



Facultad de Ingeniería
Ingeniería de Telecomunicaciones

Programa Especial de Titulación

“Implementación de una solución remota con doble factor de autenticación y control de acceso de dispositivo para incrementar la seguridad informática en una empresa privada”

Ever Paul Pastor Caballero

para optar el Título Profesional de Ingeniero de
Telecomunicaciones

Asesor: Carlos Daniel Rodríguez Vilcaromero

Lima – Perú

2022

RESUMEN

En la actualidad y durante la pandemia Covid-19 todos los empleados necesariamente trabajan en modalidad de home office y se valida la necesidad de usar de forma más recurrente este tipo de servicio remoto por lo cual se volvió crítico para las operaciones actuales de toda compañía, es por ello que surge la necesidad de prevenir, contener y solucionar problemas de amenazas de cualquier tipo de ataque mediante virus o malware, también prevenir fuga de información confidencial y sensible de servicios la cual podría ingresar mediante la conexión remota de VPN(Virtual Private Network) SSL(Secure Socket Layer).

El presente informe de suficiencia profesional con título “Implementación de una solución remota con doble factor de autenticación y control de acceso de dispositivo para incrementar la seguridad informática en una empresa privada”, se elaboró en base a una necesidad de una entidad privada de asegurar el acceso, conectividad y comunicación segura de los usuarios remotos mediante red privada virtual SSL y lograr cumplir el objetivo de implementar una solución remota con autenticación de doble factor y control de acceso de dispositivo para incrementar la seguridad informática en una empresa privada permitiendo controlar de forma muy detallada sobre qué dispositivos pueden acceder a la red de Interna, debido a que en la actualidad tenemos la obligación de asegurarnos de mantener nuestros datos protegidos y aprovechar las ventajas y virtudes de la tecnología que ayudan a mantener asegurados a los colaboradores y a la información no importando desde que dispositivo o lugar que se conecte.

INDICE DE CONTENIDO

RESUMEN	II
INDICE DE FIGURAS	4
INDICE DE TABLAS	9
INTRODUCCION	10
CAPITULO 1	13
ASPECTOS GENERALES	13
1.1. Definición del Problema	13
1.1.1. Descripción del Problema.....	13
1.1.2. Formulación del Problema.....	14
1.2. Definición de objetivos	14
1.2.1. Objetivo general	14
1.2.2. Objetivos específicos	14
1.3. Alcances y limitaciones	15
1.3.1. Alcances.....	15
1.3.2. Limitaciones	17
1.4. Justificación	18
1.5. Estado del Arte.....	20
CAPITULO 2.....	23
MARCO TEÓRICO.....	23
2.1. Fundamento teórico	23
2.2. Marco conceptual.....	50
CAPITULO 3.....	55
DESARROLLO DE LA SOLUCIÓN.....	55
CAPITULO 4.....	130
RESULTADOS	130
4.1. Resultados	130
4.2. Presupuesto	170
CONCLUSIONES	172
RECOMENDACIONES	172
BIBLIOGRAFÍAS.....	174
ANEXOS	175

INDICE DE FIGURAS

Figura 1. Topología Global Protect.....	24
Figura 2. Autenticación Doble Factor.....	25
Figura 3. Funcionamiento de Autenticación Doble Factor.....	26
Figura 4. Ejemplos de Información.....	35
Figura 5. Ejemplos de Hardware.....	36
Figura 6. Principios Fundamentales de Seguridad Informática.....	37
Figura 7. Riesgos de activos de información.....	38
Figura 8. Amenazas de Seguridad.....	40
Figura 9. Cuadrante Mágico de Gartner de 2020 para firewalls de red.....	41
Figura 10. Infraestructura de Servicios de Red.....	43
Figura 11. Robo de Información.....	44
Figura 12. Manipulación y pérdida de datos.....	44
Figura 13. Robo de identidad.....	45
Figura 14. Servicio de Disrupción.....	45
Figura 15. Ataques de contraseñas.....	47
Figura 16. Explotación de confianza.....	48
Figura 17. Redireccionamiento de puertos.....	48
Figura 18. Ejemplo de Ataque Man-in-the-Middle.....	49
Figura 19. Cotización de firewall Palo Alto.....	58
Figura 20. Cotización de firewall Fortinet.....	59
Figura 21. Cotización de firewall Cisco.....	59
Figura 22. Evidencia de Cisco Duo como mejor alternativa para el 2FA.....	61
Figura 23. Calificación de Cisco Duo en Gartner como mejor opción para 2FA.....	61
Figura 24. Evaluación de denuncias semestrales por delitos informáticos.....	62
Figura 25. Aumento de denuncias de robo de identidad.....	63
Figura 26. Histórico de conexiones remotas de marzo del año 2020.....	63
Figura 27. Histórico de conexiones remotas de mayo del año 2021.....	64
Figura 28. Detalle histórico de conexiones remotas de mayo del año 2021.....	64
Figura 29. Organigrama de integrantes del Proyecto.....	66
Figura 30. Diagrama de red previo al desarrollo del proyecto.....	68
Figura 31. Diagrama de red previo desarrollo del Proyecto mostrando la nueva conexión de acceso básico.....	69
Figura 32. Estructura de desglose del Trabajo (EDT).....	70
Figura 33. Diagrama de red propuesto para el desarrollo del Proyecto.....	76
Figura 34. Diagrama de red propuesto mostrando los componentes de la nueva solución implementada.....	77
Figura 35. Cronograma del Proyecto.....	78
Figura 36. Costos de Asignación de Personal.....	80
Figura 37. Costos de Consumibles y Servicios.....	80
Figura 38. Flujo de Caja.....	81
Figura 39. Resumen de Flujo de Caja.....	81
Figura 40. Organigrama de Integrantes del Proyecto - RH.....	82
Figura 41. Asignación de Personal.....	83
Figura 42. EDT de categorías de Riesgos.....	88
Figura 43. Diagrama de Red con la nueva solución y sus componentes principales.....	98

Figura 44. Creación de certificado para VPN SSL.	99
Figura 45. Validación de certificado para VPN SSL.	99
Figura 46. Detalle de certificado para VPN SSL.	99
Figura 47. Perfil de seguridad SSL/TLS.	100
Figura 48. Perfil de autenticación para la VPN SSL.....	101
Figura 49. Portal Global Protect para la VPN SSL.	101
Figura 50. Detalle general de configuración del portal Global Protect.....	101
Figura 51. Detalle de autenticación del portal Global Protect.....	102
Figura 52. Gateway de Global Protect para la VPN SSL.....	102
Figura 53. Detalle general de configuración de Gateway de Global Protect.	102
Figura 54. Detalle de autenticación de cliente de Gateway de Global Protect.....	103
Figura 55. Detalle de configuración de agente de Gateway de Global Protect.	103
Figura 56. Detalle de configuración de servicios de red del Gateway de Global Protect.	103
Figura 57. Detalle de cuenta administrador de la solución Cisco Duo Security.	104
Figura 58. Configuración de la aplicación “VPN SSL de Palo Alto” en Cisco Duo.	104
Figura 59. Detalle de Configuración de “VPN SSL de Palo Alto” en Cisco Duo.	105
Figura 60. Configuración de política de acceso global en Cisco Duo.....	105
Figura 61. Validación de recursos disponibles en el servidor Autenticación Proxy.	106
Figura 62. Ruta de descarga de aplicación Autenticación Proxy.	106
Figura 63. Aplicación Autenticación Proxy.	106
Figura 64. Configuración de aplicación Autenticación Proxy.	107
Figura 65. Configuración de red de servidor Duo Proxy.	107
Figura 66. Interfaz local de red DMZ en el firewall Palo Alto.	107
Figura 67. Prueba de conectividad desde el Firewall hacia el servidor Duo Proxy.	108
Figura 68. Servicio de Autenticación Proxy.	108
Figura 69. Licencia de la plataforma Cisco Duo Security para el doble factor de autenticación	109
Figura 70. Licencia Global Protect para el HIPs Profile, para el control de acceso de.....	109
dispositivo.	109
Figura 71. Registro del server AD en el portal de 2FA.....	110
Figura 72. Conexión y sincronización del server AD en el portal de 2FA.	110
Figura 73. Metadatos de API configuración del Proxy de Autenticación.	111
Figura 74. Parámetros configurados del servidor AD(IP Server) y el DN Base.....	111
Figura 75. Atributos de perfil de usuario sincronizados y el grupo GlobalProtect2FA.....	112
Figura 76. Configuración de objeto HIP Profile.....	113
Figura 77. Configuración de perfil HIP Profile.....	113
Figura 78. Configuración de perfil HIP Profile en la política de seguridad del Firewall.....	113
Figura 79. Configuración de notificación aceptado de control de acceso de dispositivo.....	114
Figura 80. Configuración de notificación denegado de control de acceso de dispositivo.....	114
Figura 81. Grupo de usuarios de AD en la consola de administración Cisco DUO Security. ..	115
Figura 82. Grupo “GlobalProtect2FA” que tiene los usuarios de la empresa desde el AD	115
Figura 83. Detalle del grupo AD”GlobalProtect2FA” desde la consola de administración.....	115
Cisco Duo Security.....	115
Figura 84. Usuarios iniciales sincronizados del grupo “GlobalProtect2FA”.	116
Figura 85. Configuración del servidor radius en el firewall Palo Alto.	116
Figura 86. Configuración de los atributos y parámetros de red del servidor AD en el	117
Server Proxy 2FA.....	117
Figura 87. Configuración del método de autenticación en el portal Duo Security.	117
Figura 88. Configuración del perfil de autenticación en el Portal Global Protect.....	118

Figura 89. Detalle del perfil de autenticación en el Portal Global Protect	118
Figura 90. Configuración del perfil de autenticación “Perfil Duo 2FA” en el Gateway	118
Figura 91. Configuración de API y parámetros de red y seguridad del DUO Proxy Server.....	119
Figura 92. Sincronización de usuario 1	119
Figura 93. Sincronización de usuario 2.	119
Figura 94. Perfil de usuario de prueba como estado activo.....	120
Figura 95. Asignación de dispositivo para usuario de prueba.....	120
Figura 96. Activación del Duo Mobile.....	120
Figura 97. Envío de invitación de enrolamiento de usuario con la aplicación 2FA.....	121
Figura 98. Validación de notificación para activar la aplicación Duo Mobile.....	121
Figura 99. Aplicación Duo Mobile.	121
Figura 100. Cuenta asociada de la empresa privada a la aplicación Duo Mobile.	122
Figura 101. Inicio de sesión de usuario en la Aplicación Duo Mobile.	122
Figura 102. Push de validación de sesión del proceso de doble factor.	123
Figura 103. Usuarios registrados en la consola de 2FA al finalizar la implementación.	123
Figura 104. Configuración por CLI del Firewall Palo Alto relacionado el acceso remoto.....	124
Figura 105. Detalle del consumo de CPU del Firewall Palo Alto.....	124
Figura 106. Detalle del consumo de recursos del Firewall Palo Alto.	125
Figura 107. Detalle del consumo de Disco del Firewall Palo Alto.	125
Figura 108. Detalle del consumo de Memoria del Firewall Palo Alto.....	126
Figura 109. Registro 1 de usuarios enrolados y conectado.	126
Figura 110. Registro 2 de usuarios enrolados y conectado.	127
Figura 111. Registro de otros usuarios con sus respectivas conexiones por el 2FA.....	128
Figura 112. Registros del control de acceso de dispositivo.....	128
Figura 113. Capacitación de la solución implementada.....	129
Figura 114. Autenticación de acceso remoto básico para VPN SSL Check Point.....	130
Figura 115. Conexión de acceso remoto básico para VPN SSL Check Point.....	131
Figura 116. Conexión satisfactoria del acceso remoto básico para VPN SSL Check Point	131
Figura 117. Información de equipo utilizado LP-EPASTOR para el acceso remoto.....	132
Figura 118. Equipo utilizado LP-EPASTOR no tiene funciones de seguridad activas.....	132
Figura 119. Equipo utilizado LP-EPASTOR no tiene cifrado de disco activado	133
Figura 120. Equipo utilizado LP-EPASTOR no tiene antivirus o antimalware instalado	133
Figura 121. Resultado de aplicación y notificación de rechazo de acceso remoto	134
Figura 122. Registros de rechazo conexión remota el cual no fue autorizado por el usuario ...	135
real, desde la plataforma 2FA	135
Figura 123. Notificación de rechazo conexión remota el cual no fue autorizado por el usuario	135
real, desde el correo corporativo	135
Figura 124. Registro rechazado de conexión remota el cual no fue autorizado por el usuario ...	136
real desde el firewall Palo Alto donde está implementada la VPN SSL.....	136
Figura 125. Inicio de sesión de usuario epastor por el agente de conexión remota (Global P.).	136
Figura 126. Notificación de rechazo de la conexión remota por el control de acceso de	137
dispositivo debido a que no tiene las funciones de seguridad activas	137
Figura 127. Validación de funciones de seguridad activas del dispositivo LPHP-SOSORIO...	138
Figura 128. Validación de funciones activas de Protección de Antivirus y Antimalware en. ...	138
Dispositivo LPHP-SOSORIO.	138
Figura 129. Validación cifrado de disco activo en dispositivo LPHP-SOSORIO.	139
Figura 130. Antivirus y DLP instalado correctamente en el dispositivo LPHP-SOSORIO	139
Figura 131. Antimalware instalado correctamente en el dispositivo LPHP-SOSORIO	140
Figura 132. Vinculación de cuenta de usuario en la aplicación Duo Mobile con su dispositivo	140
Móvil desde la consola de administración 2FA.	140

Figura 133.Activación desde la consola Duo Doble factor de autenticación hacia el dispositivo móvil a vincular	141
Figura 134. Mensaje validado desde el celular del usuario para su enrolamiento a la consola de administración desde la aplicación Duo Mobile	141
Figura 135.Instalación de agente Global Protect parte1	142
Figura 136.Instalación de agente Global Protect parte2	142
Figura 137.Instalación de agente Global Protect parte3	143
Figura 138.Instalación de agente Global Protect VPN SSL finalizada	143
Figura 139.Configuración de la ip pública VPN SSL para el acceso remoto	144
Figura 140.Inicio de Sesión de usuario con la conexión remota segura	144
Figura 141.Proceso en curso de la conexión remota segura mediante el agente Global P	145
Figura 142.Notificación de autorización de acceso utilizando el 2FA,en donde se valida que es relamente el usuario real que se conectará	145
Figura 143.Notificación satisfactoria de control de acceso de dispositivo	146
Figura 144.Validación de conexión segura como parámetros de red, gaetway de la solución de acceso remoto,protocolo usado, tiempo de actividad entre otros	147
Figura 145.Antivirus detectado por el agente Global Protect	147
Figura 146.Cifrado de disco detectado por el agente Global Protect	148
Figura 147.El acceso remoto seguro hacia el destino 192.168.90.80(activo local) usando. El 2FA y el control de acceso de dispositivo.	148
Figura 148.Conectando remotamente al destino 192.168.90.80 (activo local) con acceso remoto seguro	149
Figura 149.Interfaz WAN(Pública) y Dmz(Interna) en el firewall Palo Alto	149
Figura 150.Interfaz Tunel de la VPN SSL en el firewall Palo Alto	150
Figura 151.Zonas asociadas a las interfaces del firewall Palo Alto	150
Figura 152.Tabla de rutas donde se encuentran las rutas estáticas configuradas	150
Figura 153.Objetos creados para el uso de las reglas de seguridad	150
Figura 154.Resultado de encuesta de usuario1(Carlos Chacchi)	151
Figura 155.Evidencia de encuesta de usuario1(Carlos Chacchi)	151
Figura 156.Resultado de encuesta de usuario2(Jean Vargas)	152
Figura 157.Evidencia de encuesta de usuario2(Jean Vargas)	152
Figura 158.Resultado de encuesta de usuario3(Sergio Osorio)	153
Figura 159.Evidencia de encuesta de usuario3(Sergio OSorio)	153
Figura 160.Precio de equipo Firewall Palo Alto 3050	154
Figura 161.Equipo Firewall Palo Alto 3050 en almacén	154
Figura 162.Equipo Firewall Palo Alto 3050 en instalado, implementado y en operación	155
Figura 163.Proyectos tecnológicos de renovación con clientes	156
Figura 164.Proyectos tecnológicos de ampliación de servicio de clientes	156
Figura 165.Nuevos proyectos tecnologicos de nuevos clientes	156
Figura 166.Trabajo antes de pandemia covid-19	157
Figura 167.La infraestructura sin deteriorarse, sin personal en sitio	157
Figura 168.Trabajo al remoto usando la nueva implementación de forma segura	158
Figura 169 Noticia sobre la activación automática del doble factor a cuentas de Google	158
Figura 170 Detalle 01 de interfaz WAN de firewall Check Point	159
Figura 171 Detalle 02 de interfaz WAN de firewall Check Point	159
Figura 172 Detalle de velocidad de negociación de la interfaz WAN del firewall Checkpoint	159
Figura 173 Detalle de velocidad de gestión de información antes del proyecto	160
Figura 174 Detalle de velocidad de negociación de la interfaz WAN del firewall Palo Alto	160
Figura 175 Detalle de velocidad de gestión de información después del proyecto	161
Figura 176 Detalle de latencia de sistema antes de la ejecución del proyecto	161
Figura 177 Detalle de latencia de sistema después de la ejecución del proyecto	162

Figura 178 Detalle 01 de compatibilidad del HIP profile con otros fabricantes	163
Figura 179 Detalle 02 de compatibilidad del HIP profile con otros fabricantes	164
Figura 180 Detalle de pruebas eléctricas.....	167
Figura 181 Certificado de Aterramiento	167
Figura 182 Disposición 01 de energía eléctrica de soporte en caso de emergencias	168
Figura 183 Disposición 02 de energía eléctrica de soporte en caso de emergencias	169
Figura 184 Disposición 03 de energía eléctrica de soporte en caso de emergencias	169
Figura 185.Costo de Personal por asignación de trabajo.	170
Figura 186.Costo de servicios y consumibles del Proyecto.	170
Figura 187.Flujo de caja del Proyecto.....	171

INDICE DE TABLAS

Tabla 1. Vulnerabilidades Tecnológicas.	46
Tabla 2. Vulnerabilidades de configuración.....	46
Tabla 3. Vulnerabilidades de política.....	47
Tabla 4. Contraseñas Débiles.	50
Tabla 5. Contraseñas seguras.	50
Tabla 6. Tabla de evaluación técnico-económica de la tecnología seleccionada.	57
Tabla 7. Tabla de evaluación técnico-económica de la tecnología usada para el doble factor . .	60
de autenticación.....	60
Tabla 8. Roles y responsabilidades de integrantes del Proyecto.....	67
Tabla 9. Detalle de entregables del proyecto.	71
Tabla 10. Planilla mensual.	79
Tabla 11. Detalle de ingresos.	80
Tabla 12. Estrategia de Comunicación de Gestión de Interesados.....	84
Tabla 13. Matriz de comunicaciones.....	85
Tabla 14. Roles y Responsabilidades.....	86
Tabla 15. Presupuesto del personal por proceso de Gestión de Riesgo.	87
Tabla 16. Escalas de Impacto de un Riesgo sobre los Principales Objetivos del Proyecto.....	89
Tabla 17. Matriz Probabilidad e Impacto.....	89
Tabla 18. Clasificación de Riesgo.....	89
Tabla 19. Matriz de Riesgo.	90
Tabla 20. Registro de Interesados Preliminar.	94
Tabla 21. Registro de Interesados.	94
Tabla 22. Matriz de Análisis de los Interesados.....	95
Tabla 23. Estrategia de gestión de Interesados.....	95
Tabla 24. Planilla mensual del personal.....	170
Tabla 25. Detalle de ingresos del proyecto.	171

INTRODUCCION

En los últimos años y hasta la actualidad durante la pandemia Covid-19, el campo de ciberseguridad y seguridad de la información tiene una gran participación, un notable desarrollo y un fuerte crecimiento, casi exponencial en el mundo de la tecnología, asimismo existen diferentes tipos de amenazas las cuales son los famosos malware, los virus, los cibercriminales, spyware y varias formas de amenazas existentes que también crecieron exponencialmente y que son un peligro muy alto, crítico y constante que atentan contra el correcto funcionamiento de las redes empresariales. Las empresas y Organizaciones en la actualidad en todo momento buscan mejorar y reforzar la protección de su información que en la actualidad es uno de sus activos principales y muy importante dentro de cualquier negocio, también buscan mejorar las condiciones actuales mediante el aseguramiento de la conectividad y comunicación de forma segura para lograr garantizar la disponibilidad y continuidad de la operación de sus servicios, para asegurar operatividad de servicios se utilizan soluciones basadas en altas tecnologías que brindan en todo momento integridad y seguridad de la información con costos manejables en comparación al gran impacto financiero que podría tener ante algún incidente de seguridad.

El presente proyecto consiste en asegurar el acceso, conectividad y comunicación segura de los usuarios remotos mediante red privada virtual SSL(Secure Socket Layer) la cual es un tipo de conexión de red privada

virtual segura hacia los recursos internos de la red interna de una empresa privada y además mediante una solución de red privada virtual SSL segura que permita controlar de forma muy granular del acceso del tipo de dispositivos que pueden ingresar por la red privada virtual a la red de interna, debido al estado de emergencia por el COVID-19 en donde todos los empleados necesariamente trabajan en modalidad de home office y se valida la necesidad de usar de forma más recurrente este tipo de servicio por lo cual se volvió crítico para las operaciones actuales de toda compañía, es por ello que surge la necesidad de prevenir, contener y solucionar problemas de amenazas de cualquier tipo de ataque ya sea a través de virus o malware en computadoras o laptops, prevenir fuga de información confidencial y sensible de servicios la cual podría ingresar mediante la conexión VPN(Virtual Private Network) SSL.

El trabajo se ha desarrollado de la siguiente manera:

En el capítulo 1

Se detalla el problema que se quiere resolver, también los objetivos, y la descripción del informe de suficiencia profesional.

En el capítulo 2

Se describe el fundamento Teórico y marco conceptual de la solución planteada.

En el capítulo 3

Se describen los métodos y procedimientos, las tecnologías utilizadas, resultados y la sustentación de la solución propuesta, así como la arquitectura a usar.

En el capítulo 4

Se presentan con pruebas la implementación y pruebas finales con los valores e interpretación evidenciadas.

Tomando en cuenta el análisis realizado en el capítulo 4, proporciono y detallo las conclusiones y recomendaciones del presente informe de suficiencia profesional.

CAPITULO 1

ASPECTOS GENERALES

1.1. Definición del Problema

1.1.1. Descripción del Problema

La empresa Privada ubicada en Manuel Olguín 325, distrito Surco de la ciudad de Lima, tiene a todos sus colaboradores trabajando en varios lugares dentro del Perú con el acceso remoto debido a la pandemia por el Covid - 19, el colaborador se conecta remotamente a la red interna de la empresa privada mediante una red pública utilizando un método de acceso remoto básico y antiguo el cual consiste en registrar el nombre del usuario y su respectiva contraseña en un software que tiene nombre Anydesk, Team Viewer y una red privada virtual SSL mediante un agente Check Point sin contar con algún mecanismo de seguridad informática como un doble factor de autenticación, el mecanismo de acceso simple que tiene en operación es un método de acceso remoto muy básico que nos lleva a tener altos riesgos de seguridad debido a que no brinda seguridad de que la información enviada y recibida no puedan ser vulnerada y alterada mediante la red pública.

Durante el proceso de acceso remoto de mecanismo simple el colaborador utiliza contraseñas de baja complejidad debido a que no usa en sus contraseñas caracteres especiales y esto ocasiona un problema a nivel de seguridad informática ya que logra facilitar a terceras personas obtener o adivinar la contraseña mediante métodos conocidos como por ejemplo ataque de fuerza bruta.

Algunos colaboradores informaron que durante sus vacaciones la primera semana del mes de mayo del año 2021 otros usuarios le reportaron y avisaron al colaborador de que ellos han estado recibiendo correos desde su cuenta de empresa a pesar de que el usuario no utilizó su laptop durante la semana reportada, lo indicado muestra el bajo nivel de seguridad que se tiene por mejorar.

El colaborador se conecta remotamente a la red de la empresa privada usando varios dispositivos diferentes entre ellos laptop asignada de la empresa, laptop propia, laptop compartida entre sus familiares, y celulares, en donde se observa que se utiliza varios dispositivos sin tener al menos un software que permita controlar el acceso de tipo de dispositivo generando un riesgo alto a nivel de seguridad informática y el riesgo que en cualquier momento una infección del dispositivo debido a que este dispositivo puede recepcionar la información manipulada, descargar cualquier tipo de documento que contenga algo malicioso e infectar al dispositivo y a su red interna.

1.1.2. Formulación del Problema

En el presente trabajo se plantea el problema general siguiente:

Determinar de qué manera la implementación de una solución remota con doble factor de autenticación y control de acceso de dispositivo logrará incrementar la seguridad informática de la empresa privada durante la Pandemia del Covid-19.

1.2. Definición de objetivos

1.2.1. Objetivo general

Implementar una solución remota con autenticación de doble factor y control de acceso de dispositivo para incrementar la seguridad informática de la empresa Privada durante la Pandemia covid-19.

1.2.2. Objetivos específicos

Los objetivos específicos que considero en mi presente trabajo son los siguientes:

- ✓ Mejorar el proceso de autenticación de acceso de los usuarios que se conectan de forma remota.
- ✓ Mejorar el proceso de control de acceso de los dispositivos que se conectan de forma remota.
- ✓ Robustecer los mecanismos de acceso remoto para lograr mitigar los posibles incidentes de seguridad que se presentan diariamente en un acceso remoto.

1.3. Alcances y limitaciones

A continuación, presentamos el alcance y las limitaciones:

1.3.1. Alcances

El desarrollo de la implementación se realiza dentro de las instalaciones de las oficinas de la empresa privada la cual se encuentra ubicado en Manuel Olgúin 325, distrito Santiago de Surco, Departamento Lima, específicamente en el data center de la empresa privada. El objetivo es implementar una solución que brinde doble factor de autenticación y control de dispositivo con la finalidad de aumentar la seguridad mediante del acceso remoto a los diferentes recursos internos de la empresa privada.

La implementación busca robustecer el método de autenticación y mitigar cualquier tipo de intento de suplantación de identidad o robo de contraseñas a los usuarios. También se busca lograr tener un mejor control de acceso de dispositivos las cuales son implementados utilizando los criterios correctos y adecuados para establecer la conexión remota segura a los recursos de la empresa privada y lograr aumentar la seguridad informática.

La implementación también busca proteger todos los activos de la empresa Privada ante cualquier tipo de incidente de seguridad informática que se podría presentar en cualquier momento por medio del acceso remoto.

Se debe cumplir con las especificaciones técnicas de hardware del equipo firewall Palo Alto 3050 que es el equipo físico que sostendrá la nueva solución implementada, estas especificaciones técnicas se encuentran en el Anexo 1, 3 y 4.

El equipamiento firewall donde se implementará la nueva solución debe pertenecer a uno de los 4 primeros líderes del cuadrante de líderes de Gartner en tecnología firewall.

El equipamiento firewall Palo Alto debe soportar protocolos de autenticación Radius, uso de protocolos de seguridad como el SSL y TLS en todas las versiones que se tienen en el mercado de tecnología actual.

En el firewall Palo Alto 3050 es donde se implementa la VPN SSL Global Protect, en la cual se configura el Gateway, interfaces de red, rutas estáticas,

a nivel de Firewall, asimismo en la VPN se implementa los componentes las cuales son el Gateway público de la VPN, el portal de acceso, el agente VPN Global Protect en donde se activa y se debe utilizar la autenticación tipo Radius la cuál es un método de autenticación que se utiliza de forma dedicada para la presente implementación.

Los protocolos de seguridad y tipo de cifrado que utilizará el acceso remoto es decir la VPN SSL Global Protect cuando se integre al mecanismo de doble factor de autenticación deben ser SSL (Transport Layer Security) /TLS (Transport Layer Security) y el algoritmo de cifrado debe ser RSA tipo SHA 512 que permite mayor longitud de cifrado de la data.

Los criterios técnicos de alto nivel en el perfil de identificación de host que proporciona el mecanismo de control de acceso de dispositivo, estos criterios deben ser que el dispositivo (Laptop) debe tener instalado y activo un antivirus, un antimalware y tener un día del último escaneo realizado, además de contar con todos los parches de Windows instalados, tener habilitado el DLP y cifrado de disco duro a nivel de laptop de usuario.

La nueva solución implementada debe tener el uso exclusivo y dedicado para la utilización del acceso remoto de todos los colaboradores de la empresa privada, considerando que el firewall Palo Alto 3050 será un equipo de seguridad dedicado para el uso de la VPN SSL.

Se debe utilizar una tecnología de fabricantes líderes en el mercado a nivel de firewall que permiten conexiones remotas y la solución debe soportar como mínimo 800 conexiones remotas seguras con capacidad de almacenar 1 TB de registros detallados de la conexión remota

La solución debe cumplir en identificar y restringir el acceso remoto a nivel de usuario a los distintos recursos informáticos de la empresa privada y mediante el control de perfiles de usuario y acceso a ciertos recursos específicos. Con la implementación de la solución planeada permite reducir el riesgo de acceso remoto no autorizado de terceros a los recursos informáticos de la empresa.

