

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

INMIGRACIÓN CON FIREWALL
FORTIGATE 200E A 40F PARA
ENVATEC S.A DE C.V

TITULACIÓN POR ESTANCIA.

QUE PARA OBTENER EL TÍTULO DE
INGENIERÍA EN SISTEMAS COMPUTACIONALES
CON LA ESPECIALIDAD
INGENIERÍA EN SOFTWARE.

PRESENTA:
ALMA ROSA MIRANDA JIMÉNEZ.

Coacalco de Berriozábal, Enero/ 2025

RESUMEN

En este documento se evidencia el proceso de implementación de un sistema integral de seguridad de red, conformado por softwares y herramientas, que son sincronizados para una mayor protección y estabilidad del despliegue. Inicialmente se describe el contexto actual de las soluciones de ciberseguridad en el entorno empresarial, posteriormente se establece el diseño de la topología de red tanto física como lógica, diseñada con equipos de la marca Fortinet, que en la actualidad es una empresa líder en la implementación de Firewalls. Más adelante se encuentra de manera detallada el proceso de implementación y despliegue, donde además se describen varios conceptos claves para entender el proceso llevado a cabo de estos servicios se adaptan desde esquemas de arquitectura tradicional de perímetro hasta configuraciones híbridas de múltiples usos, con el fin de satisfacer las particularidades y exigencias de su organización en este contexto tecnológico en constante evolución.

La relación con la empresa es la seguridad informática que debe abordar varios sistemas para proteger, debe ser eficaz a los clientes y empleados que lleva a cabo mediante la aplicación de la protección de los activos de la organización, como comunicaciones, datos, propiedad intelectual o redes utilizadas para transmitir o almacenar datos confidenciales y evitar que se produzcan accesos no autorizados. Los servicios integrales que han sido requeridos para abordar las necesidades en materia de ciberseguridad en distintas capas estos servicios se diseñan con el propósito de brindarle un nivel amplio de control sobre los recursos y activos informáticos de su organización, permitiéndole gestionar de manera más efectiva los riesgos inherentes a su actividad empresarial, es importante resaltar que una estrategia de ciberseguridad meticulosamente concebida, que se fundamente en los requerimientos específicos de su actividad empresarial y que se alinee con sus programas internos de tecnología de la información, puede aportar una significativa consolidación al valor global de la compañía.

CONTENIDO

CAPÍTULO I GENERALIDADES DEL PROYECTO	8
1. Introducción	9
1.1 Descripción de la empresa	10
1.2 Ubicación de Envatec S.A DE C.V	11
1.3 Organigrama.....	12
1.4 Sector productivo de la empresa.....	15
1.5 Misión	16
1.6 Visión.....	16
1.7 Política integral	16
1.8 Breve historia de la empresa	17
1.9 Descripción del puesto o área de trabajo	18
1.10 Justificación	19
1.11 Objetivo	20
1.12 Objetivos Específicos	20
1.13 Alcances y limitaciones	21
CAPÍTULO II MARCO TEÓRICO	22
2.1 Redes de área local LAN	23
2.1.1 Características de una LAN	23
2.1.2 VLAN.....	24
2.1.3 IPv4.....	25
2.1.4 IPv6.....	25
2.2 Redes VPN.....	25
2.2.1 Características y funcionamiento de una red VPN.....	26
2.2.2 Redes VPN privadas	26
2.3 Ciberseguridad.....	27
2.3.1 Áreas de ciberseguridad.	27
2.3.2 Medidas de seguridad en las redes LAN.....	29
2.3.3 IPSec	29
2.3.4 Firewall	30
2.3.5 Seguridad perimetral.....	30
2.3.6 Seguridad.....	30

2.3.7 Malwares	31
2.3.8 Hacking y suplantación de identidad	31
2.3.9 Secuestro de información	31
CAPÍTULO III DESARROLLO	32
3.1 Descripción del equipo	33
3.1.1 Seguridad:	33
3.1.2 Rendimiento	34
3.1.3 Certificación	34
3.1.4. Redes.....	35
3.1.5 Administración del equipo:.....	35
3.1.6 Características del equipo	36
3.1.7 Interfaces:.....	36
3.1.8 Características puntos de acceso a internet.....	37
3.2 Seguridad perimetral con FortiGate	37
3.2.1 FortiClient	38
3.2.2 FortiGuard + FortiMail	38
3.2.3 FortiManager + FortiAnalyzer	39
3.3 Metodología	39
3.4 SD-WAN.....	41
3.4.1 FortiGate Firewall.....	41
3.5 La arquitectura fortigate.....	42
3.5.1 Sistema operativo	42
3.5.2 Access point	42
CAPÍTULO IV RESULTADOS	44
4.1 CONCLUSIONES	59
4.2 COMPETENCIAS DESARROLLADAS	60
4.3 FUENTES DE INFORMACIÓN.....	61

ÍNDICE FIGURAS

Figura 1.	Mapa dónde se encuentra ubicado a empresa ENVATEC S.A de C.V	11
Figura 2.	Organigrama general de la empresa.	12
Figura 3.	Organigrama general de la empresa	13
Figura 4.	Organigrama administrativo de las áreas que forman parte de la empresa	14
Figura 5.	Red de área local LAN	23
Figura 6.	Red VLAN	24
Figura 7.	Red privada virtual (VPN)	27
Figura 8.	Firewall Fortinet Fortigate 40F.....	33
Figura 9.	Diagrama de administración de equipos fortigate	36
Figura 10.	Fortigate Fortiwifi 40F Series Hardware.	36
Figura 11.	Punto de acceso a internet.	37
Figura 12.	Ambiente de red corporativa con seguridad basada en Fortinet.	38
Figura 13.	Para el desarrollo del trabajo se siguió la metodología definida	39
Figura 14.	Se muestra cada una de las fases estipuladas que se desarrollaron en las etapas de las actividades relacionadas a la metodología	40
Figura 15.	Topología lógica de red.....	40
Figura 16.	Configuración de IP para el puerto 1.	45
Figura 17.	Interfaz para iniciar sesión.	45
Figura 18.	Interfaz principal.....	45
Figura 19.	Comando para la copia de seguridad.	46
Figura 20.	Reinicio del sistema.	46
Figura 21.	Usuarios y dispositivos.	47
Figura 22.	Políticas del Firewall.	47
Figura 23.	Políticas de salida a internet.	47
Figura 24.	Interfaces.	48
Figura 25.	Interfaz de salida a internet.	48
Figura 26.	Interfaz de red local.	49
Figura 27.	Creación de SSID.	49
Figura 28.	Direcciones.....	49
Figura 29.	Configuración DNS.	50
Figura 30.	Política local.....	50

Figura 31.	Servicios.	51
Figura 32.	IPs virtual.	51
Figura 33.	Firmas de aplicaciones.	52
Figura 34.	Firmas IPs.....	52
Figura 35.	Asistente de IPSec.	52
Figura 36.	Plantilla de túnel Isec.	53
Figura 37.	Usuarios definidos	53
Figura 38.	Grupos de usuarios.....	53
Figura 39.	Configuración en el sistema.	54
Figura 40.	Topología física.	54
Figura 41.	Calificación de seguridad.....	54
Figura 42.	Conectores de tela.....	55
Figura 43.	Centro de identidad de activos.....	55
Figura 44.	Tráfico directo.	56
Figura 45.	Eventos del sistema.....	56
Figura 46.	Eventos del sistema.....	56
Figura 47.	Switches de acceso.....	57
Figura 48.	FortiSwitch Conexión lógica.....	57
Figura 49.	Puntos de acceso inalámbrico.....	57
Figura 50.	Firewall Fortigate Conexión física antes.....	58
Figura 51.	Fortigate Conexión física después	58

ÍNDICE TABLAS

Tabla 1.	Descripción de los puntos de acceso a internet	37
----------	--	----

CAPÍTULO I GENERALIDADES DEL PROYECTO

1. Introducción

La presente documentación se refiere a la implementación que se va adquiriendo una importancia creciente con el aumento del uso de activos digitales y servicios en la red local, internet y la nube. Es muy sencillo para un usuario experto acceder de forma no autorizada a datos de carácter confidencial que toda organización por lo que se debe invertir en la implementación de procesos y tecnologías en áreas de fortalecer la seguridad informática, o lo que es hoy en día conocido como ciberseguridad estas deben disponer de información continua y confiable en el tiempo que constituye una ventaja fundamental que se puede definir a la detección oportuna de fallas y el monitoreo de los elementos que conforman una red de cómputo.

El trabajo está dividido en cuatro capítulos;

El primer capítulo describe a la empresa de ENVATEC S.A de C.V junto a su misión y visión, describe el puesto desempeñado; además de contener la problemática, justificación, los objetivos a desarrollar, descripción del puesto y la importancia que tiene para resolver

En el segundo se presenta el marco teórico que contiene el encuadre teórico, así como definiciones de varias fuentes de información donde se facilitara al lector comprender los conceptos que se van a presentar durante el proyecto.

En el tercer capítulo se presenta el desarrollo y metodología del proyecto donde brinda la descripción de los procesos de implementación, y las propuestas y acciones de solución a la problemática.

El último capítulo presenta los resultados obtenidos mediante las mejoras implementadas.

1.1 Descripción de la empresa

ENVATEC es una empresa en el ámbito de envasado en aerosoles y líquidos, siendo líder en el ramo y estando especializada en maquila de productos ya mencionados, teniendo más de 20 años de experiencia en diferentes sectores que van desde el cuidado personal, hogar, veterinaria, industriales, insecticidas, electrónicos, dispositivos médicos, cosméticos, entre otros; adaptándose a diferentes especificaciones de los clientes interviniendo en los procesos integrales que van desde la recepción de materia primas, hasta el producto final que consistió en la elaboración de una formula y concluyó en el envasado, esto teniendo un impacto positivo en costos para cada cliente. ENVATEC se mantiene en constante actualización como son las nuevas tecnologías y en el cumplimiento de las normas de seguridad e higiene, para dar así un producto de calidad, por ende, esto incluye la pertinente capacitación del personal. (ENVATEC, 2023)

Planta Allende.

Planta Sabino.

Figura 1. Mapa dónde se encuentra ubicado a empresa ENVATEC S.A de C.V
(Google.com/maps, 2023)

1.3 Organigrama

En las siguientes imágenes se muestran los organigramas de la empresa ENVATEC S.A de C.V.

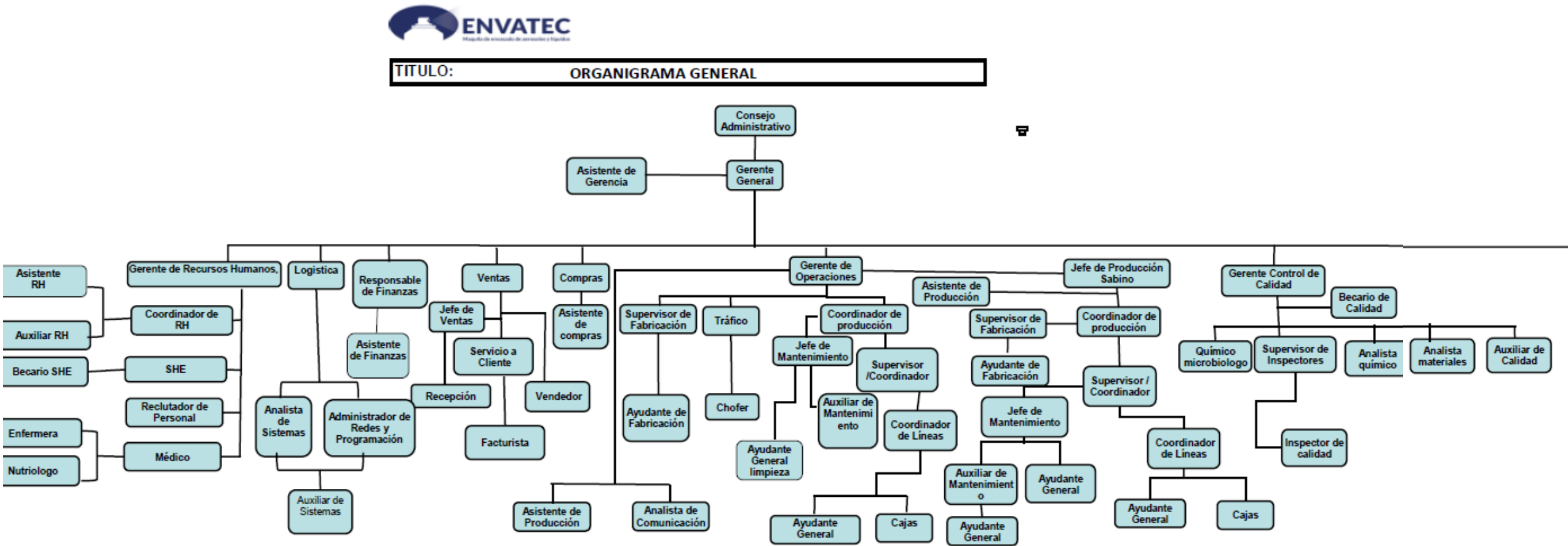


Figura 2. Organigrama general de la empresa. (ENVATEC, 2023)

