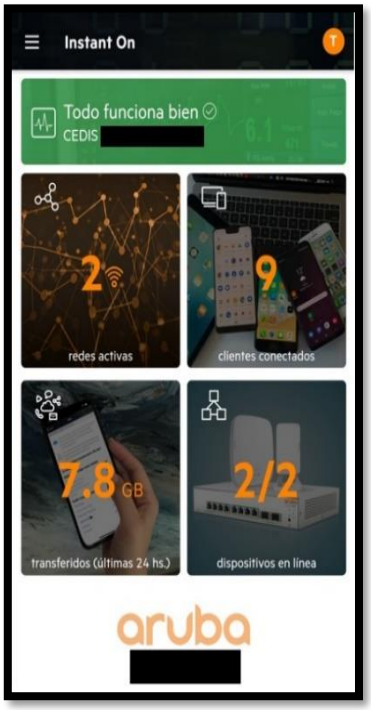


Imagen 62: Vista general en aplicación. Fuente: Autoría propia.

- Se visualiza la parte de las redes en el sitio mediante aplicación.

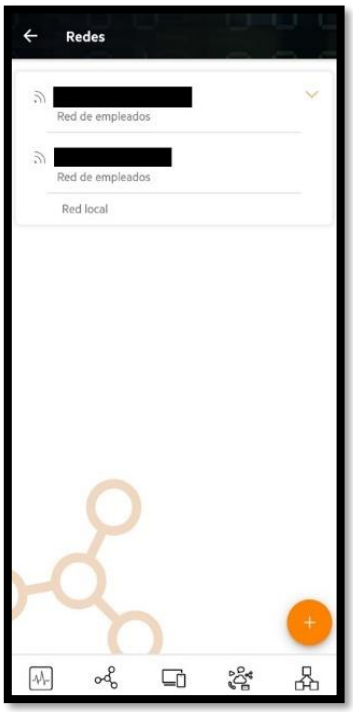


Imagen 63: Vista de redes en aplicación. Fuente: Autoría propia.

- Se visualizan los dispositivos conectados a la red mediante aplicación.

Imagen 64: Vista de clientes en aplicación. Fuente: Autoría propia.

- En este apartado, se visualiza el consumo de las aplicaciones en las redes.

Imagen 65: Consumo de redes en aplicación. Fuente: Autoría propia.

- Se puede observar el apartado de los dispositivos conectados ya en red, incluyendo el signo “+” para poder agregar un dispositivo más, y la topología de los dispositivos conectados a los AP.

Imagen 66: Dispositivos en red. Fuente: Autoría propia.

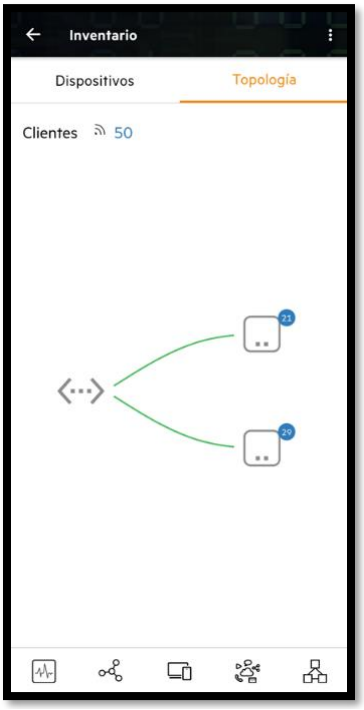


Imagen 67: Topología de dispositivos. Fuente: Autoría propia.

- Para finalizar tenemos el apartado que nos lleva a otros apartados ya conocidos y mencionados.

Imagen 68: Menú auxiliar general. Fuente: Autoría propia.

Siendo como primordial requisito interno, un dispositivo con alcances grandes con un que fuera innovador y no tan costoso, se llegó a la elección del dispositivo Aruba modelo AP11, como un efectivo resultado, se procedió a las pruebas, las cuales desde implemento el dispositivo ha dado avisos o alertas, las cuales en el momento exacto de una notificación nosotros podemos visualizar si fue una desconexión remota del dispositivo o bien, si es el servicio de internet proporcionado por el proveedor. En ciertas ocasiones ha sido de buen uso la parte del bloqueo de las aplicaciones utilizadas por el personal, específicamente en centros de distribución, ya que, por cuestiones de política de la empresa, se han tenido solicitudes especificas en la parte de aplicaciones indebidas que puedan afectar el tiempo de labor del trabajador. Sin embargo, de igual forma teniendo un dispositivo TP-Link que pueda brindar la función de un Router ha sido de gran apoyo, al igual que un equipo Fortigate, el cual es más especializado y excelente en uso empresarial.

Cabe recalcar nuevamente que el personal y único autorizado a la visualización de estas herramientas son el departamento de T.I. los cuales tienen esa responsabilidad primordial para el buen funcionamiento de los sitios remotos.

CCTV.

Para cada cedis, punto de venta, y oficina se necesitaba una manera para poder monitorear los puntos, en caso de algún altercado, un mal proceso, etc. La solicitud fue investigar, proponer y realizar la instalación de CCTV en los puntos. Primero, verificar dispositivos que entraran dentro del rango del presupuesto, de igual forma la eficacia de estos y la instalación rápida. En cuestiones de marca se eligió Hikvision y Dahua, ambas marcas distintas en software, pero con eficacia similar. Para Hikvision se usaron cámaras IP, las cuales hacen un uso de un NVR y para Dahua fueron cámaras análogas que hacen un uso de un DVR. Ambos dispositivos con un disco duro de memoria aceptable para las grabaciones. Ambas marcas usan un software diferente para la visualización de las cámaras. Hikvision usa Hik-Connect y para Dahua se usa DMSS. Actualmente se cuenta con CCTV en 5 cedis, 20 puntos de venta y 1 en el corporativo.

Dahua.

El inicio de un DVR de marca Dahua es elegir el idioma, en donde podemos elegir el idioma y región del dispositivo.

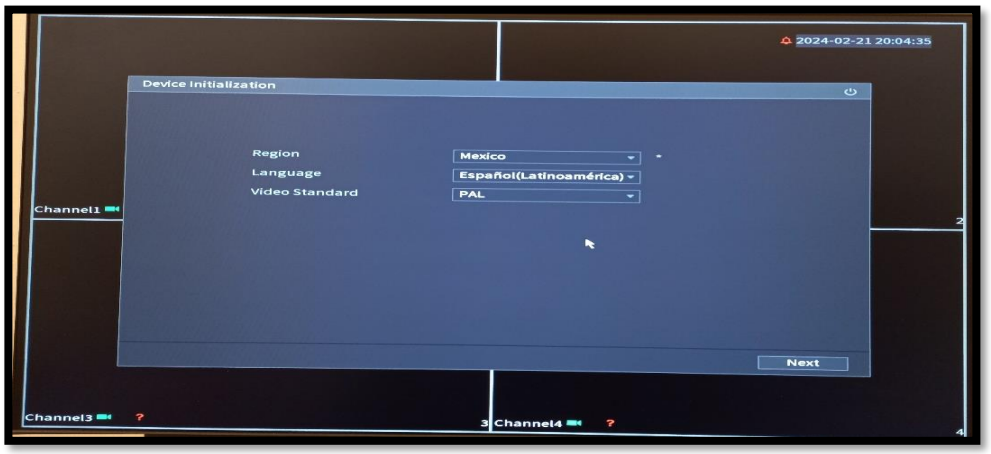


Imagen 69: Configuración inicial Dahua. Fuente: Autoría propia.

Continuando con la contraseña del dispositivo. Se configura de manera que el usuario sea el único que tenga acceso a la está.

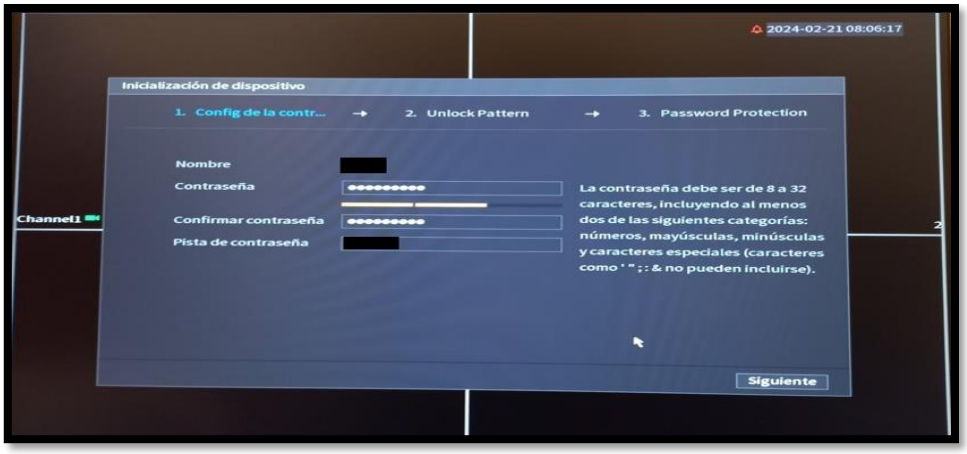


Imagen 70: Contraseña de dispositivo CCTV. Fuente: Autoría propia.

Se da continuidad con el patrón de desbloqueo, este apartado es opcional, sin embargo, en la empresa si se hace de su uso.