La solución debe soportar mecanismos de autenticación de integración basados en nube como Microsoft Azure, Duo Cisco, RSA Secure ID entre otros disponibles en el mercado tecnológico.

1.3.2. Limitaciones

Se tiene las siguientes limitaciones:

- ✓ La implementación no incluye establecer o elaboración de nuevos controles o políticas a nivel de seguridad de información de la empresa Privada.
- ✓ El implementador durante el soporte de 1 mes revisará registros o errores desde la consola de administración de la nueva solución no incluye asistir a cada usuario que presente problemas, pero si apoyará al recurso de mesa de ayuda a solucionar algún problema crítico que se presente con algún usuario como se indica no tendrá contacto directo con el usuario final, pero si con mesa de ayuda de la empresa privada.
- ✓ La implementación no incluye elaborar algún inventario de los dispositivos, debido a que el inventario de dispositivos lo debe administrar el personal de mesa de ayuda de la empresa privada.
- ✓ La implementación no contempla solucionar problemas de los usuarios con su conexión a internet ya que no corresponde.
- ✓ La empresa privada no permite facilitar y mostrar el evolutivo de ventas durante el año 2021 por políticas internas de la empresa para mostrar la estabilidad y sostenibilidad brindada de la nueva solución implementada en ventas a nivel global de la empresa, sólo permite mostrar las carpetas de los proyectos desarrollados durante el año 2021.
- ✓ Debido a que sólo se tiene disponible un equipo firewall Palo Alto en donde se realiza la implementación, no se podrá configurar la función de alta disponibilidad de equipamiento firewall debido a que la empresa privada no tiene dos equipos firewall disponibles.

1.4. Justificación

La presente implementación propone mejorar el acceso remoto seguro de una empresa privada, la cual comprende de una solución de doble factor de autenticación y control de dispositivo para mejorar e incrementar la seguridad informática del acceso remoto a los recursos internos de la empresa con esta implementación se logrará disminuir y mitigar las posibles vulnerabilidades y riesgos que se ubican actualmente presentes en el proceso de acceso remoto.

La empresa cuenta con recursos internos como servidores web, ftp entre otros equipos de red y seguridad que son parte importante de la infraestructura de red de la empresa como activos primordiales las cuales se necesita proteger en todo momento.

La implementación busca robustecer el método de autenticación y mitigar cualquier tipo de intento de suplantación de identidad o robo de contraseñas de los usuarios.

Se busca tener un mejor control de acceso de dispositivos las cuales son implementados con los criterios correctos y adecuados para establecer la conexión remota segura y robusta a los recursos de la empresa.

Con la nueva implementación realizada la empresa la utilizaría como servicio principal y dedicado para la conexión remota segura de todos sus colaboradores, a nivel económico la nueva solución brinda una buena estabilidad de mantener muy activas las operaciones de ventas y posventa que permitirá a la empresa mantener e incrementar su flujo de ingreso económico por renovaciones, ampliaciones y nuevos proyectos tecnológicos, existe un beneficio de ahorro de gastos que incurren a mantenimiento de su infraestructura física del local de la compañía como por ejemplo gastos de luz, agua y áreas compartidas utilizadas anteriormente por los colaboradores, en el aspecto de salud con la solución implementada permite que todos los colaboradores utilicen el teletrabajo de forma constante y segura con la cual se protegen y disminuyen el riesgo de contagio de covid-19 debido a que utilizar la nueva solución implementada evita que acudan a las oficinas de la empresa privada logrando realizar sus actividades laborales cotidianas con el mínimo riesgo que un colaborador se contagie con el covid-19, adicional permite ahorro económico como gastos de pasajes y

gastos en almuerzos y refrigerios incluso ahorro de tiempo que se pierde durante horas que soportamos del tráfico de tránsito de las calles de Lima.

Como justificación tecnológica el utilizar una solución de alto nivel de seguridad informática empleando equipamiento y software pertenecientes a fabricantes líderes del mercado e implementarlos con criterios técnicos de alto nivel nos coloca en estar a la vanguardia tecnológica permitiéndonos tener alto nivel tecnológico de seguridad informática al igual que empresas importantes en el mundo que planifican desde el inicio de la compañía el área de seguridad informática, asimismo mencionar como punto alto materializar la solución propuesta en la empresa privada permitirá tener una sólida reputación permitiendo mejorar notoriamente la reputación de la empresa privada.

1.5. Estado del Arte

Desde que inició la pandemia COVID-19 y las declaraciones de cuarentena en todos los países, las empresas y entidades a nivel global han tenido la obligación de adaptarse rápidamente al cambio de modalidad del teletrabajo o home office para resguardar la salud de sus trabajadores.

Lo que conocíamos que estaba controlado a nivel de seguridad informática en la infraestructura de cada organización, hoy en la actualidad se ha perdido ante un cambio muy rápido y drástico originado por la pandemia del COVID-19, esto provoca que los ciberatacantes se encuentren aprovechando el pánico para encontrar vulnerabilidades o huecos de seguridad para finalmente lograr su cometido, ya sea empleando las distintas técnicas como ingeniería social, ataques de spam, phishing, ransomware o la identificación vulnerabilidades al permitir a los usuarios el home office.

En el presente trabajo en relación a los autores que hago referencia logré observar que los objetivos se enfocan en combatir los posibles ataques que existen en la red informática para mejorar la seguridad informática además de aprovechar las diversas ventajas de las herramientas o soluciones de Red Privada Virtual que ayudan a mantener protegidos a los trabajadores y a la información no importando desde que lugar se conecten asimismo la solución significa una de las mejores opciones de acceso remoto seguro permitiendo un ahorro económico eso se logra evidenciar en los autores que investigué para el desarrollo de la presente implementación y en los próximos párrafos se detallará.

(Romero Del Carpio, 2018). Propuesta de seguridad informática para mejorar el proceso de acceso remoto en una entidad financiera.

Objetivo

Identifico que el objetivo del autor es brindar una propuesta tecnológica de seguridad informática que le permita optimizar el proceso de acceso remoto de todos los usuarios de una entidad financiera.

Conclusión

El estudio del autor logra permitir definir que una solución VPN SSL seleccionada permite lograr tener una justificación económica el cual permite brindar un ahorro financiero debido al costo menor que implica la implementación de la solución tecnológica a diferencia de la segunda opción estudiada y planteada el cual es una VPN tipo IPSEC, también determina que cuando agregamos un proceso de doble factor de autenticación a la solución seleccionada, esta solución logrará disminuir el nivel de riesgo en el acceso remoto, permitiéndonos cumplir el mejoramiento del proceso de acceso remoto.

Aporte al Proyecto

El estudio del trabajo mencionado aportó bastante conocimientos teóricos y técnicos sobre los distintos tipos de tecnologías de red privada virtual que se utilizan para el acceso remoto, lo mencionado me permitió un conocimiento más amplio sobre el tipo de tecnología de acceso remoto para seleccionar en mi presente trabajo, adicional también considero que en su análisis debió agregar alguna redundancia para cubrir el alta disponibilidad como por ejemplo considerar algún otro equipo firewall que funcione con alguna solución remota en caso exista algún problema con la solución propuesta y otra observación que considero es que debió abordar un poco más conceptualmente sobre el mecanismo de doble factor de autenticación.

(Martel, 2019). Diseño de una red de comunicación VPN sobre internet para un Distribuidor Autorizado de Claro basado en el RFC 2764.

Objetivo

El objetivo principal del trabajo presentado por el autor es permitir diseñar una red privada virtual que logre establecer una comunicación muy segura y en tiempo real para mejorar varios procesos existentes en la empresa Distribuidor Autorizado de claro, la solución debe ser diseñada basado en RFC 2764.

Conclusión

El trabajo y aporte presentado por el autor logra concluir que implementando un buen diseño de red privada virtual como una solución que se emplea en una red de comunicación de acceso remoto es una de las mejores opciones de soluciones de tecnología ya que son bastantes flexibles y económicas para cualquier tipo de empresa que requiera contar con una comunicación fiable y segura con todos sus clientes, proveedores o distintas sucursales en comparación de las redes dedicadas las cuales son muy costosas.

Aporte al Proyecto

El trabajo realizado por el autor mencionado aportó bastante conocimiento teórico sobre varios tipos de red privada virtuales que se emplean para varias conexiones remotas y también su brinda conocimiento sobre la gran importancia de conocer sus características y que debemos siempre seleccionarlas cuando se proponga implementar alguna tecnología para las comunicaciones remotas seguras ya que permite beneficiarnos en el aspecto económico, adicional también observo que no consideraron en el diseño la función de alta disponibilidad.

CAPITULO 2

MARCO TEÓRICO

2.1.Fundamento teórico

A medida que las redes evolucionan logramos percatarnos que la Seguridad Informática es primordial hoy en día debido a la gran evolución de la ciberdelincuencia, es por ello de que es muy importante y relevante en la actualidad para cualquier empresa o entidad debido a que nos permiten proteger y resguardar en todo momento la información buscando sostener la disponibilidad, confidencialidad y su integridad.

A continuación, se desarrolla conceptos teóricos la cual se basa el presente trabajo relacionados a nuestra variable independiente que es la solución remota con doble factor de autenticación y control de acceso de dispositivo y también la variable dependiente el cual es la seguridad informática.

Detallaré conceptos teóricos de la solución remota Cisco Duo Security que una vez implementado permite brindar el doble factor de autenticación y en conjunto con la función HIP (Host Information Profile) implementada permite el control de acceso de dispositivo, ambas soluciones implementadas e integradas en el Firewall Palo Alto de la empresa privada permiten lograr cumplir con el objetivo propuesto de aumentar la seguridad informática.

2.1.1 Solución remota con Doble Factor de Autenticación y Control de Acceso de Dispositivo

2.1.1.1 Definición Nominal

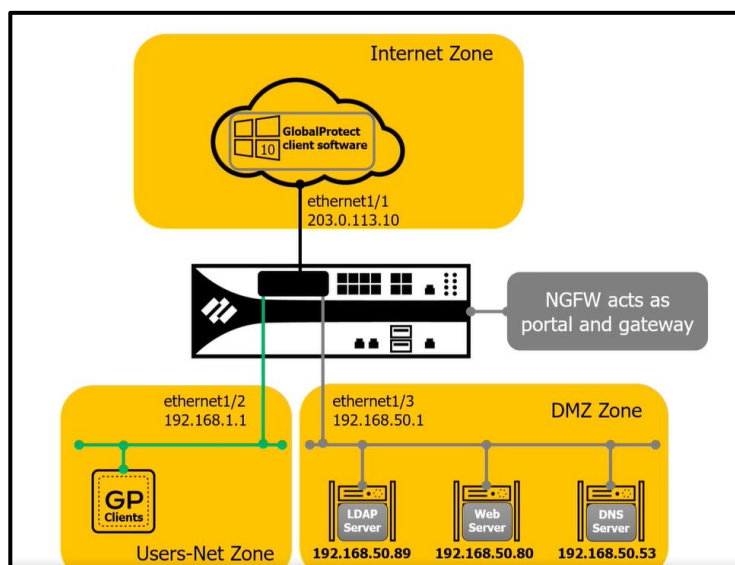
La solución remota de Global Protect se basa en una tecnología de seguridad móvil familiar la cual es la VPN SSL de acceso remoto, el agente de Global Protect asegura los niveles básicos de conectividad remota y permite integrar funciones adicionales como doble factor de autenticación la cual permite robustecer el mecanismo de acceso remoto a todos los recursos de la red local de la empresa privada.

Global Protect extiende los límites de la red física y en paralelo al mismo tiempo, establece un perímetro lógico que abarca a los usuarios de equipos tipo móviles y equipos remotos, independientemente de su ubicación. Cuando un usuario remoto inicia sesión en su dispositivo, Global Protect determina automáticamente el Gateway más cercano disponible para el dispositivo de itinerancia y establece una conexión segura mediante una autenticación sólida. Los dispositivos portátiles y móviles permanecen conectados a la red

corporativa en todo momento y están protegidos como si nunca hubieran abandonado físicamente su entorno corporativo.

Global Protect garantiza que las mismas políticas de habilitación de aplicaciones seguras que protegen a los usuarios en el sitio corporativo se apliquen a todos los usuarios, independientemente de su ubicación, brindando como resultado que se eliminen los desafíos operativos asociados con la creación y administración de políticas separadas para firewalls corporativos y usuarios remotos. Global Protect proporciona criterios de política para aplicaciones, usuarios y contenido.

Figura 1. Topología Global Protect



Fuente: Palo Alto Networks, 2021

El doble factor de autenticación es uno de los mecanismos de seguridad más importantes y emergentes en nuestra actualidad, se considera que la verificación del doble factor en estos momentos es sin duda alguna un mecanismo bien seguro para validar una identidad de cualquier persona y permite lograr garantizar una conexión con acceso remoto muy seguro a las cuentas de cada empresa, portales corporativos, redes sociales o alguna cuenta de correo electrónico personal.

El doble factor de autenticación (abreviado 2FA) llega ser un mecanismo que permite brindar al proceso de acceso remoto una capa adicional de nivel de seguridad, debido a que necesita que la persona se identifique de 2 maneras distintas, el primer paso es ingresando una contraseña y el segundo paso se elige entre varios tipos de acceso, por ejemplo, un código push de una aplicación, un código numérico o un SMS, en forma global

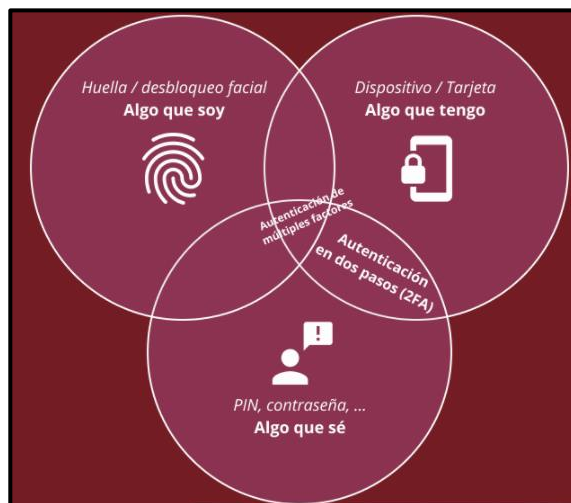
el proceso de doble factor de autenticación se encuentra enfocada a la validación unívoca de una identidad que a su vez se encuentra vinculada a “conocer algo” y “tener algo”.

Debemos considerar que usar el método doble factor de autenticación no resuelve todos los incidentes de seguridad que se presentan diariamente en un proceso de acceso remoto, pero si es considerado un excelente mecanismo que permite lograr proteger nuestras distintas cuentas de acceso que utilizamos a diario, las contraseñas que se vulneran normalmente son cuando el usuario elabora y elige contraseñas muy fáciles y débiles que generan que el atacante pueda tener un acceso no autorizado inmediato.

Este mecanismo de 2FA mitiga parcialmente los problemas que suelen tener los usuarios al momento de elegir contraseñas difíciles de recordar.

El doble factor de autenticación llega a ser una medida de seguridad muy relevante e importante hoy en la actualidad debido a que permite adicionar una segunda capa de protección a la contraseña que empleamos en la primera capa de acceso y cuando logramos agregar esta capa adicional de seguridad permitimos que el acceso remoto logre ser mucho más difícil para que un atacante pueda vulnerar las cuentas de acceso de los usuarios.

Figura 2. Autenticación Doble Factor



Fuente: A3sides Software Solutions,2020

2.1.1.2 Importancia de tener doble factor de autenticación

Puedo mencionar de acuerdo con mi experiencia que hasta el momento no existe algún mecanismo, proceso o sistema conectado a la red la cual es 100% seguro, pero si puedo mencionar que se ha logrado reducir gran parte de riesgo de robo de datos y mitigar varios incidentes de seguridad al lograr agregar un mecanismo adicional de seguridad como es el doble factor de autenticación.

El 2FA es un elemento fundamental de un modelo de seguridad de confianza cero y se utiliza para proteger los datos confidenciales y permite lograr verificar que los usuarios que intentan acceder a esos datos sean quienes dicen ser. También menciono que 2FA es una forma eficaz de protegerse contra muchas amenazas de seguridad que tienen como objetivo las contraseñas y cuentas de los usuarios, como suplantación de identidad, ataques de fuerza bruta, explotación de credenciales y más.

Es muy importante conocer que, al lograr integrar el doble factor de autenticación para sus aplicaciones, los atacantes no pueden acceder a sus cuentas sin poseer el dispositivo físico necesario para completar el segundo factor.

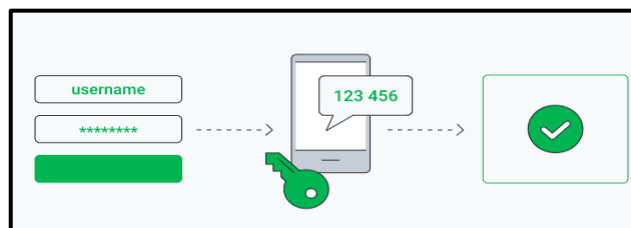
2.1.1.3 Funcionamiento del doble factor de autenticación

El doble factor de autenticación adiciona un mecanismo extra de seguridad a su cuenta, es decir, un paso adicional para iniciar la sesión y con finalidad de impedir que otras personas no autorizadas ingresen en ella, aunque tengan acceso de alguna forma a su contraseña.

Cuando inicia sesión en cualquiera de sus cuentas en línea, el nivel básico de autenticación solamente requiere la contraseña para iniciar sesión la cual es el primer paso para verificar la identidad, el 2FA incorpora otro dato adicional la cual es la segunda capa que sería un dato que el usuario debe conocer y facilitar para poder acceder a su cuenta.

El 2FA verifica un segundo dato aparte de la contraseña la cual se trata del tipo de información utilizada para la segunda parte de la verificación dependiendo del servicio en línea que emplee.

Figura 3. Funcionamiento de Autenticación Doble Factor



Fuente: Dúo de Cisco Systems,2021

Existen tres maneras distintas de activar el doble factor de autenticación:

1.-Por medio de un mensaje de texto. Es método más empleado y usual, adicional también lleva mucho tiempo empleándose en el mercado tecnológico.

2.-Por medio de aplicaciones o hardware dedicados, consiste en generar un número de codificación de validación descartable y válido por un corto tiempo por ejemplo 30 segundos, en la actualidad es una opción cada vez más popular debido a la practicidad empleada, para el caso de los hardware implican costo adicional, pero existen opciones como aplicaciones utilizadas en los smartphones como una aplicación dedicada de autenticación. Algunos ejemplos como: 2FAS Auth, Google Authenticator, Windows Authenticator entre otros.

3.-Por medio de las nuevas llaves de seguridad. En lo último del mercado se han elaborado un nuevo mecanismo de llave, asociado al estándar de seguridad FIDO U2F, el cual permite garantizar los altos niveles de seguridad informática, entre ellos tenemos a los que requieren una inserción en un puerto USB (universal serial bus) y también otros que funcionan con tecnología de comunicación de campo cercano, también llamado NFC (Near Field Communication) o mediante Bluetooth así como por ejemplo el Titan Security Keys de Google (la cual se puede emplear en móviles).

2.1.1.4 Riesgos de usar una sola contraseña

Podría ser que se encuentre preguntando ¿por qué debería usar el 2FA? o también otra pregunta como ¿No sólo bastaría con una contraseña para proteger las cuentas en línea que tengo? y finalmente nos preguntamos ¿nuestra contraseña es lo bastante segura? Esta interrogante nos hacemos debido a que los hackers pueden realizar distintos ataques de fuerza bruta o «spraying» (probar una lista con las contraseñas más habituales) para lograr descifrar fácilmente las contraseñas débiles.

Aunque también se debe tener en cuenta que, hasta una contraseña muy compleja, los hackers más habilidosos son capaces de averiguarla de varias formas:

-Filtraciones de datos: Sucede cuando una organización sufre un ataque de ciberseguridad, los nombres de usuario y las contraseñas (así como otros datos confidenciales) de millones de personas pueden terminar vendiéndose en la web oscura. Los ciberdelincuentes pueden adquirir listas de nombres de usuario y contraseñas, e intentar probarlas en toda la red para ver si con ellas pueden acceder a alguna cuenta. Por eso nunca se deben reutilizar las contraseñas para varias cuentas debido a que es considerada una mala práctica.

-Spyware: Este tipo de software malicioso es tan insidioso que es capaz de espiar a los usuarios. En general, es un software que registra las pulsaciones de las teclas capaz de guardar discretamente todo lo que usted escribe, nombres de usuario y contraseñas, para luego enviar esta información a los hackers que instalaron el malware en su dispositivo de forma oculta.

-Phishing: Es un tipo de estafa basado en la ingeniería social por la que los ciberdelincuentes suplantan un negocio o a una persona de confianza para lograr conseguir que revele su información personal. Consiste en recibir un correo electrónico falso donde se le pide confirmar su información como nombre de la persona con su respectiva contraseña de algún servicio en línea que utilice y al escribirlas lo que sucede es que las credenciales se enviarían directamente al estafador.

Si su contraseña queda expuesta y acaba en manos de un hacker, pero si se utiliza el 2FA, manteniendo ese mecanismo de defensa nadie podrá vulnerar su cuenta. Por eso este tipo de autenticación es una medida de seguridad tan importante y potente.

Si bien la 2FA es mucho más segura que una contraseña, no es infalible al 100 % debido a que, por desgracia, en Internet no hay nada infalible, pero se debe considerar que casi ningún hacker elige de víctima a una persona particular, lo que realizan es buscar víctimas fáciles con una seguridad deficiente. Si dan con una persona con credenciales difíciles de descifrar, normalmente buscan otro objetivo más fácil justo por este motivo, la 2FA lo protege en la mayoría de los casos.

“Casi ningún hacker elige víctima a una persona particular. Lo que hacen, más bien, es buscar presas fáciles con una seguridad deficiente. Si dan con una persona con credenciales difíciles de descifrar, normalmente buscan un objetivo más fácil” fuente AVG Antivirus.

La mayoría de los hackers les da igual a quién estafan debido a que les importa es conseguir todo el dinero y beneficio que puedan sacar provecho. Por lo general casi todos los ciberdelincuentes tratan de maximizar sus beneficios sin que nadie los detecte es por ello invertir demasiado tiempo y esfuerzo en una sola persona no tiene mucho sentido, pero en caso se trate de una persona famosa o es millonario, sólo en este caso sí es necesario invertir en protocolos más seguros que este como por ejemplo la adquisición de un hardware dedicado, pero para el caso de cualquier ciudadano que no es famoso o público el 2FA proporciona un nivel de seguridad considerable.

2.1.1.5 Doble Factor de autenticación con Cisco Duo Security

Cisco Duo Security, ofrece una solución de acceso confiable, potente y sin interrupciones. Una que es fácil de uso para el usuario y lo suficientemente potente como para proteger lo que más importa.

Esta solución de seguridad ayuda a defenderse de las brechas de datos al facilitar la implementación y aseguramiento efectivo de las políticas y procesos nivel de seguridad informática. Esta propuesta de CISCO DUO ofrece la solución de seguridad adecuada para proporcionar acceso confiable a escala.

La plataforma de acceso confiable propuesta es una solución de seguridad integral que reduce el riesgo de brechas de datos causadas por credenciales comprometidas y vulnerabilidades conocidas a través de una fuerte autenticación de dos factores (2FA). El 2FA perfectamente integrado verifica a los usuarios, luego verifica en sus dispositivos el software desactualizado, los certificados de seguridad faltantes y otras características. Puede restringir fácilmente el acceso a cualquier dispositivo arriesgado o no confiable, manteniéndolo al negocio más seguro.

El 2FA de DUO establece confianza en las identidades de los usuarios y protege a cada usuario con una experiencia confiable y fácil de usar. Esta solución lo ayuda a identificar y administrar:

- **Usuarios de confianza:** Verifica fácilmente las identidades con 2FA, aplique políticas de acceso de usuarios y brinde soporte a cada usuario.
 - Se obtiene un inicio de sesión fácil con un solo toque en la aplicación Duo Mobile a través de método Duo Push.
 - Admite múltiples métodos de autenticación, incluidos U2F, contraseñas de SMS, OTP móvil, devolución de llamada telefónica y tokens de seguridad.
 - Se integra con proveedores de identidad de terceros, como AD, OneLogin, Okta y Ping. Admite múltiples protocolos de autenticación, como LDAP, SAML y OIDC.
- **Dispositivos de confianza:** Verifica el estado de todos los dispositivos y aplica políticas de acceso a dispositivos.
 - Comprueba si hay sistemas, navegadores, certificados y complementos desactualizados.
 - Alerta para dispositivos roteados o liberados.

- Bloquear, notificar y restringir el acceso de usuarios con dispositivos riesgosos.
- Solicita a los usuarios que actualicen los dispositivos para mejorar el cumplimiento y el rendimiento.
- **Cada aplicación:** Proporciona acceso seguro a cualquier aplicación y aplica políticas de acceso a estas.
 - Integración con aplicaciones locales.
 - VPN seguras y puertas de enlace de acceso remoto.
 - Proporcione soporte nativo para proteger aplicaciones en la nube.
 - Conecte a los usuarios a aplicaciones web locales sin una VPN.
 - Controla aplicaciones internas accesibles para usuarios remotos.
 - Proporcione un portal web único con SSO.

2.1.1.6 Control de acceso de Dispositivo con Host Information profiles (HIP)

Los perfiles de Host Information profiles (HIPs) configurados para el acceso remoto con la red privada virtual Global Protect permiten verificar a cada dispositivo para permitir garantizar cumplir los requisitos internos de la empresa privada, por ejemplo si están instalados los últimos parches de seguridad de Windows, si las firmas de antivirus se encuentran actualizadas al día, si el usuario se encuentra conectado desde wifi o desde red cableada y también si el cifrado de disco está habilitado o si el software de cifrado de disco de la marca específica se encuentra instalado.

De forma predefinida, el agente de Global Protect permite registrar y recopilar datos detallados del proveedor a la cual pertenecen los paquetes de seguridad del usuario final que se ejecutan en la laptop del usuario y según la información recopilada lo siguiente es enviar toda esta información al Firewall Palo Alto mediante la VPN SSL GlobalProtect para permitirle el control mediante la aplicación de políticas de seguridad.

El agente Global Protect recopila información sobre categorías de forma predeterminada, para ayudar a identificar el estado de seguridad del dispositivo del usuario:

-General: Información relacionado al host la cual corresponde al nombre del host, el nombre del dominio de inicio de sesión, el sistema operativo y la versión del agente.

-Gestión de parches: Corresponde a la información sobre cualquier software de administración de parches que esté habilitado e instalado en el dispositivo del usuario y si están faltando algunos parches de seguridad.

-Firewall: Información sobre cualquier firewall de cliente de cualquier fabricante que se encuentre instalado y/o habilitado en el dispositivo del usuario.

-Antivirus: Permite mostrar la información sobre cualquier antivirus que se encuentre habilitado e instalado en el dispositivo del usuario, ya sea que la protección en tiempo real esté habilitada o no, la versión de la definición de virus, la última hora de escaneo, el fabricante y también el del producto.

El acceso remoto mediante la VPN SSL GlobalProtect utiliza la tecnología OPSWAT para detectar y evaluar aplicaciones de seguridad de terceros en el punto final. Al integrarse con el marco OPSWAT OESIS, GlobalProtect le permite evaluar el estado de cumplimiento del punto final. Por ejemplo, permite definir varios objetos y perfiles HIPs la cual verifican la presencia de una versión específica de un software antivirus, también de un fabricante específico de un agente endpoint y permite asegurarse de que tenga las firmas de definición de virus más recientes.

-Antispyware: Proporciona información sobre cualquier software anti-spyware que se encuentre habilitado y / o instalado en el dispositivo del usuario, también que la protección en tiempo real esté habilitada o no, la versión de firmas de virus, también la permite recopilar información de la hora del último escaneo, el fabricante y el nombre del producto.

-Copia de seguridad en disco: Permite recopilar información relacionado al software que gestiona las copias de seguridad, si está instalado, en ejecución y también permite validar la última fecha que se realizó una copia de seguridad, el nombre del fabricante y del producto del software instalado en el dispositivo del usuario.

-Cifrado de disco: Proporciona información en relación si el software de cifrado de disco se encuentra instalado y activo, qué unidades se encuentran cifradas y las rutas que se encuentran configuradas para el cifrado, el nombre del fabricante y del producto del software instalado en el dispositivo del usuario.

-Prevención de pérdida de datos: Información relacionada al estado del software de DLP o es decir prevención de pérdida de datos, específicamente si está instalado y activo para no permitir que la información privada confidencial salga de la red local de la empresa o

se almacene en un equipo potencialmente inseguro y peligroso. Esta información solo se recopila de los clientes de Windows.

-Dispositivos móviles: Proporciona la información sobre el equipo móvil, incluye el nombre del dispositivo, el nombre de dominio de inicio de sesión, el tipo de sistema operativo, la versión de la aplicación y la información de la red del dispositivo móvil al que está conectado. Adicional, Global Protect recopila si el dispositivo está roteado o liberado.

Puede excluir algunas categorías de información en caso para algún caso no fuese necesario recopilar en ciertos dispositivos (para ahorrar recursos como ciclos de CPU y mejorar el tiempo de respuesta del cliente), para realizar esto se procede a crear una configuración de cliente en el portal excluyendo las categorías que no le interesan.