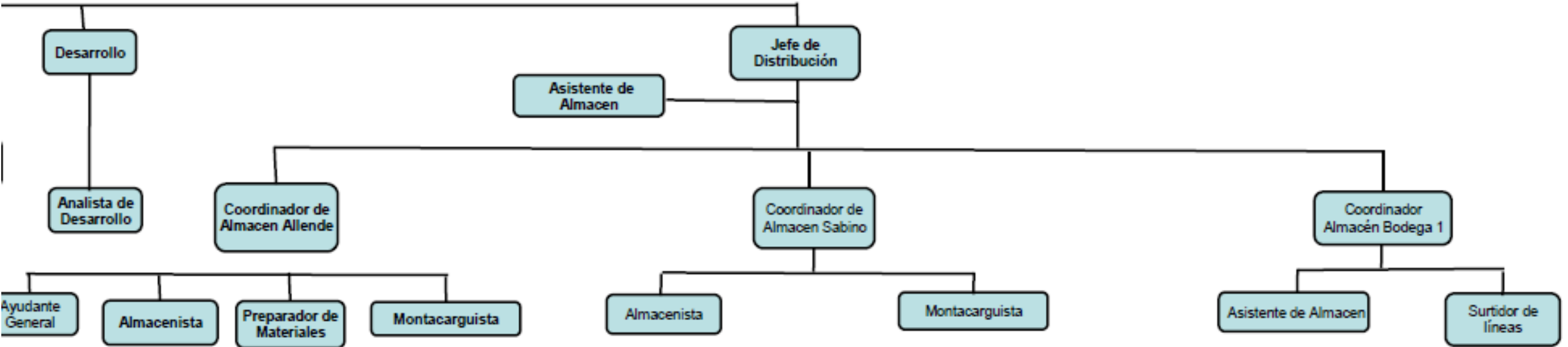


Figura 3. Organigrama general de la empresa. (ENVATEC, 2023)

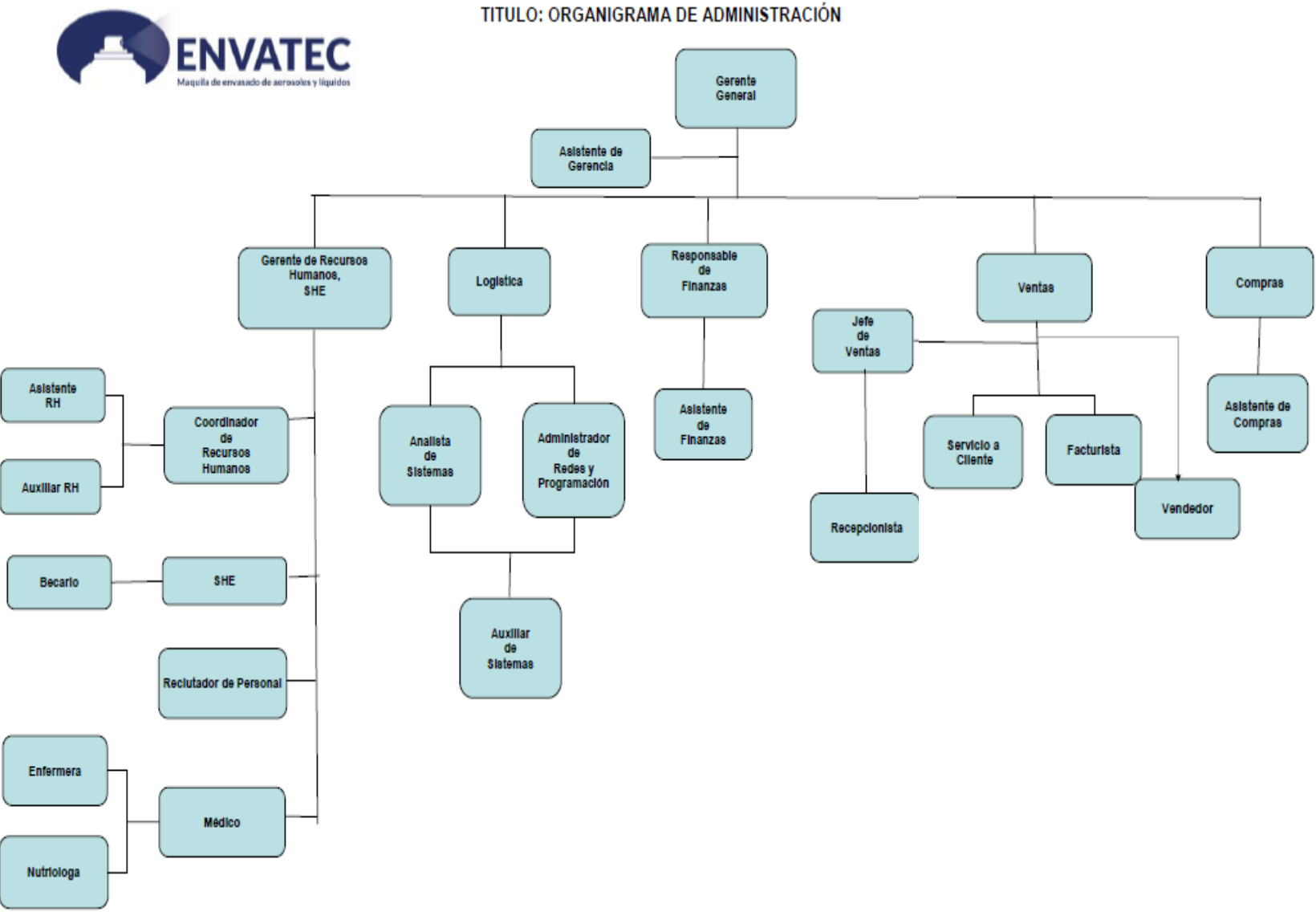


Figura 4. Organigrama administrativo de las áreas que forman parte de la empresa. (ENVATEC, 2023)

1.4 Sector productivo de la empresa

La empresa de ENVATEC S.A de C.V el sector productivo es la Maquila en envasado de aerosoles y líquidos. (ENVATEC, 2023)

1.5 Misión

Proporcionar a los clientes el mejor servicio de envasado y desarrollo de aerosoles y líquidos. (ENVATEC, 2023)

1.6 Visión

Ser una empresa globalmente competitiva y sustentable en el desarrollo y envasado de aerosoles y líquidos. (ENVATEC, 2023)

1.7 Política integral

Los asociados de ENVATEC S.A de C.V, se comprometen a proporcionar el mejor servicio, calidad y versatilidad en el desarrollo y envasado de aerosoles y líquidos, cumpliendo así con los requisitos legales y de nuestros clientes a través de la mejora continua de nuestros procesos para ENVATEC. (ENVATEC, 2023)

- La satisfacción y Lealtad de los clientes.
- El desarrollo y satisfacción de nuestros asociados.
- La seguridad y salud ocupacional en nuestros procesos.
- Prevención de la contaminación ambiental
- Productividad y rentabilidad de nuestra empresa.
- Fomentar un entorno organizacional favorable considerando los factores de riesgo psicosocial.

1.8 Breve historia de la empresa

ENVATEC S.A. de C.V, es una empresa 100% mexicana, que desde 1998 brida el servicio de maquila y envasado en aerosoles, líquidos y tubos depresibles, todos los años de experiencia han logrado que ENVATEC haya incrementado en tamaño, esto habla bien del trabajo que se ha realizado. Como bien se menciona, esta organización a través de 20 años ha logrado mantenerse al día con experiencia, equipo tecnológico y humano que se encuentra en la disposición de atender dudas y ofrecer soluciones que agreguen valor a diversos negocios.

ENVATEC a lo largo de su experiencia y buenas prácticas de manufactura ha crecido empezando así con planta Allende que consta con una plantilla en su mayoría, mujeres, quienes cuales se trabajan variedades de productos y se cuentan con varias líneas de trabajo especializadas para los productos a trabajar. La continuidad de planta Sabino, que fue fundada hace 10 años atrás y la cual cuenta con la especialización en envasadoras de la misma calidad, pero abriendo las puertas a nueva tecnología de envasado. (ENVATEC, 2023)

1.9 Descripción del puesto o área de trabajo

Las funciones principales del área Analista de Sistemas en la empresa ENVATEC S.A de C.V está a cargo del jefe de área Eduardo Arcaraz supervisando las siguientes actividades (ENVATEC, 2023):

- Instalar y mantener las redes LAN, WAN.
- Segmentos de red y operaciones tanto de internet como intranet.
- Instalar y mantener varias aplicaciones incluyendo hardware y software.
- Modificar el rendimiento de los sistemas de red cuanto sea necesario.
- Supervisar la efectividad de la red.
- Mantener medidas de seguridad eficaces.
- Supervisar las posibles actualizaciones, migraciones y reparaciones para mejorar el funcionamiento del sistema.
- Trabajar con una serie de dispositivos, como servidores, equipos de sobremesa y portátiles, enrutadores, impresoras, teléfonos móviles y Tablet
- Configuración de router.
- Actualización de servidores de datos.

1.10 Justificación

Uno de los requerimientos prioritarios de toda organización, es el manejo y salvaguarda de la información, buscando acelerar tareas de procesamiento para mantener segura sus redes corporativas, por otra parte, necesitan el respaldo de un esquema riguroso al diagnóstico que se debe de hacer para conocer las posibles vulnerabilidades en los datos y servicios.

En este panorama, Fortinet se consolida como la principal solución innovadora de alto desempeño para la seguridad de redes orientada a resolver problemas fundamentales que surgen en los entornos de redes de uso intensivo de ancho de banda donde las amenazas informáticas son cada vez más sofisticadas.

1.11 Objetivo

Implementar controles de seguridad a los activos y la implementación de Firewall Fortigate40F.

1.12 Objetivos Específicos

- Conocer la herramienta que puede ayudar en los procesos de control en las compañías y así mitigar riesgos de seguridad.
- Fomentar la cooperación contra el delito cibernético a través de asociaciones.
- Eliminar la escasez de habilidades de ciberseguridad global
- Investigar los antecedentes que conllevan al desarrollo.

1.13 Alcances y limitaciones

Es relevante destacar que, a pesar de que el nuevo Fortigate 40F cuenta con recursos más limitados en comparación con el Fortigate 200E, satisface plenamente las necesidades de la empresa que afirmar que el Fortigate 200E estaba sobredimensionado para las operaciones. Sin embargo, debido a la configuración específica de uso de diferentes puertos en el Fortigate 200E, fue necesario realizar ciertas adaptaciones en el nuevo Fortigate 40F para asegurar que todas las necesidades operativas fueran atendidas de manera eficiente.

CAPÍTULO II MARCO TEÓRICO

En este capítulo se pretende hacer referencia al marco teórico, donde se recopilan definiciones de diferentes autores que permitirán al lector familiarizarse de algunos conceptos básicos orientando el estudio, deben estar relacionados con el tema.

2.1 Redes de área local LAN

Es una red de área local cuyo alcance se restringe a un radio de unos cuantos cientos metros que normalmente cubre el espacio ocupado por una empresa. Una red LAN es de broadcast, es decir el mensaje que emite una computadora llega a todas las otras computadoras que contribuyen la red; pero solo la que reconoce la dirección destino del mensaje como su dirección copia el mensaje. La red local incluye un servidor en el cual reside el sistema operativo que es el software que permite administrar los recursos de la red como son procesador, memoria, discos, impresoras e información (Sosa, R, 2006).

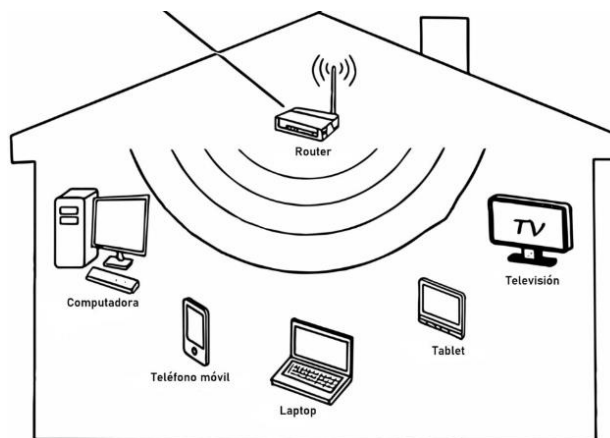


Figura 5. Red de área local LAN (Sosa, R, 2006).

2.1.1 Características de una LAN

Estas redes tienen una serie de características que las diferencian de otras; a continuación, se detallan algunas de las principales (Sosa, R, 2006):

- **Tamaño limitado:** Las redes LAN cubren un área geográfica limitada, generalmente dentro de un edificio o campus.

- Conectividad de alta velocidad: Las redes LAN ofrecen una alta velocidad de transferencia de datos entre dispositivos.
- Topología de red cableada: Las redes LAN utilizan cables para conectar dispositivos, generalmente mediante tecnología como ethernet o wifi.
- Propiedad privada: Las redes LAN son propiedad de una organización o individuo específico y se utilizan para conectar dispositivos dentro de esa organización o ubicación.
- Seguridad controlada: Las redes LAN son seguras y privadas, lo que significa que los usuarios extraños no autorizados no pueden acceder a la red sin autorización.
- Administración centralizada: Las redes LAN suelen estar administradas centralmente por un equipo de TI o administrador de red.
- Protocolos estándar: Las redes LAN utilizan protocolos de red estándar, como TCP/IP, para facilitar la comunicación entre dispositivos.

2.1.2 VLAN

Es una red virtual que se instala en una red local switchheada tomando como base el número de puertos switch al cual se conecta la computadora, la dirección física o MAC de la tarjeta de la PC o la dirección IP de la computadora.