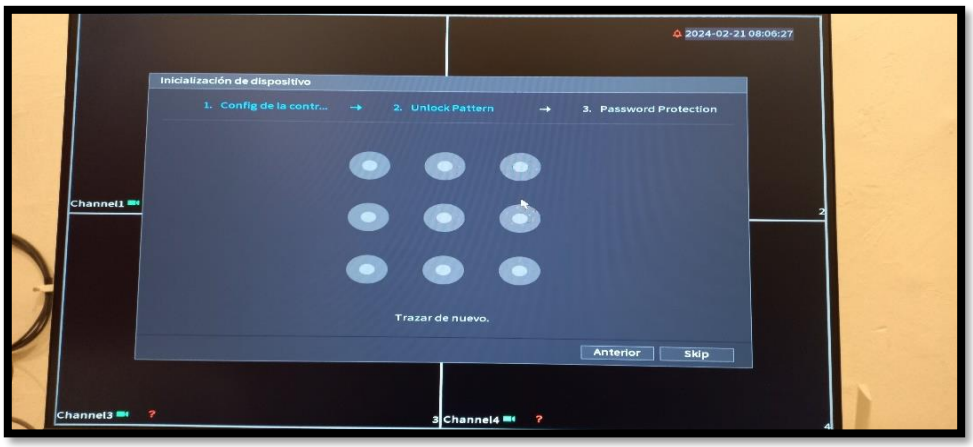


Imagen 71: Patrón de desbloqueo de CCTV. Fuente: Autoría propia.

Para poder restablecer una contraseña en caso de extravío, es posible realizar el cambio mediante correo empresarial. Se incluyen algunas preguntas default.

Imagen 72: Contraseña de CCTV. Fuente: Autoría propia.

Se pasa al apartado de la conexión directa vía cable ethernet del módem al dispositivo DVR. Normalmente se deja en la opción DHCP para tomar un IP dinámica.

Imagen 73: Asignación de IP de dispositivo CCTV. Fuente: Autoría propia.

Una vez que se tiene conectado el dispositivo a módem de internet proporcionado por el proveedor, se puede proceder a la conexión remota desde algún dispositivo en el software DMSS teniéndolo siempre y cuando en línea.

Imagen 74: Agregar dispositivo CCTV a cuenta de aplicación. Fuente: Autoría propia.

Para poder agregar el dispositivo en la aplicación, es necesario tener una cuenta en la plataforma, una vez teniendo la cuenta se visualiza de la siguiente manera.

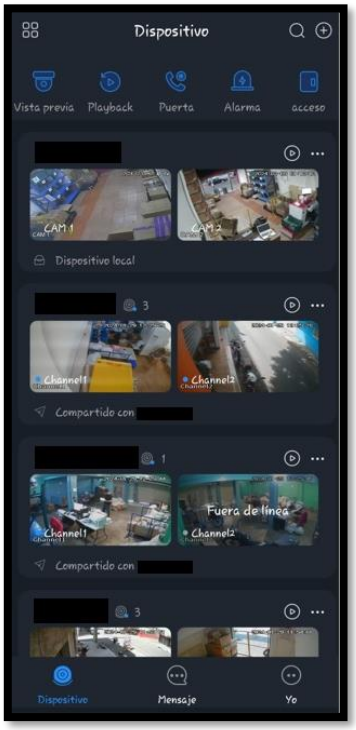


Imagen 75: Vista de aplicación de CCTV. Fuente: Autoría propia.

Seguidamente, se agrega mediante No. de serie del dispositivo para que se pueda visualizar en la aplicación.

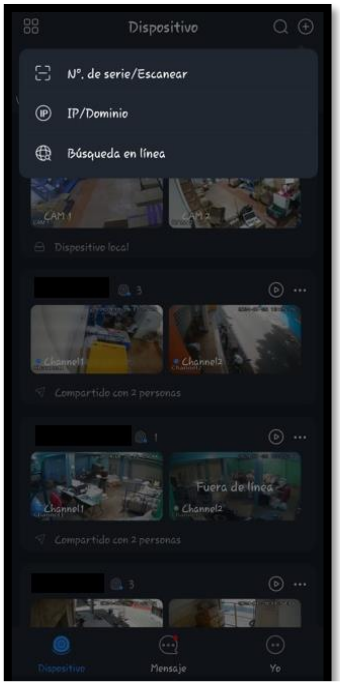


Imagen 76: Agregar dispositivo en aplicación de CCTV. Fuente: Autoría propia.

Se agrega el número de serie del dispositivo en el sitio a instalar, esa información se encuentra debajo del dispositivo.

Imagen 77: Ingreso de número de serie a aplicación de CCTV. Fuente: Autoría propia.

Se agrega la opción DVR / XVR, ya que es un DVR el que se tiene conectado al sitio y ese será el que se configurará.

Imagen 78: Elección de tipo de dispositivo a aplicación de CCTV. Fuente: Autoría propia.

Por último, se agrega el nombre que se le va a dar al sitio, el usuario y la contraseña ingresada en la primera configuración del dispositivo.

Imagen 79: Ultimas configuraciones en aplicación de dispositivo CCTV. Fuente: Autoría propia.

En ciertos casos debido a los cambios de horario, reinicios o fallas en la energía que alimenta el punto o cedis, existe el pequeño error y cambio en el horario de los dispositivos NVR. Afortunadamente, se puede realizar el cambio mediante la conexión IP del dispositivo. Esta IP se puede visualizar dentro del dispositivo o bien se puede usar otro tipo de software para asegurar que sea la correcta.

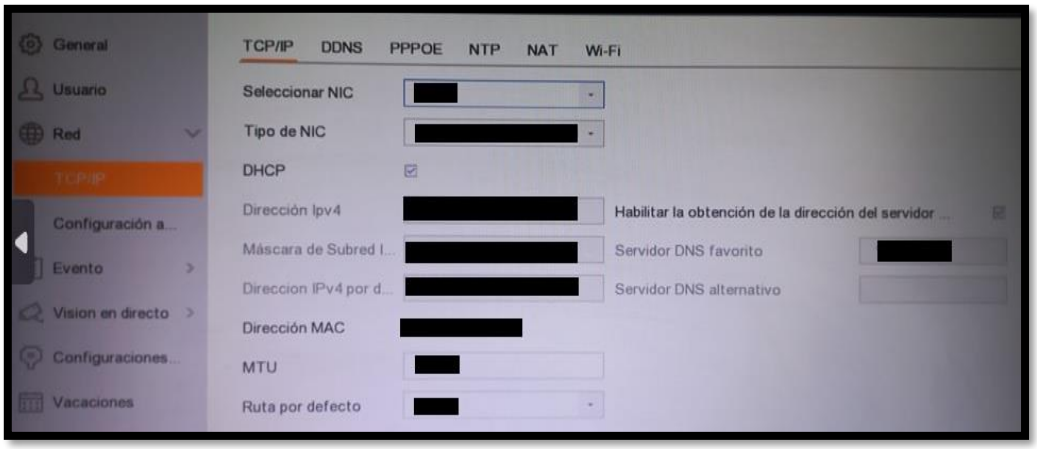


Imagen 80: IP en dispositivo en DVR CCTV. Fuente: Autoría propia.

Posteriormente, con la IP, se ingresa y se inicia sesión al dispositivo.

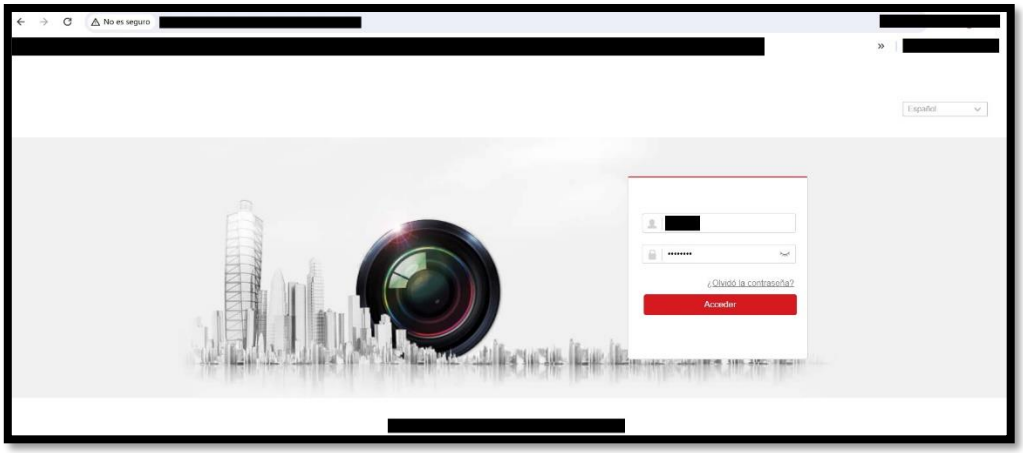


Imagen 81: Ingreso en red a dispositivo NVR. Fuente: Autoría propia.

Dentro se dirige directamente a configuración, configuración de sistema, ajuste de hora y ahí es donde se puede establecer la hora fija a la actual y no haya errores para el chequeo de algún incidente.