2.1.1.6.1 Objetos y Perfiles HIP

Cuando el agente Global Protect logra obtener información sobre el detalle de información recopilada de la configuración del usuario descargado del portal, el paso siguiente será definir los atributos del dispositivo el cual se encuentre interesado en monitorear y emplearlo para aplicar de políticas de seguridad mediante la creación de objetos HIP y perfiles HIP en los Gateway:

-Objetos HIP: Permite facilitar los criterios de coincidencia para lograr filtrar la información del host más relevante, la información que más interesa utilizar para hacer cumplir en una política de seguridad en el firewall para la conexión de acceso remoto. Por ejemplo, si bien los datos sin procesar del dispositivo pueden brindar detallada información sobre varios paquetes antivirus que se encuentra instalados y activos, es posible que solo se encuentre interesado en una aplicación específica que necesite cumplir dentro de la empresa, para este escenario crearía un objeto HIP para que coincida con la aplicación específica que le interesa aplicar el control de acceso, adicional permite flexibilidad de poder crear una política de seguridad de HIP muy granular y muy poderosa.

-Perfiles HIP: Denominamos perfil HIP a un determinado grupo de objetos HIP que se evaluarán todos juntos las cuales se pueden usar para monitoreo o para la aplicación de políticas de seguridad. Cuando se crea los perfiles HIP permite combinar los objetos HIP que elaboró anteriormente (así como otros perfiles HIP) utilizando la lógica booleana, de tal forma que cuando se evalúe un flujo de tráfico con el perfil HIP resultante, logrará coincidir o no y cuando sucede una coincidencia procederá aplicar la regla de política de

seguridad correspondiente, pero en caso de que no existe coincidencia del perfil creado, el flujo se evaluará con la siguiente regla y de no existir regla de seguridad la conexión de acceso remoto no será permitido.

Estos perfiles HIP permiten al registro HIP Match ser un buen recurso para monitorear el estado del dispositivo que ingresan mediante el acceso remoto en su red a lo largo del tiempo.

2.1.1.6.2 Notificaciones HIP

Los usuarios finales no reciben información sobre las decisiones de política que se tomaron al interno de la compañía sobre la existencia una política de seguridad que se encuentra habilitada para HIP. La función de notificación HIP permite habilitar esta funcionalidad definiendo los mensajes HIP para que se permita visualizar a los usuarios cuando un perfil de HIP en particular coincide y / o no coincide.

Por ejemplo, puedo crear un perfil HIP para la coincidencia de que contengan instalados un antivirus y un antimalware de un fabricante específico y agregar la notificación para aquellos que no coincidan mencionándoles la política de la empresa y explicarles el procedimiento para realizar la instalación de los softwares requeridos para la conexión de acceso remoto.

2.1.1.7 Dimensiones

“Las soluciones de acceso remoto como la red privada virtual consisten en hardware y software, y además requieren otro conjunto de componentes. Estos componentes son simples requisitos que garantizan que la red sea segura, este disponible y sea fácil de mantener” R. Nader Carreón (2007).

La solución remota con doble factor de autenticación y control de dispositivo brinda lo siguiente:

-Disponibilidad: Se brinda tanto al tiempo de actualización de la conexión remota como al de control de acceso VPN, la solución remota Global Protect con doble factor de autenticación y control de dispositivo permite siempre estar conectado en todo momento desde cualquier ubicación geográfica con acceso a internet, adicional se tiene una solución de VPN SSL por medio del firewall Check Point que no tiene doble factor de autenticación pero se encuentra disponible la cual se encuentra como contingencia cumpliendo la función de alta disponibilidad del servicio de red privada virtual SSL.

-Compatibilidad: Empleando la tecnología de red privada virtual SSL Global Protect e internet como un canal de transporte, la topología interna del protocolo de red de la empresa privada es compatible con la IP Nativa de internet, asimismo la solución propuesta es compatible con los distintos dispositivos que un usuario utiliza para una conexión de acceso remoto.

-Seguridad: Llega a ser lo principal en la solución implementada, desde que inicia el proceso del cifrado que se configura como el uso de protocolos de autenticación en donde se utiliza algoritmos hash como sha256 o MD5 las cuales garantizan una conexión cifrada y el mecanismo de autenticación que se implementa, las firmas digitales y también las entidades emisoras de certificados que se utiliza, la cual constituyen una seguridad robusta.

También permite el control de acceso de dispositivo con la función de HIP profile el cual logra reducir la exposición al riesgo en el proceso de transmisión de la información por el acceso remoto utilizando la conexión VPN SSL Global Protect.

-Escalabilidad: En la actualidad el desarrollo a gran escala de redes informáticas como el Internet permite que la empresa privada logre tener presencia en cualquier lugar. Lograr independizar el de acceso remoto permite escalar el ancho de banda de la red de acuerdo con la necesidad del usuario, adicional la escalabilidad de la red no incide en su gestión y operación de la propia solución implementada debido a que la red WAN es netamente responsabilidad del proveedor del servicio.

A medida que la solución desarrollada que va creciendo e incrementando la cantidad de usuarios se adapta fácilmente para satisfacer las necesidades incluso de la base de usuarios más grande y diversa. Con información intuitiva del dispositivo para los administradores, es fácil obtener una visión clara de la postura de seguridad de su red y dispositivos.

2.1.2 Seguridad Informática

2.1.2.1 Definición Nominal

La seguridad informática surge ante una necesidad a causa de los constantes cambios en el medio productivo, educación entre otros, también en la manera de cómo en la actualidad en nuestra sociedad la transformación digital ha evolucionado constantemente.

En la actualidad la información se transformó en un activo muy importante dentro de una organización y para lograr mantener los datos salvaguardados se debe invertir económicamente en este tipo de seguridad, la seguridad informática se emplea para proteger la información, también se responsabiliza en detectar y prevenir el uso no permitido y autorizado de un sistema informático.

La Información es un activo que tiene un valor bastante importante para una empresa u organización, por la cual debe ser bien protegida y también la información es algo que se elabora, almacena, procesa, también puede ser transmitida y usada, así como puede ser destruida, corrupta y extraviada.

Figura 4. Ejemplos de Información

-Informes	-Contraseñas
-Manuales	-Códigos de Programación
-Patentes	-Información de clientes
-Documentos	-Información de mercado
-Libros	-Correspondencias
-Líneas de comando	-Reportes Financieros
-Archivos de configuración	-Plan de Negocios de la empresa
-Planillas de sueldo de los empleados, etc.	

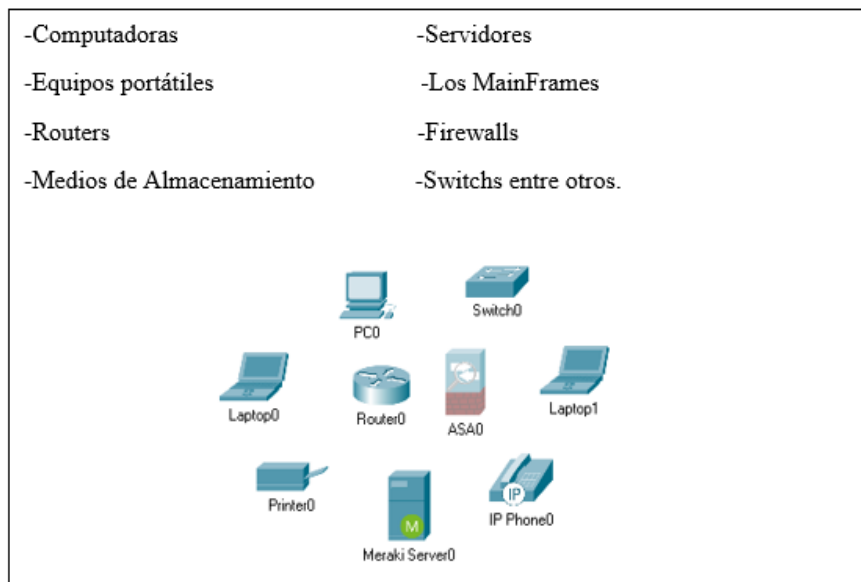
Fuente: Elaboración propia,2021

Previo a definir seguridad informática, es muy indispensable y fundamental conocer el siguiente concepto: **la informática.**

La Informática llega a ser una rama de la Ingeniería que se enfoca en realizar el estudio y análisis del hardware, redes informáticas de datos y los distintos softwares que son muy necesarios para automatizar la información que utilizamos a diario.

- **Hardware:** Es una parte física del dispositivo, ordenador, laptop, tablet, smartphones, entre otros, todos ellos están compuestos internamente por elementos electrónicos que se integran para permitir su funcionamiento.

Figura 5. Ejemplos de Hardware



Fuente: Elaboración propia,2021

- **Software:** Son todos los programas, reglas informáticas entre otros, que proporcionan la ejecución de varias tareas que puede realizar un ordenador.

La seguridad informática es responsable de buscar, detectar y localizar el empleo indebido de cualquier sistema informático cuyo fin es salvaguardar la privacidad e integridad de la data almacenada.

La seguridad informática es el encargado de implementar técnicas y controles de seguridad para proteger los datos, las cuales que pueden ser por ejemplo: antimalware, antivirus, firewalls, detección de intrusos, detección de anomalías en la red, correlación de eventos informáticos, atención de incidentes u otros controles que tienen una dependencia del usuario como la activación o desactivación de algunas características o funciones del software como por ejemplo ActiveX, Java para permitir asegurar el uso de la laptop, los recursos de red o del Internet.

La seguridad informática en todo momento busca siempre lograr que la información sea confiable, integra y disponible debido a que los datos corporativos son los activos más importantes de cualquier empresa y en todo momento se encargan de invertir en un sistema de gestión muy seguro que permitan garantizar su máxima protección.

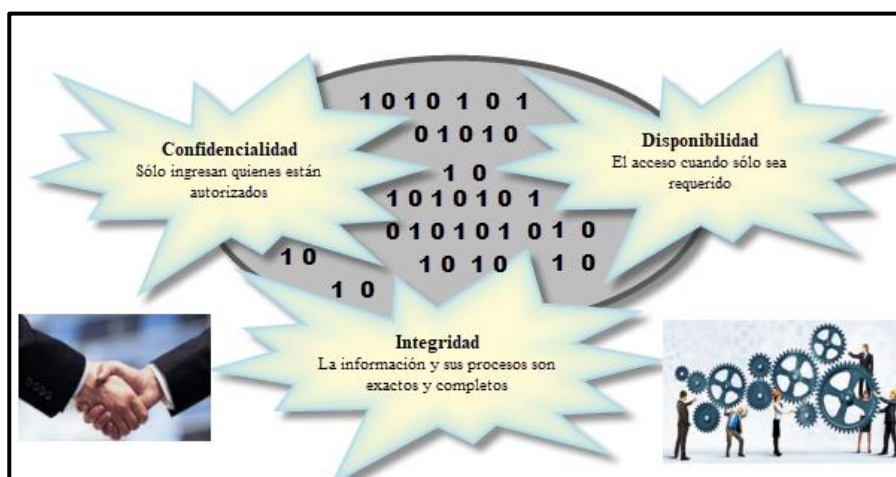
2.1.2.2 Principios Fundamentales de Seguridad Informática

Confidencialidad: La confidencialidad de la información tiene como objetivo de permitir asegurar que sólo la persona correcta acceda a la Información que se quiere utilizar o distribuir.

Integridad: Es lograr garantizar que sólo los usuarios autorizados puedan hacer modificaciones en la forma y contenido de una información, así como en la infraestructura en el cual la misma es almacenada y por el cual circula, asegurando que todos los elementos del conjunto del sistema se encuentren modificados a excepción que sean alterados por los usuarios autorizados.

Disponibilidad: En todo momento la información debe ser accesible de forma muy segura para que se pueda utilizar en un momento necesario en el que se solicita y que se garantice su integridad y confidencialidad.

Figura 6. Principios Fundamentales de Seguridad Informática



Fuente: Elaboración propia,2021

Es primordial e imperativo contar con un software y un hardware siempre disponible, de tal manera que reducimos los tiempos inactivos y lograremos evitar grandes pérdidas financieras, daños físicos y en el peor de los escenarios alguna posible amenaza que atente contra alguna vida humana.

2.1.2.3 Acerca de Seguridad Informática

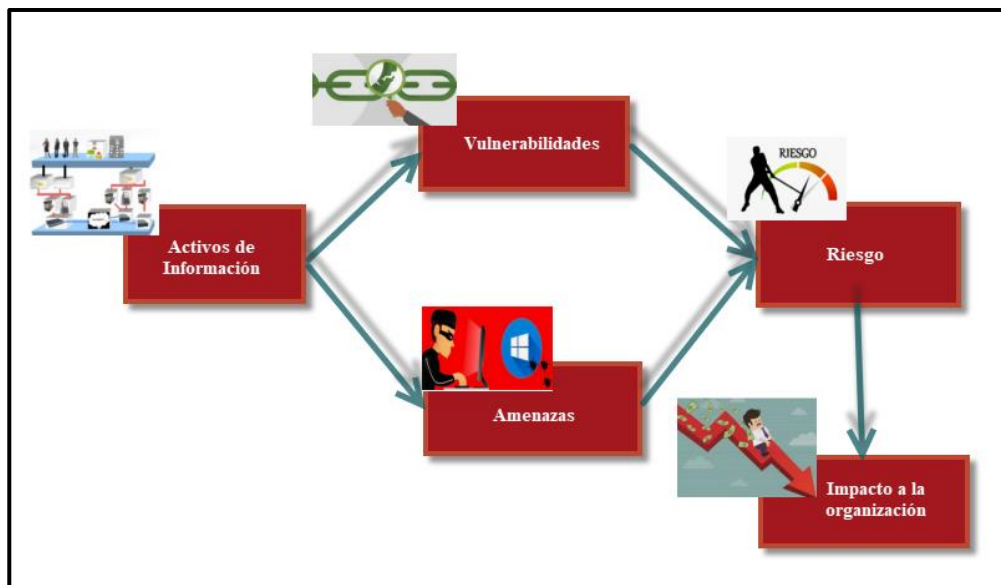
La seguridad informática protege a los activos de información de un gran y amplio mundo de amenazas para asegurar la continuidad de operación de una organización, aumentar la

seguridad informática y lograr minimizar los daños de una organización en caso de alguna pérdida, divulgación o modificación no autorizada.

¿Por qué es necesaria la Seguridad Informática?

Es necesaria para resguardar los activos de información.

Figura 7. Riesgos de activos de información



Fuente: Elaboración propia,2021

Recursos Por Proteger: La información es un activo de vital importancia dentro de una organización, tiene bastante valor para las organizaciones y requiere de protección robusta y adecuada.

La información puede ser de diferentes formas:

- Almacenada electrónicamente.
- Impresa o escrita en papel o digital.
- Reproducida en video.
- Distribuida por correo o email.
- Hablada en conversación o sesión remota.

2.1.2.4 Amenazas Informáticas:

Normalmente se valida publicaciones de noticias sobre ataques informáticos a la red de alguna empresa, la cual proporciona a los ciber atacantes el acceso a los datos personales del usuario y de la compañía de miles de usuarios afectados, debido a ello la seguridad informática de la organización siempre y necesariamente será una máxima y total prioridad para los administradores de red de cualquier compañía.

Seguridad de la red informática es un elemento fundamental como prioritario dentro del mundo informático, así ya fuese desde la red que está casa con alguna conexión a Internet o si también es una gran empresa con demasiados usuarios, la seguridad de la red informática siempre deberá considerar su entorno que lo rodea y también así como las distintas herramientas, procesos y requisitos de la red que se emplean, adicional una de sus funciones fundamentales es proteger la información y al mismo tiempo permite una buena calidad de servicio que cualquier usuario espera de la red informática.

Contar con una red bien segura y robusta involucra varios protocolos, dispositivos/elementos, tecnologías, técnicas, procesos y herramientas para cumplir el objetivo de proteger la información de la empresa o personal y mitigar las amenazas. Tener en cuenta que los vectores de amenazas pueden llegar a ser internos o externos y en gran parte de amenazas de seguridad en la actualidad se originan de las redes externas, hoy en día en Internet se encuentran múltiples amenazas externas ya conocidas:

-Virus: Es un tipo de software malicioso y este software contiene varios códigos que se ejecutan en un equipo de red de cualquier usuario cuya existencia tiene como objetivo lograr alterar el correcto funcionamiento de cualquier equipo informático de red sin contar con el permiso del propietario.

-Adware y Spyware: También es un software malicioso que al instalarse en el equipo informático permite recolectar todo tipo de información del usuario y lo realiza de forma minuciosa, en secreto y no visible para el usuario.

-Ataques de día cero: Son muy conocidos y populares hoy en la actualidad y también es conocido como tipo de ataque hora cero el cual consiste en producir el primer día y hora que se descubre la vulnerabilidad.

-Amenazas de Ciber atacantes: Sucede cuando una persona con mala intención realiza ataque a varios equipos informáticos y a sus recursos de red corporativa empleando cualquier tipo de herramienta para tener acceso a los dispositivos de cualquier usuario.

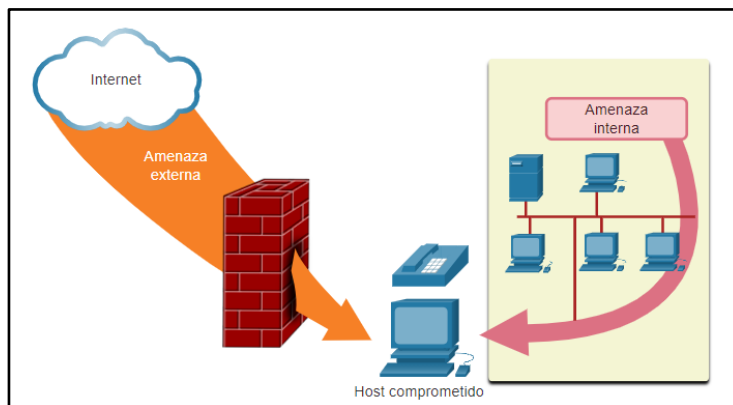
-Denegación de servicio: Es un tipo de ataque cuya finalidad es hacer que ralenticen o bloqueen las procesos y aplicaciones válidas en cualquier equipo de red, para afectar la disponibilidad de los recursos asignados.

-Robo e interceptación de Información: Es un tipo de ataque en donde se realiza la captura de datos privados de una red empresarial para finalmente comercializarla en la dark web y otros medios para obtener una finalidad que afecte a la empresa.

-Robo de identidad: Este tipo de ataque consiste en robar las credenciales acceso de sesión de cualquier persona para lograr acceder a su información y poder realizar alguna actividad maliciosa.

Debemos considerar como dato muy importante y resaltante a las amenazas internas debido a que varios estudios demuestran que las violaciones de seguridad más usuales son provocadas por el personal interno de la red en donde suceden los siguientes escenarios como son los equipos robados o perdidos y también al accidental o uso inadecuado por parte de personal interno e incluso empleados maliciosos. Hoy en día contando con la estrategia de BYOD, la información corporativa es mucho más vulnerable y sensible, actualmente para elaborar una política de seguridad, se debe considerar amenazas de seguridad internas y externas, como a continuación muestro en la figura 8.

Figura 8. Amenazas de Seguridad



Fuente: Cisco Systems,2021

2.1.2.5 Componentes de Seguridad Informática

No existe alguna solución tecnológica única que permita resguardar una infraestructura de red combatiendo contra todos los tipos de amenazas existentes esto quiere decir que las soluciones de seguridad deben implementarse considerando más de una capa de seguridad es decir usando varias soluciones tecnológicas de seguridad informática que permita

brindar seguridad y robustez cuya finalidad es proteger los datos del personal y de la empresa debido a que en caso algún equipo de seguridad no logre reconocer y proteger la red de la empresa, lo demás equipos informáticos de seguridad si puedan lograr tener éxito en identificar y proteger a la red corporativa.

Los elementos y dispositivos de seguridad para una red personal son los siguientes:

-Antivirus y antispyware: Son aplicaciones que permiten ayudar con la protección de los diversos dispositivos utilizados por los usuarios cuya finalidad es no infectarse con algún tipo de software o elemento malicioso.

-Filtrado de Firewall: Permite bloquear el ingreso no autorizado a la red interna ya sea de ingreso o salida de información.

Las redes informáticas hoy en día emplean varios filtros de antispyware, antimalware, antivirus y firewalls dedicados e incluso algunos firewalls tienen las características de las funciones incluidas en los firewalls y otros dedicados:

1.-Sistemas de firewall dedicados: Este sistema permite tener funciones de firewall mucho más avanzado la cual permiten analizar y filtrar demasiada cantidad de tráfico y con bastante particularidad y granularidad, hoy en día se utiliza bastante los firewalls de próxima generación entre los diferentes y principales fabricantes tenemos a Palo Alto Networks, Fortinet, Cisco, Check Point entre otros.

Figura 9. Cuadrante Mágico de Gartner de 2020 para firewalls de red



Fuente: Gartner, Agosto 2020

2.-Listas de control de acceso o también llamado ACL: Están enfocados en el acceso y en reenviar información en relación con las direcciones IP, servicios y aplicaciones no profundizan a una granularidad como un firewall.

3.-Sistemas de prevención de intrusiones o también llamado IPS: Este sistema se encarga de reconocer y bloquear los distintos tipos de amenazas que tienen rápida propagación, como por ejemplo los ataques de hora cero.

4.-Redes Privadas Virtuales o también llamado VPN: Este sistema proporciona acceso remoto de forma segura a los usuarios de una organización a su red interna, hoy en la actualidad se utiliza bastante la VPN SSL para el teletrabajo la cual este tipo de red privada virtual opera en la capa 7 del modelo OSI.

5.-Información de Seguridad y gestión de eventos (SIEM): Es un sistema de seguridad muy utilizado en la actualidad la cual permite proporcionar a una empresa una respuesta rápida, oportuna y precisa para lograr detectar, analizar y tomar una acción ante cualquier amenaza que se presente.

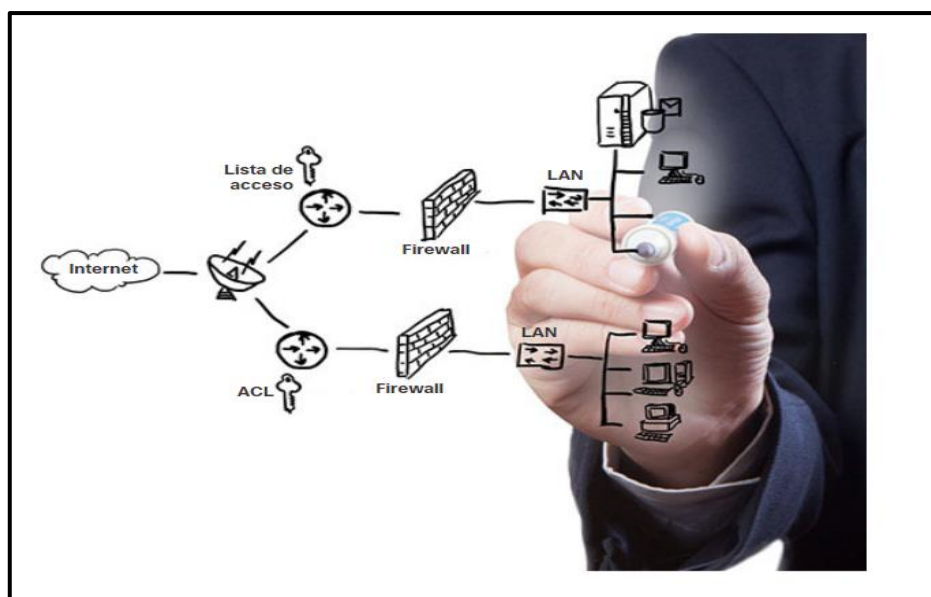
El análisis de los diferentes tipos de amenazas de seguridad de red informáticas y sobre las distintas técnicas de mitigación la cual debe iniciar con una comprensión muy clara de la infraestructura de red a nivel de switching y routing subyacente la cual en toda organización es empleada para organizar todos los servicios de red.

De acuerdo con lo publicado por ESET Security Report 2020 de Latinoamérica, menciona que un 61% de las empresas peruanas encuestadas afirmó que cuenta con políticas de seguridad; sin embargo, solo un 29% indicó que cuenta con un plan de respuesta y continuidad del negocio, y tan solo un 23% clasifica su información.

Adicional se tiene que las medidas más básicas de control, el cual se espera que la mayoría de las empresas la tengan implementada, como por ejemplo un antivirus, una copia de seguridad de información o un Firewall, la cual sorprende que no se encuentren implementadas en la totalidad de las empresas privada (78%, 62% y 62%, respectivamente).

Por otro lado, en relación con la Encuesta Global de Seguridad de la Información 2019-2020 de EY, pero solo el 27% de empresas en el Perú incluye la ciberseguridad o seguridad informática desde la etapa de planificación en sus nuevas iniciativas empresariales; mientras que un 51% sostiene que la relación entre la ciberseguridad y sus líneas de negocio es inexistente o neutral

Figura 10. Infraestructura de Servicios de Red.



Fuente: Cisco Systems,2021

2.1.2.6 Tipos de amenazas

Las redes informáticas tanto cableadas e inalámbricas son muy primordiales para las actividades diarias debido a que tanto las personas como las empresas en la actualidad dependen de la interconexión de las redes y equipos informáticos. Los ingresos no autorizados podrían ocasionar grandes degradaciones e interrupciones de servicio las cuales desencadenan pérdidas muy costosas para la red y también pérdida de trabajo. Los ataques a cualquier red informática suelen ser a gran escala y muy devastadores, también podrían dar como resultado una gran pérdida de tiempo y dinero a causa de daños ocasionados por el robo de información de activos muy valiosos y trascendentales de la empresa u organización.

El Perú sufrió más de 613 millones de intentos de ciberataques hasta junio del 2020, según la plataforma Threat Intelligence Insider Latin América de Fortinet, herramienta que se encarga de registrar y estudiar incidentes de ciberseguridad en todo el mundo.

En un último reporte de Junio de la muestra que el Perú sufrió más de 1.000 millones de intentos de ciberataques en el primer trimestre de 2021. La cifra total para el mismo período en la región de América Latina asciende a 7.000 millones de intentos de ciberataques, informó Fortinet.

Los ciberatacantes también podrían obtener cierto acceso a una red corporativa mediante vulnerabilidades, ataques dirigidos a hardware o tratando de adivinar el nombre de usuario

y contraseña de cualquier otro usuario, una vez que los atacantes logran tener el acceso pueden llegar a modificar o alterar el software o también explotando las vulnerabilidades de software si éste se encuentra muy desactualizado, una vez que el ciberatacante logra tener el acceso a la red privada, pueden suceder los siguientes tipos de amenazas:

Robo de información: Corresponde a intervenir o interrumpir en una computadora para lograr obtener información clave y confidencial por ejemplo: El sustraer información de una organización, así como son los datos de investigación y desarrollo entre otro tipo de información que son de alta importancia para la operación de cualquier empresa.

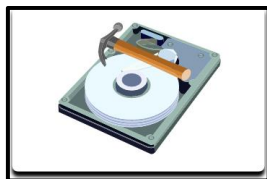
Figura 11. Robo de Información



Fuente: Cisco Systems,2021

Manipulación y pérdida de datos: Ocurre cuando el atacante ingresa en una laptop o computadora cuyo objetivo es destruir o modificar los registros de datos como por ejemplo, cuando un atacante que envía un malware o virus que ejecuta la acción de formatear o cifrar el disco duro de un dispositivo informático(computadora o laptop), otro ejemplo de manipulación de información es irrumpir dentro de un sistema de registros para alterar información, como un ejemplo puntual cuando realizan algún precio de un artículo en lugar de 500 nuevo soles a 1 nuevo sol.

Figura 12. Manipulación y perdida de datos



Fuente: Cisco Systems,2021

Robo de identidad: Es una forma de realizar una sustracción o robo de información en la que se extrae información tanto de la compañía como personal y el objetivo de apoderarse de la identidad de alguien o varias personas para que luego el ciberatacante pueda obtener información sensible como documentos legales, efectuar compras en línea no permitidas y solicitar algún crédito, en la actualidad lograr identificar un robo cibernético llega a ser

un problema creciente que cuesta dinero como miles de millones de dólares aproximadamente por año.

Figura 13. Robo de identidad



Fuente: Cisco Systems,2021

Servicio de Disrupción: Es la forma de lograr impedir que las personas legítimas puedan ingresar a todos los servicios disponibles a los que debe tener acceso, un ejemplo es un ataque de denegación de servicio o también llamado DoS a los servidores web o FTP, también otros equipos de red informática o enlaces de comunicaciones de red lo más empleado hoy en la actualidad.

Figura 14. Servicio de Disrupción



Fuente: Cisco Systems,2021

2.1.2.7 Tipos de vulnerabilidades

La vulnerabilidad es una manera de contar con uno o varios puntos débiles dentro de una red o un dispositivo. Normalmente una vulnerabilidad es inherente a los conmutadores, enrutadores, servidores y equipos de escritorio e incluso equipos de seguridad como firewalls, pero existe constantes ataques que van dirigidos a los dispositivos como los servidores y las computadoras o laptop.