El concepto de red virtual permite que se construya una red con computadoras que pertenecen a redes físicas distintas, con lo cual se puede crear un conjunto de PC que usen el protocolo IP, otro con computadoras que empleen IPX, otro con las PC de los funcionarios de la empresa. (Fernando Andrew, I. P, 2006)

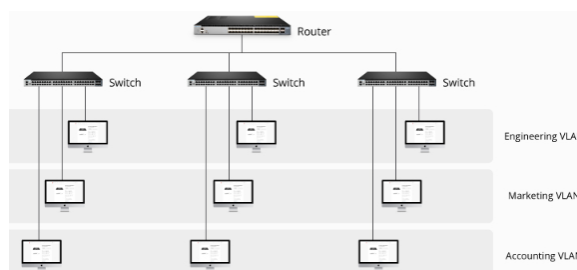


Figura 6. Red VLAN (Fernando Andrew, I. P, 2006)

2.1.3 IPv4

IPv4 (Internet Protocol versión 4) es el formato de dirección estándar que permite que todas las máquinas en Internet se comuniquen entre sí. IPv4 se escribe como una cadena de dígitos de 32 bits y una dirección IPv4 se compone de cuatro números entre 0 y 255, separados por puntos. Estandariza la forma en que los ordenadores se comunican entre sí en Internet. Es un protocolo sin conexión, lo cual significa que los datos se pueden enviar sin que las partes inviertan tiempo en establecer una conexión directa, y solo requiere pequeñas cantidades de memoria. (Tanenbaum, A. S, 2003)

2.1.4 IPv6

IPv6 (Internet Protocol versión 6) es un estándar actualizado para identificar ordenadores en Internet. Al igual que IPv4, proporciona un identificador único a cada dispositivo, pero uno que se ha ajustado para adaptarse al creciente número de ordenadores conectados a Internet en la actualidad. IPv6 agiliza las transferencias de datos al hacer que dos direcciones sean directamente accesibles entre sí nuevamente. IPv4 tuvo que introducir pasos adicionales para compensar la relativa falta de direcciones únicas. (Fernando Velez Verela, L. G, 2016)

2.2 Redes VPN

Un servicio VPN encriptará tu tráfico antes de que llegue a Internet. Esto evitará que los piratas informáticos, las agencias gubernamentales y las empresas puedan ver lo que estás haciendo en Internet. Una vez encriptado, nadie podrá ver tus datos. Una VPN es una buena opción si necesitas la experiencia de navegación más segura posible. No obstante, siempre debe leer los términos y condiciones de cualquier VPN que estés considerando antes de usarlo. Debido a que, el tráfico de su red virtual está encriptado, el proveedor de servicios de Internet no puede ver o analizar los datos que envía o recibe en línea. Esta característica es especialmente beneficiosa para los empleados con planes de datos. (Evelio Martinez Martinez, A. S, 2012)

2.2.1 Características y funcionamiento de una red VPN

Una conexión VPN disfraza sus datos en línea y los protege del acceso externo. Cualquiera que tenga acceso a la red y quiera hacerlo puede ver los datos no cifrados. Con una VPN, los hackers y los cibercriminales no pueden descifrar estos datos a continuación se presentarán algunas de las características (Evelio Martinez Martinez, A, S, 2012):

- Cifrado seguro: Para leer los datos, necesita una clave de cifrado. Sin ella, le llevaría millones de años a una computadora descifrar el código en caso de un ataque de fuerza bruta. Con la ayuda de una VPN, sus actividades en línea se ocultan incluso en redes públicas.
- Disfrazar su paradero: Los servidores de VPN principalmente actúan como sus servidores proxy en internet.
- Acceso a contenido regional: El contenido web regional no siempre es accesible desde cualquier parte.
- Transferencia segura de datos: Si trabaja de forma remota, puede necesitar acceder a archivos importantes en la red de su empresa.

2.2.2 Redes VPN privadas

Una VPN (Virtual Private Network) permite a sus usuarios enviar y recibir datos como si sus dispositivos estuvieran conectados a la red privada, incluso si no lo están. De esta forma, a través de una conexión virtual, los usuarios pueden acceder a una red privada de forma remota. Así, una red de tipo VPN te permite crear una red local sin que todos los integrantes de esta estén conectados entre ellos. Además, este tipo de conexión de red permite que se pueda acceder a puntos de Internet que no serían accesibles desde nuestra propia conexión. (Evelio Martinez Martinez, A, S, 2012)

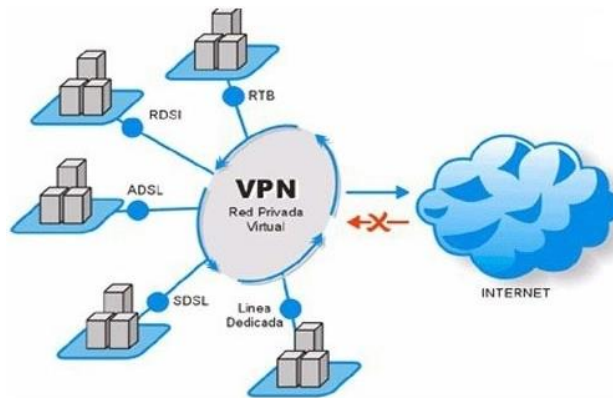


Figura 7. Red privada virtual (VPN). (Evelio Martinez Martinez, A, S, 2012)

2.3 Ciberseguridad

La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; Extorsionar a los usuarios o los usuarios o interrumpir la continuidad del negocio.

Actualmente, la implementación de medidas de seguridad digital se debe a que hay más dispositivos conectados que personas, y los atacantes son cada vez más creativos. (Be a Cyber Defender With Cybersecurity Courses Networking Academy, 2022)

2.3.1 Áreas de ciberseguridad.

Las instituciones bancarias y financieras, personas famosas y gobiernos, son los principales blancos de los ataques cibernéticos. Existen distintas acciones para prevenirlos, para solucionar sus efectos negativos e, incluso, para averiguar quién es y dónde se localiza el autor. Al ser un campo bastante complejo, existen distintas ramas de la ciberseguridad (María Ángeles Caballero Velasco, Laura Baus Lerma, Diego Cilleros Serrano, 2023):

- Ciberseguridad de la infraestructura crítica: La infraestructura crítica hace referencia a sistemas digitales importantes para la sociedad, como la energía, la comunicación y el transporte. Las organizaciones requieren, en estas áreas, un enfoque sistemático de ciberseguridad debido a que la interrupción o la pérdida de datos pueden desestabilizar la sociedad.
- Seguridad de la red: La seguridad de la red es una protección de ciberseguridad para los equipos y dispositivos conectados a una red. Los equipos de TI utilizan las tecnologías de seguridad de red, como los firewalls y el control de acceso a la red para regular el acceso de usuarios y administrar los permisos para recursos digitales específicos.
- Seguridad en la nube: La seguridad en la nube describe las medidas que toma una organización para proteger los datos y las aplicaciones que se ejecutan en la nube. Es importante para reforzar la confianza del cliente, proteger las operaciones tolerantes a errores y cumplir con la normativa de la privacidad de datos en un entorno escalable.
- Seguridad de IoT: El término Internet de las cosas (IoT) hace referencia a dispositivos electrónicos que funcionan remotamente en Internet. Por ejemplo, una alarma inteligente que envía actualizaciones periódicas al smartphone podría considerarse un dispositivo IoT.
- Seguridad de los datos: La seguridad de los datos protege los datos en tránsito y en reposo con un sistema sólido de almacenamiento y una transferencia de datos segura. Los desarrolladores usan medidas protectoras, como el cifrado y las copias de seguridad aisladas, para la resistencia operativa frente a posibles brechas de datos.
- Seguridad de las aplicaciones: La seguridad de las aplicaciones es un trabajo coordinado para fortalecer la protección de una aplicación frente a la manipulación no autorizada durante las etapas de diseño, desarrollo y prueba.
- Seguridad de los puntos de conexión: La seguridad de los puntos de conexión aborda los riesgos de seguridad que surgen cuando los usuarios acceden remotamente a la red de una organización.

2.3.2 Medidas de seguridad en las redes LAN

Las medidas de seguridad en una red LAN competen a las grandes y pequeñas empresas por igual: todas necesitan conocer los niveles y políticas de seguridad en redes LAN para evitar ataques de intrusos a continuación se presentan las medidas de seguridad (Sosa, R, 2006):

- Seguridad de red física: Mantener actualizado el hardware, incluido servidores y enrutadores.
- Contraseñas: Con respecto a las contraseñas, se pueden tomar en cuenta los siguientes aspectos a la hora de establecer una para el acceso a la red, y también para la configuración de aplicaciones en la nube o de almacenamiento:
- Autenticación: Consiste en verificar los usuarios que ingresan a la red y corroborar que sean quienes dicen ser. El método de verificación más frecuente es el nombre de usuario y contraseña, pero se pueden usar controles de seguridad biométrica también (como la huella digital) para protección adicional.
- Soluciones de software y hardware: Además de las medidas anteriores, en la seguridad de una red LAN pueden emplearse software y hardware para mitigar ataques, por ejemplo: programas de cifrado y protección de datos o hardware que permitan el reconocimiento de usuarios para impedir intrusiones.
- Control de acceso seguro: Manejando un control de acceso, se puede saber quién está usando una red y permitir o negar el ingreso a usuarios específicos.

2.3.3 IPSec

IPSec (Internet Protocol Security) es un conjunto de protocolos de seguridad en internet diseñado para proteger los paquetes de datos enviados a través de una red IP. IPSec emplea la encriptación para garantizar la privacidad de los datos enviados y para verificar que solo son leídos por sus legítimos destinatarios, impidiendo su acceso a terceros. IPSec es uno de los protocolos preferidos para proteger los datos enviados por internet gracias a que cuenta con varias ventajas frente a otros protocolos. (Gerardus, 2019).

2.3.4 Firewall

Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad. Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet. (Anatomía de un ataque, 2024)

2.3.5 Seguridad perimetral

Es el proceso mediante el cual se asegura el perímetro de una red a través de la implementación de una combinación de software, dispositivos y técnicas.

Algunas estrategias o directrices utilizadas dentro de la seguridad del perímetro informático pueden incluir la vigilancia pasiva o activa, la detección de amenazas y el análisis de patrones. Por supuesto, existen también una serie de herramientas utilizadas para reforzar la seguridad de la red que detallaremos más adelante. (Evelio Martinez Martinez, A, S, 2012)

2.3.6 Seguridad

La defensa en profundidad es una estrategia de seguridad cibernética que utiliza una serie de medidas defensivas redundantes en capas para proteger los datos confidenciales, la información de identificación personal y los activos de tecnología de la información. Si falla un control de seguridad, la siguiente capa de seguridad frustra el posible ataque cibernético.

Este enfoque de varias capas reduce la amenaza cibernética de que una explotación de vulnerabilidad en particular tenga éxito, mejorando la seguridad del sistema en su conjunto y reduciendo en gran medida el riesgo de seguridad cibernética. (Evelio Martinez Martinez, A, S, 2012)

2.3.7 Malwares

El Malware es un tipo de software diseñado para obtener acceso no autorizado o causar daños en una computadora. Malware es un término que abarca cualquier tipo de software malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable. Los delincuentes cibernéticos generalmente lo usan para extraer datos que pueden utilizar como chantaje hacia las víctimas para obtener ganancias financieras. Dichos datos pueden variar desde datos financieros, hasta registros de atención médica, correos electrónicos personales y contraseñas. La variedad de información que puede verse comprometida se ha vuelto ilimitada. (Be a Cyber Defender With Cybersecurity Courses Networking Academy, 2022)

2.3.8 Hacking y suplantación de identidad

La suplantación de identidad (phishing) es la práctica de enviar correos electrónicos fraudulentos que se asemejan a correos electrónicos de fuentes de buena reputación. El objetivo es robar datos sensibles, como números de tarjetas de crédito e información de inicio de sesión. Es el tipo más común de ciberataque. Puede protegerse mediante la educación o una solución tecnológica que filtre los correos electrónicos maliciosos. (Be a Cyber Defender With Cybersecurity Courses Networking Academy, 2022)

2.3.9 Secuestro de información

Ransomware nos referimos específicamente al secuestro de datos, pero para que lo entiendas mejor, aquí te lo explicamos fácilmente.

El Ransomware es un tipo de software malicioso, o lo que se conoce como malware, que ha sido creado para acceder al sistema de un usuario y bloquear el acceso a su propia información y archivos personales. Esto se hace con el objetivo de exigir el pago de un rescate para liberar la información. (Be a Cyber Defender With Cybersecurity Courses Networking Academy, 2022)

CAPÍTULO III DESARROLLO

Este capítulo se describen los lineamientos metodológicos empleados para realizar el proyecto, referidos al tipo y diseño de investigación, instrumentos de recolección de la información, fases de la metodología aplicada y lo que va a contener el capítulo 3.

3.1 Descripción del equipo

La gama FortiGate 40F introduce una propuesta de vanguardia al amalgamar la funcionalidad inherente a un SD-WAN con un cortafuegos de última generación, desplegando una eficiencia operativa ágil y garantizando una salvaguardia sólida. Su configuración física de reducidas dimensiones y exenta de sistemas de ventilación ha sido meticulosamente diseñada con el propósito de atender las demandas de sucursales empresariales y empresas de tamaño mediano, al conferir una presencia eficaz y de baja visibilidad en estos contextos operacionales. (Dr. Hidaia Mahmood Mohamed Alassouli, 2024)

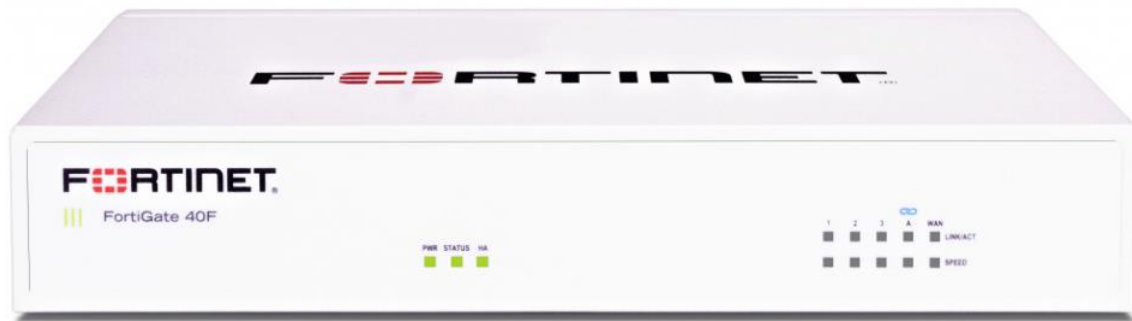


Figura 8. Firewall Fortinet Fortigate 40F. (Dr. Hidaia Mahmood Mohamed Alassouli,2024)

El Fortinet FortiGate 40F se distingue por una serie de características que convergen para ofrecer una solución integral en materia de seguridad, rendimiento, certificación, gestión de redes y administración del equipo.