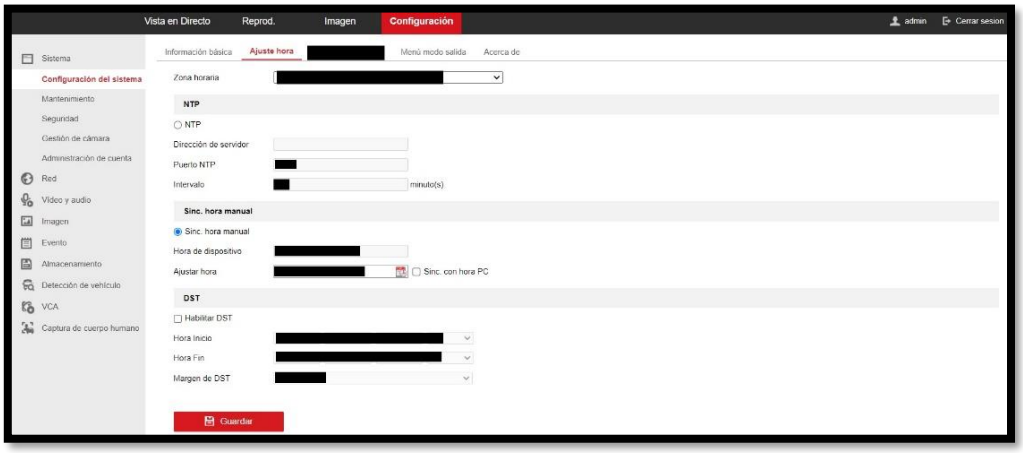


Imagen 82: Configuración de hora de dispositivo NVR. Fuente: Autoría propia.

Por último, para poder tomar el cambio es necesario reiniciar el dispositivo NVR y se podrá visualizar la hora adecuada en las aplicaciones de vista en nuestros dispositivos laptop o celular, dependiendo el departamento.

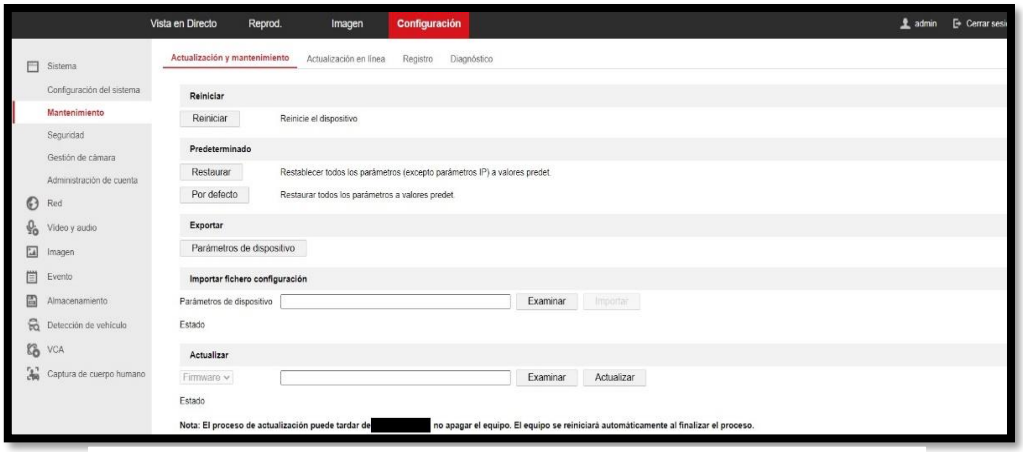


Imagen 83: Reinicio de dispositivo NVR. Fuente: Autoría propia.

Implementaciones generales al área T.I.

Telefonía IP.

En cuanto a la telefonía IP, se maneja actualmente en corporativo para ciertas áreas de la oficina, debió a que no todo el personal lo requiere, sin embargo, departamentos como recursos humanos, finanzas, administración son algunos que si lo requieren para fines internos.

Imagen 84: Teléfono Grandstream. Extraído de: https://www.afgsoluciones.com/index.php?id_product=23&rewrite=gxp1625&controller=product

El teléfono IP PoE que se maneja es de marca Grandstream, con modelo GXP1625 962-00080-31C, ha tenido un rendimiento estable, el proveedor con quien se maneja esta telefonía es por medio de GoToConnect. En la parte de la configuración se tiene que realizar una configuración estática por IP a los dispositivos junto con el proveedor de manera remota, pese a que se cuenta con una aplicación web interna, la cual muestra los datos de cada dispositivo, asignaciones estáticas de IP, entre otros. Actualmente se manejan 8 dispositivos repartidos en los departamentos de la oficina, lo que, es decir, 8 IP's estáticas en uso.

Solo en el apartado principal se puede visualizar lo siguiente, incluyendo su ip estática.

Imagen 85: Teléfono Grandstream pantalla. Fuente: Autoría propia.

Impresoras multifuncionales IP.

Después se tienen las impresoras multifuncionales, actualmente se manejan 2 marcas, de Kyocera se maneja 1 modelo y Ricoh 3 modelos, las cuales de igual forma tienen una ip estática. Ambas usan diferentes controladores al momento de instalación al usuario.

Imagen 86: Impresora Kyocera M3655idn. Extraído de: https://www.kyoceradocumentsolutions.es/es/smarter-workspaces/insights-hub/articles/the-new-ecosys-m3655idna.html

Imagen 87: Impresora Ricoh 430F. Extraído de: https://www.ricoh-americalatina.com/es-mx/productos/pd/equipo/impresoras-y-fotocopiadoras/impresoras-multifunci%C3%B3n-fotocopiadoras/im-430f-impresora-multifunci%C3%B3n-en-blanco-y-negro

Se asigna una ip estática desde la impresora, el cual será el identificar siempre cuando se instale en un dispositivo PC – Laptop.

Su instalación viene dentro del panel de control como cualquier impresora, en caso de ser manualmente y que tome una ip estática. Como primer paso se agrega la impresora con la dirección IP elegida para el dispositivo.

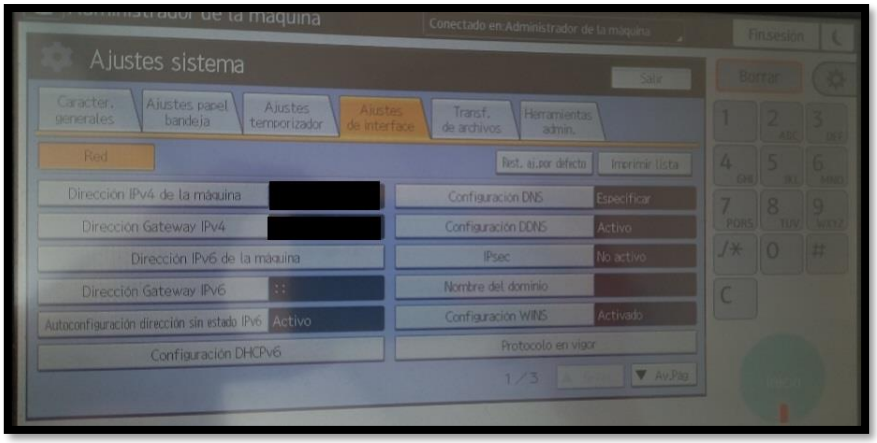


Imagen 88: Asignación de IP a impresora Ricoh. Fuente: Autoría propia.

Como primer paso se elige la opción de agregar la impresora mediante una IP.

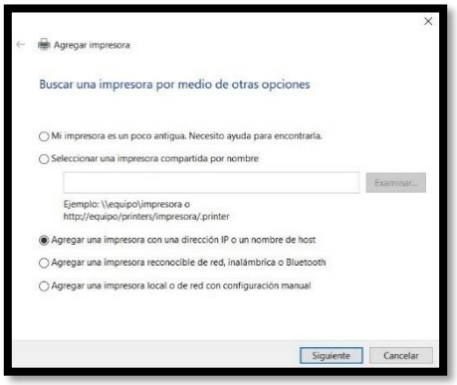


Imagen 89: Asignación de IP a impresora Ricoh en panel de control. Fuente: Autoría propia.

Después se elige la opción TCP/IP. Y se agrega la ip asignada anteriormente en físico.

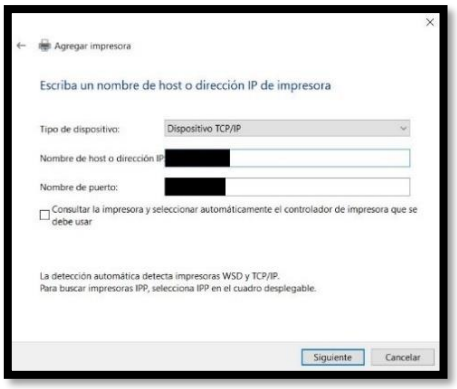


Imagen 90: Asignación de IP a impresora. Fuente: Autoría propia.

Dentro de este apartado se elige el controlador ya ejecutado desde el disco local principal del equipo. Por consiguiente, se nombra la impresora y tenemos la impresora instalada.

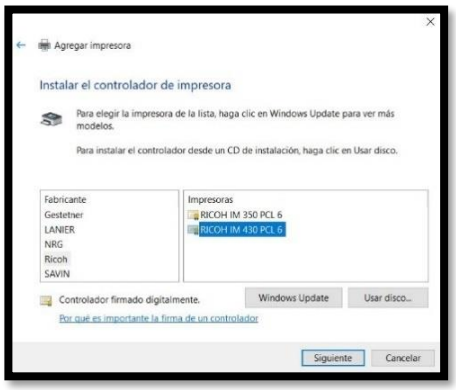


Imagen 91: Controlador de impresora. Fuente: Autoría propia.

Inventario, refacciones y licencias office en equipos de cómputo.