En la actualidad existen 3 vulnerabilidades principales y conocidas como son: política tecnológica, de configuración y de seguridad. Las tres mencionadas son principales fuentes de vulnerabilidades que podrían dejar como consecuencia a una red o dispositivo abierto dejarlos expuestos a varios ataques, incluido a todo tipo de ataques de ya sea código malicioso y ataques de red.

2.1.2.7.1 Vulnerabilidades Tecnológicas

Tabla 1. Vulnerabilidades Tecnológicas

Vulnerabilidad	Descripción
Usar protocolo TCP/IP inseguro	-Por ejemplo, usar protocolos conocidos como FTP (File Transfer Protocol), HTTP (Hypertext Transfer Protocol) y también el Protocolo de mensajes de control de Internet también llamado ICMP, las cuales son inseguros. -También se incluyen los siguientes protocolos inseguros: SNMP -Simple Network Management Protocol y SMTP Simple Mail Transfer Protocol.
Debilidades existentes en los Sistemas Operativos	-Cada sistema operativo tiene varios problemas de seguridad que deben tratarse, estos sistemas operativos son Linux, Mac OS, Windows Server 2012, Windows 10 entre otros -Están debidamente documentados en el Equipo de respuesta ante emergencias informáticas (CERT), archivos en http://www.cert.org
Debilidad en los equipos de la infraestructura de red.	Todos los equipos de red, entre enrutadores, switch, firewalls entre otros tienen varias debilidades de seguridad que deben reconocerse y protegerse en contra. Entre sus debilidades conocidas son la protección con contraseña, protocolos de enrutamiento, falta de autenticación y agujeros de firewall.

Fuente: Cisco Systems,2021

2.1.2.7.2 Vulnerabilidades de configuración

Tabla 2. Vulnerabilidades de configuración

Vulnerabilidad	Descripción
Uso de cuentas de usuario inseguras	Los datos de la cuenta del usuario pueden transmitirse por la internet de forma insegura permitiendo exponer a los usuarios con sus respectivos nombres y contraseñas a ciberatacantes.
Usar las contraseñas fáciles de adivinar para las cuentas del sistema informático	Este problema común es el resultado de contraseñas de usuario mal creadas, por ejemplo: admin1, Password admin1
Los servicios de internet que se encuentren mal configurados	Por ejemplo, el tener activo el JavaScript en los exploradores web permite ciberataques mediante el control de JavaScript, esto es aprovechado por los ciberatacantes para lograr acceder a lugares que no son de confianza. Otros ejemplos de deficiencias de servicios mal configurados son FTP o servidores web (como son Microsoft Internet Información Servicios (IIS) y Apache HTTP Server).
Tener las configuraciones por default e inseguras dentro de productos	Debido a la facilidad de configuración que otorgan los fabricantes para las implementaciones de los diferentes equipos de seguridad informática, varios productos tienen configuraciones por default que se crean o habilitan agujeros en la seguridad.
Dispositivos de red mal configurados.	La configuración incorrecta de cualquier equipo informático puede ocasionar una inseguridad significativa en los equipos, como, por ejemplo: protocolos de enrutamiento incorrectos, listas de acceso mal configuradas o cadenas de comunidad SNMP en V2 pueden habilitar agujeros en la seguridad.

Fuente: Cisco Systems,2021

2.1.2.7.3 Vulnerabilidades de política

Tabla 3. Vulnerabilidades de política

Vulnerabilidad	Descripción
Políticas inseguras	No tener conocimiento correcto sobre seguridad informática pueden dificultar la elaboración de una política de seguridad coherente y segura.
Falta de seguridad en la autenticación	Las contraseñas mal creadas o elegidas son fácilmente descifradas y permiten el acceso no autorizado a la red corporativa.
No tener controles de acceso lógico.	Realizar el monitoreo y auditoría inadecuada es una falla que permiten ataques y accesos no autorizados cuyo resultado es desperdiciar los recursos de la empresa, también puede traer acciones legales o terminación contra técnicos de TI, administración de TI.
Cambios en los dispositivos que no respetan la política de seguridad	Son los cambios que no están permitidos en la topología de red y también se refiere a manipulación como una instalación de alguna aplicación o software no aprobada por las políticas de la empresa.
No contar con un plan de recuperación tras un desastre	No tener un plan de recuperación ante posibles desastres permite tener incertidumbre, caos, pánico y la confusión ante algún desastre natural o cuando un ciberdelincuente ataca a la red.

Fuente: Cisco Systems,2021

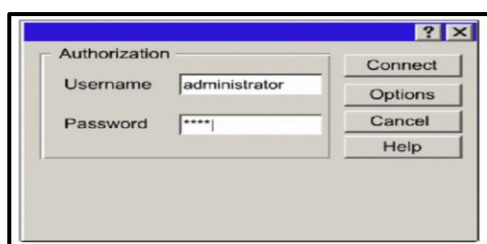
2.1.2.8 Tipos de Ataque de Acceso

Son las que explotan varias vulnerabilidades en varios servicios como el de autenticación, Web entre otros cuyo objetivo es lograr el ingreso a los diferentes tipos de cuentas Web, bases de datos las cuales tienen información confidencial y sensible. Una instrucción de acceso se puede clasificar de varios tipos:

2.1.2.8.1 Ataques de contraseña

Los ciberatacantes implementan ataques de contraseña empleando varios métodos diferentes y algunos conocidos como son por ejemplo ataques por fuerza bruta, ataques de caballos de Troya, programas detectores de paquetes entre otros.

Figura 15. Ataques de contraseñas

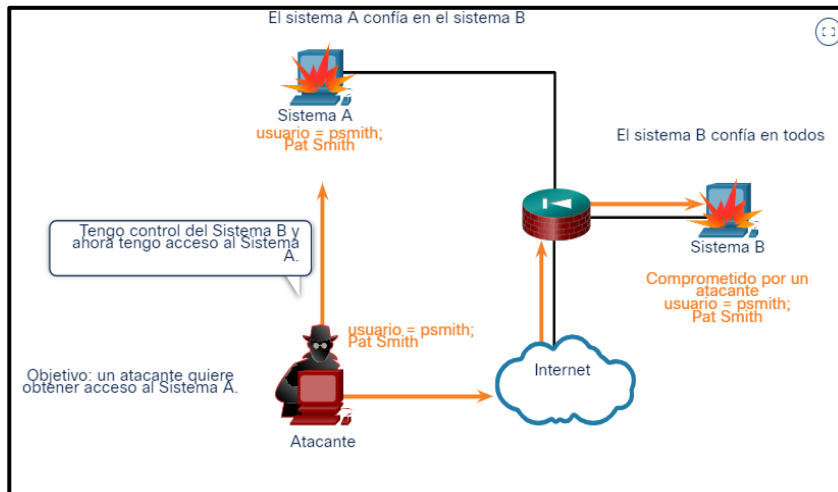


Fuente: Cisco Systems,2021

2.1.2.8.2 Explotación de confianza

Sucede cuando el atacante utiliza los privilegios no autorizados para permitirse el acceso a un sistema sensible y lograrlo comprometerlo. En la figura se muestra un ejemplo de ataque a un host de confianza.

Figura 16. Explotación de confianza

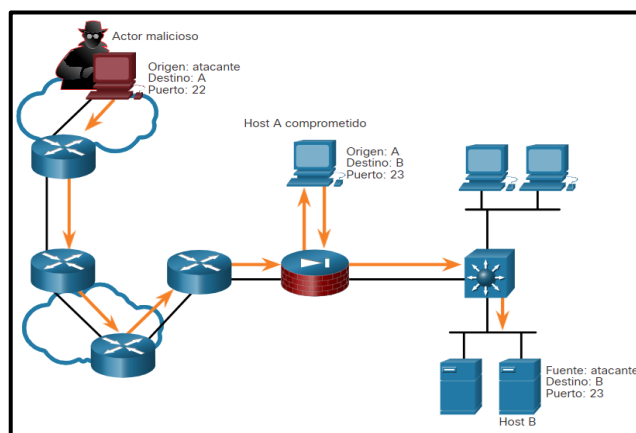


Fuente: Cisco Systems,2021

2.1.2.8.3 Redireccionamiento de puertos

Ocurre cuando el ciberatacante emplea un sistema vulnerable y lo utiliza como base principal para ataques contra otros objetivos que manejan información sensible. Un ejemplo es de imagen donde se muestra que un atacante usa SSH (puerto 22) para conectarse a un host A vulnerable. El host B confía en el host A y, por la cual el ciberatacante puede emplear un Telnet (puerto 23) para lograr ingresar.

Figura 17. Redireccionamiento de puertos

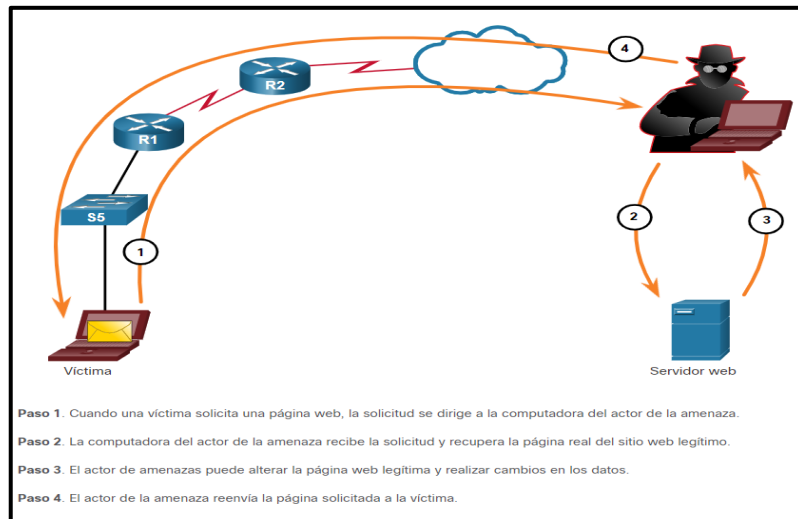


Fuente: Cisco Systems,2021

2.1.2.8.4 Ataque Man-in-the-Middle

También llamado ataque del intermediario, ocurre cuando un atacante se posiciona entre dos entidades válidas y legítimas para interceptarlos y efectuar lectura, modificar o redirigir los datos que se transmiten entre las dos entidades válidas.

Figura 18. Ejemplo de Ataque Man-in-the-Middle



Fuente: Cisco Systems,2021

2.1.2.9 Uso de Contraseñas

Para proteger y resguardar los dispositivos de la infraestructura de red se debe utilizar contraseñas muy seguras cuyas características son las siguientes:

-La contraseña debe tener al menos ocho caracteres, preferiblemente 12 o más caracteres en donde se debe considerar mientras la contraseña sea más larga es una contraseña más segura.

-Crear contraseñas muy seguras y complejas en donde pueda incluir una alguna combinación entre letras mayúsculas y letras minúsculas, símbolos, números, alfanuméricos, hasta espacios en caso el sistema lo permita.

-Evitar usar contraseñas repetidas la cual no debemos realizarlas debido a que es una mala práctica, no usar algunas palabras conocidas de diccionario, las cadenas o secuencias de números o letras conocidas, los nombres de cada usuario, hermanos, padres o mascotas, también información como ejemplo fecha de nacimiento del usuario, número de identificación como ejemplo DNI o pasaporte, nombres de antepasados y contraseñas por default como por ejemplo: admin, 1234 o alguna otra información muy común e identificable.

-Se debe emplear contraseña con algunos errores ortográficos como, por ejemplo, Jesus = Jysus = J3suS, o Privacidad = pr1v4c1dad.

-Debe utilizar la práctica de cambiar las contraseñas con frecuencia, si por algún motivo tiene una contraseña comprometida sin tener conocimiento sería una buena oportunidad para que el atacante use la contraseña de forma limitada.

-Definitivamente no se debe escribir o apuntar las contraseñas y también no dejarlas en lugares muy comunes como ejemplo en el escritorio de la oficina o pegado una nota en el monitor donde trabajo o utilizo cotidianamente.

Las tablas muestran ejemplos de contraseñas seguras y débiles.

Tabla 4. Contraseñas Débiles

Contraseña débil	Motivo de debilidad
rodriguez	Nombre de soltera de la madre
nissan	Marca de un auto
jesus1967	Nombre y cumpleaños del usuario.
redes1234	Palabras y números simples
admin	Contraseña por default y diccionario simple
1234	Contraseña por default y diccionario simple

Fuente: Elaboración Propia,2021

Tabla 5. Contraseñas seguras

Contraseña segura	Por qué es segura
S3cur3n42d39c	Combinación de caracteres alfanuméricos
\$23^Hu4@ 1r7\$	Se combina caracteres alfanuméricos, espacios, símbolos, mayúsculas permitiendo ser robusta.

Fuente: Elaboración Propia,2021

2.2.Marco conceptual

A continuación, presentamos el detalle del marco conceptual.

RFC 2764:

Describe el entorno para redes privadas virtuales también conocidas como VPN las cuales operan en redes troncales IP, también abarca el detalle de varios tipos de VPN con cada uno de sus respectivos requisitos y propuestas para su implementación y configuración de forma correcta y adecuada.

Se especifican varios procesos específicos que se usan para la implementación o desarrollo de cualquier tipo de VPN. Su objetivo es servir como pautas para la implementación de protocolos relacionados al desarrollo requerido para realizar un despliegue generalizado de soluciones VPN interoperables.

Determinan que las VPN pueden encontrarse interconectadas entre ellas y de la misma manera que los equipos informáticos actuales se conectan a las redes físicas, las cuales están interconectadas entre sí entre ellos tenemos switch o enrutadores.

Hash y Cifrado SHA 256:

SHA (Secure Hash Algorithm) que también se le denomina Algoritmo de Hash Seguro es un conjunto de funciones de hash criptográficas la cual fueron publicadas por el National Institute of Standards and Technology (NIST).

El algoritmo de cifrado es un mecanismo que permite convertir o transformar la información que se transmitirá en una serie aleatoria e ilegible, en donde utiliza una llave de cifrado que permite obtener el mensaje original, pero lo realiza sólo a los usuarios que conocen dicha clave y utilizan este proceso, la información privada puede ser transmitida de forma pública por internet sin tener mayor riesgo a que pueda ser interceptada y alterada.

SHA es uno de los algoritmos hash y una de ellas es igual a una firma para un texto y el algoritmo SHA-256 es un algoritmo hash de 64 dígitos hexadecimales como por ejemplo ca4127514frf3b11662c2f1rr26d35c39ff11381g8741e5e18d71ad447ef44132 la cual es de un tamaño de 256 bits igual a 32 bytes.

SHA se denomina SHA-0 para evitar confusiones con los siguientes algoritmos sucesores. Luego un par de años de su creación se validó al primer sucesor de SHA-0 el cual fue nombrado como SHA-1 y los siguientes 4 sucesores que salieron y sus diferencias se enfocan en un modelo variado y los aumentados rangos de salida como son SHA-224, SHA-256, SHA-384, y SHA-512 a los cuales se les conoce como SHA-2.

El algoritmo SHA-2 se usa en varios mecanismos a nivel de seguridad y protocolos, entre alguno de los conocemos son SSH, TLS, SSL, IPsec entre otros.

Cifrado MD5:

Message Digest Algorithm 5 o también conocido como MD5 el cual es un algoritmo que fue elaborado en 1991 por Ronald Rivest en Instituto Tecnológico de Massachusetts, para reemplazar al antiguo algoritmo denominado MD4.

MD5 es un algoritmo cuya función es de resumir los de mensajes de codificación de 128 bits que están conformadas por 32 caracteres hexadecimales la cual se podría decir que es un algoritmo de reducción criptográfico y usualmente se emplea para encriptar algunos documentos y contraseñas en las bases de datos.

Ejemplos:

MD5("Networking") = a5fa5746370b608090b994a97b49e98b

MD5("Mi mejor mecanismo de seguridad") = d2940fbb272447962af39b154a2ad73f

TCP/IP:

TCP/IP es un conjunto de protocolos de red que realizan que ocurra la transferencia de datos en redes y entre los distintos dispositivos de red e internet. TCP/IP referencia a un conjunto de protocolos:

-Protocolo de Control de Transmisión o también denominado TCP permite la conexión e intercambio de información entre dos o varios dispositivos de comunicación.

-Protocolo de internet o también denominado IP emplea direcciones de red en una serie de cuatro octetos como ejemplo 84.3.120.41. El presente protocolo es el responsable en trasladar la información a otros dispositivos informáticos.

TCP/IP logra realizar un intercambio de información dentro de la red informática, desde que se origina el envío de la información en paquetes hasta la etapa que son recepcionados, por el destino y logra emplear un grupo de capas con jerarquías.

Capas del modelo TCP/IP

TCP/IP tiene 4 capas las cuales son:

1.-Capa de Enlace: Llega a ser la primera capa de TCP/IP y proporciona el ingreso físico a la red, la cual podría ser una topología bus, estrella, anillo, entre otros.

2.-Capa de Red o Internet: Brinda los paquetes de datos y permite administrar las distintas direcciones IP. También es la capa más primordial e importante y conforma protocolos como IP, ICMP, ARP, RARP e IGMP.

3.-Capa de Transporte: Brinda información sobre el estado de la transmisión de la información, adicional también proporciona la información de enrutamiento en donde emplean puertos para relacionar una aplicación con algún tipo de información.

4.-Capa de Aplicación: Es la capa superior de TCP/IP y proporciona las aplicaciones de red tales como FTP, SMTP o Telnet, las cuales se intercomunican con las capas de los procesos anteriores es decir protocolos TCP o UDP.

TCP/IP es un protocolo muy importante debido a que logra que la información enviada llegue a su destino sin algún tipo de error y la información completa tal y como fueron enviados inicialmente.

OSI:

Es el modelo de interconexión de sistemas abiertos o también conocido como OSI (en siglas significa Open Systems Interconnection), fue creado en 1980 por la Organización Internacional de Normalización (ISO) y permite la comunicación entre varios sistemas informático empleando protocolos estándar. En resumen, el modelo OSI brinda a los distintos sistemas informáticos un estándar para que estos sistemas informáticos puedan comunicarse entre ellos.

Son 7 capas que corresponden al modelo OSI:

1.-Capa física: Llega a ser la primera capa del modelo OSI y es el responsable de la topología de red y las conexiones entre los hosts y la infraestructura de red, en resumen, es el medio físico de la forma en los datos se transmiten para garantizar la

existencia de una conexión física, esta capa define el medio físico a utilizar es decir tipo de cableado, microondas, entre otros.

2.-Capa de enlace de datos: Es el responsable del direccionamiento físico, brindar acceso al medio, la detección de errores, y también responsable del control del flujo de datos durante el establecimiento de la comunicación, forma parte de la elaboración de protocolos básicos para regular la conexión entre los sistemas informáticos, ejemplo MAC/LLC, ATM (modo de transferencia asíncrona), Frame Relay, PPP (redes punto a punto) entre otros.

3.-Capa de red: Es responsable de reconocer y definir el enrutamiento que emplearán las redes, con objetivo que la información pase a ser paquetes y puedan clasificarse en protocolos de enrutamiento que se emplean. Por ejemplo, los primeros que seleccionan rutas como RIP, EIGRP, OSPF entre otros y también los que se trasladan con los paquetes como IP, IPX, entre otros.

4.-Capa de transporte: En la presente capa se realiza el transporte de la información almacenado en cada paquete que se transmiten desde un dispositivo informático desde el origen hasta el destino, utilizando cualquier medio físico su función se efectúa mediante puertos lógicos denominados Sockets IP: Puerto.

5.-Capa de sesión: Su responsabilidad es mantener y controlar el diálogo entre los dispositivos informáticos que intercambian datos y cuando se logra establecer la comunicación entre ambos sistemas informáticos, en caso de interrumpirse el canal de comunicación de información pueda retomarse una vez más.

6.-Capa de presentación: Es responsable de la representación de la información definiendo el formato en resumen se encarga de traducir la información para asegurar que la información recibida en el destino sea del todo legible y reconocible. Adicional permite realizar el cifrado y la codificación de la información, así como también su correcta compresión en el dispositivo informático destino.

7.-Capa de aplicación: La capa aplicación se encarga de definir protocolos que usan las aplicaciones para lograr el intercambio de información. Brinda los servicios que son usados por distintas aplicaciones cuya finalidad es que los usuarios se comuniquen mediante la red informática. Es la capa más cercana al usuario.

FIDO U2F:

Fast Identity Online también conocido como FIDO es un método de autenticación más seguros que existen en la actualidad y Universal Second Factor, también conocido como U2F es un estándar universal emergente para tokens con soporte nativo en plataformas y navegadores.

FIDO U2F es compatible con FIDO Alliance y ha sido implementado por servicios a gran escala, incluidos Facebook, Gmail, Dropbox, GitHub y Salesforce, también es un estándar de autenticación abierto, es decir se encuentra disponible públicamente y tiene varios derechos de uso asociados.

Los tokens FIDO U2F permiten acceder de segura y rápida a cualquier sitio web o servicio en línea que admita el protocolo FIDO U2F utilizando un solo dispositivo y

para autenticarse, un usuario simplemente inserta un token de bus serie universal (USB) en cualquier puerto . Luego, el usuario presiona el botón del token U2F e ingresa su contraseña o PIN.

OPSWAT:

OPSWAT es una empresa internacional de ciberseguridad, desde 2002 brinda soluciones para que empresas identifiquen, detecten y remedien amenazas de seguridad avanzadas provenientes de los datos que entran y salen de sus redes. Varias organizaciones en toda parte del mundo se encuentran confiando en este flujo seguro de datos. OPSWAT logra prevenir amenazas de seguridad avanzadas en múltiples canales de transferencia de archivos y de flujo de datos, con opciones flexibles de soluciones Meta Defender, plataformas de desarrollo y de inteligencia de amenazas basados en API.

BYOD:

Bring your own device también conocido como BYOD que significa trae tu propio dispositivo, la cual es una política corporativa que consta en que todos los empleados o colaboradores de las empresas puedan llevar y usar sus propios equipos personales (laptops, tablets, iPad, móviles, entre otros) en su lugar de trabajo es decir dentro de la empresa con finalidad de tener acceso a recursos internos de la empresa entre algunos ejemplos son las bases de datos, correos electrónicos e información en servidores, así como aplicaciones e información personal.

CAPITULO 3

DESARROLLO DE LA SOLUCIÓN

Mediante el uso de la metodología de Gestión de proyectos usando las buenas prácticas y fundamentos de la guía PMBOK que significa Project Management Body of Knowledge del PMI (Project Management Institute), la gestión del proyecto de la implementación está compuesta por cinco (5) etapas, las cuales deben cumplirse y son los entregables del proyecto:

1.-Inicio del Proyecto

2.-Planificación del Proyecto

3.-Implementación

4.-Seguimiento y control

5.-Cierre del Proyecto

La presente implementación se basa en una conexión de acceso remoto seguro mediante una VPN (Red Privada Virtual) SSL la cual se emplea la mejor tecnología del presente mercado, además es implementado con el mejor de los criterios teóricos y técnicos a nivel de seguridad informática que comprenderá la aplicación de los mejores conocimientos, estándares y herramientas, también aplicando la mejor metodología de proyectos basada en el PMBOK de PMI permitiendo lograr tener una solución de acceso remoto con doble factor de autenticación y criterios sólidos de control de acceso de dispositivo en la cual cumple el objetivo de aumentar la seguridad informática y mitigar cualquier incidente de seguridad.

En el presente informe explicaremos las fases de la implementación tecnológica a desarrollar la cual es una solución remota segura con doble factor de autenticación y control de acceso de dispositivo utilizando los mejores criterios técnicos a nivel de seguridad informática y utilizando la mejor de la metodología de proyectos basada en el PMBOK de PMI como ya antes se había mencionado.

3.1 Fase de Inicio de Proyecto:

En la presente fase se realizó una reunión inicial mediante una sesión remota por la aplicación teams con todos los interesados que corresponden al proyecto con el objetivo de tratar algunos aspectos de la nueva solución implementada así como también se identificó el equipo del proyecto, así como sus responsabilidades, detalle de la problemática y también se explica el objetivo que se debe lograr el cual sería materializar la implementación de la solución remota con doble factor de autenticación y control de acceso de dispositivo para lograr cubrir la necesidad de la empresa privada; todo lo tratado en la reunión se establecerá en una minuta y un acta de inicio de proyecto.

La solución remota nueva a implementar consiste en que los usuarios remotos se conecten desde sus dispositivos informáticos a través de un agente endpoint llamado global protect el cual corresponde a un componente de la red privada virtual, luego el usuario apunta al Gateway público de la interfaz WAN del firewall, el Gateway es otro componente, donde se coloca el usuario y contraseña en el portal de la red privada virtual que también es otro componente y una vez que el usuario valida su primer mecanismo de autenticación el cual es

el usuario y password el siguiente proceso es que el servidor proxy valida con la consola de administración de doble factor de autenticación e identifica el dispositivo registrado asociado al usuario para poder otorgarle el factor de autenticación en la aplicación del celular duo Mobile, una vez que el usuario autoriza el acceso válido el tercer mecanismo es validar el control de acceso de dispositivo el cual se encarga de reconocer y revisar que el dispositivo debe pasar la aprobación de los filtros y criterios de funciones activas de seguridad informática una vez validada se permite el acceso y la conexión a los recursos internos de la empresa privada.

La relación al equipamiento firewall que soportará la nueva solución que se implementa muestro las consideraciones técnicas y no técnicas por la cual opté por el equipamiento mencionado para poder cumplir los objetivos propuestos de la nueva implementación, a continuación, detallo lo siguiente:

1.-El firewall Palo Alto Networks es el líder absoluto en el cuadrante mágico de Gartner en el 2021, por su capacidad de tener gran visibilidad de ciberseguridad de NGFW.

2.-El firewall Palo Alto es escalable ya que se integra y de adapta a cualquier necesidad de integración técnica que se requiere maneja y soporta el modelo OSI y TCP/IP.

3.-El firewall Palo Alto ofrece políticas de uso y un control bien granular a nivel de seguridad informática sobre todas las aplicaciones.

4.-Palo Alto tiene los precios más elevados del mercado al ser la plataforma de seguridad líder en firewall sin embargo para este caso ya contamos con un firewall el cual será reutilizado en la implementación y no es necesario adquirir uno nuevo.

5.-De acuerdo con mi experiencia técnica y profesional el firewall Palo Alto en comparación con otros firewalls de otros fabricantes como son Cisco, Check Point y Fortinet estos equipos no son muy estables debido a que presentan a cada momento incidentes ya sea por recursos: alto uso de memoria, elevado uso de CPU, consumo elevado de disco la cual la reflejan que son plataformas que no brindan estabilidad a diferencia del Firewall Palo Alto que es más estable, incluso el firewall Palo Alto maneja su propio sistema operativo denominado PAN-OS con últimas versiones muy estables.

6.-El firewall Palo Alto maneja y soporte redes privadas virtuales tipo SSL y IPSEC, para este caso de acuerdo con mi experiencia trabaja de forma muy estable con las VPN tipo SSL con la cual se utilizará en la presente implementación.

7.-El firewall Palo Alto soporta protocolos seguros de autenticación tipo SSL y TLS, asimismo también soporta varios tipos de cifrados como MD5, SHA las cuales son lo más conocidos.

Se puede observar que en la Figura 9 del presente informe hace referencia al cuadrante Mágico de Gartner de 2020 para firewalls de red y a Palo Alto Networks lo ubica como el máximo líder de todos los fabricantes en firewall.

En la implementación de la solución remota de la VPN SSL se utilizará protocolos de seguridad lo más conocidos y estables como son el SSL y TLS en versión superior a la 1.2, asimismo utilizaré el algoritmo RSA aplicando el cifrado SHA 512 el cual tiene la longitud más amplia que otros tipos de cifrado en comparación con el MD5 la cual es un cifrado ya desfasado aunque aún lo siguen empleando también es un algoritmo de cifrado de resumen el

cual no lo hace muy seguro, adicional al momento que cifra el mensaje este tipo de cifrado destruye el mensaje y de ocurrir algún error no habría forma de recuperar el mensaje es esos motivos que opté por el tipo de cifrado SHA 512 el de mayor longitud debido al nivel de seguridad que ofrece y haciendo que si algún atacante intente descifrar la información este demore muchos años en hacerlo incluso hasta imposible.

-Evaluación Técnico-Económica de la Tecnología seleccionada para el Proyecto

A continuación, se detalle la evaluación Técnico – Económica de la tecnología seleccionada para la implementación del proyecto.