3.1.1 Seguridad:

A continuación, se detallan algunas prevenciones de seguridad que cuenta el fortigate (Dr. Hidaia Mahmood Mohamed Alassouli, 2024):

- Prevención de amenazas avanzada: El FortiGate 40F emplea tecnologías de inspección profunda de paquetes y análisis de comportamiento para detectar y mitigar amenazas cibernéticas, incluyendo malware, ataques de día cero.
- Protección contra intrusiones: Ofrece una capa de seguridad adicional mediante la detección y prevención de intentos de intrusión y ataques dirigidos.
- VPN segura: Permite la creación de túneles VPN cifrados para conexiones seguras entre sucursales y trabajadores remotos, garantizando la confidencialidad de la comunicación.
- Filtrado de contenido: Facilita el control del acceso a Internet y la aplicación de políticas de uso mediante la inspección y filtrado de contenido web

3.1.2 Rendimiento

Se muestran dos tipos de rendimientos del hardware (Dr. Hidaia Mahmood Mohamed Alassouli, 2024):

- Procesamiento en hardware: Gracias a su diseño basado en aceleración de hardware, el FortiGate 40F logra un procesamiento eficiente de los datos sin sacrificar el rendimiento, incluso en entornos de tráfico intensivo.
- SD-WAN dinámico: Optimiza el uso de múltiples conexiones de Internet al dirigir el tráfico de manera inteligente, mejorando la eficiencia y reduciendo la latencia.

3.1.3 Certificación

Las certificaciones de seguridad del FortiGate 40F cumple con normativas y estándares de seguridad reconocidos a nivel internacional, lo que garantiza su confiabilidad y su capacidad para satisfacer requisitos de cumplimiento.

3.1.4. Redes

Se detallan dos tipos de redes y se especifica lo que desarrolla cada una de ellas (Dr. Hidaia Mahmood Mohamed Alassouli, 2024):

- Enrutamiento avanzado: Proporciona funcionalidades de enrutamiento avanzado para optimizar la gestión del tráfico y la conectividad entre redes.
- Segmentación de redes: Permite la creación de segmentos de red virtuales para mejorar la seguridad y el aislamiento de los recursos.

3.1.5 Administración del equipo:

En la figura 9 se muestra la administración de los equipos y explica lo que se desarrolla cada una de ellas (Dr. Hidaia Mahmood Mohamed Alassouli, 2024):

- Interfaz intuitiva: La interfaz de administración ofrece una experiencia de usuario intuitiva que simplifica la configuración y gestión del dispositivo.
- Monitoreo en tiempo real: Proporciona herramientas de monitoreo en tiempo real que permite la visualización del tráfico y eventos de seguridad.
- Actualizaciones automáticas: Las capacidades de actualización automáticas garantiza que el dispositivo este siempre protegido con las ultimas definiciones y parches de seguridad.

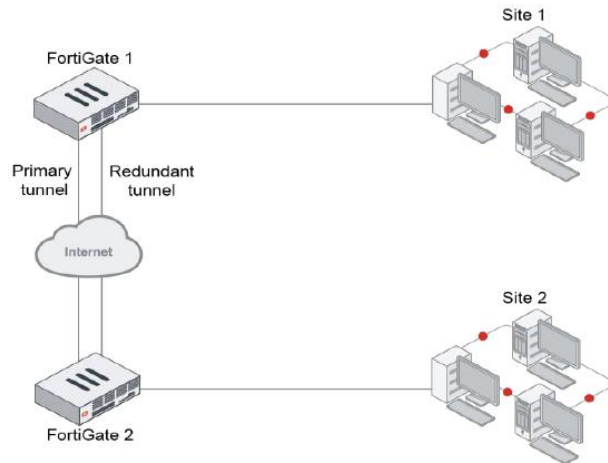


Figura 9. Diagrama de administración de equipos fortigate. (Dr. Hidaia Mahmood Mohamed Alassouli,2024)

3.1.6 Características del equipo

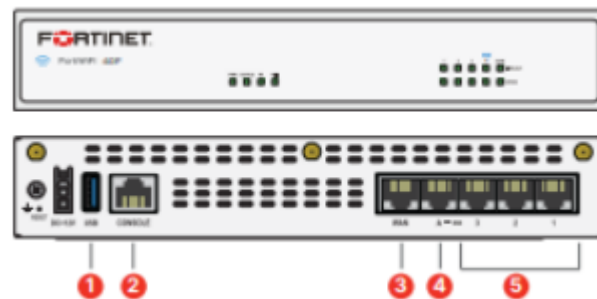


Figura 10. Fortigate Fortiwifi 40F Series Hardware. (Dr. Hidaia Mahmood Mohamed Alassouli,2024)

3.1.7 Interfaces:

1. 1 x USB Port
2. 1x Console Port
3. 1 x GE RJ45 WAN Port
4. 1 x GE RJ45 Fortilink Port
5. 3 x GE RJ45 Ethernet Ports

3.1.8 Características puntos de acceso a internet



Figura 11. Punto de acceso a internet. (Fernando Andreu, Izaskun Pellejero, Amaia Lesta, 2006)

Access point ubiquiti networks	Cantidad de puerto LAN:1
Unifi AC lite, inalámbrico, 1000	Cantidad de antena: 2
Mbit/s, 2.4/5 GHz, 2 antenas de 3dbi- incluye adaptador Poe	Ganancia de la antena (max): 3 dbi
	5GHz: Si 2.4GHz: Si
	Tasa de transferencia (max): 1000 Mbit/s

Tabla 1. Descripción de los puntos de acceso a internet. (Fernando Andreu, Izaskun Pellejero, Amaia Lesta, 2006)

3.2 Seguridad perimetral con FortiGate

Fortinet con sus equipos FortiGate trae la nueva generación de dispositivos de seguridad en tiempo real Unified Threat Management (UTM) o Gestión Unificada de Amenazas. Una solución integral de seguridad, con equipos que pueden mitigar las amenazas de seguridad de manera casi independiente.

Estos equipos se basan en el principio de detener en tiempo real los ataques de contenido, del tráfico que entra y sale de los accesos principales de una red corporativa. FortiGate incluye una serie de funciones de seguridad como firewalls de nueva generación (NGFW),

prevención de intrusiones, filtrado web y protección frente a malware o correo no deseado. (Dr. Hidaia Mahmood Mohamed Alassouli, 2024).



Figura 12. Ambiente de red corporativa con seguridad basada en Fortinet. (Dr. Hidaia Mahmood Mohamed Alassouli, 2024)

La figura 11 muestra que Fortinet basa su seguridad en un sistema centralizado, donde el equipo ocupa la parte perimetral de la red. Dependiendo de las posibilidades económicas del cliente corporativo, se puede adoptar sistemas de alta disponibilidad, es decir, más de un equipo de seguridad perimetral, en línea.

3.2.1 FortiClient

El software de VPN FortiClient brinda una conexión segura a los dispositivos o usuarios que se encuentran fuera de la red local. Es un producto de seguridad de endpoint para PC de escritorio, teléfonos y otros dispositivos. (Dr. Hidaia Mahmood Mohamed Alassouli, 2024)

3.2.2 FortiGuard + FortiMail

Los productos antispam de FortiGuard y de seguridad de mensajería FortiMail integran capacidades avanzadas para proteger contra amenazas versátiles como suplantación de identidad, malware, ransomware y ataques BEC (Business Email Compromise). (Dr. Hidaia Mahmood Mohamed Alassouli, 2024)

3.2.3 FortiManager + FortiAnalyzer

FortiAnalyzer es uno de varios sistemas de censado y análisis que brinda funciones de generación de informes para los productos de Fortinet, incluidos registro de eventos, informes de seguridad y análisis de amenazas. (Dr. Hidaia Mahmood Mohamed Allassouli, 2024)

3.3 Metodología

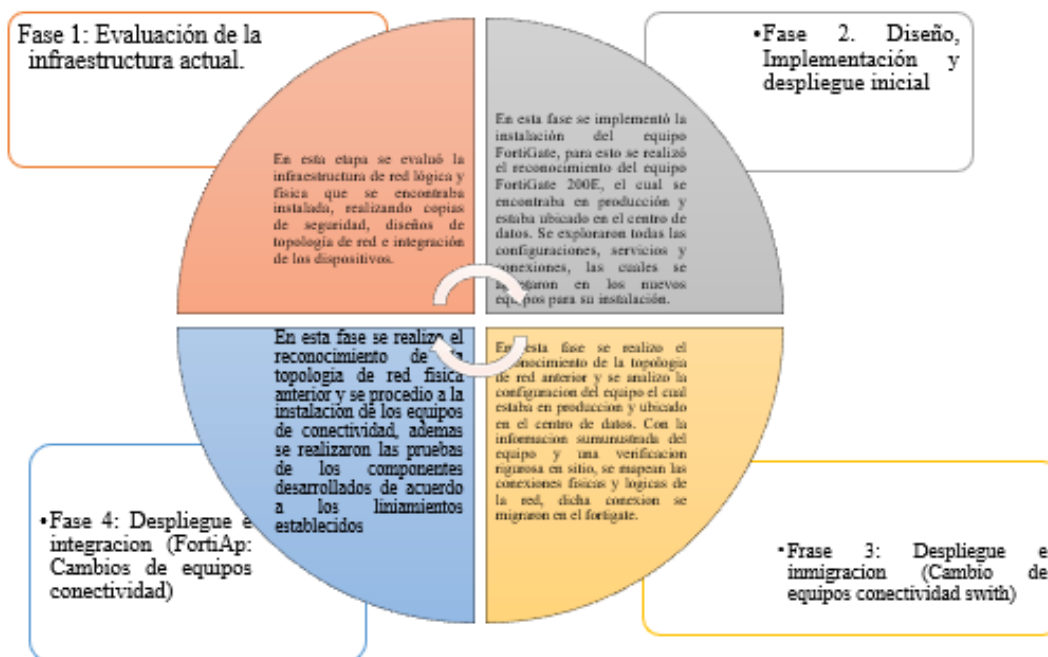


Figura 13. Para el desarrollo del trabajo se siguió la metodología definida, (ARMJ, 2024)

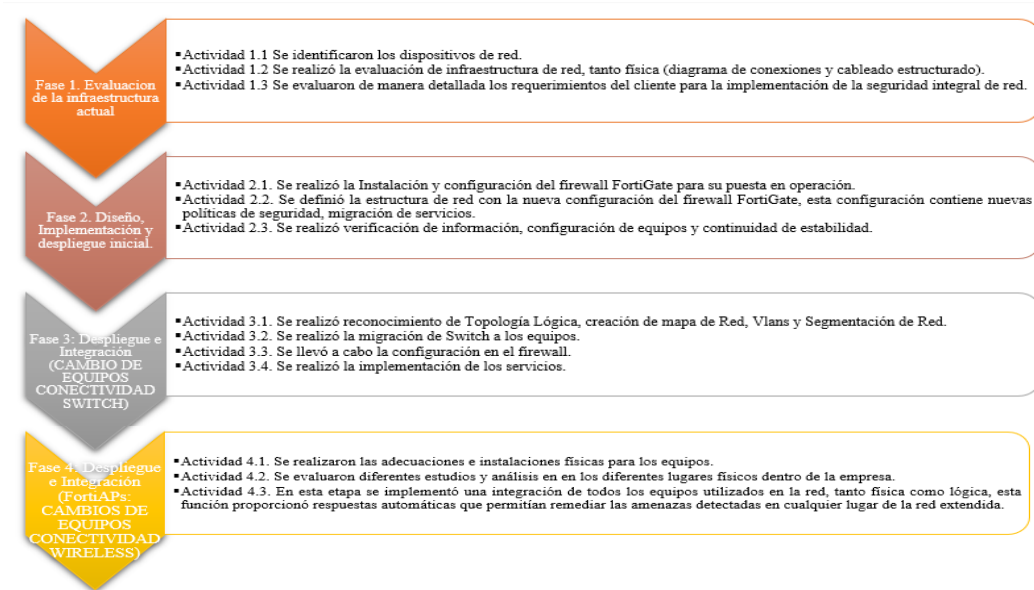


Figura 14. Se muestra cada una de las fases estipuladas que se desarrollaron en las etapas de las actividades relacionadas a la metodología. (ARMJ, 2024)

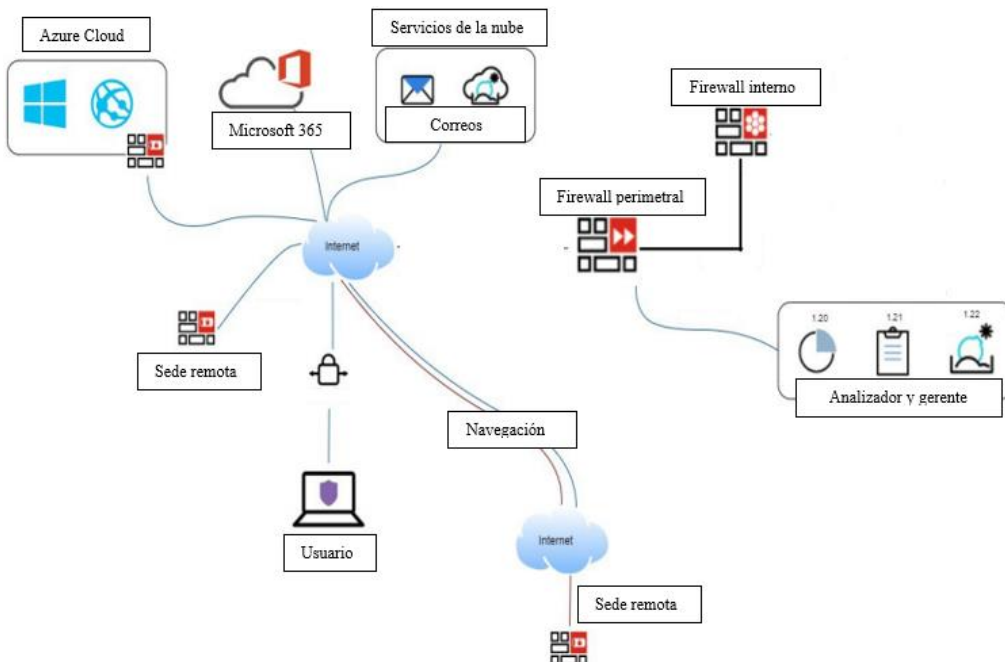


Figura 15. Topología lógica de red. (Joaquín Andreu, 2011)

En la figura 14 se evidencia el diagrama lógico diseñado, el cual muestra las herramientas que se van a utilizar para la red, estas herramientas se sincronizan entre ellas para alertar y evitar cualquier amenaza en la red.