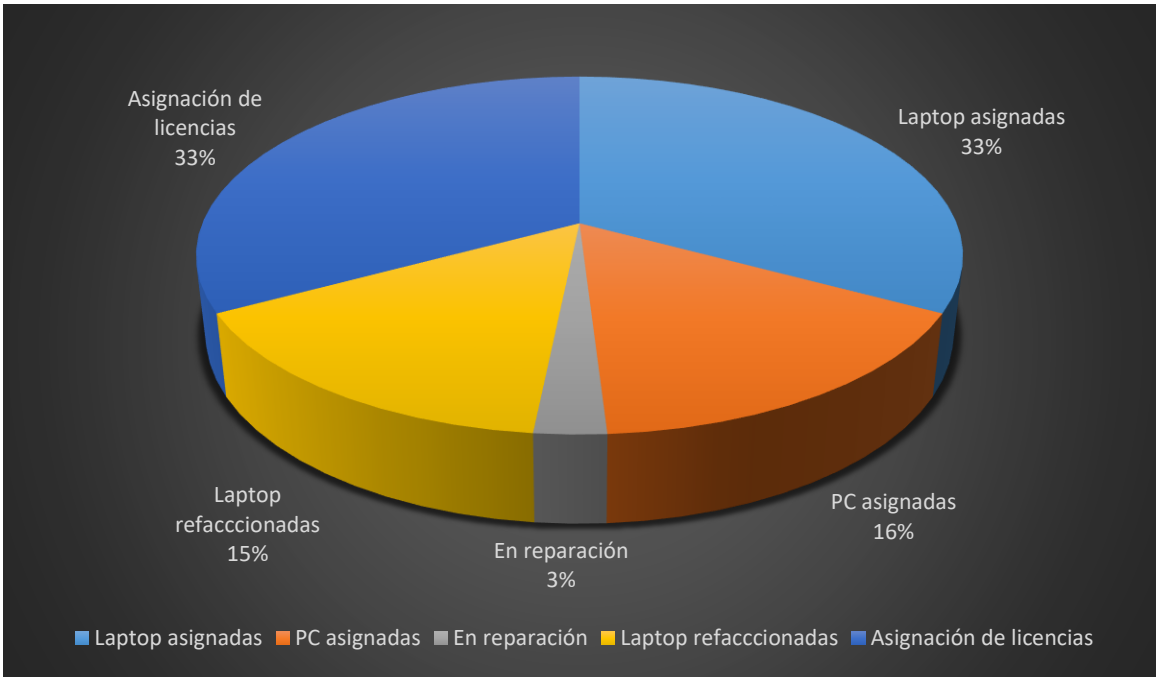
El inventario que se maneja actualmente se mantiene mediante un documento Excel interno del área T.I. Se han proporcionado alrededor de **102 equipos** laptop asignados por medio de una hoja responsiva y **50 PC** de igual forma asignados con hojas responsivas internas del área, es importante mencionar que se tiene un historial de uso de los equipos, ya que debido a que son equipos laptop se han transferido a diferentes usuarios debido a la rotación de personal.

Referente a las refacciones se han realizado 48 modificaciones de discos solidos M2 de 240GB a **48 equipos**, de los cuales 4 de igual forma han sido RAM de 4 a 8GB, para tener un mejor rendimiento, instalando el sistema operativo Windows 10 Pro, que es el más viable en cuanto a compatibilidad. Y se tienen en reparación **8 equipos** laptop.

En cuanto al licenciamiento office se utiliza la versión 365 para negocio, actualmente se tienen proporcionadas **108 licencias asignadas** en los equipos.

A continuación, se visualiza de manera grafica como está distribuida la información previa.

Tabla 2: General de Laptops y PC's. Muestra en porcentaje los dispositivos.



En la operación se manejan dispositivos PDA los cuales tienen como función principal el escaneo de guías de la empresa, de igual forma tiene un uso como de un dispositivo celular, ya que cuenta con las funciones de este. Sin embargo, como en todo debe de haber una configuración en cada dispositivo PDA para la seguridad y resguardo de la información de la empresa. Una vez teniendo la solicitud por parte del departamento de operaciones, el departamento de T.I. es el encargado de realizar la configuración de las PDAS, para proceder a entregar al departamento correspondiente para su continuidad con operaciones. La siguiente tabla muestra el proceso a seguir de dicha configuración.

Tabla 3: Configuración de PDA. Tabla que muestra pasos a seguir.

[redacted]	[redacted] Departamento T.I.
Paso	**Objetivo**
1	Verificar que la hora e idioma del dispositivo estén configuradas correctamente.
2	Instalar aplicación AppLock.
3	Dentro de AppLock cambiar patrón de contraseña.
4	Dentro de AppLock entrar a ajustes y activar la opción "Interruptor de bloqueo rápido".
5	Instalar las aplicaciones de la empresa.
6	Activar ubicación en todas las opciones.
7	Verificación final de apps instaladas.
Notas	
Después de 3 minutos la aplicación AppLock se inicia y activa.	
Únicamente el personal autorizado puede reiniciar de resetear los equipos PDA.	
Apoyo directo de encargado del punto para el funcionamiento correcto de las apps.	
En caso de no activarse la aplicación AppLock, entrar e iniciar.	

Actualmente, en corporativo los dispositivos PDA que se configuraron por el departamento de T.I. ronda alrededor de 300 a 400 dispositivos alrededor de los puntos y cedis. El área administrativa es la encargada de llevar el registro de números de serie y salidas que se han realizado.

En la mayoría de las instalaciones, se presenta una cotización por parte del departamento de T.I., en donde se cuentan con proveedores internos del personal, los cuales apoyan a tener una mejor propuesta, ya que la solicitud fue tener un menor gasto y funcionalidad en los dispositivos. La siguiente cotización muestra tipos de cámaras que se usan para el dispositivo DVR.

RESUMEN EJECUTIVO

PROPUESTA ECONÓMICA

Fecha de elaboración: [redacted] 2021

Contacto: [redacted]
Teléfono:
e-mail:

Dirección:

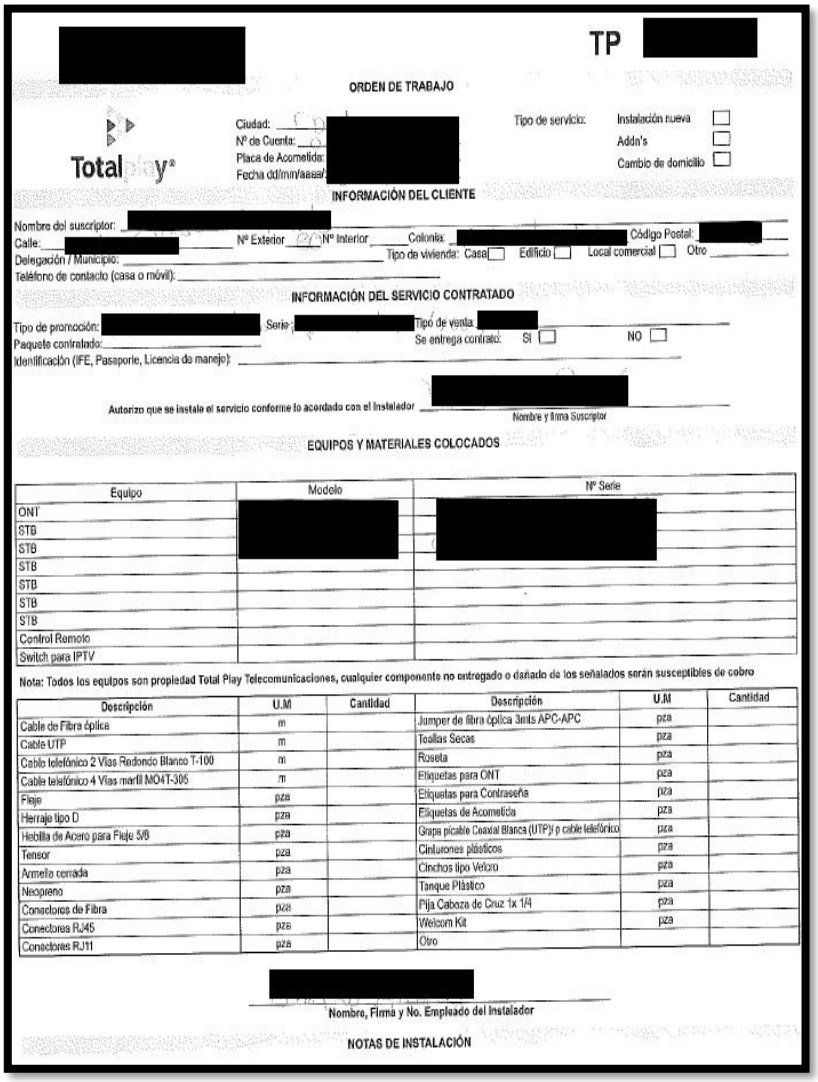
Contacto Quimera Networks: [redacted]

Enviamos la cotización de acuerdo a los requerimientos presentados. Si tienen alguna pregunta respecto a los productos listados o requieren más información favor de contactarnos en los emails o teléfonos presentados. Gracias por su interés en Nuestros servicios.