Tabla 6. Tabla de evaluación técnico-económica de la tecnología seleccionada

Criterios	Características Firewall / Modelo de Equipo-Fabricante	Palo Alto PA-3050	Fortigate FG-200E	Check Point 3200	Cisco 2110
Técnicos	Throughput del firewall	4 Gbps	1.8 Gbps	4 Gbps	2.6 Gbps
	Throughput del Threat Prevention	2 Gbps	1.2 Gbps	580 Mbps	2 Gbps
	Máxima cantidad de sesiones	50,000	2,000,000	3.2,000,000	1,000,000
	Cantidad de nuevas sesiones por segundo	500,000	135,000	48,000	14,000
	Cantidad de túneles/interfases de túnel IPsec VPN	2,000	2,000	N/A	1,500
	Cantidad de usuarios SSL VPN	2,000	500	200	1,500
	Cantidad de routers virtuales	10	N/A	10	10
	Sistemas virtuales (base/max.)	1/06	10/10	1/10	1/10
	Cantidad de zonas seguras	40	N/A	N/A	N/A
	Cantidad máxima de políticas	5000	10000	1024	N/A
	Host Checker	Global Protect Hip Profile	Forticlient Host Check	Endpoint Security - Compliance	Cisco Any Connect
	Interfaces I/O	(12) 10/100/1000, (8) SFP Optical gigabit	(14) 10/100/1000, (4) SFP Optical gigabit	5x 10/100/1000Base-T RJ45 ports	(14) 10/100/1000, (4) SFP
	Almacenamiento	120GB SSD	480 GB SSD	240GB SSD	100 GB
Fuente de alimentación	Single 250W AC (150/200)	Single 100– 240V AC, 50–60 Hz	Single Power Supply rating: 40W	Single integrated 250W AC power supply.	
Económico	Precio	\$15000	\$77214.55	\$18000	\$137387.1 (2 equipos) \$68693.55 (1 equipo)

Fuente: Elaboración Propia, 2021

En relación a la selección de equipamiento firewall que se implementará en el siguiente proyecto con los componentes que integran el presente proyecto para cumplir los objetivos considerando la evaluación técnica y económica realizada se define que el equipamiento Firewall Palo Alto 3050 es la más adecuada y seleccionada para realizar la implementación del proyecto debido a que tiene ventajas a nivel técnico de mejor capacidad y rendimiento (Throughput) en las interfaces para procesar toda la información de red privada virtual para la empresa privada, además se considera en relación al procesamiento de transacciones nuevas por segundo 500,000 es superior en comparación de las otras opciones las cuales tienen un rendimiento y procesamiento mucho menor, en relación a la capacidad para las conexiones de red privada virtual SSL soporta 2000 usuarios una cantidad mayor a la de los otros firewalls que se encontraban dentro de la evaluación, permite integrar la opción de host checker mediante la tecnología de hip profile que permite realizar un control granular de acceso a los dispositivos que se conectan mediante la red privada virtual y en relación a sus interfaces poseen 4 interfaces de fibra adicionales a lo que ofrecen otros fabricante esto ayuda ante algún crecimiento de red el presente equipamiento seleccionado pueda adaptarse sin ningún problema, asimismo el precio es una buena opción debido a que es mucho menor y mejor a comparación de las otras opciones.

Figura 19. Cotización de firewall Palo Alto

Westcon Comstor Americas
A SYNNEX Corporation Company

CONTRATO DE COMODATO

Contrato de comodato que celebran por una parte **AFINA PERÚ SAC** quien en lo sucesivo se denominará **"EL COMODANTE"** y por la otra parte **SECURESOFT CORPORATION SAC**, que en lo sucesivo se denominará **"EL COMODATARIO"**, sujetándose a las siguientes:

CLÁUSULAS


1. El representante de **EL COMODATARIO** acepta estar debidamente autorizado por su representada para comprometer a la empresa con su firma en el presente contrato y acepta expresamente las responsabilidades y obligaciones derivadas del mismo.
2. **EL COMODATARIO** recibe a su entera satisfacción y en buen estado el(los) equipo(s) detallados abajo en calidad de comodato (en lo sucesivo denominados como los "equipos"):

Descripción de el(los) equipo(s) y accesorios:	Cantidad	Núm.(s) de parte:	Precio de Lista USD (sin IVA)
Palo Alto PA-3050	1	PA-3050	\$ 15,000

3. La duración del presente contrato será por un plazo de 90 días, obligándose **EL COMODATARIO** a devolver el(los) equipo(s) en el domicilio de **EL COMODANTE**, en un plazo máximo de 90 días naturales contados a partir de la notificación que se haga para este efecto/ en el plazo previsto. En caso de que la devolución de los equipos descritos en la cláusula 2 anterior implique su traslado transfronterizo, y **EL COMODANTE** no hubiere emitido instrucción por escrito en contrario, **EL COMODATARIO** se obliga a asumir la totalidad de los gastos inherentes al mismo, asumiendo total responsabilidad sobre los equipos, hasta su recepción en el domicilio de **EL COMODANTE**, a su entera satisfacción.
4. **EL COMODANTE** puede exigir la devolución del equipo(s) antes de que venza el plazo señalado en la cláusula anterior en caso de que haya peligro de que el(los) equipo(s) sufra(n) daños físicos y/o técnicos si continúa(n) en poder de **EL COMODATARIO**, o si este ha autorizado a un tercero a servirse del equipo(s).
5. Queda estipulado que si **EL COMODATARIO** no devuelve el(los) equipo(s) el día siguiente a la terminación del presente contrato, pagará como pena convencional el (2% mensual o proporcional) del precio de venta del equipo(s) por cada día que transcurra entre la fecha de compromiso de devolución y la fecha real de devolución de el(los) equipo(s).
6. Queda estipulado que el(los) equipo(s) dado(s) en comodato deberá(n) devolverse únicamente a personal autorizado por **EL COMODANTE** y contra la devolución del original del contrato firmado por **EL COMODATARIO**, de lo contrario, dicho(s) equipo(s) se tendrá(n) como no devuelto(s).


Fuente: Westcon Comstor,2021

Figura 20. Cotización de firewall Fortinet

		AFINA PERU S.A.C. R.U.C. 20517584399 Av. Larco 880 2do Piso - Miraflores Tel: +51 1 748 0670				
Fabricante: FORTINET Empresa: SECURESOFT CORPORATION País: Perú						
AM	Cotizacion	Moneda	País	Terminos Pago	Entrega	
Mila Berrospi	SS1077	Dólar	Perú	90 días	DDP Lima	
Qty	Part Number	Tipo	Descripcion		Precio Unitario	Total
2	FG-600E-BDL-950-36	Hardware	FortiGate-600E Hardware plus 3 Year 24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)		\$ 14,654.25	\$29,308.50
6	FC-10-FBH0E-175-02-12	Software	FortiGate-600E 1 Year FortiGuard Security Rating Service		\$ 1,032.91	\$6,197.46
2	FG-200E-BDL-950-36	Hardware	FortiGate-200E Hardware plus 3 Year 24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)		\$ 6,143.06	\$12,286.12
6	FC-10-00207-175-02-12	Software	FortiGate-200E 1 Year FortiGuard Security Rating Service		\$ 493.06	\$2,958.36
1	FG-200E	Hardware	18 x GE RJ45 (including 2 x WAN ports, 1 x MGMT port, 1 X HA port, 14 x switch ports), 4 x GE SFP slots. SPU NP6Lite and CP9 hardware accelerated.		\$ 2,409.04	\$2,409.04
2	SP-FG300E-PS	Hardware	AC power supply for FG-300/301E, FG-400/401E, FG-500/501E, FG-600/601E, FG-1100/1101E, FAZ-200F/FAZ-300F/FMG-200F and FAZ-800F/FMG-300F. power cable SP-FGPCOR-XX sold separately		\$ 626.08	\$1,252.16
1	FMG-200G	Hardware	Centralized management appliance - 4 x RJ45 GE, 8 TB storage, manages up to 30 Fortinet devices/Virtual Domains.		\$ 6,941.30	\$6,941.30
1	FC-10-M200G-247-02-36	Software	FortiManager-200G 3 Year 24x7 FortiCare Contract		\$ 4,083.12	\$4,083.12
TOTAL US\$					\$65,436.06	
IGV US\$					\$11,778.49	
TOTAL IGV INCLUIDO US\$					\$77,214.55	
CONDICIONES COMERCIALES: Las condiciones de venta de Afina Perú aplican para esta y cualquier otra cotización. El no pago de la factura en los tiempos definidos generara un interés por mora. El descuento por registro de oportunidad es válido siempre que la oportunidad sea registrada y aprobada. Validez de Propuesta: 15 días No se aceptarán devoluciones. Sujeto a penalización del 20%. Precios sujetos a cambio, según condiciones vigentes del Fabricante. Los precios No incluye servicios de implementación, ni configuración por parte de Westcon. Tiempo de Entrega Cliente Sector Privado: HW 60 días calendario / SW 5 días útiles, luego de recibida y aceptada la orden de compra. El plazo de entrega esta sujeto a la fecha de despacho del fabricante. Tiempo de Entrega Cliente Sector Gobierno: HW 75 días calendario / SW 15 días calendario, luego de recibida y aceptada la orden de compra. Se requiere Carta de Export Compliance firmada por el cliente final. El plazo de entrega esta sujeto a la fecha de despacho del fabricante. Para procesar su orden sera necesario que incluya la siguiente información del usuario final: Empresa, Contacto, E-mail, Dirección y teléfono. Consulte por otros servicios de Afina o Westcon en el país						

Fuente: Synnex Westcon,2021

Figura 21. Cotización de firewall Cisco

End User: SECURESOFT Reseller: SECURESOFT Contact: Pablo Castillo Project: Deal ID 52659771		 AM: Patricia Rodríguez								
Line Number	Item Name	Description	P/S	Service Duration (Months)	T.Fab	Qty	GPL Unit	GPL Total	Precio Unit	Precio Total
1.1	FPR2130-NGFW-K9	Cisco Firepower 2130 NGFW Appliance, 1U, 1 x NetMod Bay	P	---	98	2	39,289.32	78,578.64	13,356.00	26,712.00
1.1.0.1	CON-SNTP-FPR2130W	SNTC-24X7X4 Cisco Firepower 2130 NGFW Appliance, 1U,	S	36	N/A	2	20,637.39	41,274.78	9,026.90	18,053.80
1.1.1	FPR2K-PWR-AC-400	Firepower 2000 Series 400W AC Power Supply	P	---	14	2	2,958.10	5,916.20	1,005.60	2,011.20
1.1.10	SFP-10G-SR-S	10GBASE-SR SFP Module, Enterprise-Class	P	---	14	8	828.27	6,626.16	281.60	2,252.80
1.2.0.1	L-FPR2130T-TM-3Y	Cisco FPR2130 Threat Defense Threat and Malware 3Y Subs	P	36	N/A	2	21,609.72	43,219.44	8,450.30	16,900.60
2.0	SF-FMC-VMW-10-K9	Cisco Firepower Management Center, (VMWare) for 10 devices	P	---	3	1	3,745.00	3,745.00	1,756.00	1,756.00
2.0.1	CON-ECMU-SFMCCK9VC	SWSS UPGRADES Cisco Firepower Management Center, (VMWa	S	36	N/A	1	2,584.05	2,584.05	1,130.30	1,130.30
3.0.1	L-AC-APX-3Y-54	Cisco AnyConnect Apex License, 3YR, 500-999 Users	P	36	N/A	600	15.49	9,294.00	4.40	2,640.00
4.1	FPR2130-NGFW-K9	Cisco Firepower 2130 NGFW Appliance, 1U, 1 x NetMod Bay	P	---	98	2	39,289.32	78,578.64	13,356.00	26,712.00
4.1.0.1	CON-SNTP-FPR2130W	SNTC-24X7X4 Cisco Firepower 2130 NGFW Appliance, 1U,	S	36	N/A	2	20,637.39	41,274.78	9,026.90	18,053.80
4.1.1	FPR2K-PWR-AC-400	Firepower 2000 Series 400W AC Power Supply	P	---	14	2	2,958.10	5,916.20	1,005.60	2,011.20
4.1.10	SFP-10G-SR-S	10GBASE-SR SFP Module, Enterprise-Class	P	---	14	8	828.27	6,626.16	281.60	2,252.80
4.2.0.1	L-FPR2130T-TM-3Y	Cisco FPR2130 Threat Defense Threat and Malware 3Y Subs	P	36	N/A	2	21,609.72	43,219.44	8,450.30	16,900.60
366,853.49									137,387.10	
CONDICIONES COMERCIALES 1 Los precios están expresados en dólares americanos. No incluye Impuesto General a las Ventas (IGV) 2 Para realizar su compra, por favor genere una orden de compra formal a nombre de AFINA PERU SAC 3 Para procesar su orden sera necesario que incluya la siguiente información del usuario final: Empresa, Contacto, E-mail, Dirección y teléfono. 4 Las condiciones de venta de Afina Perú aplican para esta y cualquier otra cotización. 5 No se aceptarán devoluciones. Sujeto a penalización del 20%. 6 El descuento por registro de oportunidad es válido siempre que la oportunidad sea registrada y aprobada.										

Fuente: TD Synnex,2021

Tabla 7. Tabla de evaluación técnico-Económica de la tecnología usada para el doble factor de autenticación.

Crterios	Características 2FA Vendor	Duo Security	RSA SecurID	Google Workspace
Técnicos	Acceso móvil	SI	SI	SI
	API	SI	SI	SI
	Autenticación de dos factores	SI	SI	SI
	Creación de informes/análisis	SI	NO	SI
	Gestión de políticas	SI	SI	NO
	Controles o permisos de acceso	SI	SI	SI
	Integraciones de terceros	SI	SI	SI
	Solicitud de acceso de autoservicio	SI	SI	NO
	Compatibilidad Sistema Operativo Móvil	SI	SI	SI
Económicos	Precio x mes	\$3	\$3	\$4

Fuente: Elaboración Propia,2021

En relación a la selección de la tecnología de doble factor de autenticación que se implementará en el siguiente proyecto, considerando la evaluación técnica y económica realizada se define que la solución Duo Security es la más adecuada y seleccionada para realizar la implementación del proyecto debido a que tiene ventajas a nivel técnico debido a que tiene gestión de políticas granulares a comparación de las otras opciones además que incorpora la creación y gestión de informes que es primordial ante alguna auditoría de seguridad, permite integrar e implementar la función principal del doble factor de autenticación que se funciona y es compatible con la integración del firewall Palo Alto seleccionada para la gestión de la red privada virtual y el control de acceso de dispositivo, en relación a lo económico es una buena opción y a nivel técnica es la más completa que las otras opciones evaluadas y presentadas.

Con respecto a evaluar y seleccionar entre todas las soluciones tecnológicas de autenticación de doble factor de diversos fabricantes y escoger la mejor solución que me permita implementar un mecanismo de doble factor de autenticación que pueda integrarse a red privada virtual SSL Global Protect, entre las soluciones Duo Security de Cisco, Microsoft, IBM y RSA procedí a escoger la solución Duo Security de Cisco la cual es una plataforma de seguridad de acceso escalable y fácil de usar para los colaboradores debido a que adicionalmente usa una validación de acceso mediante una segunda fuente o dispositivo como es un smartphone que tiene instalado la aplicación Duo Mobil, esta aplicación registrada permite verificar la identidad del usuario antes de brindar acceso, la solución es híbrida debido a que tiene su consola de administración en nube y se comunica con el servidor Proxy que es el intermediario entre la consola de administración de 2FA en nube y el directorio activo, esta aplicación se puede implementar e integrar en entornos y dispositivos como Cloud, SaaS, Web, Android (móvil), iPhone (móvil), iPad (móvil), el componente servidor Proxy se comunica mediante API hacia la consola en nube de administración del doble factor de autenticación para validar al usuario y el dispositivo conectado y enrolado, el servidor Proxy establece una comunicación con el protocolo de autenticación Radius con el directorio activo y con el firewall Palo Alto para poder establecer políticas de seguridad de acceso para los usuarios que lograron conectarse pasando los mecanismos adicionales de autenticación, el Duo Security tiene un mejor servicio de soporte fabricante , es más adaptable a integrarse y

despliegue debido a la situación actual de la pandemia covid-19 es la más idónea y seleccionada para integrar e implementar.

Figura 22. Evidencia de Cisco Duo como mejor alternativa para el 2FA



Fuente: Gartner,2021

Figura 23. Calificación de Cisco Duo en Gartner como mejor opción para 2FA



Fuente: Gartner,2021

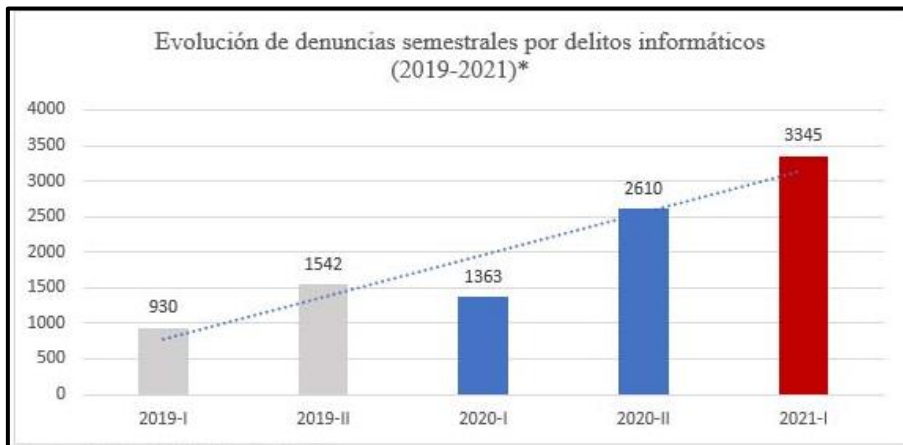
Sobre el perfil de identificación de host que permite el control de acceso de dispositivo entre todos los fabricantes que evalué como son Palo Alto , Checkpoint , Cisco y Fortinet seleccioné la opción de HIP profile de Palo Alto debido a que se tiene un firewall Palo Alto con una red privada virtual SSL Global Protect en funcionamiento al ser del mismo fabricante permite ser mucho más adaptable, esta solución ofrece dentro de sus perfiles disponibles todo tipo de funciones a nivel de host de cualquier fabricante y utiliza conectores lógicos booleanos como son AND,OR Y NOT para asociar los perfiles de identificación de host a diferencia de otros fabricantes que no lo tienen, existen varios fabricantes que permiten esta funcionalidad como el host Checker del fabricante pulse secure, Check Point, Fortinet sin embargo basándome en la experiencia técnica y a la reputación de Palo Alto como líder en Firewall

asimismo que ya la solución HIP Profile se implementaría en el mismo equipo Firewall sin necesidad de incurrir a un gasto adicional por otro equipo de otro fabricante para integrarlo, seleccioné la mejor opción considerando varios aspectos.

A continuación, registro y evidencio la información histórica que se emplea previamente para validar la necesidad del requerimiento además ayudó a identificar y clarificar la necesidad para finalmente implementada la solución como resultado se logre realizar los objetivos propuestos del proyecto.

En relación con los ataques informáticos en el Perú, la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (DIVINDAT), confirmó que en el periodo del mes de octubre del año 2013 al mes de diciembre del año 2020, se notificaron y registraron 12 169 delitos vinculados estrictamente a delitos informáticos, entre ellos el 78 % (9515) fueron fraudes informáticos. Complementando información, en el 2020 se produjo el pico en lo más alto con un crecimiento exponencial del 134 % frente a años anteriores.

Figura 24. Evaluación de denuncias semestrales por delitos informáticos



Fuente: División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú ,2021

Tal y como se evidencia en la gráfica el primer semestre del 2021 ha sido un período con mayor cantidad de denuncias en relación con delitos informáticos.

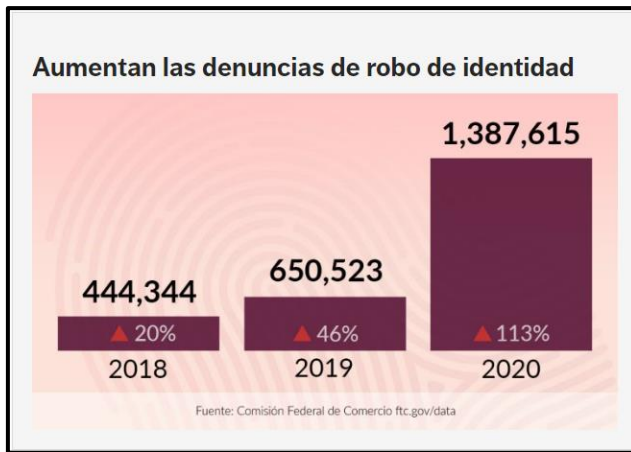
Los tipos de delitos informáticos más comunes es el fraude informático es decir ventas fraudulentas, compras por internet no autorizadas, transferencias no autorizadas, clonación de tarjetas y retiro de dinero no autorizado. Otro de los delitos informáticos muy usual y denunciado es la suplantación de identidad, con la cual busca perjudicar a la persona usando como ejemplo métodos de ingeniería social que buscan engañar a la víctima, también existen denuncias contra vulneración de datos y sistemas informáticos, ataques a dispositivos informáticos, entre otros delitos cometidos mediante el uso de tecnologías de la información (TIC).

En relación con información internacional en EE.UU los casos de robo de identidad se incrementaron de forma exponencial a tal punto de duplicarse en el 2020 con respecto al 2019, según un informe de la FTC(Comisión Federal de Comercio) una agencia de protección al consumidos en Estados Unidos, evidencian que las denuncias de robo de identidad de usuario del año 2020 fueron más del triple en comparación al año 2018.

Existen 1,387,615 casos en el año 2020, en el año 2019 fueron 650,523 casos y en el año 2018 fueron 444,344 casos.

Se muestra un asombroso aumento anual del 2,920% en el número de casos de robo de identidad en los que las víctimas mencionaron que su información se empleó para solicitar o recibir beneficios del Gobierno, como por ejemplo una compensación por desempleo durante la pandemia covid-19.

Figura 25. Aumento de denuncias de robo de identidad



Fuente: Comisión Federal de Comercio,2021

Registro de reporte histórico de conexiones remotas de marzo del año 2020 donde muestra la necesidad de seguridad que cubrir no tiene control de acceso de dispositivo ni doble factor de autenticación.

Figura 26. Histórico de conexiones remotas de marzo del año 2020

Time	Origin	Type	Action	Service	Source	Destination	User	2FA	Endpoint	Operating System	Community
07:31:09	FW-SS-0	connection	Decrypt	SIP	172.31.1.10	192.168.25.10	epastor	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:31:10	FW-SS-0	connection	Decrypt	SIP	172.31.1.21	192.168.25.10	cchacchi	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:33:04	FW-SS-0	connection	Decrypt	DNS	172.31.1.35	192.168.25.21	jzema	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:33:06	FW-SS-0	connection	Decrypt	DNS	172.31.1.44	192.168.25.21	ksalinas	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:33:27	FW-SS-0	connection	Decrypt	FTP	172.31.1.13	192.168.99.41	mmorales	NA	NA	NA	RemoteAccess
07:33:32	FW-SS-0	connection	Decrypt	DNS	172.31.1.10	192.168.25.21	epastor	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:33:35	FW-SS-0	connection	Decrypt	SIP	172.31.1.41	192.168.25.10	jpvargas	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:33:45	FW-SS-0	connection	Decrypt	SIP	172.31.1.32	192.168.25.10	agarcia	NA	NA	NA	RemoteAccess
07:33:54	FW-SS-0	connection	Decrypt	HTTPS	172.31.1.44	192.168.99.27	ksalinas	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:33:55	FW-SS-0	connection	Decrypt	HTTPS	172.31.1.13	192.168.99.27	mmorales	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:33:56	FW-SS-0	connection	Decrypt	HTTPS	172.31.1.35	192.168.99.27	jzema	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:33:57	FW-SS-0	connection	Decrypt	HTTPS	172.31.1.35	192.168.99.27	jzema	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:34:07	FW-SS-0	connection	Decrypt	FTP	172.31.1.44	192.168.99.41	ksalinas	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:34:42	FW-SS-0	connection	Decrypt	FTP	172.31.1.17	192.168.99.41	jsandonas	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:35:42	FW-SS-0	connection	Decrypt	FTP	172.31.1.93	192.168.99.41	lcardenas	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:37:34	FW-SS-0	connection	Decrypt	FTP	172.31.1.84	192.168.99.41	bnavarrete	NA	NA	NA	RemoteAccess
07:37:34	FW-SS-0	connection	Decrypt	DNS	172.31.1.17	192.168.25.21	jsandonas	NA	NA	NA	RemoteAccess
07:43:08	FW-SS-0	connection	Decrypt	DNS	172.31.1.35	192.168.25.21	jzema	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:43:20	FW-SS-0	connection	Decrypt	DNS	172.31.1.32	192.168.25.21	agarcia	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:43:23	FW-SS-0	connection	Decrypt	DNS	172.31.1.44	192.168.25.21	ksalinas	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:43:25	FW-SS-0	connection	Decrypt	DNS	172.31.1.21	192.168.25.21	cchacchi	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:43:25	FW-SS-0	connection	Decrypt	DNS	172.31.1.17	192.168.25.21	jsandonas	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84
07:43:29	FW-SS-0	connection	Decrypt	DNS	172.31.1.17	192.168.25.21	jsandonas	NA	NA	NA	ConnectraRemoteAccess(3E2FBBD8-513E-6D46-B48F-FE84

Fuente: Elaboración Propia,2021

Figura 27. Histórico de conexiones remotas de mayo del año 2021

Usuario/Día	Suma de count
aalfarop	16
10-May	1
11-May	1
12-May	2
13-May	2
14-May	1
17-May	1
18-May	3
19-May	2
21-May	2
24-May	1
aarciniiega	22
10-May	3
11-May	2
12-May	3
13-May	1
14-May	1
15-May	2
17-May	4
18-May	2
19-May	1
20-May	1
24-May	2
aarubiaga	28
10-May	1
11-May	1
13-May	1
14-May	2
16-May	2
17-May	5
18-May	2
19-May	2
20-May	3
21-May	3
22-May	2
23-May	3
24-May	1
acampana	16

Fuente: Elaboración Propia,2021

Figura 28. Detalle histórico de conexiones remotas de mayo del año 2021

Event Receive Time	Event Type	Event Name	Source IP púb.	count	User	Reason for Error
24/05/2021 12:01	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.116.172	1	aarciniiega	login successfully
24/05/2021 11:58	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	190.86.109.235	1	aalfarop	login successfully
24/05/2021 10:54	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.145.198	1	aarubiaga	login successfully
24/05/2021 10:37	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.116.172	1	aarciniiega	login successfully
24/05/2021 02:54	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	78.187.72.104	1	acampana	login successfully
24/05/2021 00:08	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	78.187.72.104	1	acampana	login successfully
23/05/2021 09:16	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.145.198	1	aarubiaga	login successfully
23/05/2021 09:14	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.145.198	1	aarubiaga	login successfully
23/05/2021 09:14	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.145.198	1	aarubiaga	login successfully
23/05/2021 01:14	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	176.88.85.151	1	acampana	login successfully
22/05/2021 10:42	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.145.198	1	aarubiaga	login successfully
22/05/2021 09:01	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.145.198	1	aarubiaga	login successfully
21/05/2021 19:01	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	179.51.4.72	1	aalfarop	login successfully
21/05/2021 15:06	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.145.198	1	aarubiaga	login successfully
21/05/2021 10:16	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	179.51.4.72	1	aalfarop	login successfully
21/05/2021 08:38	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.145.198	1	aarubiaga	login successfully
21/05/2021 08:38	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.145.198	1	aarubiaga	login successfully
21/05/2021 08:12	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	78.187.72.104	1	acampana	login successfully
21/05/2021 00:04	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	78.187.72.104	1	acampana	login successfully
20/05/2021 15:23	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.145.198	1	aarubiaga	login successfully
20/05/2021 15:08	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.116.172	1	aarciniiega	login successfully
20/05/2021 14:15	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.145.198	1	aarubiaga	login successfully
20/05/2021 07:53	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.145.198	1	aarubiaga	login successfully
20/05/2021 06:47	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	78.187.72.104	1	acampana	login successfully
19/05/2021 23:57	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	78.187.72.104	1	acampana	login successfully
19/05/2021 19:26	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	179.51.4.72	1	aalfarop	login successfully
19/05/2021 16:38	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.145.198	1	aarubiaga	login successfully
19/05/2021 14:00	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	179.51.4.72	1	aalfarop	login successfully
19/05/2021 09:38	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.116.172	1	aarciniiega	login successfully
19/05/2021 08:19	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.145.198	1	aarubiaga	login successfully
18/05/2021 17:33	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	179.51.4.72	1	aalfarop	login successfully
18/05/2021 15:25	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.145.198	1	aarubiaga	login successfully
18/05/2021 13:30	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	179.51.4.72	1	aalfarop	login successfully
18/05/2021 13:11	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	179.51.4.72	1	aalfarop	login successfully
18/05/2021 11:26	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.116.172	1	aarciniiega	login successfully
18/05/2021 09:36	Checkpoint-ssl-vpn-user-tunnel-ur	Checkpoint ssl vpn user tunnel ur	201.240.145.198	1	aarubiaga	login successfully

Fuente: Elaboración Propia,2021

En relación con el análisis de empleo de la solución con otras tecnologías vigentes se considera lo siguiente:

Tecnología SD-WAN: El firewall Palo Alto donde se encuentra implementada la solución permite agregar la tecnología tipo SD-WAN (Software-Defined Wide Area Network) es decir la red de área amplia definida por software es un tipo de tecnología que permite utilizar varios servicios privados y de internet para crear una red WAN muy dinámica e inteligente lo que permite reducir costos, incrementar la calidad y brindar un fácil uso y acceso a las diversas aplicaciones tecnológicas.

En un futuro la implementación actual se puede adaptar a integrar la tecnología SD-WAN para la conexiones de red privada virtual para hacerla mucho más óptima, rápida y muy segura debido a que en lugar de usar MPLS la cual es costoso y lento usando routers y optimizadores de WAN, la tecnología SD-WAN es una gran opción que se puede implementar e integrar en el firewall Palo Alto debido a que no necesita equipamiento adicional y optimizar la parte WAN de la red por donde se conectan los usuarios que usan la red privada virtual SSL.