3.4 SD-WAN

Una solución SD-WAN de Fortinet permite a los usuarios de la red conectarse a cualquier aplicación de la nube, además determina de forma inteligente qué ruta satisface mejor los requerimientos de una aplicación específica, para enrutar el tráfico por la ruta ideal de la WAN y mejorar su rendimiento. La SD-WAN brinda un mayor control y mejor administración de los servicios de red, lo cual proporciona un mejor rendimiento en la capa de aplicación de las políticas de servicios, garantizando una óptima productividad de esta. (Dr. Hidaia Mahmood Mohamed Alassouli, 2024)

3.4.1 FortiGate Firewall

El principal objetivo de los firewalls es brindar protección a la red, prevenir ataques, intrusiones y amenazas que pongan en riesgo la información de las organizaciones, lo que lo vuelve una herramienta necesaria para la protección de datos en la actualidad, para el desarrollo de la implementación de la infraestructura de red en la empres

Dentro de los servicios de firewall de FortiGate (Dr. Hidaia Mahmood Mohamed Alassouli, 2024) encontramos:

- FortiGuard Antivirus: Es una solución diseñada específicamente para proteger las redes de la empresa y los dispositivos.
- FortiGuard IPS: los NGFW de FortiGate brindan a las organizaciones capacidades de protección contra intrusiones a través del servicio FortiGuard IPS.
- Control de aplicaciones de FortiGuard: Permite a las empresas controlar fácilmente el uso de aplicaciones y cumplir con los requisitos de cumplimiento, al mismo tiempo que mejora su postura de seguridad general, también brinda a los usuarios visibilidad en tiempo real de las aplicaciones que se ejecutan en la red, así como las tendencias de uso a lo largo del tiempo.

- Filtrado web de FortiGuard: Protege la información de la empresa, evitando que los empleados de esta accedan a contenido web malicioso o sitios web sospechosos que podrían poner en riesgo la red de la empresa.

3.5 La arquitectura fortigate

La tecnología Fortinet es una poderosa combinación de software y hardware basada en el uso de “Circuitos Integrados de Aplicación Específica”, conocidos por sus siglas en inglés como ASIC, a través de la cual es capaz de ofrecer el procesamiento y análisis del contenido del tráfico de la red sin que ello suponga ningún impacto en el rendimiento de las comunicaciones. La tecnología incluye el Procesador FortiASICTM y el Sistema Operativo FortiOSTM los cuales forman el núcleo de los equipos FortiGate y son la base del alto rendimiento ofrecido por los equipos. (Dr. Hidaia Mahmood Mohamed Alassouli, 2024)

3.5.1 Sistema operativo

Fortigate cuenta con un sistema operativo denominado FortiOSTM el cual brinda más Protección, Control e Inteligencia de red más avanzada de seguridad del sistema operativo del mundo. FortiOS es un sistema operativo especialmente diseñado con la seguridad endurecida que es el fundamento de todas las plataformas de seguridad de red FortiGate Puede ser utilizado en toda su infraestructura grande o pequeña empresa. Sobre la base de la historia de Fortinet de la innovación, el completo conjunto de características FortiOS ayuda a combatir las amenazas avanzadas, simplificar las configuraciones de seguridad y despliegues y mejorar amenaza a la seguridad de informes y la visibilidad de la red. (Dr. Hidaia Mahmood Mohamed Alassouli, 2024)

3.5.2 Access point

Los wireless access point brindan acceso a la red de forma inalámbrica, permitiendo administrar el acceso a los mismos para evitar posibles amenazas de seguridad, actualmente un gran número de usuarios cuentan con dispositivos tecnológicos que se integran en el ámbito empresarial, por lo que se hace importante prestar atención a estas conexiones para mitigar el riesgo de amenazas desde dispositivos que no se tienen controlados. Es importante

aclarar que estos dispositivos se integran con el Fortigate, permitiendo una extensión de las políticas establecidas y el control de los usuarios que acceden a estos puntos de red. (Dr. Hidaia Mahmood Mohamed Alassouli, 2024)

CAPÍTULO IV RESULTADOS

En este capítulo se muestra los resultados obtenidos de acuerdo con el desarrollo del proyecto, en las siguientes imágenes se tapará la información confidencial por parte de la empresa ENVATEC S.A de C.V por su privacidad.

En la figura 15 se ejecutó el comando System Interfaz VoIP greet port que ese comando trae las líneas que tengan la cadena de caracteres y mostrara la configuración del puerto.

```
SITE-1 # get system interface | grep port1
== [ port1 ]
name: port1  mode: dhcp  ip: 192.168.1.255.255.0  status: up  netbios-forward: disable  type:
physical  netflow-sampler: disable  sflow-sampler: disable  src-check: enable  explicit-web-proxy: disa
ble  explicit-ftp-proxy: disable  proxy-captive-portal: disable  mtu-override: disable  wccp: disable
drop-overlapped-fragment: disable  drop-fragment: disable

SITE-1 #
```

Figura 16. Configuración de IP para el puerto 1. (ENVATEC, 2024)

En la figura 16 se ingresó la IP del puerto y mostrara una ventana de usuario y contraseña para la sesión.

Figura 17. Interfaz para iniciar sesión. (ENVATEC, 2024)

En la figura 17 se ingresó el usuario y la contraseña donde va a abrir la interfaz principal del fortigate.

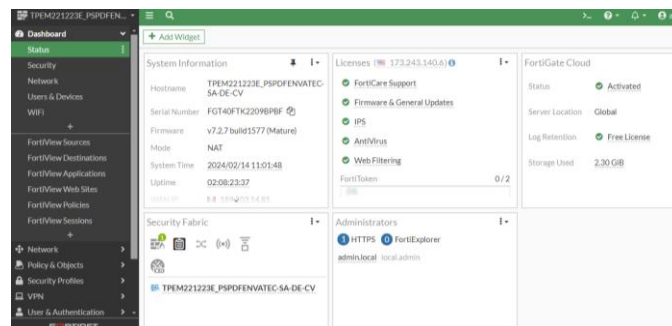
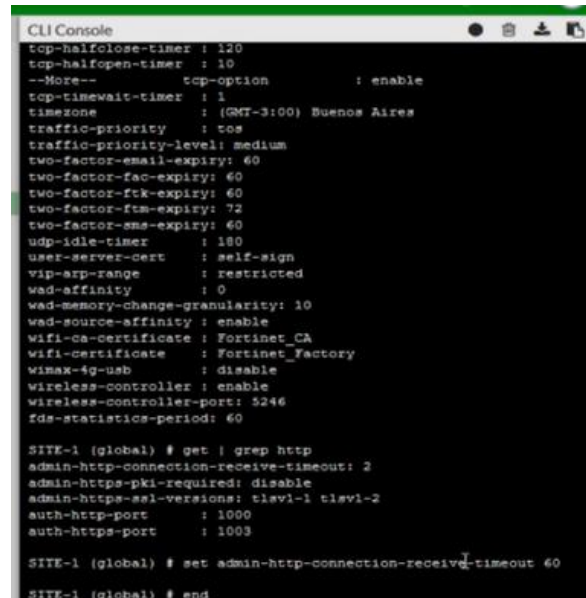


Figura 18. Interfaz principal. (ENVATEC, 2024)

Figura 18 se hace la copia de seguridad que se ingresó en el apartado del usuario y en la opción configuración backup to arrojó una consola donde los comandos de la copia en 60 segundos.



```
CLI Console
top-halfclose-timer : 120
top-halfopen-timer : 10
--More--          top-option          : enable
top-timewait-timer : 1
timezone           : (GMT-3:00) Buenos Aires
traffic-priority   : tos
traffic-priority-level: medium
two-factor-email-expiry: 60
two-factor-fac-expiry: 60
two-factor-ftk-expiry: 60
two-factor-ftm-expiry: 72
two-factor-sms-expiry: 60
udp-idle-timer     : 180
user-server-cert   : self-sign
vip-arp-range       : restricted
wad-affinity        : 0
wad-memory-change-granularity: 10
wad-source-affinity : enable
wifi-ca-certificate : Fortinet_CA
wifi-certificate    : Fortinet_Factory
wimax-4g-usb        : disable
wireless-controller : enable
wireless-controller-port: 5246
fde-statistics-period: 60

SITE-1 (global) # get | grep http
admin-http-connection-receive-timeout: 2
admin-https-pki-required: disable
admin-https-ssl-versions: tlsv1-1 tlsv1-2
auth-http-port : 1000
auth-https-port : 1003

SITE-1 (global) # set admin-http-connection-receive-timeout 60
SITE-1 (global) # end
```

Figura 19. Comando para la copia de seguridad. (ENVATEC, 2024)

Figura 19 se está reiniciando el sistema y aplicando el archivo de configuración para la restauración.

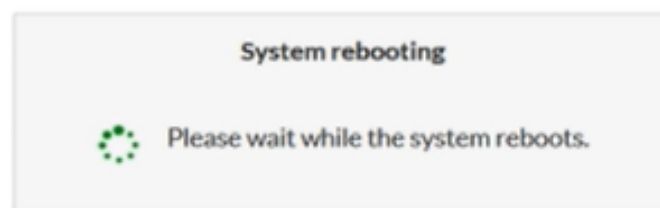


Figura 20. Reinicio del sistema. (ENVATEC, 2024)

Figura 20 muestra el apartado de Users y devices se muestra los usuarios y dispositivos que están conectados y muestra unas graficas de cuantos son y que tipo de modelo, en el otro lado muestra una segunda grafica de los tipos de software que están conectados.

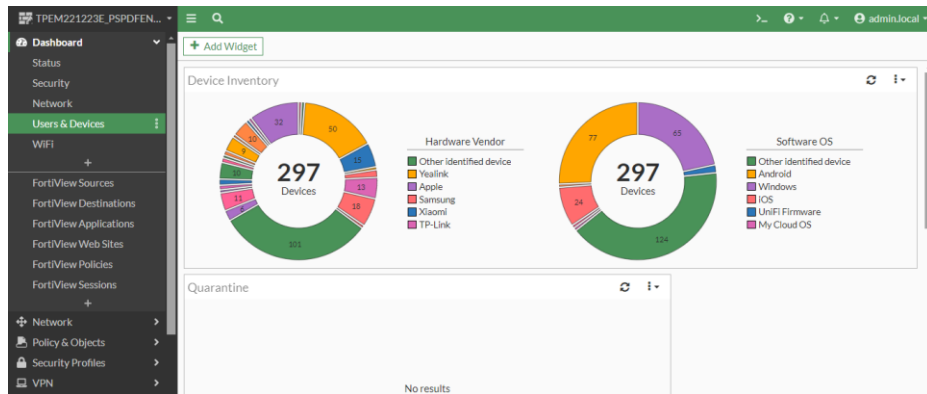


Figura 21. Usuarios y dispositivos. (ENVATEC, 2024)

Figura 21 de la política de firewall es el filtro que permite o deniega el tráfico según una dirección de origen, dirección de destino y servicio de una forma predeterminada, las reglas de política de firewall tienen estado si se permite el tráfico de cliente a servidor.

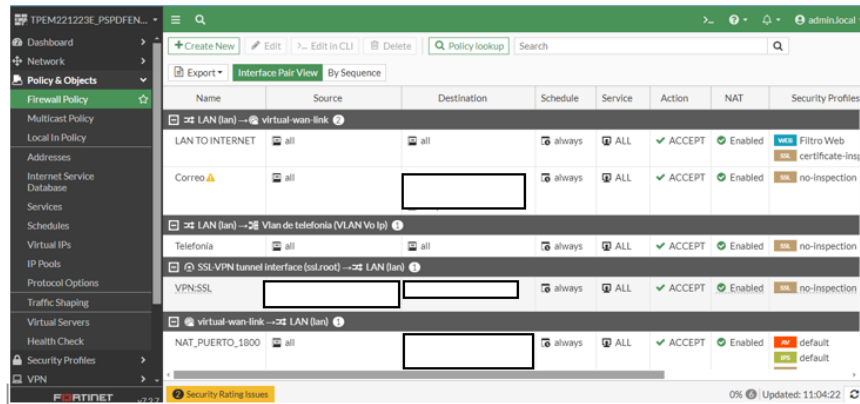


Figura 22. Políticas del Firewall. (ENVATEC, 2024)

Figura 22 se crearon las políticas de salida a internet y también las políticas de VIP (NAT) para poder gestionar las cámaras desde red externa.

Nombre	Origen	Destino	Calendario	Servicio	Acción	NAT	Perfiles de Seguridad	Registro de trafico	Bytes
lan → virtual-wan-link			always	ALL	ACEPTAR	Habilitado	SSL no-inspection	UTM	31.78 GB
virtual-wan-link → LAN			always	ALL	ACEPTAR	Habilitado	SSL no-inspection	UTM	2.31 GB
VLAN VOZ			always	ALL	ACEPTAR	Habilitado	SSL no-inspection	Todo	0 B
VOZ-SDWAN			always	ALL	ACEPTAR	Habilitado	SSL no-inspection	Todo	0 B
Implicito									

Figura 23. Políticas de salida a internet. (ENVATEC, 2024)

Figura 23 es la interfaz permiten que el tráfico fluya entre las redes internas y entre Internet y las redes internas tiene opciones para configurar interfaces y grupos de subredes que pueden escalar a medida que crece su organización.