Cantidad	Identificador	Descripción	Costo Unitario
1	IPC-B121H	HiLook Series / Bala IP 2 Megapixel / 30 mts IR / Exterior IP67 / PoE / dWDR / Lente 2.8 mm / H.265+	$ 840.00
1	DS-2CV1021G0-IDW1(D)	Bala IP 2 Megapixel / 30 mts IR EXIR / Exterior IP66 / dWDR / Lente 2.8 mm / WIFI / Micrófono Integrado / Memoria Micro SD	$ 1,238.72
1	DS-2CD1023G0-IU	Bala IP 2 Megapixel / Lente 2.8 mm / Microfono Integrado / 30 mts IR EXIR / Exterior IP66 / H.265 / PoE	$ 1,235.64
1	DS-2CD2023G0-I	Bala IP 4 Megapixel / Lente 2.8 mm / 40 mts IR EXIR / Exterior IP67 / WDR 120 dB / PoE / Micrófono Integrado / Videoanaliticos (Filtro de Falsas Alarmas) / Ultra Baja Iluminación Fabricadas en metal.	$ 2,112.04
1	DS-2CD2T43G0-I5	Bala IP 4 Megapixel / Serie PRO / Lente 4 mm / 50 mts IR EXIR / Uso en Exterior IP67 / WDR / PoE (Fabricadas en Metal)	$ 2,662.24
1	IPC-B621H-Z	Bala IP 2 Megapixel / Lente Motorizado 2.8 - 8 mm / 20 mts IR EXIR / PoE / Exterior IP66 / dWDR / Micro SD / Micrófono Integrado (Fabricadas en Metal)	$ 1,970.42

Imagen 92: Ejemplo de cotización de proveedor. Fuente: Autoría propia.

Cada vez que se recibe un servicio de internet con proveedor es importante acudir al punto para verificar la instalación correcta, ya que se debe validar el servicio, latencia y correcta adecuación de la fibra óptica.



TP [redacted]

ORDEN DE TRABAJO

Total y

Ciudad: [redacted]
Nº de Cuenta:
Placa de Acometida:
Fecha dd/mm/aaaa:

Tipo de servicio: Instalación nueva ☐ Adda's ☐ Cambio de domicilio ☐

INFORMACIÓN DEL CLIENTE

Nombre del suscriptor: [redacted]
Calle: [redacted] Nº Exterior Nº Interior Colonia: [redacted] Código Postal: [redacted]
Delegación / Municipio: Tipo de vivienda: Casa ☐ Edificio ☐ Local comercial ☐ Otro
Teléfono de contacto (casa o móvil):

INFORMACIÓN DEL SERVICIO CONTRATADO

Tipo de promoción: [redacted] Serie: [redacted] Tipo de venta: [redacted]
Paquete contratado: Se entrega contrato: SI ☐ NO ☐
Identificación (IFE, Pasaporte, Licencia de manejo):

Autorizo que se instale el servicio conforme lo acordado con el Instalador [redacted]
Nombre y firma Suscriptor

EQUIPOS Y MATERIALES COLOCADOS

Equipo	Modelo	Nº Serie
ONT	[redacted]	[redacted]
STB		
STB		
STB		
STB		
STB		
STB		
Control Remoto		
Switch para IPTV		

Nota: Todos los equipos son propiedad Total Play Telecomunicaciones, cualquier componente no entregado o dañado de los señalados serán susceptibles de cobro

Descripción	U.M	Cantidad	Descripción	U.M	Cantidad
Cable de Fibra óptica	m		Jumper de fibra óptica 3mts APC-APC	pza	
Cable UTP	m		Toallas Secas	pza	
Cable telefónico 2 Vías Redondo Blanco T-100	m		Roseta	pza	
Cable telefónico 4 Vías marfil MOHT-305	m		Etiquetas para ONT	pza	
Fleje	pza		Etiquetas para Contraseña	pza	
Herraje tipo D	pza		Etiquetas de Acometida	pza	
Hebilla de Acero para Fleje 5/8	pza		Grapa picable Coaxial Blanca (UTP) y cable telefónico	pza	
Tensor	pza		Cinturones plásticos	pza	
Armella cerrada	pza		Cinchos tipo Velcro	pza	
Neopreno	pza		Tanque Plástico	pza	
Conectores de Fibra	pza		Pija Cabeza de Cruz 1x 1/4	pza	
Conectores RJ45	pza		Welcom Kit	pza	
Conectores RJ11	pza		Otro		

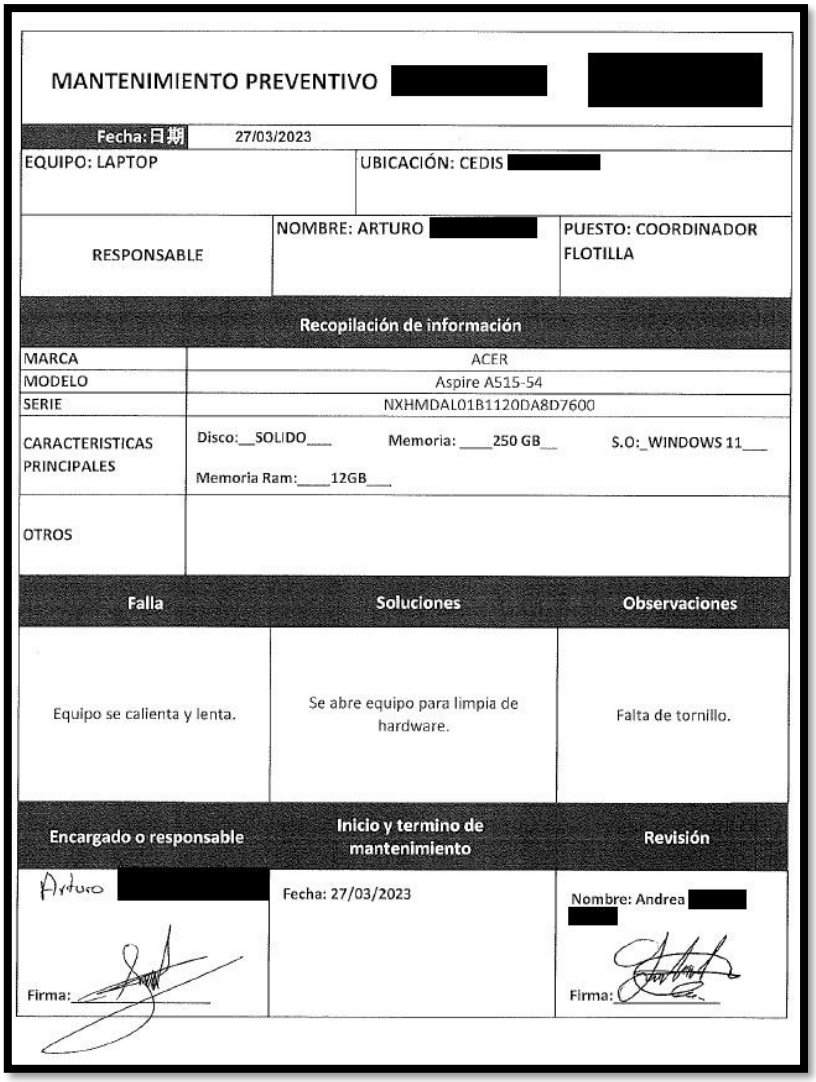
[redacted]
Nombre, Firma y No. Empleado del Instalador

NOTAS DE INSTALACIÓN

Imagen 93: Ejemplo de formato de entrega de servicio de internet de proveedor. Fuente: Autoría propia.

Mantenimiento preventivo.

El mantenimiento preventivo es el proceso que se realiza de manera anticipada con el fin de prevenir errores o averías en dispositivos y equipos electrónicos. Consta de realizar ajustes, limpieza, análisis, calibración y cambios de piezas. En la empresa hay con frecuencia los cambios de equipos laptop de usuario a usuario, de igual forma para poder mejorar un equipo es necesario la instalación de memorias RAM o SSD de buena calidad para poder tener un mejor rendimiento en los equipos. Siempre se debe anotar los cambios, un historial basta para no perder las anotaciones realizadas con anterioridad. Fue creado un formato para poder tener el consentimiento del usuario del mantenimiento realizado a su equipo asignado.



MANTENIMIENTO PREVENTIVO [redacted] [redacted]

Fecha: 日期 27/03/2023		
EQUIPO: LAPTOP	UBICACIÓN: CEDIS [redacted]	
RESPONSABLE	NOMBRE: ARTURO [redacted]	PUESTO: COORDINADOR FLOTILLA

Recopilación de información

MARCA	ACER
MODELO	Aspire A515-54
SERIE	NXHMDAL01B1120DA8D7600
CARACTERISTICAS PRINCIPALES	Disco:__SOLIDO___ Memoria: ____250 GB__ S.O:_WINDOWS 11___ Memoria Ram:____12GB___
OTROS	