SD-WAN permite agrupar varios enlaces físicos con la opción de usar diferentes proveedores de servicios de internet en una interfaz virtual SD-WAN esto permitiría distribuir y disminuir la carga de un solo enlace ante algún crecimiento de conexión de usuarios asimismo el SD-WAN te permitiría mantener y asumir en un solo enlace de forma automática todas las conexiones en caso la caída de enlace de uno de los proveedores de enlace de internet.

SD-WAN es compatible con los tipos de conexiones WAN como son: ADSL/DSL, Tipo módem por cable, Tipo Ethernet, fibra óptica, LTE/3G/4G/5G, MPLS, microondas/radio, satélite, Wi-Fi y cualquier elemento que termine como Ethernet en la interfaz del firewall.

Ventajas de usar SD-WAN:

- Se puede realizar combinación de diferentes tipos de conexiones (entre ellas DSL, MPLS, 4G, VPN entre otras) en cualquier ubicación para brindar alta disponibilidad o realizar la suma de anchos de banda.
- Despliegue de forma fácil y adaptable a nuevas sedes
- Permite administrar y monitorear de forma centralizada
- Logra priorizar un tráfico específico sobre cualquier otro (SMTP, WEB, VoIP, por ejemplo)
- Permite brindar priorización de conexión para aplicaciones críticas frente a las no críticas, permite diferenciarlas.
- Permite configurar de forma avanzada e inteligente los balanceos por aplicaciones específicas.
- Permite configurar caminos dependientes de destino o aplicación de forma granular sin la necesidad realizar la conexión a través de un punto central.
- Permite configurar SLAs por servicio específico.
- Se puede configurar políticas de tipo QoS y HA

- Permite brindar un ahorro de costos en un futuro en lo que concierne a inversión de líneas de comunicación.

Tecnología AntiDDoS: Se puede aplicar tecnología de protección AntiDDoS a futuro en las interfaces WAN para proteger ante algún intento de denegación de servicio y no permitir la saturación de enlace para ello se debe adquirir una licencia adicional en cuanto se tenga un presupuesto adicional podría integrarse el AntiDDoS al proyecto actual.

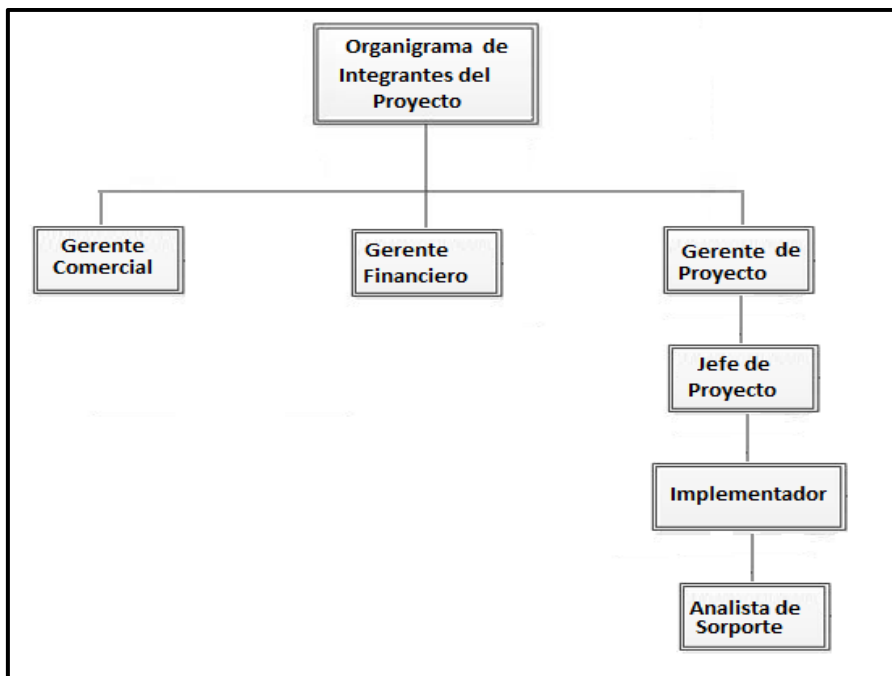
Esta tecnología AntiDDoS permite proteger ante ataques de denegación de servicio ya que este tipo de ataques tiene como objetivo interrumpir la continuidad de operativa para generar crisis interna.

Tecnología SandBox: La tecnología Sandboxing permite integrarse en un futuro a al proyecto implementado ya que es compatible y permite llevar muestras de tráfico sospechoso a un entorno aislado en entornos de infraestructura física y nube.

La tecnología SandBox permite aislar, abrir y analizar la muestra del tráfico observado en un entorno aislado para proteger la red de la empresa privada, esta tecnología también tiene un costo adicional de licenciamiento el cual en un futuro podría ser adquirido e implementado.

La implementación es realizada en el data center de la empresa privada que se encuentra ubicada en Avenida Manuel Olguín 325 que corresponde al distrito de Santiago de Surco, Departamento De Lima; adicional logramos identificar y definir el equipo que participa durante toda la implementación del proyecto con sus respectivos roles.

Figura 29. Organigrama de integrantes del Proyecto



Fuente: Elaboración Propia,2021

Tabla 8. Roles y responsabilidades de integrantes del Proyecto

N ^o	Interesado	Cargo en la organización	Ubicación	Rol en el Proyecto	Fase en el proyecto de mayor participación	Responsabilidades
1	Ismael N.	Gerente Comercial	Área comercial	Usuario Indirecto	Inicial, Planificación y cierre	<ul style="list-style-type: none"> • Apoyar en la cotización del licenciamiento de las tecnologías Palo Alto y Cisco. • Coordinar la compra del licenciamiento de las tecnologías Palo Alto y Cisco.
2	Francisco S.	Gerente Financiero	Área administrativa	Patrocinador	Inicial, Planificación y cierre	<ul style="list-style-type: none"> • Indicadores de rentabilidad • Disponer y controlar el presupuesto asignado a Ingeniería. • Cumplimiento de las políticas financieras de la empresa. • Indicadores comerciales de rentabilidad por el proyecto.
3	Percy S.	Gerente de Proyecto	Área de Ingeniería	Gerente de Proyecto	Inicial, Planificación, Ejecución, Seguimiento y control y Cierre	<ul style="list-style-type: none"> • Organizar el funcionamiento adecuado del presente proyecto y permitir el aseguramiento y cumplimiento de los objetivos del proyecto
4	Ever Pastor	Jefe de Proyecto	Área de Ingeniería	Jefe de Proyecto	Inicial, Planificación, Ejecución, Seguimiento y control y Cierre	<ul style="list-style-type: none"> • Efectuar un seguimiento adecuado y cumplimiento de las fases del proyecto, así como validar el cumplimiento de los objetivos.
5	Ever Pastor	Implementador	Área de Ingeniería	Ingeniero Implementador	Inicial, Planificación, Ejecución, Seguimiento y control y Cierre	<ul style="list-style-type: none"> • Encargado de completar con todas las actividades programadas del presente proyecto. • Cumplir correctamente con las configuraciones correctas para el desarrollo de la nueva solución tecnológica que se está implementando.
6	Carlos C.	Analista de Soporte	Área de Ingeniería	Usuario de Pruebas	Ejecución y Seguimiento y Control	<ul style="list-style-type: none"> • Realizar pruebas de funcionamiento de la nueva solución implementada.

Fuente: Elaboración Propia, 2021

Con relación al equipo de proyecto se estableció que los medios de comunicación son: correo electrónico, comunicaciones telefónicas y reuniones remotas por la plataforma Teams.

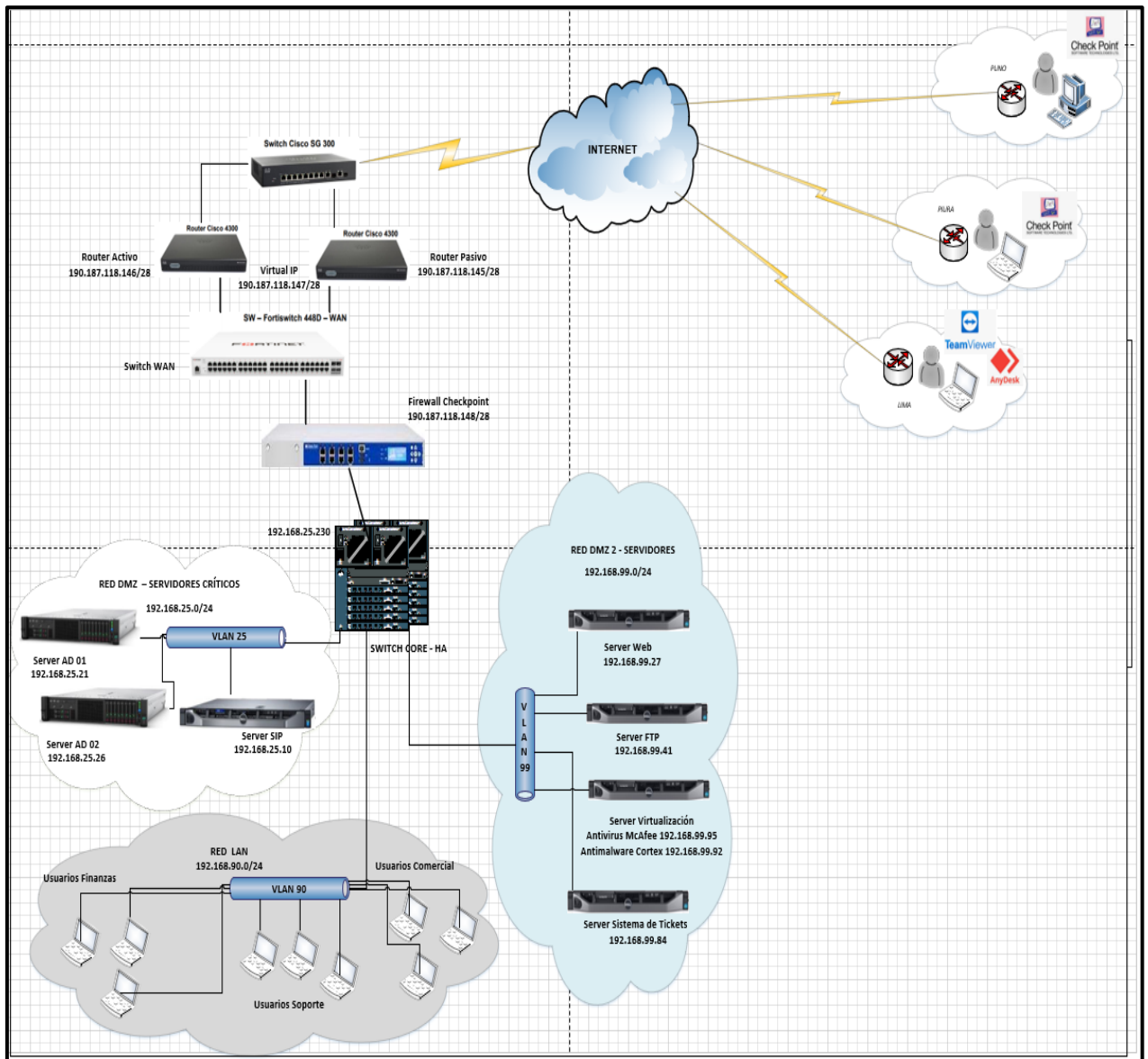
Diagrama de red de acceso remoto antes de la implementación:

En el presente diagrama se evidencia la topología de red con los equipos de seguridad y comunicaciones que tiene la empresa privada, la compañía en el presente diagrama de red muestra la comunicación del tráfico de acceso remoto usando el agente remoto Check Point mediante una conexión de protocolo SSL (Secure Sockets Layer) con la cual todos los usuarios colocan el nombre de usuario y contraseña además de la ip pública 190.187.118.148 que se encuentra configurado en el firewall Checkpoint donde transita todo tráfico de entrada y salida de la empresa privada, esta solución ya se encontraba en uso pero como informo se tiene implementado sólo un factor de autenticación el cual es el acceso remoto por contraseña en la conexión de acceso remoto implementado que se encuentra ubicado firewall Checkpoint de la empresa privada, a continuación explico el diagrama en donde la empresa privada tiene dos routers del proveedor Americatel en donde su enlace es redundante y funciona un router

como pasivo y otro como activo por el cual pasa toda la carga de red, asimismo se tiene el firewall Checkpoint con la interfaz WAN con la ip 190.187.118.148 donde se tiene implementada la solución de VPN de un solo factor de autenticación es decir la VPN sólo está integrada al directorio activo con ip 192.168.25.21 usando el protocolo de autenticación LDAP(Lightweight Directory Access Protocol), luego de ello se tiene la red interna con el SW Core con ip 192.168.25.23 que contienen las VLANs de las redes internas donde están los servidores críticos segmento 192.168.25.0/24 como el Directorio Activo y otra VLAN 99 de servidores con el segmento 192.168.99.0/24 donde se encuentran los servicios como publicaciones WEB, FTP, entre otros, además otra VLAN 90 la cual corresponde a la red 192.168.90.0/24 donde se encuentran los dispositivos de trabajo de cada colaborador a la que corresponde la red LAN.

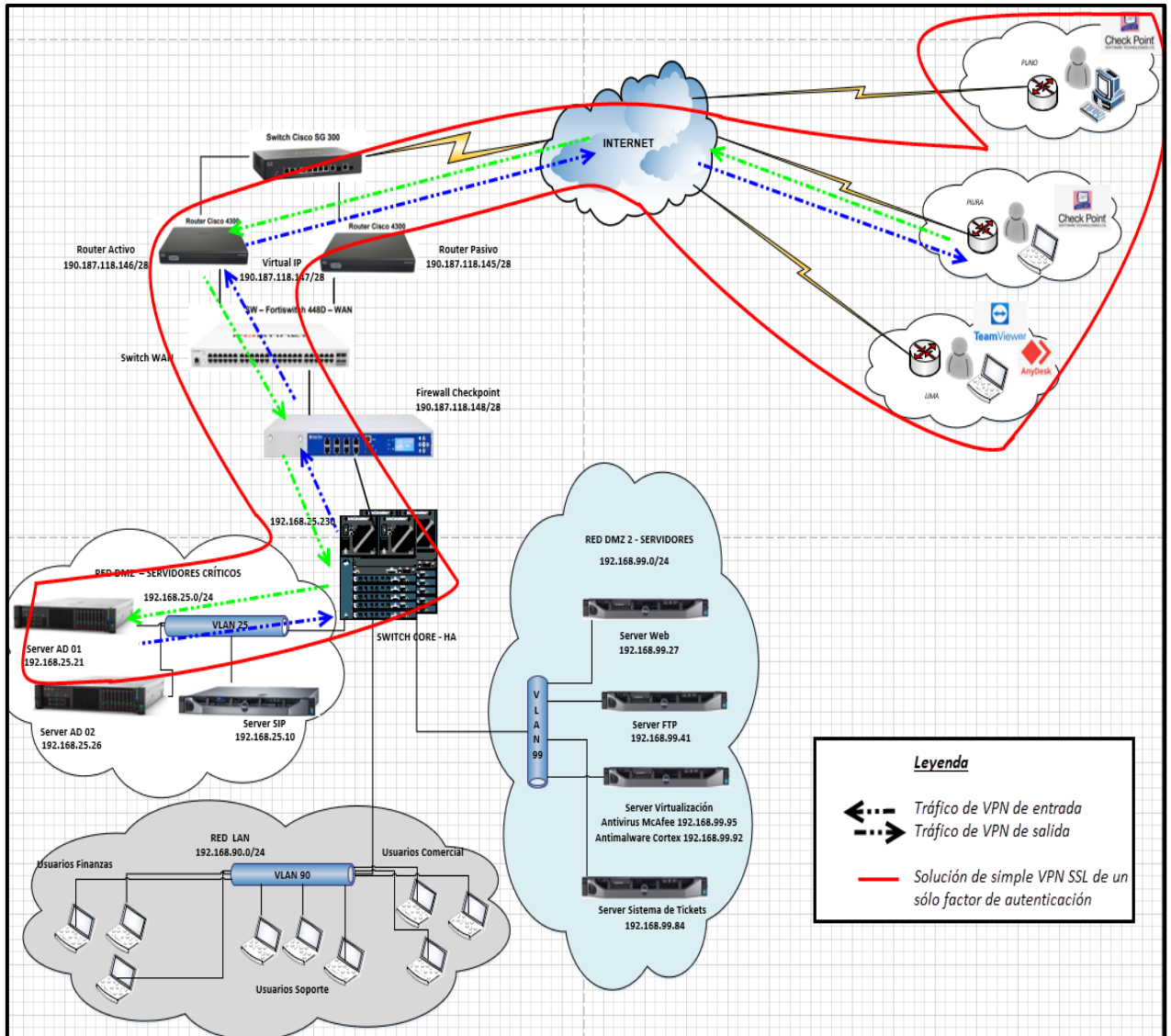
A continuación, presento el diagrama de red de la empresa privada previo el desarrollo la nueva solución.

Figura 30. Diagrama de red previo al desarrollo del proyecto.



Fuente: Elaboración Propia,2021

Figura 31. Diagrama de red previo al desarrollo del proyecto mostrando la conexión remota de acceso básico.



Fuente: Elaboración Propia, 2021

3.2 Fase de Planificación del Proyecto:

En la presente etapa luego de lograr identificar los requerimientos específicos de la nueva solución, personal asignado y validar su factibilidad se definen la duración de los tiempos para las actividades que se utilizan para instalar, configurar, desplegar y dejar operativa la nueva solución tecnológica.

3.2.1 Alcance de Proyecto:

La implementación se realiza dentro de las instalaciones de las oficinas de empresa privada la cual se encuentra ubicado en Manuel Olguín 325, distrito Santiago de Surco, Departamento Lima, específicamente en el data center de la empresa Privada, Ubicación Gabinete 1 – RU (Unidad de Rack) 25.

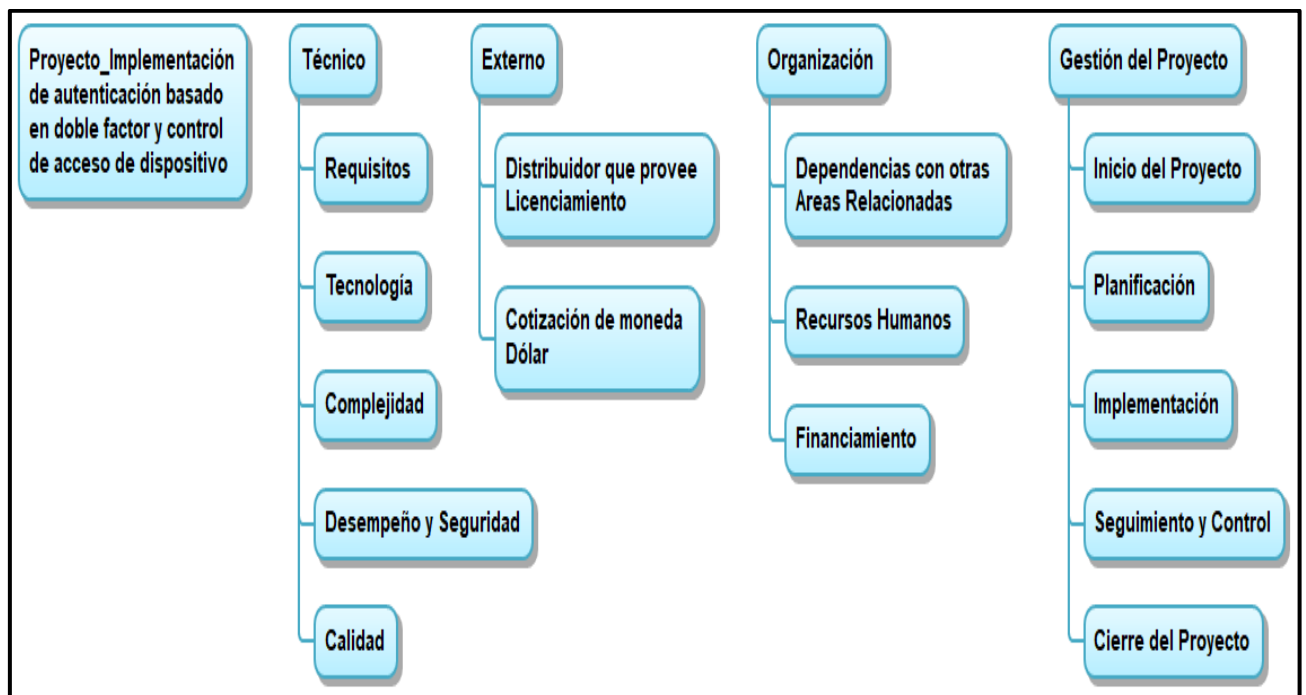
El objetivo es implementar una solución que brinde doble factor de autenticación y control de dispositivo con la finalidad de aumentar la seguridad mediante del acceso remoto as los recursos internos de la empresa privada.

La implementación busca robustecer el método de autenticación usando protocolos seguros de autenticación que permitan un cifrado de alto nivel como los protocolos SSL y TLS asimismo el algoritmo de cifrado SHA 512 y mitigar cualquier tipo de intento de suplantación de identidad o robo de contraseñas de los usuarios.

También se busca lograr tener un mejor control de acceso de dispositivos las cuales deben tener los criterios correctos y adecuados para establecer la conexión remota segura a los recursos de la empresa Privada.

La finalidad y justificación es proteger los activos de la empresa Privada ante cualquier tipo de incidente relacionada a seguridad de la informática.

Figura 32. Estructura de desglose del Trabajo (EDT)



Fuente: Elaboración Propia, 2021

Tabla 9. Detalle de entregables del proyecto

N° EDT	Nombre del entregable	Descripción actividad del Entregable
1	Inicio del Proyecto	<ul style="list-style-type: none"> • Organigrama y registro de Integrantes del Proyecto. • Roles y responsabilidades de integrantes del Proyecto • Diagrama de red de la conexión de acceso remoto actual. • Estrategia de gestión de interesados
2	Planificación	<ul style="list-style-type: none"> • Plan de Gestión del Proyecto: Elaboración y aprobación del plan integrador del proyecto (dinámico conforme avanza el proyecto). Contempla lo siguiente: Alcance de Proyecto, Cronograma de Proyecto, Plan de gestión financiera, Plan de Recursos Humanos, Plan de gestión de comunicaciones, Plan de Gestión de Riesgos, Plan de Gestión de los interesados.
3	Implementación	Actividad de gestión que consiste dirigir y gestionar la ejecución del proyecto, actualizar el mismo producto de las solicitudes de cambios e informar sobre el desempeño de trabajo.
4	Seguimiento y Control	Actividad de gestión que consiste en monitorear, analizar y regular el progreso y desempeño del Proyecto implementado, con el fin de identificar áreas en las que el Plan requiere cambios y aseguramiento del correcto funcionamiento de la solución implementada.
5	Cierre	Actividad de gestión que consiste en cerrar formalmente el proyecto. Incluye: <ul style="list-style-type: none"> • Documentar toda la configuración de la nueva solución • Documentar Lecciones Aprendidas. • Archivar toda la documentación relevante del proyecto para ser usado como datos históricos.

Fuente: Elaboración Propia,2021

La nueva solución de acceso remoto con doble factor de autenticación y control de acceso dispositivo consiste en establecer una conexión de acceso remoto a un alto nivel de seguridad empleando el protocolo SSL(Secure Sockets Layer) que es un protocolo de capa sesión de OSI que permite autenticar, cifrar y descifrar toda la información enviada a través del internet adicional complementa el protocolo TLS(Transport Layer Security) versión 1.2 que permite sumar y brindar una conexión remota más segura es decir técnicamente me refiero a una VPN(Virtual Private Network) tipo SSL/TLS, también a la VPN SSL/TLS se agrega un certificado auto firmado permitiendo establecer parámetros y criterios de cifrado muy robusto y la mejor opción empleado es el cifrado SHA512 que permite brindar una longitud amplia y robusta para que en caso algún atacante intente descifrar la contraseña este intento demore demasiados años a diferencia de establecer criterios simples de cifrados más bajos que permitiría que un atacante puede lograr vulnerarlo, el cifrado implementado en la nueva solución pertenece al algoritmo RSA(Rivest, Shamir y Adleman) la cual es uno de los sistemas de cifrado asimétricos más exitosos y robustos en comparación al algoritmo MD5 y otros en la actualidad debido a que RSA tipo SHA usa dos claves diferentes: una pública y una privada en donde ambos operan de forma complementaria entre sí, lo que significa que una data cifrada con uno de ellos sólo puede ser descifrado por su contraparte, la nueva solución permite implementar varios componentes principales que trabajan entre sí una vez culminada la implementación y son los siguientes:

1.-Firewall Palo Alto:

Es un componente principal que integra la solución remota VPN SSL con el doble factor de autenticación y el control de acceso de dispositivo, este equipo contiene las configuraciones de redes tanto segmentos internos y externos en sus interfaces de red y rutas estáticas configuradas, adicional para mayor detalle en las especificaciones técnicas de hardware, red y seguridad del Firewall 3050 ver Anexo 1, Anexo 3 y Anexo 4

2.-Agente VPN SSL Global Protect: Debe estar instalado y configurado en los dispositivos de cada colaborador para poder establecer la conexión remota segura, en este agente se configura la ip pública de la VPN es decir la interfaz WAN del Firewall Palo Alto a donde todos los usuarios apuntarán para habilitar la sesión remota segura, también es el componente la cual el colaborador ingresará su usuario y Password para la autenticación.

3.-Portal VPN SSL Global Protect: Es un componente que a nivel de configuración permite asociar el perfil de autenticación radius (Remote Access Dial In User Service), además de brindar la página de inicio que mostrará el agente VPN SSL que permite brindar la opción de usuario y password para la autenticación de cada usuario.

4.-Gateway VPN SSL Global Protect: Es el componente que proporciona seguridad para el tráfico de aplicaciones de la VPN SSL, tener en cuenta que todos los agentes Global Protect necesitan apuntar a un Gateway para que pueda aplicar la validación de autenticación y mecanismos de acceso de los usuarios a los recursos internos de la empresa privada, maneja el access list de acceso donde se coloca la red remota asignada(172.31.1.0/24) a la VPN y el destino la cual son las redes privadas internas (192.168.25.0/24, 192.168.90.0/24, 192.168.99.0/24) de la empresa privada, el Gateway de la VPN es la IP 190.187.118.157.

5.-Servidor Virtual Radius: Es el componente que se utiliza como intermediario entre el servidor de directorio activo 192.68.25.21 y el firewall Palo Alto a la cual se integra este servidor Proxy usando el método de autenticación Radius que es uno de los protocolos de autenticación muy seguro además este componente protege y sirve como proxy evitando un contacto directo hacia el directorio activo, adicional se instala el servicio de doble factor y mediante API (Application Programming Interface) se comunica hacia la consola de administración de doble factor de autenticación la cual es la siguiente: <https://admin-ae6f5f68.duosecurity.com/admins/profile>.

6.-Consola de administración doble factor de autenticación: El presente complemento una vez implementado se encarga de realizar el mecanismo del doble factor de autenticación a los usuarios registrados que intentan autenticarse por el acceso remoto a través de la VPN SSL Global Protect otorgándole una capa de seguridad adicional en el proceso de autenticación, en el presente componente se configura los dispositivos(smartphone) y se sincronizan los usuarios autorizados para poder brindarles acceso mediante el mecanismo del doble factor de autenticación.

7.-Perfil HIP Profile de control de acceso de dispositivo: El componente llamado perfil de identificación de host el cual permite el control de acceso de dispositivo validando las características activas y de ejecución de varios software permitidos y recomendados a nivel de seguridad informática, dentro de los perfiles se ha configurado considerando la experiencia técnica y profesional el cual consiste en permitir que el dispositivo tenga instalado y activo un antivirus y un antimalware por lo menos con 1 día de escaneo realizado, también se considera dentro de los criterios que debe tener activa la función de cifrado de disco duro, el software que también debe tener instalado y activo en el dispositivo es la función DLP (Data Loss Prevention) para evitar la fuga de datos, adicional deben tener instalados y activos los parches de Windows a nivel de sistema operativo y el firewall de Windows activo y habilitado, otro criterio técnico a considerar es el sistema operativo versión Windows 10 Enterprise, debe estar dentro del dominio de la empresa privada y utilizar la versión 5 del agente Global Protect.