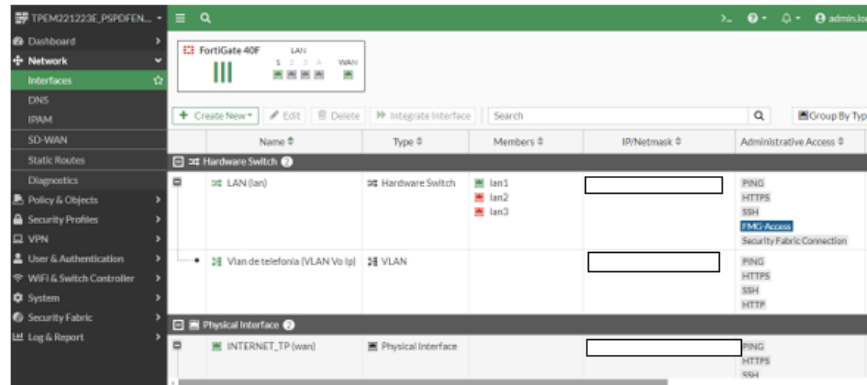


Figura 24. Interfaces. (ENVATEC, 2024)

Figura 24 es la interfaz de salida a internet se realizo una configuración de SDWAN con 2 enlaces Totalplay, con SLA de monitoreo del SDWAN y utilizando 2 de los 5 puertos disponibles.

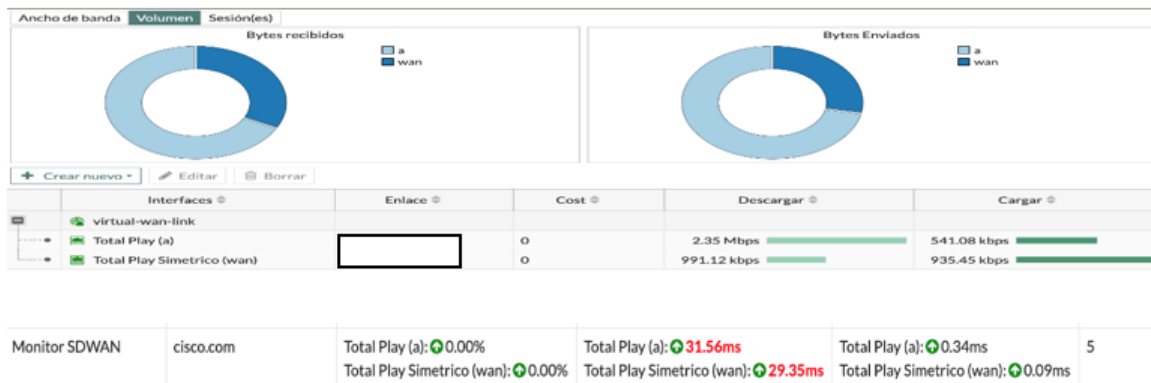


Figura 25. Interfaz de salida a internet. (ENVATEC, 2024)

Figura 25 interfaz de red local se configuro la segmentación con 3 puertos de los 5 disponibles, se activó un DHCP y también se creó un Vlan ID20 que en el archivo de configuración hace relación a un segmento de VoIp, cabe mencionar que monitoreado el funcionamiento de los teléfonos no se pudo detectar tráfico por dicha VLAN, se sospecha

que los teléfonos tienen un switch dedicado con una VLAN independiente y que no necesita estar asociada al Fortigate, los teléfonos quedan funcionando de forma adecuada.

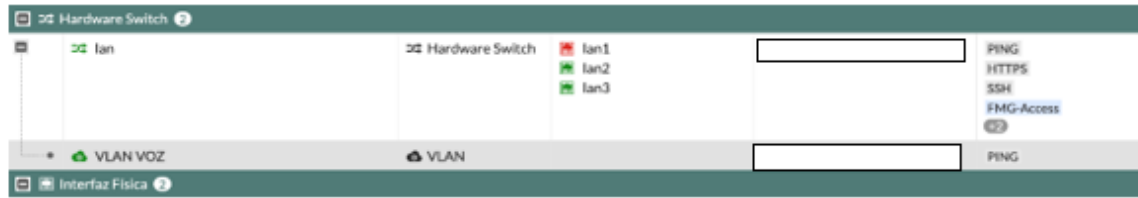


Figura 26. Interfaz de red local. (ENVATEC, 2024)

Figura 26 la creación de 2 SSID y perfil de configuraciones, con salida por la interfaz SDWAN.

Nombre	SSID	Modo de tráfico	Seguridad	Programar	Estatus	Referencia
ECOHUD_38_CON		Puente Local	WPA2 Personal	always	Arriba	8
ECOHUD_ADMIN		Puente Local	WPA2 Personal	always	Arriba	6

Figura 27. Creación de SSID. (ENVATEC, 2024)

Figura 27 las direcciones son las que se permiten al entrar al servidor y aparece el rango de la IP/Subred, Subred de interfaz, dispositivos (dirección MAC) como los detalles de las IP y las interfaces.

Nombre	Detalles	Interfaz	Tipo	Árbitro
Rango IP/Subred				
FABRIC_DEVICE			DIRECCIÓN	0
FIREWALL_AUTH_PORTAL_ADDRESS			DIRECCIÓN	0
LAN_192.168.2.0			DIRECCIÓN	1
SISTEMASALL		LAN (LAN)	DIRECCIÓN	0
SSLVPN_TUNNEL_ADDR1			DIRECCIÓN	4
todo			DIRECCIÓN	7
ninguno			DIRECCIÓN	0
Subred de interfaz				
dirección SUBRED		Telefonía (SUBRED)	DIRECCIÓN	0
Dirección IP VLAN Vo		Vlan de telefonía (VLAN Vo Ip)	DIRECCIÓN	0
LAN		LAN (LAN)	DIRECCIÓN	0
Dispositivo (dirección MAC)				
SistemasAll.envatec.net	b4:45:06:7b:28:98	LAN (LAN)	DIRECCIÓN	0

Figura 28. Direcciones. (ENVATEC, 2024)

Figura 28 es la configuración de DNS se encontrarán los campos DNS estático y DNS estático 2, debe ingresar el servidor DNS primario que desea usar en el primer campo DNS y el servidor DNS secundario en el segundo.

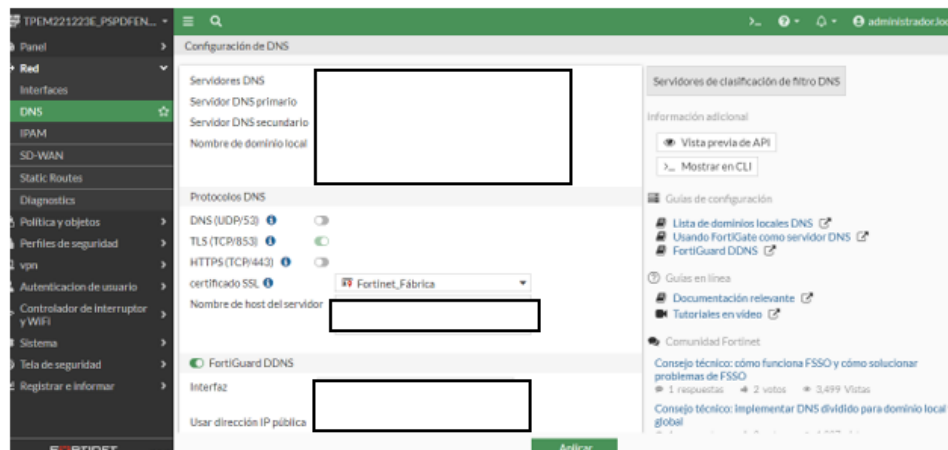


Figura 29. Configuración DNS. (ENVATEC, 2024)

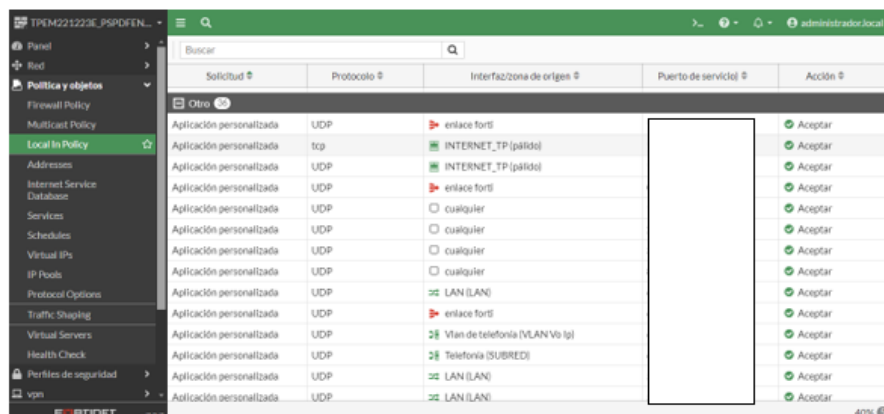


Figura 30. Política local. (ENVATEC, 2024)

Figura 30 de la interfaz de los servicios de red que se ejecutan a través de la red y muestra la gráfica de las categorías y el porcentaje que tienen y la gráfica de los protocolos de los que aparecen con las IP y categorías que se les asigno.

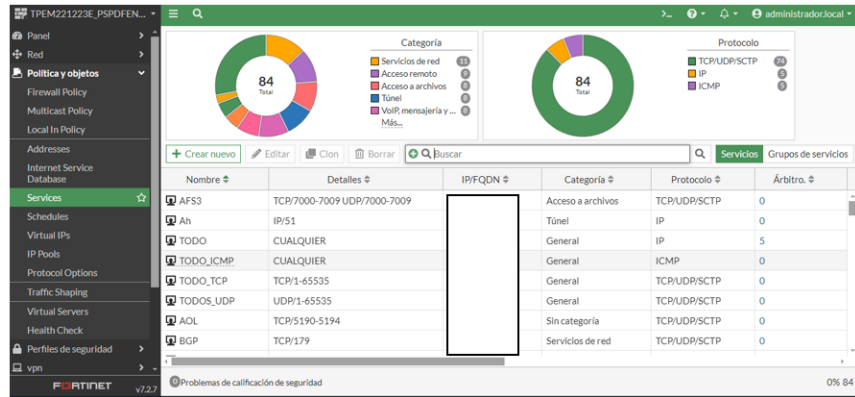


Figura 31. Servicios. (ENVATEC, 2024)

Figura 31 se utilizan normalmente para realizar NAT de direcciones IP públicas o externas a direcciones IP internas o privadas con los puertos de DNS, muestra 2 graficas diferentes del tipo Ipv4 virtual y la segunda de la interfaz con las ip del mapeado y la ip asignada.

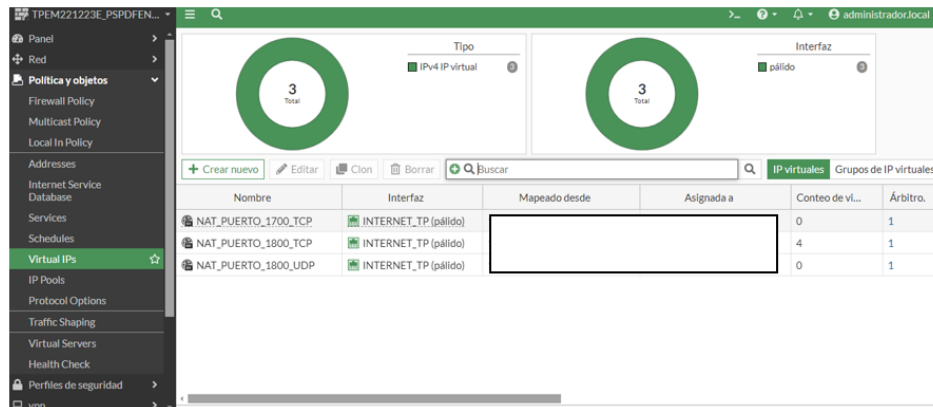


Figura 32. IPs virtual. (ENVATEC, 2024)

Figura 32 y 33 muestra las aplicaciones de firma de los servidores que se crearon al ejecutar y muestra el nombre, categoría, tecnología y el riesgo que tiene cada una y al final nos muestra las 3 graficas del porcentaje que tiene cada una de ellas.

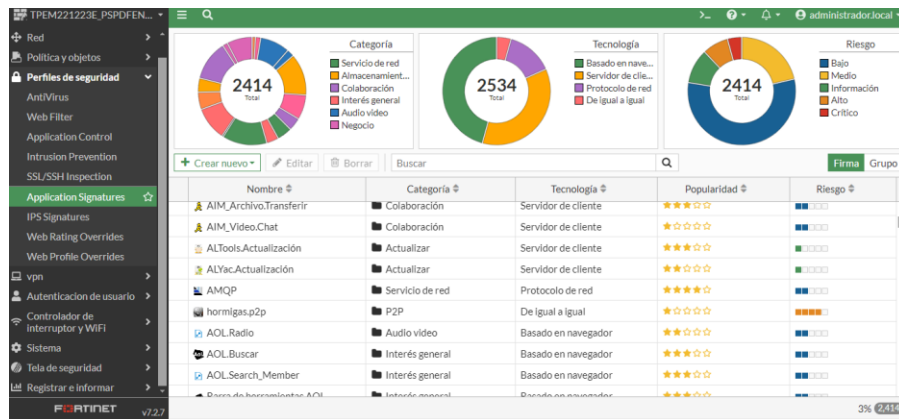


Figura 33. Firmas de aplicaciones. (ENVATEC, 2024)

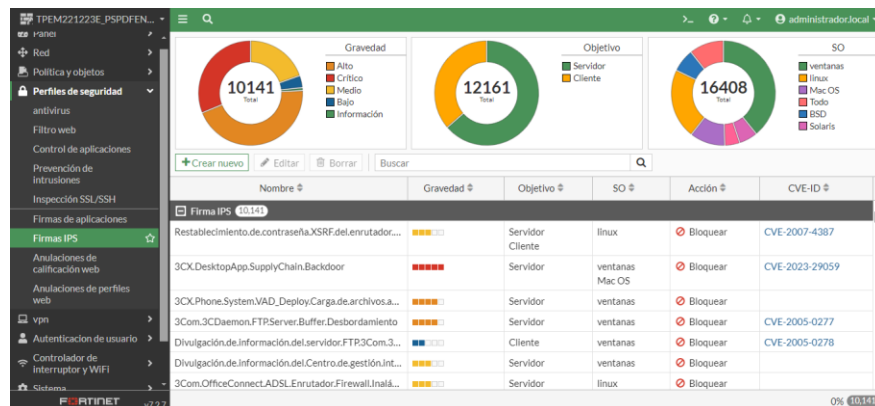


Figura 34. Firmas IPs. (ENVATEC, 2024)

Figura 34 interfaz de asistente de creación de VPN para la configuración, autenticación, política para la configuración nat y dispositivos remotos.