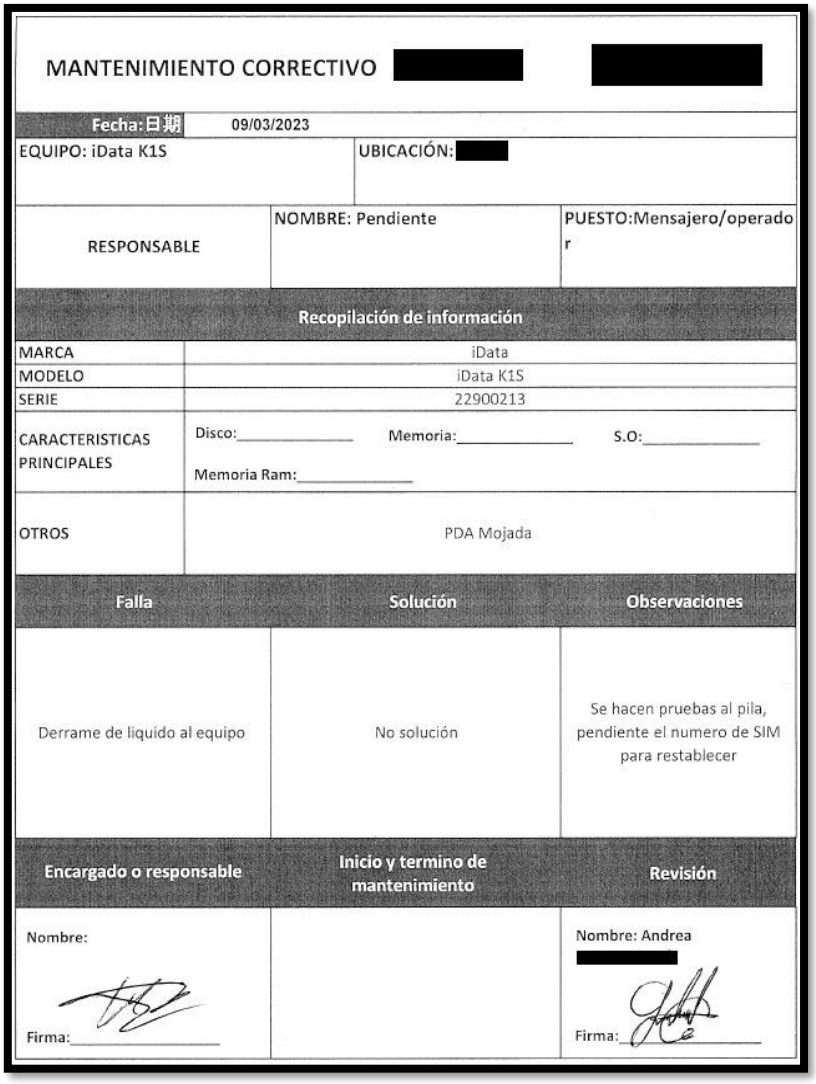
Falla	Soluciones	Observaciones
Equipo se calienta y lenta.	Se abre equipo para limpia de hardware.	Falta de tornillo.

Encargado o responsable	Inicio y termino de mantenimiento	Revisión
Arturo [redacted] Firma:	Fecha: 27/03/2023	Nombre: Andrea [redacted] Firma:

Imagen 94: Ejemplo de mantenimiento preventivo a usuario. Fuente: Autoría propia.

Mantenimiento Correctivo.

El mantenimiento correctivo, es aquel que busca reparar los errores, desperfectos o averías de los equipos y herramientas se puedan presentar, con tal de asegurar un funcionamiento estable. A diferencia del mantenimiento preventivo, en la empresa las desventajas son que algunos equipos no serán de mayor utilidad como antes, el tiempo y costo puede ser elevado debido a los reemplazos de piezas originales. De igual forma, fue creado un formato para poder tener el consentimiento del usuario del mantenimiento realizado a su equipo asignado.



MANTENIMIENTO CORRECTIVO [redacted] [redacted]

Fecha: 日期	09/03/2023	
EQUIPO: iData K1S	UBICACIÓN: [redacted]	
RESPONSABLE	NOMBRE: Pendiente	PUESTO:Mensajero/operador

Recopilación de información	
MARCA	iData
MODELO	iData K1S
SERIE	22900213
CARACTERISTICAS PRINCIPALES	Disco:_____ Memoria:_____ S.O:_____ Memoria Ram:_____
OTROS	PDA Mojada

Falla	Solución	Observaciones
Derrame de liquido al equipo	No solución	Se hacen pruebas al pila, pendiente el numero de SIM para restablecer

Encargado o responsable	Inicio y termino de mantenimiento	Revisión
Nombre: Firma:_____		Nombre: Andrea [redacted] Firma:_____

Imagen 95: Ejemplo de mantenimiento correctivo a usuario. Fuente: Autoría propia.

También fue importante las capacitaciones que se tomaron por la oficina central, la cual siempre nos daba un documento en donde se aplicaba la asistencia para la correcta aplicación laboral con los temas que se iban presentando. Un ejemplo de una capacitación con el tema de API (interfaz de programación de aplicaciones), el cuál era el manejo de un sistema básico para la comunicación de la aplicación del cliente con el sistema interno de la empresa.

Ciudad de México. 03/10/2023

CAPACITACIÓN API

Capacitación en temas de API, impartida por la especialista Lizbeth Marcial Nicolas de casa matriz HQ, el día 03/10/2023.

Temas por tratar:

- Errores comúnes
- Validaciones
- Procesos
- Simulaciones

A continuación, las personas presentes que acuden a la capacitación:

[redacted]

[redacted]

[redacted]

[redacted]

Imagen 96: Ejemplo de capacitación. Fuente: Autoría propia.

De igual forma es necesario compartir actividades mediante capacitaciones al personal de T.I. de nuevo ingreso, es importante el apartado compartido, debido a que estás actividades únicamente se pueden ejecutar por el área T.I.

[redacted]

CAPACITACIÓN T.I

Departamento T.I.

Curso	Objetivo	Fecha	Cumplimiento
Creación y soporte de correos para nuevos ingresos.	Cumplimiento en soporte.	Febrero 2023	Completado
Asignación, otorgación de permisos, y depuración de sistema JMS.	Cumplimiento en soporte.	Febrero 2023	Completado
Configuración y reinicio Scanner PDA.	Cumplimiento en soporte.	Marzo 2023	Completado
Configuración de equipos (usuario, administrador, local, host, activación de Office, instalación de impresora, escaner y red).	Cumplimiento en soporte.	Marzo 2023	Completado
Configuración de celulares de la organización.	Cumplimiento en soporte.	Marzo 2023	Completado
Manejo de protocólo TCP/IP.	Cumplimiento en soporte.	Marzo 2023	Completado
Realiza reportes de corte de fibra o daños al servicio de internet.	Cumplimiento en soporte.	Abril 2023	Completado
Mantenimiento correctivo y preventivo.	Cumplimiento en soporte.	Abril 2023	Completado
Configuración de NVR y DVR.	Cumplimiento en soporte.	Abril 2023	Completado
Configuración de las impresoras arrendadas.	Cumplimiento en soporte.	Mayo 2023	Completado
Reparacion de cámaras y otros dispositivos.	Cumplimiento en soporte.	Mayo 2023	Completado
Implementación y desarrollo de redes para corporativo, pdv y cedis.	Cumplimiento en soporte.	Junio 2023	Completado
Diagnósticos para solucionar problemas tecnológicos.	Cumplimiento en soporte.	Julio 2023	Completado
Soluciones de infrestructura y de tecnólogias con menor presupuesto y acorta tiempos.	Cumplimiento en soporte.	Julio 2023	Completado
Cableado estructurado para oficinas, pdv y cedis.	Cumplimiento en soporte.	Agosto 2023	Completado
Seguimiento con área de T.I. de todas las regiones y de China, capacitaciones de sistemas.	Cumplimiento en soporte.	Septiembre 2023	Completado
Soporte y Administración a equipos de computo, sistema operativo y organizacional (JMS y JMS VIP) para usuarios de oficinas, PDV y CEDIS.	Cumplimiento en soporte.	Septiembre 2023	Completado
Verificaciones de inventario a equipos de cómputo.	Cumplimiento en soporte.	Septiembre 2023	Completado
Mantenimientos preventivos y correctivos de equipos de cómputo.	Cumplimiento en soporte.	Octubre 2023	Completado
Configuración de red de dispositivo biométrico.			
Gestiona las altas de contratos de internet o dispositivos de red (firewall o switch), (entrega) validando la disponibilidad latencia y simetría.	Cumplimiento en soporte.	Octubre 2023	Completado
Implementación de herramientas para asistencia remota.	Cumplimiento en soporte.	Noviembre 2023	Completado
Implementación de procesos y política de área de T.I.	Cumplimiento en soporte.	Noviembre 2023	Completado
Configuracion de software, hardware de voz IP y análoga.	Cumplimiento en soporte.	Diciembre 2023	Completado
Garantizar el funcionamiento de redes mediante monitoreo.	Cumplimiento en soporte.	Diciembre 2023	Completado
Requerimientos para el área de T.I.	Cumplimiento en soporte.	Enero 2023	Completado

Supervisor T.I. Daniel [redacted]

Especialista T.I. Andrea [redacted]

Imagen 97: Ejemplo de capacitación a personal. Fuente: Autoría propia.

CAPÍTULO 4

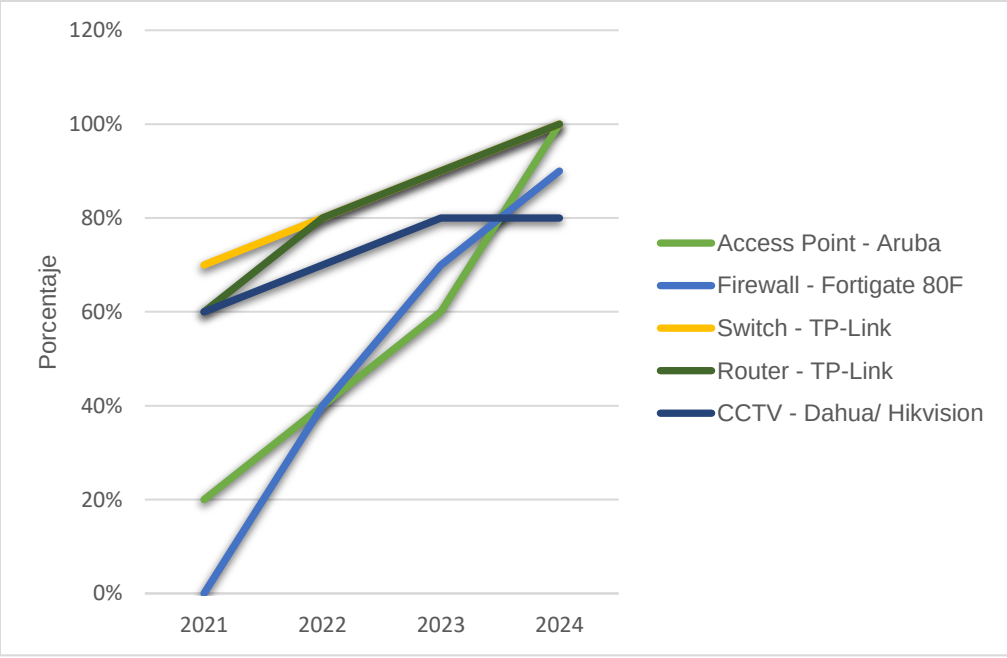
RESULTADOS

Hasta ahora, se han obtuvieron resultados favorables, como resultado de los procesos, medidas y tecnologías implementadas para la validación interna de la empresa, como tal cumpliendo el requisito solicitado de manera rápida con un costo menor. Llegando desde una idea en propuesta, resultando ser una muy buena.