Dentro del alcance general del proyecto de implementación de la nueva solución, también se contemplan los siguientes puntos a realizar:

- ✓ Gestionar e Instalación de 250 Licencias Duo MFA Cisco y Licencia Global Protect de Palo Alto con Soporte Fábrica por 1 año, dentro de las cuales incluye las 10 licencias que corresponden a los usuarios de pruebas.
- ✓ Se utilizará licencias temporales en caso exista demora en la adquisición de licenciamiento definitivo, las licencias temporales tienen una duración de 6 meses con una prórroga de extensión de 6 meses adicionales para completar el año para el caso del control del dispositivo y para el caso de doble factor de autenticación la licencia temporal tiene una limitante de 10 usuarios de forma definitiva.
- ✓ Configuración de la red privada virtual Global Protect con los mejores parámetros de seguridad en el Firewall Palo Alto de Producción de la empresa Privada.
- ✓ Implementación y configuración de la solución Duo doble factor de autenticación y el control de dispositivo para 10 agentes iniciales y progresivamente se completarán el despliegue a los 200 agentes restantes en grupo de 50.
- ✓ El implementador realizará uso del mejor criterio a nivel de seguridad informática para la implementación de doble factor de autenticación y también los mejores criterios de acceso de dispositivo basados en las mejores prácticas de seguridad informática y utilizando su amplia experiencia, los criterios técnicos mencionados de seguridad informática son el uso de protocolos de autenticación como el SSL y TLS, además del cifrado usando un mecanismo de alto nivel como el algoritmo RSA empleando el cifrado tipo SHA 512 y también criterios técnicos de alto valor a nivel de seguridad informática como el tener mínimo 1 antivirus y 1 antimalware instalado y activo con 1 día como mínimo de último escaneo y entre otras funciones activas como el cifrado de disco duro, DLP activo, versión de parches de Windows instalados todo esto relacionado en función a permitir el control de acceso de dispositivo implementado en firewall Palo Alto para la conexión de red privada virtual SSL/TLS Global Protect .

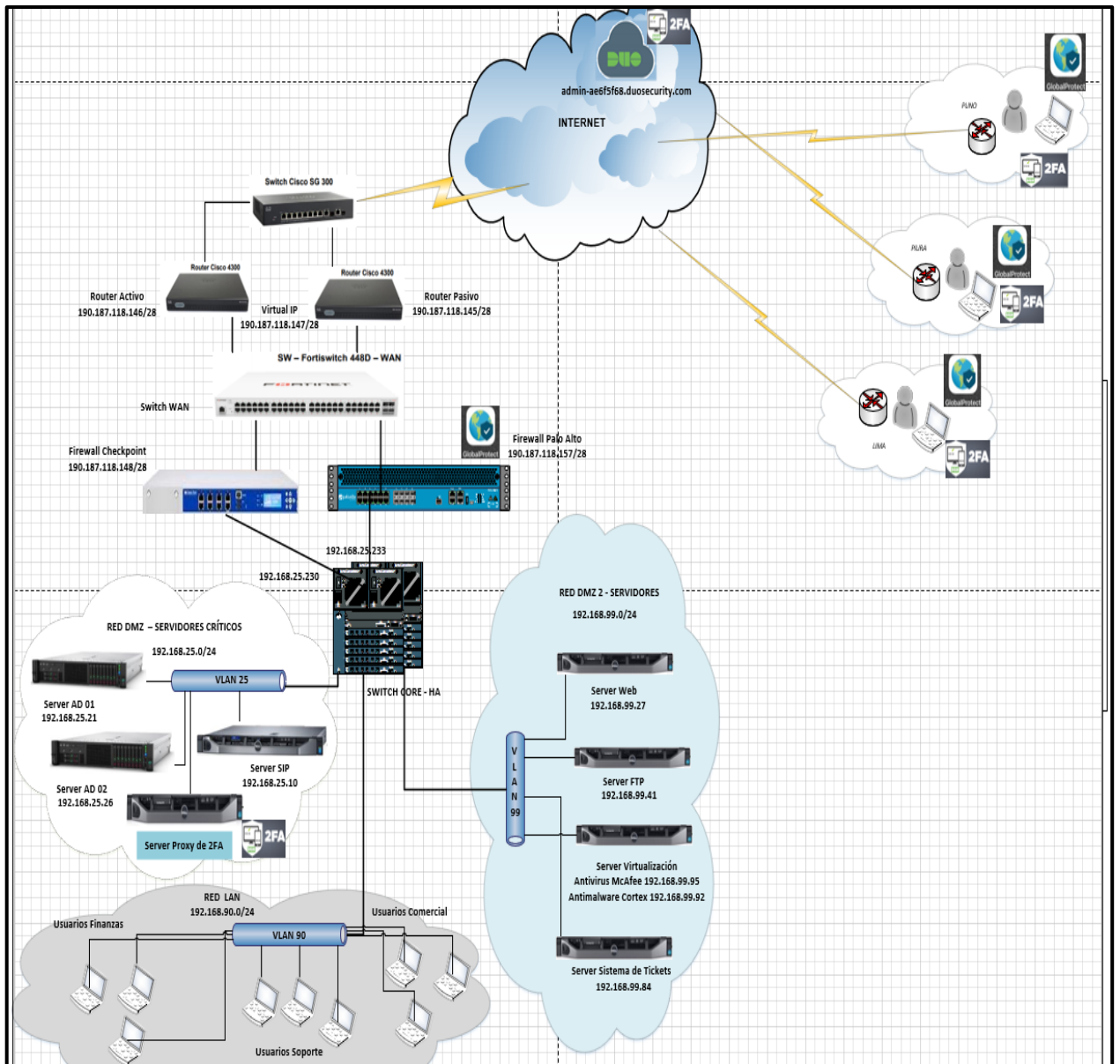
- ✓ Para la autenticación de usuarios se debe implementar en la integración entre el firewall, el servidor proxy además del directorio activo mediante el protocolo RADIUS (Remote Access Dial In User Service) la cual es un protocolo que destaca por ofrecer un mecanismo de seguridad, flexibilidad, capacidad de expansión y una administración simplificada de las credenciales de acceso a un recurso de red, el presente protocolo de autenticación fue seleccionado debido a que necesitaba tener un protocolo dedicado para la solución implementada ya que el protocolo LDAP es usando para la conexión VPN SSL Checkpoint de un solo factor de autenticación, ambos protocolos de autenticación soy muy utilizados y muy similares pero consideré implementar el Radius para permitir usar el protocolo de autenticación de forma dedicada para la nueva solución implementada.
- ✓ El implementador brindará un manual detallado para despliegue de la solución para los 10 agentes iniciales.
- ✓ Capacitación remota de administración de la solución implementada durante 4 horas sobre el procedimiento de autenticación y gestión administrativa de solución para el personal de la empresa privada.
- ✓ El implementador garantizará el correcto funcionamiento de la plataforma doble factor de autenticación y control de dispositivo implementado por un periodo de un mes, contando desde la fecha de aceptación de la entrega, plazo durante el cual la empresa privada podrá hacer uso del sistema a efectos de comprobar el cumplimiento del alcance solicitado y dentro del cual el implementador tiene la obligación de atender la solicitudes y resolver los incidentes presentados por la plataforma implementada y que son de su responsabilidad.
- ✓ El servidor proxy virtual implementado que corresponde a un componente de la solución de doble factor de autenticación será proporcionado por la empresa privada instalado en sus ambientes virtuales.
- ✓ Detallo los recursos mínimos necesarios para implementar el ambiente virtual del servidor proxy mencionado:
 - 2 virtual CPU
 - 200 GB de disco duro
 - 4 Gb de RAM
 - Sistema operativo Windows Server 2016
- ✓ Para el servidor Proxy del 2FA la empresa privada debe brindarle a nivel del firewall Palo Alto los permisos de acceso a internet por el puerto TCP 1812 para establecer la comunicación entre el servidor proxy y consola de administración en nube ambos componentes corresponden a la solución de doble factor de autenticación.

- ✓ La empresa privada brindará una cuenta de AD perfil administrador que se integrará a los componentes de la solución Duo 2FA, la cuenta será empleada únicamente para integrar la solución, luego de ello será custodiada por la empresa privada.
- ✓ Validar que la conexión remota nueva entre los agentes de los dispositivos y la consola de administración de la nueva solución, la cual debe ser de forma segura y controlada a nivel de dispositivo.
- ✓ El implementador brindará toda la documentación detallada de la implementación realizada como entregable de proyecto de implementación de la solución de doble factor de autenticación y control de acceso de dispositivo, la cual se detallará en la etapa de implementación.

El funcionamiento y operación de la nueva solución implementada consiste en lo siguiente el cual se puede identificar en el diagrama de red mostrado:

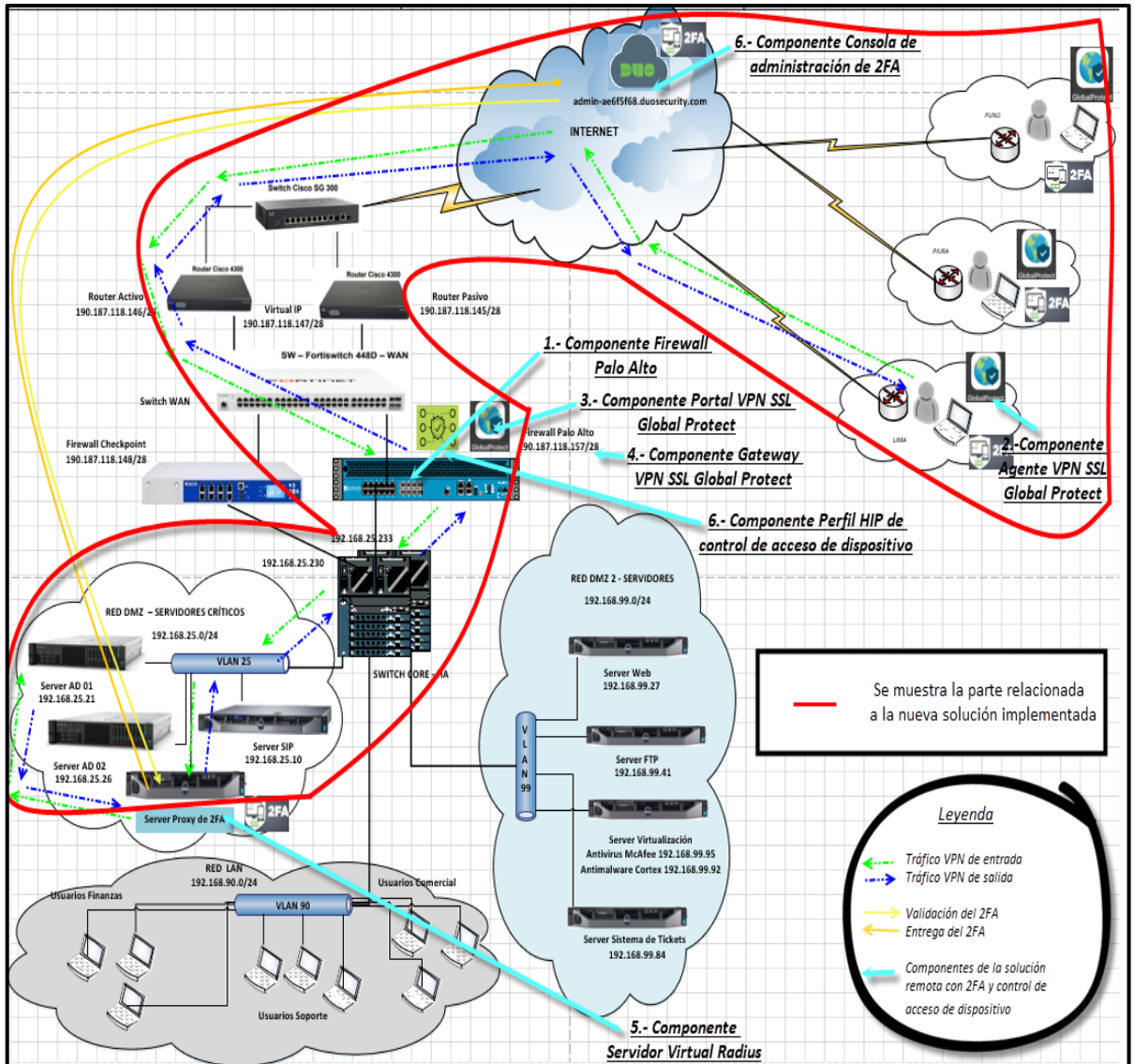
- 1.-El usuario se autentica en el agente VPN SSL/TSL Global Protect
- 2.-El firewall registra la petición de autenticación y se comunica con el servidor Proxy implementado y éste rápidamente consulta al directorio activo sobre la validez del usuario y password ingresado.
- 3.-Una vez validado el usuario y password el servidor Proxy se comunica con la consola de administración del doble factor de autenticación para validar el registro del usuario y dispositivo para finalmente responder y otorgarle al usuario el segundo factor de autenticación mediante la aplicación DUO Mobile de Cisco
- 4.-El usuario real mediante la aplicación DUO Mobile acepta la conexión y brinda autorización de la autenticación de doble factor.
- 5.-El proceso que en paralelo se revisa en el firewall Palo Alto es el de control de acceso de dispositivo mediante el perfil de identificación de host, el firewall realiza una validación de los componentes y funciones activas del dispositivo que inicia la conexión para finalmente dar por validado el dispositivo y brindar acceso a los recursos internos mediante RDP a través de políticas de seguridad de acceso a los recursos internos de la empresa privada.

Figura 33. Diagrama de red propuesto para el desarrollo del Proyecto.



Fuente: Elaboración Propia, 2021

Figura 34. Diagrama de red propuesto mostrando los componentes de la nueva solución implementada.



Fuente: Elaboración Propia, 2021

3.2.2 Cronograma de Proyecto:

Las actualizaciones del avance de las tareas del cronograma (archivo Microsoft Project), se realiza semanalmente por el Jefe de proyecto, los miércoles al finalizar el día, para luego presentarlos en las reuniones del avance del proyecto definido para el jueves de cada semana.

Las actividades son desarrolladas sobre la base de EDT, a través de una técnica de descomposición para cada actividad que tendrá una duración como máxima de 48 Horas.

La definición de los atributos para las actividades es desarrollada utilizando la EDT y el diccionario de EDT, en conjunto con el implementador.

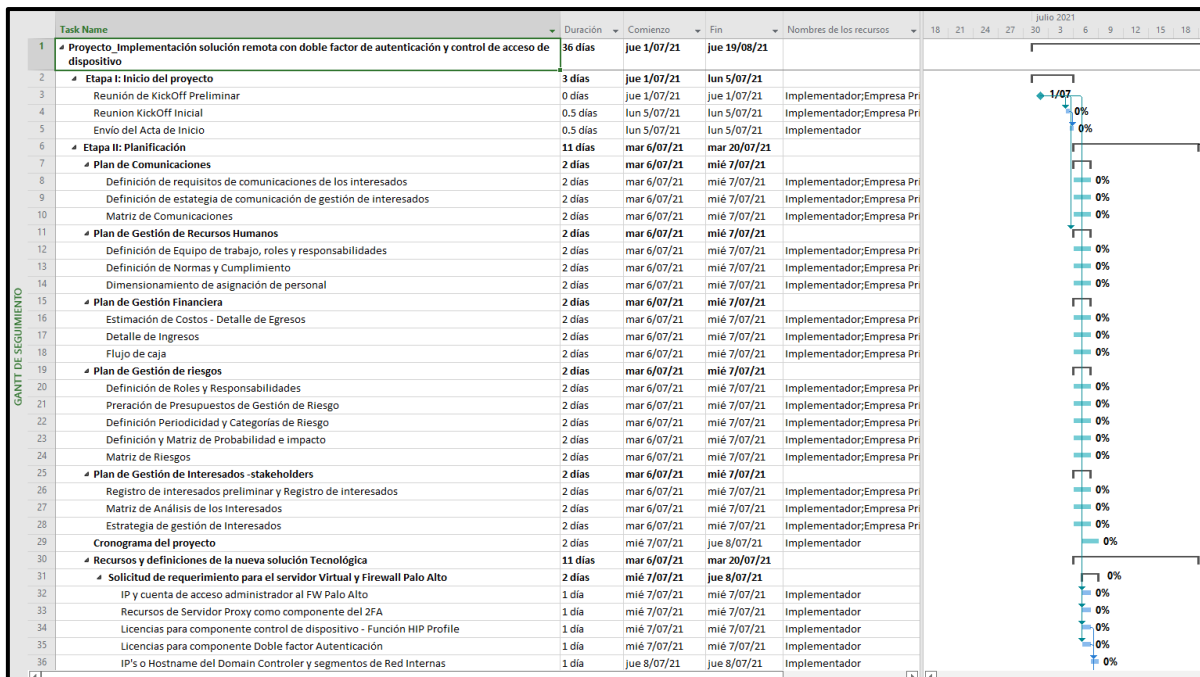
El listado de Hitos será definido por juicio del especialista implementador: Ever Pastor y será tomado en cuenta el desglose del EDT.

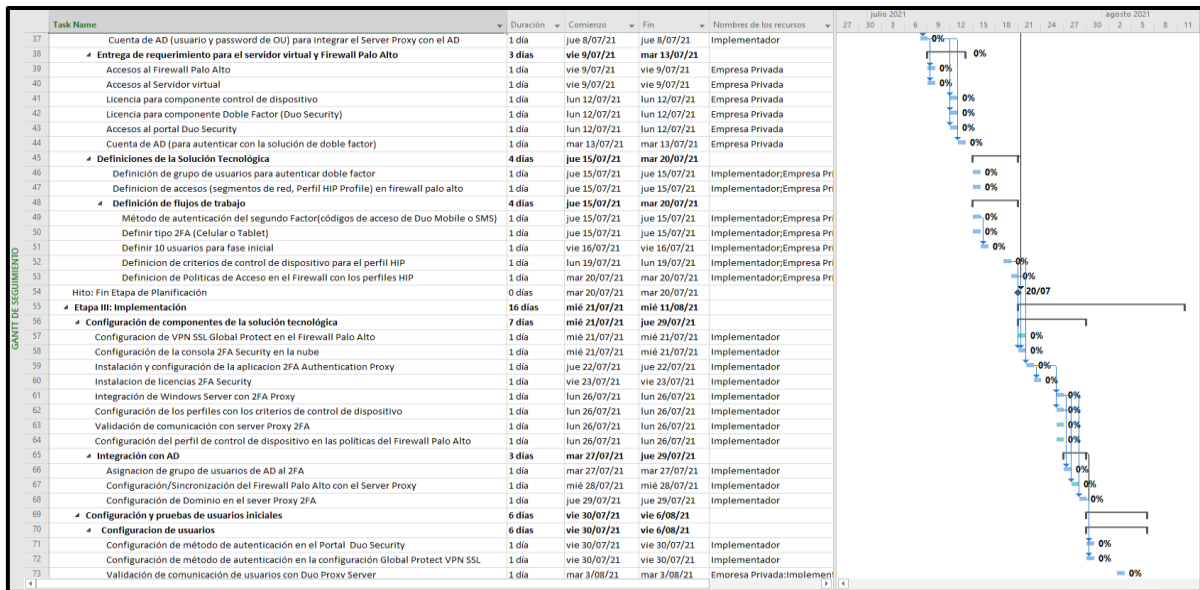
La actualización de adelantos y retrasos de las actividades se aplicarán de acuerdo con la disponibilidad de recursos y sus tiempos siempre y cuando se encuentre aprobado por jefe del proyecto.

Los requisitos de los recursos serán efectuados tomando en cuenta la siguiente información: La lista de actividades, los atributos de la actividad, uso de calendario de recursos, se considerará el criterio de la experiencia del implementador. Con relación a los recursos empleados en el presente proyecto serán de los siguientes tipos: Recursos Humanos, equipos y software.

La estimación de la duración será realizada con lo siguiente: Una lista de actividades, atributos de la actividad, calendario de recursos, requisitos de recursos, considerando el criterio y experiencia manejados en proyectos similares del especialista implementador Ever Pastor.

Figura 35. Cronograma del Proyecto





Fuente: Elaboración Propia,2021

3.2.3 Plan de Gestión Financiera

Se define los procesos de estimación de costos, detalle de ingresos y flujo de caja.

Para la estimación de costos dentro de las técnicas y herramientas en los procesos se utiliza la experiencia del personal de Implementaciones, Jefe y Gerente de Proyecto quienes ya anteriormente han participado en similares proyectos de tecnología en plataformas de seguridad de la información y para estimar los costos utilizamos el software de Excel la cual se elabora en el presente proyecto con un documento llamado cuadro de costo, los nombres de los expertos son Ever Pastor y Percy S.

En el proceso de determinar el presupuesto se utilizará la técnica de Suma de Costos considerando cronograma de proyecto y alcance como base para determinar los costos de cada paquete y componente, llegando a definir el costo del proyecto.

3.2.3.1 Detalle de Egresos

Tabla 10. Planilla mensual

PUESTO DE TRABAJO	PLANILLA MENSUAL \$
Gerente de Proyecto	1,800
Jefe del Proyecto	1,500
Implementador	1,200
Analista de Soporte	500
Gerente Comercial	1,800
Gerente Financiero	1,800

Fuente: Elaboración Propia,2021

Figura 36. Costo de Asignación de Personal

% DE ASIGNACION PERSONAL DE PROYECTO Implementación de 2FA y control de acceso de dispositivo							
Fecha de ultima actualización:		16/08/2021		Dolares		Utilización Mensual de Personal por %	
Moneda:		Dolares		INSERT			
Total Costo Personal:		1,826.43		TC:			
						1	2
DETALLE	Nro	PUESTOS DE TRABAJO	COSTO	ESTUDIOS	TOTAL	Julio-21	Agosto-21
PERSONAL	1	Gerente de Proyecto	673.32		40.40	2%	2%
PERSONAL	2	Jefe del Proyecto	561.10		392.77	30%	30%
PERSONAL	3	Implementador	503.74		957.11	80%	80%
PERSONAL	4	Analista de Soporte	187.03		355.36	80%	80%
PERSONAL	5	Gerente Comercial	673.32		40.40	2%	2%
PERSONAL	6	Gerente Financiero	673.32		40.40	2%	2%

Fuente: Elaboración Propia,2021

Figura 37. Costos de Consumibles y Servicios

COSTOS VALOR AGREGADO DEL PROYECTO Implementación de 2FA y control de acceso de dispositivo												
Fecha de ultima actualización:		16/08/2021		INSERTAR FILAS								
Moneda:		Dolares										
Costo Bienes y Servicios:		12,771.80		4.01								
Descripción	PROVEEDOR	#T/D	TIPO DE ITEM	CONDICIÓN DE CUOT.	CANTIDAD ITEM	CANTIDAD de CUOTA	Moneda	Costo U	COSTO MENSU.	MES INICIC	#MESES PAG	TOTAL
HABILITACION DEL PERSONAL									0.00			
Prueba Covid	Rimac	D	SERVICIO	UNICO	4	1	Dolares	40.00	160.00	1	0	160.00
SCTR - SALUD (Mediano Riesgo)	Rimac	D	SERVICIO	UNICO	2	1	Dolares	30.00	60.00	1	0	60.00
SCTR - PENSION (mediano Riesgo)	Rimac	D	SERVICIO	UNICO	2	1	Dolares	30.90	61.80	1	0	61.80
EQUIPOS DE PROTECCION PERSONAL // UNIFORMES									0.00			
Mascarilla,guantes,protector facial	Sodimac	D	CONSUMIBLE	UNICO	16	1	Dolares	40.00	640.00	1	0	640.00
Maletin de herramienta Soporte Microinformatico	Sodimac	D	BIEN	UNICO	2	1	Dolares	80.00	160.00	1	0	160.00
Utiles de oficina	Sodimac	D	CONSUMIBLE	UNICO	1	1	Dolares	50.00	50.00	1	0	50.00
TELEFONÍA- INTERNET									0.00			
Servicio Datos x 2 meses	Servicios	D	SERVICIO	UNICO	2	1	Dolares	300.00	600.00	1	0	600.00
OTROS									0.00			
Insumos / Consumibles / Refrigerios	Servicios	D	CONSUMIBLE	UNICO	2	1	Dolares	80.00	160.00	1	0	160.00
EPP	Servicios	D	CONSUMIBLE	UNICO	2	1	Dolares	40.00	80.00	1	0	80.00
Movilidad	Servicios	D	SERVICIO	UNICO	1	1	Dolares	300.00	300.00	1	0	300.00
Licenciamiento Palo Alto y Cisco por 12 meses	Servicios	D	SERVICIO	UNICO	1	1	Dolares	10,000.00	10,000.00	1	0	10,000.00
Caja chica // Contingencia	Servicios	D	SERVICIO	UNICO	1	1	Dolares	500.00	500.00	1	0	500.00

Fuente: Elaboración Propia,2021

3.2.3.2 Detalle de Ingresos

Tabla 11. Detalle de ingresos

Descripción	Tipo	Marca	Precio (\$)
Standard Cisco Duo 2FA edition	Licencia	CISCO	3,800.00
GlobalProtect subscription for device in an HA pair year 1, PA-850 - Fecha de inicio 01/06/21	Licencia	Palo Alto	4,800.00
Servicio de implementación de la solución.	IMPLEMENTACION	Servicios	7,000.00
Soporte de la solución por 3 meses	SOPORTE	Servicios	2,000.00
Capacitación remota de la solución - 04 horas	CAPACITACIÓN	Servicios	300.00
Gestión del proyecto	PROYECTOS	Servicios	3,100.00
Precio Total (\$)			21,000.00

Fuente: Elaboración Propia,2021

3.2.3.3 Flujo de Caja

A continuación, se presenta el flujo de caja:

Figura 38. Flujo de Caja

Concepto	Totales Dolares	VPN Dolares	%	1	2
				Jul-21	Ago-21
Ingresos	21,000.00	20,934.84	100.00%	15,000	6,000
Fijos	21,000.00	20,707.50		15000	6000
Variables	-	0.00			
Egresos	14,162.08	13,997.28	67.44%	13,357	585
Personal sueldo	1,390.28	1,364.18	9.82%	584.79	584.79
Personal bono	-	0.00	0.00%	-	-
Personal movilidad	-	0.00	0.00%	-	-
Bienes	160.00	158.26	1.13%	160.00	-
Servicios	11,681.80	11,554.94	82.49%	11,681.80	-
Arrendamiento	-	0.00	0.00%	-	-
Capex	-	0.00	0.00%	-	-
Consumibles	930.00	919.90	6.57%	930.00	-
Valor agregado	-	0.00	0.00%	-	-
Costo financiero	-	0.00	0.00%	-	-
Utilidad de Proyecto	6,837.92	6,937.56	32.56%	1,643	5,415
Contingencia	-	-	0.00%	-	-
Gestión del Servicio	-	-	0.00%	-	-
Utilidad bruta	6,837.92	6,937.56	32.56%	1,643	5,415
Utilidad bruta acumulada				1,643	7,059
			% Utilidad Bruta Acumulada	11.0%	33.6%

Fuente: Elaboración Propia,2021

Figura 39. Resumen de Flujo de Caja

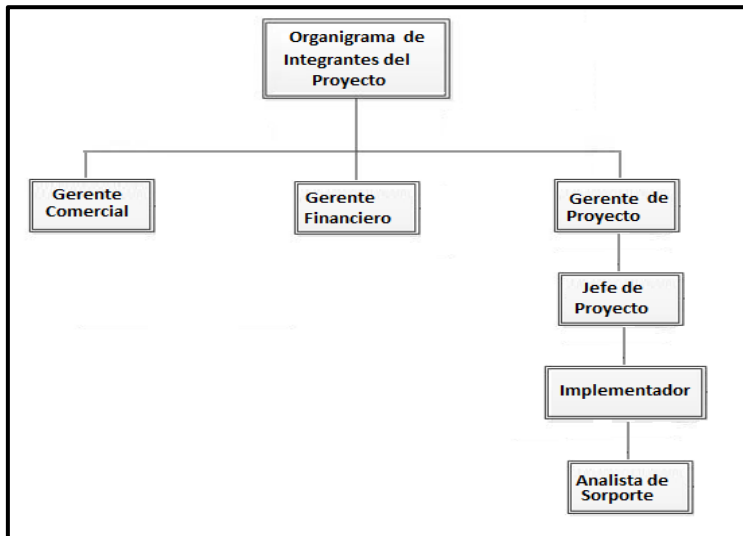
Ingresos	21,000.00	100.0%
Fijos	21,000.00	100.0%
Variables	-	0.0%
Egresos	14,162.08	67.4%
Personal sueldo	1,390.28	9.8%
Personal bono	-	0.0%
Personal movilidad	-	0.0%
Bienes	160.00	1.1%
Servicios	11,681.80	82.5%
Arrendamiento	-	0.0%
Capex	-	0.0%
Consumibles	930.00	6.6%
Valor agregado	-	0.0%
Costo financiero	-	0.0%
Utilidad de Proyecto	6,837.92	32.6%
Contingencia	-	0.0%
Gestión del Servicio	-	0.0%
Utilidad bruta	6,837.92	32.6%

Fuente: Elaboración Propia,2021

3.2.5 Plan de Recursos Humanos:

A continuación, presento la estructura organizacional:

Figura 40. Organigrama de Integrantes del Proyecto - RH



Fuente: Elaboración Propia,2021

3.2.5.1 Roles y Responsabilidades:

-Gerente Financiero: Su rol es ser el responsable ejecutivo para la Calidad del Proyecto. Se encarga de aprobar e informar la Calidad del proyecto al directorio y su responsabilidad es Proteger en todo momento al proyecto de amenazas externas, adicional logra evitar cambios innecesarios.