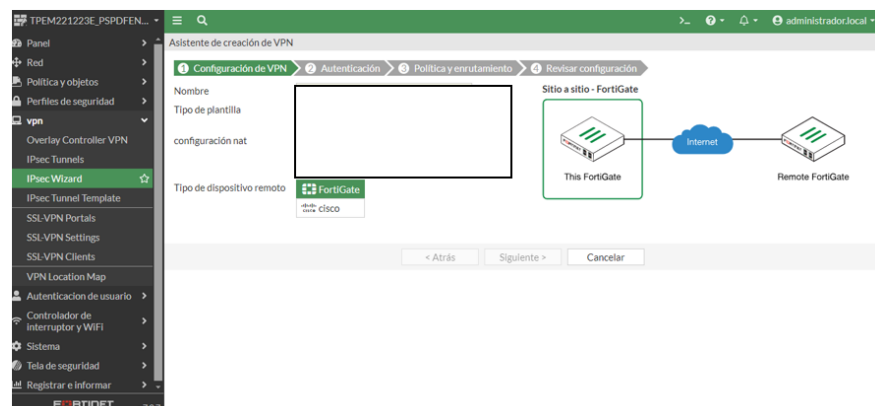


Figura 35. Asistente de IPSec. (ENVATEC, 2024)

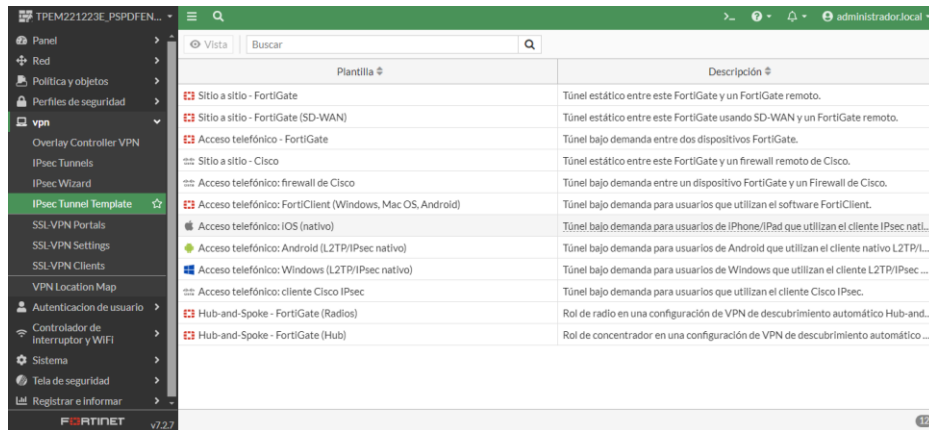


Figura 36. Plantilla de túnel Ipsec. (ENVATEC, 2024)

Figura 36 y 37 en la interfaz de autenticación de usuarios se crearon 4 y se designaron tipo local y en grupo.

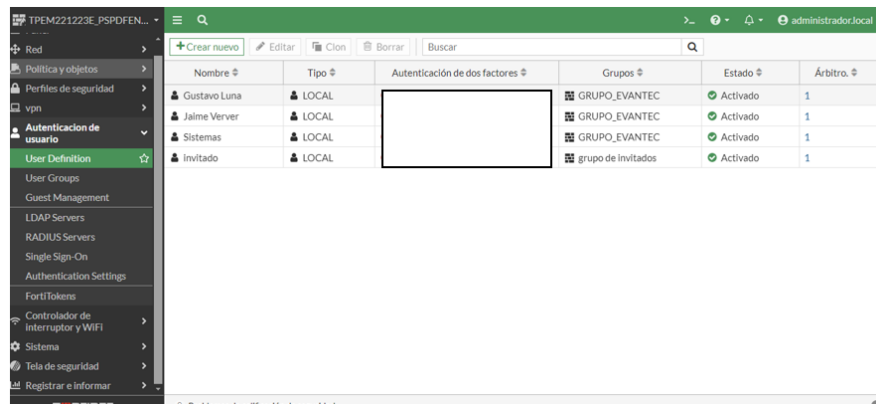


Figura 37. Usuarios definidos. (ENVATEC, 2024)

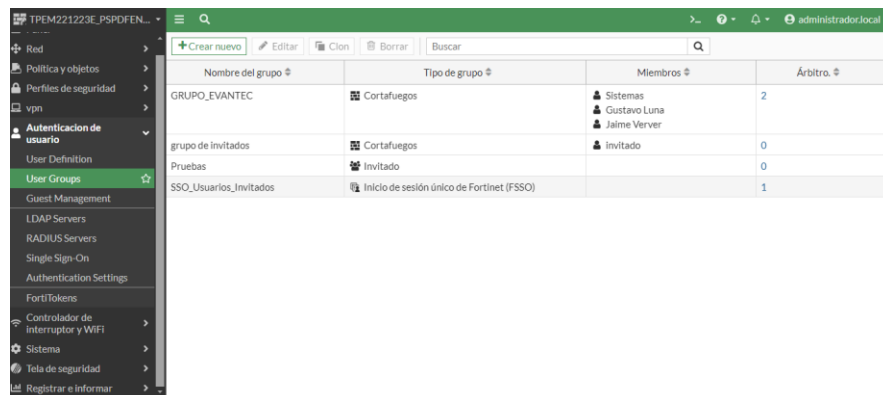


Figura 38. Grupos de usuarios. (ENVATEC, 2024)

Figura 38 interfaz para ajustar el sistema donde se agrega el nombre del host y muestra las opciones de la hora del sistema, zona de horario, el servidor que se está manejando, configuración de administración como los puertos.

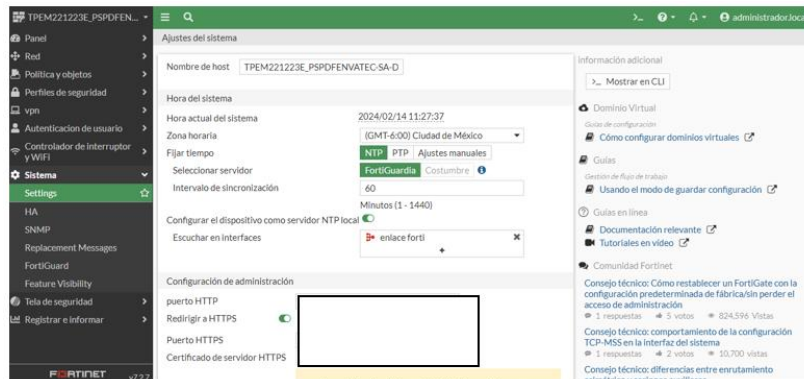


Figura 39. Configuración en el sistema. (ENVATEC, 2024)

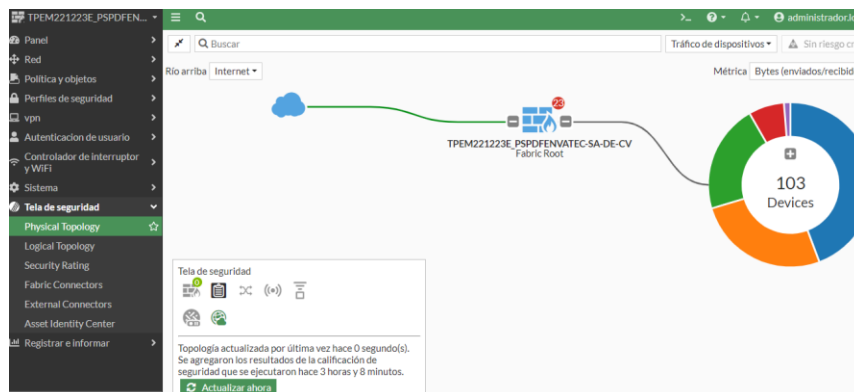


Figura 40. Topología física. (ENVATEC, 2024)



Figura 41. Calificación de seguridad. (ENVATEC, 2024)

Figura 41 son los conectores de seguridad de red central se hizo la configuración de tejido, arrojó el registro y análisis y los dispositivos de borde LAN.

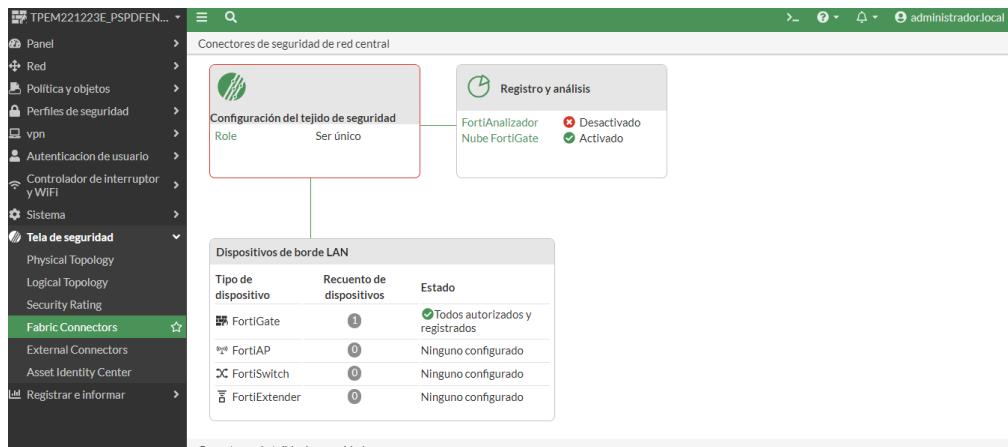


Figura 42. Conectores de tela. (ENVATEC, 2024)

Figura 42 son los dispositivos, software, hardware y el estatus que están conectados a la red como las impresoras, las nas, teléfonos, equipos y entre otros usuarios.

Device	Software OS	Hardware	FortiClient User	User	Status	IoT Vulnerability
00:07:4d:84:7c:93	Other identified device	Zebra			Online	
MyCloudPR2100	My Cloud OS	Western Digital / My Cloud / Pro Series 2-Bay ...			Online	
ServerAspel	Windows	Microsoft			Online	
00:15:65:69:c1:38	Other identified device	Yealink			Online	
00:15:65:73:b9:20	Other identified device	Yealink			Online	

Figura 43. Centro de identidad de activos. (ENVATEC, 2024)

Figura 43 son los tráfico de red que se generan en la IP.

Figura 49 y 50 se observa la conexión física implementada del Fortigate y la configuración establecida de los firewalls en la empresa antes y después.

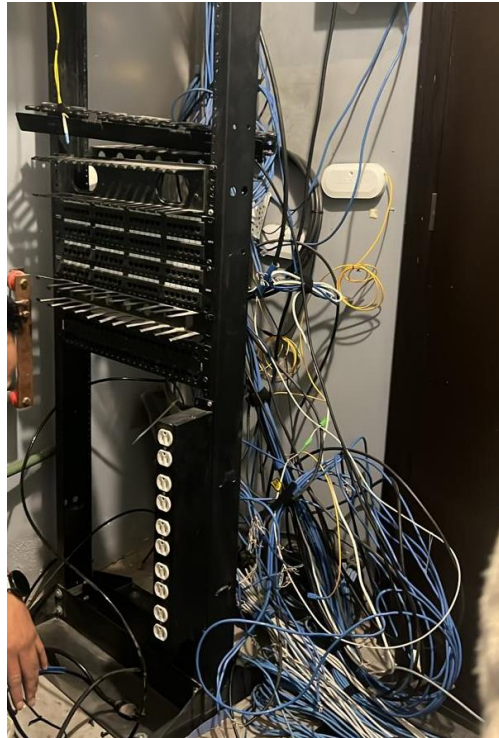


Figura 50. Firewall Fortigate Conexión física antes. (ENVATEC, 2024)



Figura 51. Fortigate Conexión física después. (ENVATEC, 2024)

4.1 CONCLUSIONES

De acuerdo a lo abordado en este documento, se puede concluir que, el sistema de seguridad integral de red, requiere herramientas de hardware y software, que cuenten con características como: modernidad, eligiendo las versiones más vigentes y estables de cada una; compatibilidad, que permita la adaptación a la infraestructura de red de la empresa y que pueda convivir con las diferentes versiones de sistemas operativos, reduciendo costos de licencias y soporte permanente; seguridad, adquiriendo herramientas que brinden respaldo y garanticen la completa integración de red de forma segura. Fortinet ofrece el soporte a nivel mundial, proporciona soporte correctivo durante toda la vida útil de sus productos a través de su red de centros regionales de asistencia técnica, conocida como FortiCare. El funcionamiento del servicio es muy sencillo

Hasta el momento los servicios necesarios fueron cubiertos, es importante afinar las políticas con base en la operación de organización, ya que se detectaron algunas configuraciones en el backup que no son las más recomendadas por distintos motivos como ciberseguridad y también funcionamiento y en el transcurso de la ejecución del proyecto, se identificó una situación problemática en el servidor, caracterizada por una falta de organización adecuada. En vista de esta circunstancia, se tomó la decisión de dejar el equipo Fortinet en una ubicación accesible, con el propósito de facilitar futuros esfuerzos para reorganizarlo y resolver las problemáticas detectadas.

4.2 COMPETENCIAS DESARROLLADAS

Perfil de Egreso

1. Implementa aplicaciones computacionales para solucionar problemas de diversos contextos, integrando diferentes tecnologías, plataformas o dispositivos.
2. Diseña, desarrolla y aplica modelos computacionales para solucionar problemas, mediante la selección y uso de herramientas matemáticas.
3. Diseña e implementa interfaces para la automatización de sistemas de hardware y desarrollo del software asociado.
4. Coordina y participa en equipos multidisciplinarios para la aplicación de soluciones innovadoras en diferentes contextos.
5. Diseña, implementa y administra bases de datos optimizando los recursos disponibles, conforme a las normas vigentes de manejo y seguridad de la información.
6. Desarrolla y administra software para apoyar la productividad y competitividad de las organizaciones cumpliendo con estándares de calidad.
7. Evalúa tecnologías de hardware para soportar aplicaciones de manera efectiva.
8. Detecta áreas de oportunidad empleando una visión empresarial para crear proyectos aplicando las Tecnologías de la Información y Comunicación.
9. Diseña, configura y administra redes de computadoras para crear soluciones de conectividad en la organización, aplicando las normas y estándares vigentes.