Gráfica de resultados.

Conforme a los resultados del departamento T.I. Esta gráfica muestra cómo se ha ido avanzando anualmente y en porcentaje para resumir en medida los dispositivos proporcionados por el área de T.I. Se visualiza el porcentaje en poco tiempo, debido a la necesidad de la empresa en concretar dicho resultado para los puntos de venta, cedis y corporativo, sin embargo, se basa la información visual desde el arranque hasta la fecha actual usando los dispositivos Aruba, TP-Link, Fortigate 80F, Dahua y Hikvision compartiendo el avance de instalaciones y lo funcional que es comprar este tipo de dispositivos.

Tabla 4: Gráfica de resultados. Muestra en porcentaje el avance de dispositivos anualmente.

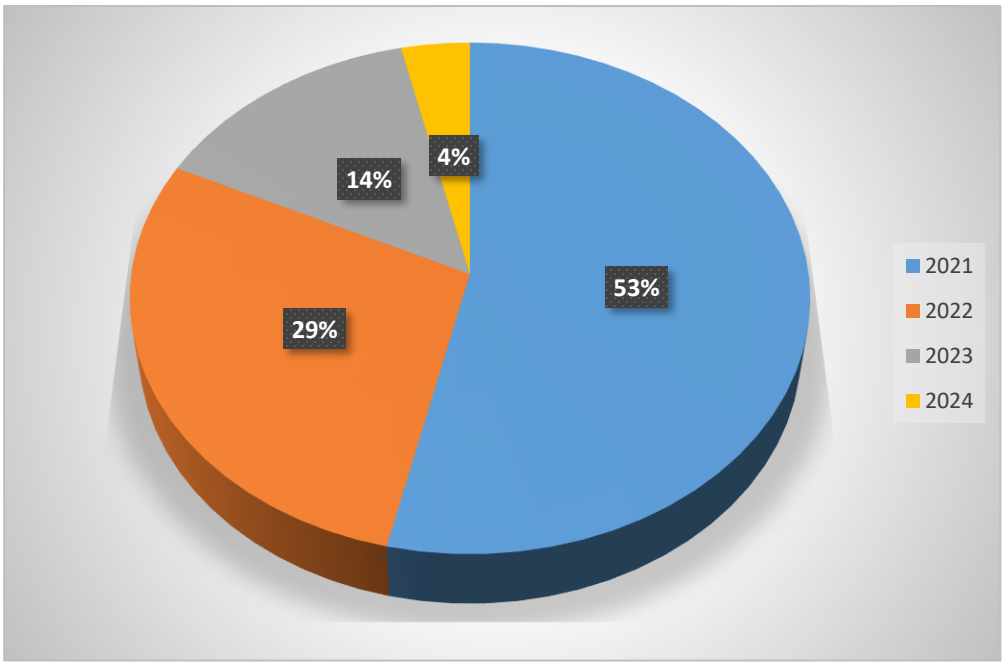


Gráfica de informe.

Se sabe que el porcentaje sirve para poder llevar a cabo la comparación entre cantidades, basados en las anotaciones y resultados conforme al avance en tiempo. La gráfica de informe anual se basa en la reducción de incidencias que se presentaron en su momento sin dispositivos de red y actualmente se presentan con los dispositivos proporcionados. Se visualiza de manera anual, debido a que a principios de comenzar con la propuesta no se tenían los dispositivos de red adecuados. Acorte a los tiempos ya realizados, fue importante continuar con la asignación por puntos, ya que, reiterando, la finalidad era apresurar la determinación de las funciones correctas en los dispositivos.

Es importante hacer énfasis en el hecho de que al momento de realizar el cálculo de los porcentajes se tiene que hacer dependiendo de las variables proporcionales de la información de las anotaciones internas del departamento T.I. Es por eso que la disminución de incidencias fue evidente año tras año en general.

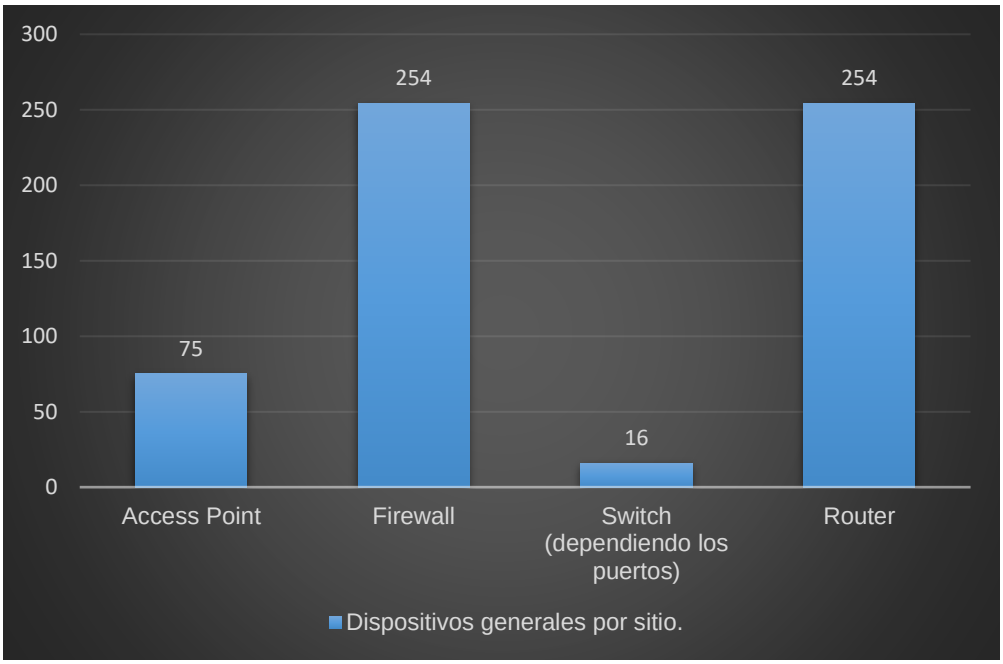
Tabla 5: Gráfica de informe. Muestra la reducción de incidencias anualmente.



Gráfica de dispositivos.

Esta gráfica se enfoca al número de dispositivos que se pueden conectar a la red dependiendo de la ONT del proveedor a los dispositivos proporcionados por el área de T.I. tales como el punto de acceso, Switch y Router los cuales tiene cierto límite por DHCP, después los que se pueden visualizar aproximadamente en varios sitios de la empresa.

Tabla 6: Gráfica de dispositivos. Muestra el número de usuarios que se pueden conectar a los dispositivos de red.



Cabe mencionar que el Router y Firewall nos permiten determinar cuántos dispositivos pueden ser conectados a la red asignada, a comparación del switch ya que están determinados por nodos y los puntos de acceso por el límite por tipo de dispositivo.

CONCLUSIONES

Los resultados obtenidos fueron favorables, ya que el departamento de T.I. y la empresa tuvieron la certeza y comprobación de ver como la forma solución de conectividad funciona favorablemente, así como la gestión de los dispositivos acatando los requerimientos que se demandaban. Así mismo el cumplimiento esencial de este trabajo fue a medida de su avance breve a través de aquel tiempo, actualmente se puede comentar que todos los procesos, elecciones, propuestas y control de lo que se ha instalado resulta para bien con la empresa, ya que se ha verificado cada dispositivo para un funcionamiento correcto y sin tanto problema para resolver en caso de errores.

Afortunadamente, se puede comentar que no se ha tenido ninguna baja de los dispositivos instalados en los sitios, de igual forma, no ha habido algún problema de software tanto en la aplicación como vía web. Anexando de manera específica que el aprendizaje laboral adquirido da respuesta a la situación de que es sumamente diferente al aprendizaje escolar, ya que este mismo antes mencionado da la experiencia aplicada al conocimiento escolar, lo que da un resultado favorable para el egresado, puesto que este tipo de propuestas enriquece un futuro y vida laboral exitoso, es muy satisfactorio poder desarrollar más habilidades de las que se obtienen en el ámbito escolar, ya que depende de cada individuo seguir proponiendo innovaciones mediante la tecnología que a la par avanza con el tiempo.

FUENTES DE INFORMACIÓN

1) Reyes, D. (2019a). Hipótesis y variables de estudio. Recuperado de: https://es.scribd.com/doc/17020400/Hipotesis-y-Variables-de-estudio

2) Pérez, J. y Gardey, A. (2016a). Configuración - Qué es, en la química, definición y concepto. Recuperado de: https://definicion.de/configuracion/

3) Diario del exportador. (2023a). El monitoreo y evaluación clave en la gestión de la empresa exportadora. Recuperado de: https://www.diariodelexportador.com/2017/08/el-monitoreo-y-evaluacion-clave-en-la.html

4) Laoyan, S. (2022a). Qué es la metodología waterfall y cuándo utilizarla. septiembre 29, 2022, de asana. Recuperado de: https://asana.com/es/resources/waterfall-project-management-methodology

5) Anzil, F. (2010a). Concepto de Control. Recuperado de web: https://www.zonaeconomica.com/control

6) Contreras, M. (2016a). Bases Teóricas. Recuperado de: http://educapuntes.blogspot.com/2011/04/bases-teoricas.html

7) Araujo, m. (2011a). Variables de estudio. Recuperado de: http://www.medwave.cl/link.cgi/Medwave/Series/mbe01/4933?ver=sindiseno

8) Sánchez, J. (2019a). Administración. Recuperado de: https://economipedia.com/definiciones/administracion-de-empresas.html

9) Incuatro. (2019a). Redes informáticas: Definición y elementos que las componen. Recuperado de: https://incuatro.com/redes-informaticas/

10) Muradas, Y. (2018a). Metodologías ágiles. Recuperado de: https://openwebinars.net/blog/conoce-las-3-metodologias-agiles-mas-usadas/

12) Questionpro. (2023a). Monitoreo de empleados en época de pandemia. Recuperado de: https://www.questionpro.com/blog/es/monitoreo-de-empleados/

13) Maldonado, D. (2018a). ¿Qué es Infraestructura de TI y cuáles son sus componentes? 2018 de icorp. Recuperado de: https://icorp.com.mx/blog/infraestructura-de-ti-componentes/

14) Última Reforma DOF (2023a). Código Penal Federal. Libro Segundo. Título Noveno - Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática. Capítulo II - Acceso Ilícito a Sistemas y Equipos de Informática. 2023 de Justia. Recuperado de: https://mexico.justia.com/federales/codigos/codigo-penal-federal/libro-segundo/titulo-noveno/capitulo-ii/

15) Gaceta del Senado. (2021a). Recuperado de: https://www.senado.gob.mx/65/gaceta_del_senado/documento/13967#:~:text=Art%C3%ADculo%20211%20bis%201.,cien%20a%20trescientos%20d%C3%ADas%20m

16) Global Suite Solutions. (2024a). Recuperado de: https://www.globalsuitesolutions.com/es/que-es-cobit/

17) Advisera. (2024a). Recuperado de: https://advisera.com/20000academy/es/que-es-itil/#:~:text=El%20marco%20de%20ITIL%20est%C3%A1,su%20propia%20publicaci%C3%B3n%20de%20apoyo.

18) Wikipedia. (2024a). Recuperado de: https://es.wikipedia.org/wiki/Multiplexaci%C3%B3n_por_divisi%C3%B3n_de_frecuencias_ortogonales.

ANEXOS

Glosario de términos.

1) Aruba: Es una subsidiaria de redes inalámbricas con sede en Santa Clara, California, de la compañía Hewlett Packard Enterprise.

2) Conector rj45: Son dispositivos modulares de interconexión emparejados con un cable que proporcionan comunicación de datos a diversos sistemas electrónicos. Contienen 8 contactos y 8 posiciones de cables utilizados para señales o alimentación, lo que significa que permiten 4 pares de cables trenzados.

3) Ethernet: Tecnología que permite que los dispositivos de redes de datos conectados por cable se comuniquen entre sí.

4) Infraestructura: Es el conjunto de componentes tecnológicos que soportan la operación y entrega de uno o varios servicios de TI, es decir, todo lo que está detrás de un servicio de TI. Y su objetivo es habilitar herramientas que soporten la operación de la organización y habiliten su competitividad.

5) Mbps: Megabits por segundo, es una unidad de medida para saber cuánta información viaja por Internet en un segundo.

6) IP: Protocolo de internet, como dice el nombre de un protocolo de comunicaciones a través de la red.

7) PoE: Es una tecnología para cable Ethernet LAN que permite que la corriente eléctrica necesaria para el funcionamiento de cada dispositivo sea transportada por los cables de datos en lugar de por los cables de alimentación.

8) Punto de acceso: Es un dispositivo de red que interconecta equipos de comunicación inalámbricos, para formar una red inalámbrica que interconecta dispositivos móviles o tarjetas de red inalámbricas.

Carta de validación laboral.

CIUDAD DE MÉXICO A 30 DE ABRIL DE 2024

A QUIEN CORRESPONDA:

PRESENTE

Por este medio hacemos constar que el/la C. **MENDOZA GONZALEZ DANIEL JOEL** laboró dentro de la empresa CONEJO CORRIENDO S. DE R.L. DE C.V., ocupando el Puesto SUPERVISOR IT durante el periodo del 04 DE OCTUBRE DE 2021 al 30 DE ABRIL DE 2024

Se extiende la presente a petición del interesado.

CONEJO CORRIENDO

Atentamente

Lic. Abraham Andrade Leon.
RECURSOS HUMANOS
abraham.andrade@jtexpress.mx
55-9225-3939 ext. 1012

Patriotismo 201 3-A, Col. San pedro de los Pinos, Del Benito Juárez, CP 03800

Imagen 98: Carta de validación laboral. Fuente: Autoría propia.

Carta de recursos humanos.

J&T EXPRESS

Ciudad de México, a 21 de Junio de 2023

Mtro. Rigoberto Salinas Cortes

Jefatura de división SIC TESCo

Presente:

Se extiende la presente constancia laboral a favor del **C. Daniel Joel Mendoza Gonzalez** con Registro Federal de Contribuyente (RFC) [redacted], con clave única de Registro de Población (CURP), [redacted] quien presta sus servicios, a la empresa CONEJO CORRIENDO S. DE RL. DE C.V. ocupando el puesto de Especialista de T.I. a partir de 04 de octubre de 2021 a la fecha ACTUAL, dando un tiempo de antigüedad de 1 año y 9 meses perteneciendo a la compañía.

Se podrá documentar el proyecto "Administración, configuración y monitoreo mediante Aruba para asegurar la conectividad de la empresa", para documentar sin presentar información sensible para la compañía, para procesos de titulación.

Descripción de responsabilidades:

- Telecomunicaciones (diseño, desarrollo de red y cableado estructurado).
- Instalación, configuración y administración de CCTV.
- Mantenimiento preventivo y correctivo en software y hardware.
- Gestión de redes y manejo de protocolos.
- Inventario y control de licencias Office 365.
- Instalación y configuración de teléfonos análogos y VoIP.
- Asignación de permisos, así como altas y bajas en sistema ERP.
- Creación y gestión de sistema de correos ERP.
- Garantizar el funcionamiento de redes mediante monitoreo con Puntos de acceso.
- Implementación de herramientas para asistencia remota.
- Diagnósticos para solucionar problemas tecnológicos.
- Configuración de dispositivos PDA.
- Configuración y gestión de impresoras de alta gama arrendadas.

Se expide la presente constancia para todos los fines que el interesado convenga.

ATENTAMENTE

Gerente de Recursos Humanos

CONEJO CORRIENDO

Av. Patriotismo 229 Torre 2, Piso 3. San Pedro de los Pinos, Benito Juárez, 03800, CDMX
www.jtexpress.mx

Imagen 99: Carta de recursos humanos. Fuente: Autoría propia.

Carta de jefe inmediato.

J&T EXPRESS

Ciudad de México, a 21 de Junio de 2023

Mtro. Rigoberto Salinas Cortes

Jefatura de división SIC TESCo

Presente:

Se extiende la presente constancia laboral a favor del C. **Daniel Joel Mendoza Gonzalez** con Registro Federal de Contribuyente (RFC) [redacted] quien presta sus servicios, a la empresa CONEJO CORRIENDO S. DE RL. DE C.V. ocupando el puesto de Especialista de T.I. a partir de 04 de octubre de 2021 a la fecha ACTUAL, dando un tiempo de antigüedad de 1 año y 9 meses perteneciendo a la compañía.

Se podrá documentar el proyecto "Administración, configuración y monitoreo de la infraestructura mediante Aruba para asegurar la conectividad de la empresa", para documentar sin presentar información sensible para la compañía, para procesos de titulación.

Descripción de actividades:

- Telecomunicaciones (diseño, desarrollo de red y cableado estructurado).
- Instalación, configuración y administración de CCTV.
- Mantenimiento preventivo y correctivo en software y hardware.
- Gestión de redes y manejo de protocolos.
- Inventario y control de licencias Office 365.
- Instalación y configuración de teléfonos análogos y VoIP.
- Asignación de permisos, así como altas y bajas en sistema ERP.
- Creación y gestión de sistema de correos ERP.
- Garantizar el funcionamiento de redes mediante monitoreo con Puntos de acceso.
- Implementación de herramientas para asistencia remota.
- Diagnósticos para solucionar problemas tecnológicos.
- Configuración de dispositivos PDA.
- Configuración y gestión de impresoras de alta gama arrendadas.

Se expide la presente constancia para todos los fines que el interesado convenga.

ATENTAMENTE

Gerente de T.I.

Luiggi Chek-Tong Martínez Wong

CONEJO CORRIENDO

Av. Patriotismo 229 Torre 2, Piso 3. San Pedro de los Pinos, Benito Juárez, 03800, CDMX

www.jtexpress.mx

Imagen 100: Carta de jefe inmediato. Fuente: Autoría propia.