4.3 FUENTES DE INFORMACIÓN

- [1] Sosa, R. (2006). *Redes de Computadora*.
- [2] Fernando Andrew, I. P. (2006). *Fundamentos y aplicaciones de seguridad de redes VLAN*.
- [3] Tanenbaum, A. S. (2003). *Redes de Computadora*.
- [4] Fernando Velez Verela, L. G. (2016).
- [5] IPv6. Evelio Martinez Martinez, A. S. (2012). *Fundamentos de telecomunicaciones y redes*.
- [6] https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html. (s.f.). Obtenido de https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html.
- [7] Gerardus. (2019). *IPsec VPN*.
- [8] https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html. (s.f.). Obtenido de https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html.
- [9] Evelio Martinez Martinez, A. S. (2012). *Fundamentos de telecomunicaciones y redes*.
Fortinet Resources and Documents. Fortinet . (2022). Obtenido de <https://www.fortinet.com/resources>.

4.4 ANEXOS

Constancia que evidencia al menos un año de la estancia laboral.



ENVATEC
Maquila de envasado de aerosoles y líquidos

TULTITLAN EDO. DE MÉX. A 04 DE OCTUBRE DE 2023

A QUIEN CORRESPONDA

PRESENTE:

CONSTANCIA LABORAL

POR MEDIO DE LA PRESENTE HACEMOS CONSTAR QUE LA SRA. ALMA ROSA MIRANDA JIMENEZ LABORA EN ESTA EMPRESA BAJO LO SIGUIENTES DATOS SEÑALADOS:

CURP:	MIJA990927MMCRM106
R.F.C.	MIJA990927QS4
NSS:	19179992565
PUESTO:	ANALISTA DE SISTEMAS
FECHA DE INGRESO:	05/09/2022
SUELDO:	\$311.43

DATOS GENERALES DE LA EMPRESA:

RAZON SOCIAL	ENVATEC, S.A. DE C.V.
CALLE Y No.	CANARIAS 317
COLONIA	PORTALES
ALCALDÍA	BENITO JUÁREZ
C.P.	03300
CIUDAD	CIUDAD DE MÉXICO
R.F.C.	ENV-980512-JG8
REGISTRO PATRONAL	Y68-54256-10-1
TELÉFONO:	5888 02 92 / 5888 30 48 EXT. 114

ENVATEC, S.A. DE C.V.

04 OCT 2023

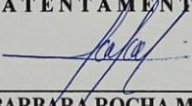
RECURSOS HUMANOS
SHE

DATOS DE UBICACIÓN CENTRO DE TRABAJO:

CALLE Y NO.	ESQ. PASEOS DE TULTITLAN PROL. MIGUEL ALLENDE S/N
COLONIA	BO. DE SANTIAGUITO
MUNICIPIO	TULTITLAN EDO. DE MÉX.
C.P.	54900

SE EXTIENDE ESTA CONSTANCIA PARA LOS FINES QUE A LA INTERESADA CONVENGAN.

ATENTAMENTE



L.E.D BARBARA ROCHA MARQUEZ
RECURSOS HUMANOS

Planta: Prolongación Miguel Allende Col. Barrio de Santiaguito, Tultitlan, Edo. de Mex. 54900 Tel: 5888-0292
Oficinas: Canarias No. 317 Col. Portales, México, D.F. C.P. 03300

Carta de autorización por parte del centro, empresa u organización.



ENVATEC

Maquila de envasado de aerosoles y líquidos

TULTITLAN EDO. DE MÉX. A 04 DE OCTUBRE DE 2023

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

A QUIEN CORRESPONDA

PRESENTE:

Por medio de la presente, hago constar que la alumna **ALMA ROSA MIRANDA JIMENEZ** estudiante de la carrera de **INGENIERIA DE SISTEMAS COMPUTACIONALES** con matrícula **201720568**, trabaja en nuestras instalaciones bajo los siguientes términos:

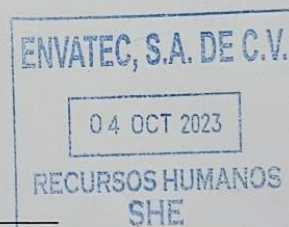
Institución:	Envatec, S.A. de C.V.
Departamento:	Sistemas Computacionales
Nombre del Jefe Inmediato:	Eduardo Arcaraz Vargas
Puesto del Jefe Inmediato:	Analista de Sistemas
Teléfono de oficina:	55 58 88 02 92

Así mismo, realizando actividades que pertenecen a la ingeniería cursada, como lo son las siguientes: Planificación e implementación de redes; programación de base de datos; analizar, diseñar e implementar sistemas de información, brindando solución a las necesidades pertenecientes a la organización; programación, administración e instalación de sistemas operativos; entre otras.

Sin más por el momento quedo de Usted.

ATENTAMENTE

ING. EDUARDO ARCARAZ VARGAS
DPTO. SISTEMAS COMPUTACIONALES



Comprobante de Ingresos de nómina el primero recibido.

ENVATEC S.A DE C.V.

CANARIAS No. 317, Col. PORTALES, BENITO JUAREZ,
CIUDAD DE MEXICO, MEXICO, C.P. 03300
RFC: ENV980512JG8
General de Ley Personas Morales
Registro Patronal IMSS: Y6854256101

No. Trab.: 2369
Nombre: ALMA ROSA MIRANDA JIMENEZ
CURP: MJJA990927MMCRML06
RFC: MJJA990927QS4
R. IMSS: 19179992565
Régimen Trabajador: Sueldos

RECIBO DE NÓMINA

PERCEPCIONES	
P001	SUELDO
1,929.20	

DEDUCCIONES	
D001	ISR
146.84	
D002	IMSS
47.89	

Total Percepciones 1,929.20
Neto Pagado 1,734.47
Total en Efectivo 1,734.47

Total Deduciones 194.73

FIRMA: _____

Comprobante Fiscal Digital por Internet

Folio Fiscal: E46329CD-13DA-AF47-8400-EABA77E12716
Fecha y hora de certificación: 2022-10-06T12:59:02
No de Serie del CSD del SAT: 00001000000502000436
Forma de pago: Por definir

Lugar de emisión: 03300
Fecha y hora de emisión: 2022-10-06T12:58:11
No. de serie del CSD del emisor: 00001000000503832875
Serie y Folio interno: NOMENV134267



Total percepciones:	1,929.20
Total otros pagos:	0.00 +
Otros pagos:	0.00
Subsidio efectivamente entregado al trabajador	
Total deducciones sin ISR:	47.89 -
ISR retenido:	146.84 -
Total:	1,734.47 =

Sello Digital del Contribuyente Emisor:
AdmeRMKX+KqWd1EzSLsROEWOniZT0aw6maPOQeRJCnZuILe0/QS2wD52vNkVROB6e7LFNUAIDXAnfcu6RyL39ID2JeDDAaH85WnjGEM7E2DIWU6cMLF6bSgHkuaIUlSwPc9mWVCmmPqD8GtTX+C2uARj9nNUmHPiMD+36IFnIA8AYOQYyZ2du1abUo7OxplVpMeuUBoyHJNM61hqH2wQAITMRQ36mVwvY351EtB9ZcD5mI+dcUix7Mj3ZeBg9a9Qo6FJZE1826qRbauiYN3smStaNK4CiaVHBVZGVbLTqAksHvccGJhKNcCZRdsGCcQQ==

Sello Digital del SAT:
ScXQXNIGQS8raoBkvQyJ5U8h+FA0ID4Z2zysbTJHup1dZ0a3H90KveOdmAAmzwngEQUfip8IwC11Y/5z2QDOvb8h7ZdZ3PzSB3JWZnWAPUwaaN7uJQwZJm4XsibY75M8BK9L10B9HJUDxWo7oz2xwKAO9wEjps+ZSQ+MA5W3NNa2+y6TT33QSGtoYNPqa8QULrdeMFpRU+bl3nMZEapb5rDQjCR9WJUC8ZDZz5g1sacVvAatp+ao5QNP6wCK9AZaa1H8y6JSeL97KmsIP9Zm6FaUHAa9pW53mEPG0ECdbEQ==

Cadena Original del complemento de certificación digital del SAT:
[1.1]E46329CD-13DA-AF47-8400-EABA77E12716|2022-10-06T12:59:02|SCD110105654|AdmeRMKX+KqWd1EzSLsROEWOniZT0aw6maPOQeRJCnZuILe0/QS2wD52vNkVROB6e7LFNUAIDXAnfcu6RyL39ID2JeDDAaH85WnjGEM7E2DIWU6cMLF6bSgHkuaIUlSwPc9mWVCmmPqD8GtTX+C2uARj9nNUmHPiMD+36IFnIA8AYOQYyZ2du1abUo7OxplVpMeuUBoyHJNM61hqH2wQAITMRQ36mVwvY351EtB9ZcD5mI+dcUix7Mj3ZeBg9a9Qo6FJZE1826qRbauiYN3smStaNK4CiaVHBVZGVbLTqAksHvccGJhKNcCZRdsGCcQQ==|00001000000502000436

Este documento es una representación impresa de un CFDI

Comprobante de Ingresos de nómina del último.

ENVATEC

CANARIAS No. 317, Col. PORTALES, BENITO JUAREZ,
CIUDAD DE MEXICO, MEXICO, C.P. 03300
RFC: ENV980512JG8
General de Ley Personas Morales
Registro Patronal IMSS: Y6854256101

RECIBO DE NÓMINA

No. Trab.: 2369
Nombre: ALMA ROSA MIRANDA JIMENEZ
CURP: MUA990927MMCRML06
RFC: MUA990927QS4
R. IMSS: 19179992565
Régimen Trabajador: Sueldos

Depto.: SISTEMAS ALLENDE
Puesto: ANALISTA DE SISTEMAS
No. Nómina: 4
Periodo del: 22/ene./2024 al 28/ene./2024
Días trabajados: 7
Faltas: 0

PERCEPCIONES		DEDUCCIONES	
P001	SUELDO	2,180.00	
		D001	ISR
		D002	IMSS
			164.41
			54.76

Total Percepciones2,180.00

Neto Pagado1,960.83

Total en Efectivo1,960.83

Total Deducciones219.17

FIRMA:

Comprobante Fiscal Digital por Internet

Folio Fiscal: 6E52EBA9-2A8B-4DAF-8005-0FBFF7FE220E
Fecha y hora de certificación: 2024-01-26T07:23:55
No de Serie del CSD del SAT: 00001000000702693654
Forma de pago: Por definir

Lugar de emisión: 03300
Fecha y hora de emisión: 2024-01-26T07:21:37
No. de serie del CSD del emisor: 00001000000503832875
Serie y Folio interno: NOMENV 154559

Total percepciones:2,180.00

Total otros pagos:0.00 +

Otros pagos:0.00

Subsidio efectivamente entregado al trabajador

Total deducciones sin ISR:54.76 -

ISR retenido:164.41 -

Total:1,960.83 =

Sello Digital del Contribuyente Emisor:

hb+2IRK7u9ycmUWv78LqhtTnJBHHSRuzgH11VpF9aEWglwTc3dybHCbNJxQH5ZRY2v6l2Nivf8pR M0dpqm3Y9684L0oAK5jAgCw60WDgFNG2yeOaLdNg+orgfuyd9j7TBYalqii6/70MTExSRwFUEWDe
HAYW6AhzCFFm5ihmFFVu4AK3/YRqboqbMbtF96AYWkmytPqIBaYipIHdp/OcPPkb3/Z3Gr12z+njpXm GacWQbvx9r1HLINQYftz369VuwTcavRPazYsnQSNXnGU8XAdgyEcwZP5dRLQqj/GsICniQp8Hju63IX8
h8yuy51Vif66PIOK9TusA==

Sello Digital del SAT:

HAGXAd6cp4dNJC21w11zRtD9vHg2huYjua9n6VZiZd1YIOF9apZrieJ3ZJ8aFrRkx3PdbckZuKauDxs1S(Wy14w/OQYewA)TX/UEnpoTKBYZdmcng2F9UedC3k2NmpoFB+KP8bTWgJMHd+VXA8nZuIGNPxYB
hPOXjLLSRJN5eDBZDUjgZWNh1Pav30DLIDV50YW2PS+FH5KGLcxqyEQdHY/9ALgB9GrcBia3/dwEzZ+7Vyg4nLlcWWZB/2p8FhaKtqiwmihoy5FgHDDVFeoAb0YhSWmsEv0HUyVnT2YIS8nOMYzBF
x891JA1MD6U6bdcFNH8gS9==

Cadena Original del complemento de certificación digital del SAT:

[1,1]6E52EBA9-2A8B-4DAF-8005-0FBFF7FE220E[2024-01-26T07:23:55]TSPO80724QW8[hb+2IRK7u9ycmUWv78LqhtTnJBHHSRuzgH11VpF9aEWglwTc3dybHCbNJxQH5ZRY2v6l2Nivf8pRMD0dpqm3Y9684L0oAK5jAgCw60WDgFNG2yeOaLdNg+orgfuyd9j7TBYalqii6/70MTExSRwFUEWDeHAYW6AhzCFFm5ihmFFVu4AK3/YRqboqbMbtF96AYWkmytPqIBaYipIHdp/OcPPkb3/Z3Gr12z+njpXmGacWQbvx9r1HLINQYftz369VuwTcavRPazYsnQSNXnGU8XAdgyEcwZP5dRLQqj/GsICniQp8Hju63IX8h8yuy51Vif66PIOK9TusA==]00001000000702693654

Este documento es una representación impresa de un CFDI