Sus niveles de autoridad son los siguientes:

- ✓ Autoriza cambios que afecten la línea base del Proyecto
- ✓ Se encarga de reportar a Directorio
- ✓ Supervisa al Gerente de Proyecto

-Gerente del Proyecto: Su rol es realizar las actividades necesarias para gestionar la calidad del proyecto y su responsabilidad es asegurar el cumplimiento del nivel y grado de calidad establecido y Revisar estándares, revisar entregables, aceptar entregables o disponer su reproceso, deliberar para generar acciones correctivas, aplicar acciones correctivas

Sus niveles de autoridad son los siguientes:

- ✓ Exigir al equipo de proyecto que los entregables cumplan con el nivel y grado de calidad.
- ✓ Reporta a Patrocinador
- ✓ Supervisa al Equipo de Proyecto

-Gerente Comercial: Su rol es realizar las coordinaciones necesarias con logística para gestionar el licenciamiento de la solución implementada.

-Equipo de Proyecto (Implementador y Jefe de Proyecto): Su rol es realizar las actividades necesarias para asegurar la calidad según estándares y activos de la organización tomando en cuenta las listas de control de calidad. Elaborar los entregables con la calidad requerida y según estándares. Su responsabilidad es aplicar los estándares y metodologías de Calidad de Punto Visual y las establecidas en el Proyecto en la elaboración de los entregables. Ejecución de la implementación de los cambios aprobados. Sus niveles de autoridad son los siguientes:

- ✓ Aplicar los recursos que se le han asignado.
- ✓ Reporta a Gerente del Proyecto
- ✓ Supervisa a N/A

3.2.5.2 Normas y Cumplimiento:

A continuación, se describe las principales normas de cumplimiento:

Horario de trabajo:

- La hora de entrada de trabajo es a partir de las 9:00 a.m. y la hora de salida es a las 6:00 p.m.
- Las justificaciones por tardanza deberán ser informadas al gerente de proyecto.
- Las ausencias deberán ser justificadas por el trabajador según el formato del área de recursos humanos

Reglamento de Vestimenta:

- Hombres: camisa clara, pantalón y saco oscuro, cabello corto, portar doble mascarilla y protector facial.
- Mujeres: vestimenta formal, cabello recogido, portar doble mascarilla y protector facial.

3.2.5.3 Dimensionamiento de asignación de personal:

Se establece el dimensionamiento de la asignación del personal por mes durante el proyecto.

Figura 41. Asignación de Personal

% DE ASIGNACION PERSONAL DE PROYECTO Implementación de 2FA y control de acceso de dispositivo							
Fecha de ultima actualizacion:		16/08/2021				Utilización Mensual de Personal por %	
Moneda:		Dolares		INSERT			
Total Costo Personal:		1,826.43					
				TC:			
						1	2
DETALLE	Nro	PUESTOS DE TRABAJO	COSTO	ESTUDIOS	TOTAL	Julio-21	Agosto-21
PERSONAL	1	Gerente de Proyecto	673.32		40.40	2%	2%
PERSONAL	2	Jefe del Proyecto	561.10		392.77	30%	30%
PERSONAL	3	Implementador	503.74		957.11	80%	80%
PERSONAL	4	Analista de Soporte	187.03		355.36	80%	80%
PERSONAL	5	Gerente Comercial	673.32		40.40	2%	2%
PERSONAL	6	Gerente Financiero	673.32		40.40	2%	2%

Fuente: Elaboración Propia,2021

3.2.6 Plan de Gestión de Comunicaciones

3.2.6.1 Definición de requisitos de comunicaciones de los interesados

Definimos los requisitos de comunicaciones de todos los interesados/integrantes del proyecto:

- Claridad:** Fácilmente comprensibles y si es posible, con ejemplos prácticos o casos demostrativos.
- Precisión:** Completa y precisa en todas partes, sin lagunas u omisiones.
- Adecuada redacción:** Lenguaje adaptado a la mentalidad y capacidad del receptor y además adoptar una forma interesante y la forma mínima de extensión posible.
- Objetividad:** Tanto de parte del comunicador como del receptor.
- Difusión:** Llegada efectiva a todos los interesados en el momento más oportuno.
- Bloqueadores:** Se ha identificado como posible bloqueador el estado organizacional del Área Comercial, ya que al ser el core del negocio gozan de un gran poder en la organización y podrían presentar resistencia al cambio o indisposición para comunicar y compartir.
- Canales de Comunicación:** Se tienen 3 canales de comunicación el cual es el correo electrónico, llamada telefónica, reuniones por la aplicación teams o zoom.

3.2.6.2 Estrategia de Comunicación de Gestión de Interesados

Tabla 12. Estrategia de Comunicación de Gestión de Interesados

Interesado	Interés en el Proyecto	Impacto	Estrategia para obtener apoyo y reducir conflictos
Gerente Comercial	Disponibilidad de Información oportuna y exacta para la toma de decisiones comerciales	Alto	- Las reuniones con el interesado deben ser previamente planeados con el patrocinador. - En las reuniones el patrocinador debe estar presente
Gerente Financiero-Patrocinador	Rentabilidad de los elementos publicitarios de la Organización. Integridad de la información. Cumplimiento de políticas de empresa	Alto	- Cualquier aviso de conflicto en el proyecto que presente alto riesgo debe ser previamente discutido con el patrocinador -Correos dirigidos con copia a Gerencia deben ser copiados también al gerente financiero
Gerente de Proyecto	Responsable de que la implementación se realice de forma adecuada y correcta en los tiempos establecidos	Media	-Mostrar los avances en fases del de proyecto -Estar presente siempre en las reuniones de seguimiento del proyecto.
Jefe de Proyecto	Facilidad en las operaciones diarias (gestión de reservas, recursos) y reportes de estados de seguimiento del Proyecto	Media	-Mostrar el seguimiento adecuado de los avances de las actividades de las fases de la implementación.
Implementador	Información oportuna y confiable de los avances de la implementación realizada.	Baja	-Confirmar los avances de la implementación mostradas por el Jefe del Proyecto

Fuente: Elaboración Propia,2021

3.2.6.3 Matriz de comunicaciones

Tabla 13. Matriz de comunicaciones

Interesados principales	Responsables de distribuir la información	Información que será comunicada (entregables)	Método de Comunicación para utilizar (Llamada Telf., correo electrónico,	Frecuencia de comunicación (mensual, semanal,	Dimensión de Comunicación	Escalamiento		
						Tipo	Tiempo	Responsable
Gerente de Proyecto	Equipo de proyecto	Registro de Interesados	Correo electrónico	Mensual	Formal Escrito	Push	>5 días	Patrocinador
Gerente Comercial	Gerente de proyecto	Informe de desempeño	Reunión, Correo electrónico	Quincenal	Formal Verbal y Escrito	Interactivo, Push	>10 días	Patrocinador
Gerente Comercial	Gerente de Proyecto	Objetivos del Proyecto	Reunión, Correo Electrónico	Una sola vez	Formal Verbal y Escrito	Interactivo, Push	>10 días	Patrocinador
Gerente de Proyecto	Equipo del proyecto	Solicitud de Cambio	Correo electrónico	Semanal	Formal Escrito	Push	>5 días	Comité de control de cambios
Gerente de proyecto	Gerente Financiero (Patrocinador)	Cambio en la prioridad del proyecto o en el plan estratégico de la empresa	Reunión, Correo Electrónico	Una sola vez	Formal Verbal y Escrito	Interactivo, Push	>10 días	Gerente General Punto Visual
Gerente Financiero (Patrocinador)	Gerente de proyecto	Informe de desempeño	Correo Electrónico	Mensual	Formal Escrito	Push	>5 días	Gerente Comercial
Gerente de Proyecto	Equipo del proyecto	Estrategia de Gestión de los interesados	Correo electrónico	Mensual	Formal Escrito	Push	>5 días	Gerente Comercial
Jefe del Proyecto	Equipo de proyecto	-Plan de Gestión de las comunicaciones - Actualizaciones a los documentos del proyecto - Actualización al Plan para la dirección del proyecto - Actualización a los activos de los procesos de la organización.	Correo Electrónico	Quincenal	Formal Escrito	Push	>5 días	Gerente de Proyecto
Comité de control de Cambios	Equipo de proyecto	Solicitud de cambio aprobada	Reunión	Semanal	Formal Verbal	Interactivo	>10 días	Patrocinador

Implementador	Equipo de proyecto	Estándares de Tecnología	Correo Electrónico	Semanal	Formal Escrito	Pull	>5 días	Gerente del Proyecto
Implementador	Equipo de proyecto	Propuesta de Solución 2FA Entregada	Reunión, Correo electrónico	Una sola vez	Formal Verbal y Escrito	Interactivo, Push	>5 días	Gerente del Proyecto
Implementador	Equipo de proyecto	Informe de desempeño de la Solución 2FA	Reunión, Correo Electrónico	Quincenal	Formal Verbal y Escrito	Interactivo	>3 días	Gerente del Proyecto

Fuente: Elaboración Propia, 2021

3.2.7 Plan de Gestión de Riesgo

El presente plan de utiliza como herramienta una serie de procesos para gestionar los riesgos, se realiza el proceso de planificación de gestión de riesgos la cual consta del análisis de riesgos de todos los involucrados del proyecto, luego se identifican los riesgos como segundo proceso y como tercer proceso se efectúa un análisis cualitativo de riesgos, para finalmente establecer una respuesta a los riesgos identificados para este caso se traduce en controles a todos los riesgos registrados.

También se establece los roles y responsabilidades de los integrantes del proyecto en cada proceso del desarrollo del plan de riesgo.

Se elabora la preparación del tiempo y costo empleado de los integrantes del proyecto de implementación en cada proceso del desarrollo del plan de riesgo, la periodicidad de la gestión de riesgos es sólo 1 vez y en la fase de planificación del presente proyecto, también se elabora la definición de probabilidad e impacto, matriz de probabilidad e impacto, finalmente se elabora la matriz de riesgos con las estrategias de respuesta.

Para la elaboración el plan de riesgos se definió analizar activos a proteger como información, personal, servicios y en general identificar riesgos en los procesos del proyecto.

3.2.7.1 Roles y Responsabilidades

Defino los roles y responsabilidades del equipo de gestión de riesgos.

Tabla 14. Roles y Responsabilidades

Proceso	Roles del Equipo de Gestión de Riesgos	Personas	Responsabilidades
Planificación de Gestión de Riesgos	Líder	Gerente de Proyecto	Definir el plan de Gestión de Riesgos. Dirigir las actividades de gestión de riesgos.
	Miembros	Jefe de Proyecto, Implementador	Ejecutar las actividades de gestión de riesgos.
Identificación de riesgos	Líder	Gerente de Proyecto	Organizar entrevistas. Dirigir reuniones de expertos.
	Miembros	Patrocinador, Jefe de Proyecto, Implementador	Proveer Juicio de Expertos. Analizar las amenazas y oportunidades de los riesgos. Ejecutar entrevistas organizadas.
Análisis Cualitativo de Riesgos	Líder	Gerente de Proyecto	Dirigir actividades.
	Miembros	Jefe de Proyecto, Implementador	Definir las escalas de probabilidad e impacto. Desarrollar la matriz de probabilidad e impacto.
	Líder	Gerente de Proyecto	Planificar la ejecución de respuestas. Justificar de los costos de respuesta a los riesgos.

Planificación de Respuesta a los Riesgos	Miembros	Jefe de Proyecto, Implementador	Definir las respuestas a los riesgos que amenazan la continuidad del proyecto.
Seguimiento y Control de Riesgos	Líder	Jefe de Proyecto	Supervisar la ocurrencia de riesgos y ejecución de las respuestas.
	Miembro	Implementador	Ejecutar las respuestas a los riesgos. Identificar riesgos secundarios.

Fuente: Elaboración Propia,2021

3.2.7.2 Preparación de Presupuesto del personal por proceso de Gestión de Riesgo

A continuación, se detalla el presupuesto que interviene en la gestión de riesgos del proyecto, el presente costo está definido dentro de la asignación de costo de personal.

Tabla 15. Presupuesto del personal por proceso de Gestión de Riesgo

Procesos	Personas		Días	Costo / hora	Total (USD)
Planificación de Gestión de Riesgos	Líder	Gerente de Proyecto	1	30	30
	Miembros	Jefe de Proyecto	2	20	40
		Implementador	2	10	20
	Total				90
Identificación de riesgos	Líder	Gerente de Proyecto	1	30	30
	Miembros	Jefe de Proyecto	2	20	40
		Implementador	2	10	20
	Total				90
Análisis Cualitativo de Riesgos	Líder	Gerente de Proyecto	2	30	60
	Miembros	Jefe de Proyecto	1	20	20
		Implementador	1	10	10
	Total				90
Planificación de Respuesta a los Riesgos	Líder	Gerente de Proyecto	1	30	30
	Miembros	Jefe de Proyecto	1	20	20
		Implementador	2	10	20
	Total				70
Seguimiento y Control de Riesgos	Líder	Jefe de Proyecto	1	20	20
	Miembro	Implementador	2	10	20
	Total				40
Costo Total				380	

Fuente: Elaboración Propia,2021

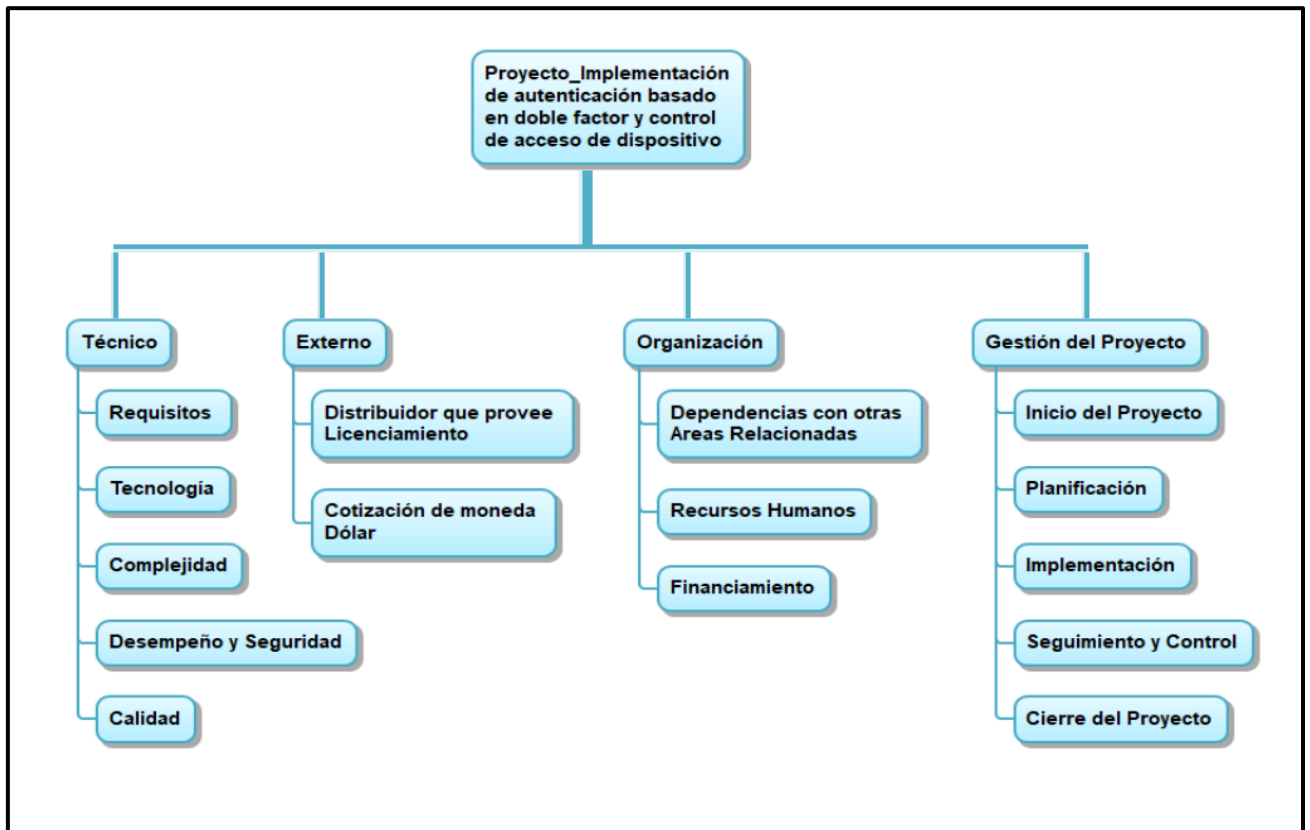
3.2.7.3 Periodicidad

La Planificación de Gestión de Riesgos se realiza en la fase de Planificación del Proyecto con la periodicidad de solo una vez; con respecto a Identificación de riesgos, Análisis Cualitativo de Riesgos y Planificación de Respuesta a los Riesgos se ejecuta también en la fase de Planificación del Proyecto considerando que su periodicidad es una sola vez.

3.2.7.4 Categorías de Riesgos

Las categorías de riesgos: Técnicas, Externas, Organización y Gestión del proyecto las cuales cada categoría consta de subcategorías de acuerdo con lo presentado.

Figura 42. EDT de categorías de Riesgos



Fuente: Elaboración Propia,2021

3.2.7.4 Definición de Probabilidad e impacto

Se describen las escalas de probabilidades e impacto:

Escala de Probabilidad:

0.8 = Me sorprendería si no ocurriese

0.6 = Más probable a que ocurra a que no ocurra.

0.4 = Tan Probable que ocurra como que no ocurra.

0.3 = Más Probable que no ocurra a que sí.

0.2 = Me sorprendería si ocurre

Escala de Impacto:

0.8 = Muy Alto; 0.7 = Alto; 0.5 = Medio; 0.3 = Bajo; 0.1 = Muy Bajo

Tabla 16. Escalas de Impacto de un Riesgo sobre los Principales Objetivos del Proyecto

Condiciones definidas para Escalas de Impacto de un Riesgo sobre los Principales Objetivos del Proyecto					
Objetivos del Proyecto	Muy Bajo (0.1)	Bajo (0.3)	Moderado (0.5)	Alto (0.7)	Muy Alto (0.8)
Costo: El costo total del proyecto será de US\$ 21,000	Aumento del presupuesto < 3%	Aumento del presupuesto < 5%	Aumento del presupuesto entre 5 y 8 %	Aumento del presupuesto entre 8 y 10 %	Aumento del presupuesto > 10%
Tiempo: El proyecto tiene una duración de 2 meses y se inició el 1 de Julio de 2021	Retraso de la finalización del proyecto < 5 días	Retraso de la finalización del proyecto < 10 días	Retraso de la finalización del proyecto entre 10 y 20 días	Retraso de la finalización del proyecto entre 20 y 30 días	Retraso de la finalización del proyecto > 30 días
Alcance: El proyecto debe completar la culminación de los entregables en las siguientes fases del Proyecto: -Inicialización -Planeamiento -Implementación -Seguimiento y Control -Cierre	Cambios mínimos que no afectan ni al presupuesto ni al cronograma.	Cambios que afectan al presupuesto < 5% y/o al cronograma < 10 días	Cambios que afectan al presupuesto entre 5 y 8% y/o al cronograma entre 10 y 20 días	Cambios que afectan al presupuesto entre 8 y 10% y/o al cronograma entre 20 y 30 días	Cambios que afectan al presupuesto > 10% y/o al cronograma en > 30 días
Calidad: El proyecto debe generar pocas incidencias o defectos operacionales durante la fase de implementación de la solución, de tal manera que no retrase el cronograma y costo del proyecto.	Número de defectos en la solución < 3	Número de defectos en la solución entre 3 y 8	Número de defectos en la solución entre 8 y 15	Número de defectos en la solución entre 15 y 20	Número de defectos en la solución > 20

Fuente: Elaboración Propia,2021

3.2.7.5 Matriz Probabilidad e Impacto

Tabla 17. Matriz Probabilidad e Impacto

Prob.	Amenazas					Oportunidades				
0.8	0.08	0.24	0.4	0.56	0.64	0.64	0.56	0.4	0.24	0.08
0.6	0.06	0.18	0.3	0.42	0.48	0.48	0.42	0.3	0.18	0.06
0.4	0.04	0.12	0.2	0.28	0.32	0.32	0.28	0.2	0.12	0.04
0.3	0.03	0.09	0.15	0.21	0.24	0.24	0.21	0.15	0.09	0.03
0.2	0.02	0.06	0.1	0.14	0.16	0.16	0.14	0.1	0.06	0.02
	0.1	0.3	0.5	0.7	0.8	0.8	0.7	0.5	0.3	0.1

Fuente: Elaboración Propia,2021

Tabla 18. Clasificación de Riesgo

Riesgo Aceptable	
Riesgo Moderado	
Riesgo Alto	

Fuente: Elaboración Propia,2021

3.2.7.6 Matriz de Riesgo

Como objetivo se tiene documentar todas las lecciones aprendidas durante el desarrollo del proyecto y ante cualquier inconveniente se registra las incidencias presentadas con relación a sus riesgos y sus resoluciones, a continuación, evidenciamos la matriz de riesgo elaborada.

Tabla 19. Matriz de Riesgo

Tipo	Activo	Descripción	ID Riesgo	Descripción del Riesgo	Responsable	Impacto	Probabilidad de ocurrencia	Riesgo	Evaluación del Riesgo	Opc.de tratamieto de riesgo	Controles
AMENAZA	PROYECTO	Proyecto con licencias	R01	Demora en la entrega de la licencia por parte de proveedor	Gerente de Proyecto	0.3	0.4	0.12	Aceptable	Aplicar controles	- Hacer un buen seguimiento a la llegada de la licencia (Preventivo) - Escalar el caso para licencia temporal (Correctivo)
			R02	Falta de acceso a la gestión de la licencia en el portal del proveedor	Gerente de Proyecto	0.3	0.3	0.09	Aceptable	Aplicar controles	- Revisión previa del acceso a la gestión de los productos en el portal del fabricante (Preventivo) - Solicitar acceso a la gestión de licencia en el portal del fabricante (Correctivo)
			R03	Entrega de la licencia incompleto por parte de proveedor	Gerente de Proyecto	0.3	0.3	0.09	Aceptable	Aplicar controles	- Hacer una revisión de la licencia entregados (Preventivo) - Escalar el caso para solicitar una licencia temporal (Correctivo)
			R04	Producto no contemplados en el alcance	Gerente de Proyecto	0.5	0.4	0.2	Moderado	Aplicar controles	- Hacer revisión detallada del alcance en el kickoff (Preventivo) - Escalar con la ejecutiva de cuentas para la validación de la adquisición del producto no contemplado (Correctivo)
			R05	Falta de seguimiento al requerimiento de los recursos, incluyendo el tiempo del cliente	Jefe de Proyecto	0.3	0.4	0.12	Aceptable	Aplicar controles	- Hacer una verificación de los recursos necesarios para la implementación (Preventivo) - Escalar con el Sponsor del proyecto (Correctivo)
			R06	Indisponibilidad del ingeniero implementador a cargo del proyecto a causa de la pandemia	Jefe de Proyecto	0.5	0.4	0.2	Moderado	Aplicar controles	- Mantener ingenieros con conocimiento similares (Preventivo) - Asignar a otro ingeniero con trabajo remoto (Correctivo)
			R07	No se cuenta con un alcance bien definido	Gerente de Proyecto	0.5	0.2	0.1	Aceptable	Aplicar controles	- Hacer revisión detallada del alcance en el kickoff (Preventivo) - Escalar con el Gerente de proyectos para revisión de alcance (Correctivo)
			R08	El acuerdo con el cliente no contemple la extensión de fechas en el cronograma	Gerente de Proyecto	0.7	0.3	0.21	Moderado	Aplicar controles	- Adecuada coordinación con el cliente en referencia a las actividades programadas (Preventivo) - Escalar el caso para que se coordine un prórroga en las fechas (Correctivo)
	INFORMACION	Acta de Inicio	R09	Política incorrecta para el control de acceso	Jefe de Proyecto	0.5	0.2	0.1	Aceptable	Aplicar controles	- Tener perfil definido de usuarios que pueden acceder a la información compartida(Preventivo) - Limitar y definir el acceso temporal a los usuarios que necesiten información del proyecto(Correctiva)

		R10	No existe respaldo de informacion		0.7	0.3	0.21	Mo dera do	Aplicar controles	- Guardar información en el compartido SharePoint del proyecto (Preventivo) - Establecer un control o bitácora semanal de validación de backup (Correctivo)
		R11	No existe contrato de confidencialidad		0.5	0.2	0.1	Ace ptab le	Aplicar controles	-Establecer un contrato de confidencialidad(Preventivo) -En las reuniones quincenales mencionar el aspecto de confidencialidad(Correctivo)
	Cronograma del proyecto	R12	Política incorrecta para el control de acceso	Jefe de Proyecto	0.5	0.2	0.1	Ace ptab le	Aplicar controles	-Tener perfil definido de usuarios que pueden acceder a la información compartida(Preventivo) -Limitar y definir el acceso temporal a los usuarios que necesiten información del proyecto(Correctiva)
		R13	No existe respaldo de informacion		0.7	0.3	0.21	Mo dera do	Aplicar controles	- Guardar información en el compartido SharePoint del proyecto (Preventivo) - Establecer un control o bitácora semanal de validación de backup (Correctivo)
		R14	No existe contrato de confidencialidad		0.5	0.2	0.1	Ace ptab le	Aplicar controles	-Establecer un contrato de confidencialidad(Preventivo) -En las reuniones quincenales mencionar el aspecto de confidencialidad(Correctivo)
		R15	Política incorrecta para el control de acceso		0.5	0.2	0.1	Ace ptab le	Aplicar controles	-Tener perfil definido de usuarios que pueden acceder a la información compartida(Preventivo) -Limitar y definir el acceso temporal a los usuarios que necesiten información del proyecto(Correctiva)
	Diagrama de Red Final	R16	No existe respaldo de informacion	Impleme ntador	0.7	0.3	0.21	Mo dera do	Aplicar controles	- Guardar información en el compartido SharePoint del proyecto (Preventivo) - Establecer un control o bitácora semanal de validación de backup (Correctivo)
		R17	No existe contrato de confidencialidad		0.5	0.2	0.1	Ace ptab le	Aplicar controles	-Establecer un contrato de confidencialidad(Preventivo) -En las reuniones quincenales mencionar el aspecto de confidencialidad(Correctivo)
		R18	Política incorrecta para el control de acceso		0.5	0.2	0.1	Ace ptab le	Aplicar controles	-Tener perfil definido de usuarios que pueden acceder a la información compartida(Preventivo) -Limitar y definir el acceso temporal a los usuarios que necesiten información del proyecto(Correctiva)
	Plan de Trabajo	R19	No existe respaldo de informacion	Impleme ntador	0.7	0.3	0.21	Mo dera do	Aplicar controles	- Guardar información en el compartido SharePoint del proyecto (Preventivo) - Establecer un control o bitácora semanal de validación de backup (Correctivo)
		R20	No existe contrato de confidencialidad		0.5	0.2	0.1	Ace ptab le	Aplicar controles	-Establecer un contrato de confidencialidad(Preventivo) -En las reuniones quincenales mencionar el aspecto de confidencialidad(Correctivo)
		R21	Política incorrecta para el control de acceso		0.5	0.2	0.1	Ace ptab le	Aplicar controles	-Tener perfil definido de usuarios que pueden acceder a la información compartida(Preventivo) -Limitar y definir el acceso temporal a los usuarios que necesiten información del proyecto(Correctiva)
	Informe de Estado Final de la			Impleme ntador	0.5	0.2	0.1	Ace ptab le	Aplicar controles	-Tener perfil definido de usuarios que pueden acceder a la información compartida(Preventivo) -Limitar y definir el acceso temporal a los usuarios que necesiten información del proyecto(Correctiva)

		solución	R22	No existe respaldo de informacion		0.7	0.3	0.21	Moderado	Aplicar controles	- Guardar información en el compartido SharePoint del proyecto (Preventivo) - Establecer un control o bitácora semanal de validación de backup (Correctivo)
			R23	No existe contrato de confidencialidad		0.5	0.2	0.1	Aceptable	Aplicar controles	-Establecer un contrato de confidencialidad(Preventivo) -En las reuniones quincenales mencionar el aspecto de confidencialidad(Correctivo)
		Acta de Cierre	R24	Política incorrecta para el control de acceso	Jefe de Proyecto	0.5	0.2	0.1	Aceptable	Aplicar controles	-Tener perfil definido de usuarios que pueden acceder a la información compartida(Preventivo) -Limitar y definir el acceso temporal a los usuarios que necesiten información del proyecto(Correctiva)
			R25	No existe respaldo de informacion		0.7	0.3	0.21	Moderado	Aplicar controles	- Guardar información en el compartido SharePoint del proyecto (Preventivo) - Establecer un control o bitácora semanal de validación de backup (Correctivo)
		Cliente	R26	No existe contrato de confidencialidad	Jefe de Proyecto	0.5	0.2	0.1	Aceptable	Aplicar controles	-Establecer un contrato de confidencialidad(Preventivo) -En las reuniones quincenales mencionar el aspecto de confidencialidad(Correctivo)
	PERSONAS		R27	Acceso lógico sin restricciones		0.3	0.2	0.06	Aceptable	Aplicar controles	-Tener perfil definido de usuarios que pueden acceder a la solución (Preventivo) -Definir el acceso temporal a la solución (Correctiva)
		Ingeniero de Implementación	R28	No existe contrato de confidencialidad	Jefe de Proyecto	0.5	0.4	0.2	Moderado	Aplicar controles	-Establecer un contrato de confidencialidad(Preventivo) -En las reuniones quincenales mencionar el aspecto de confidencialidad(Correctivo)
			R29	Acceso lógico sin restricciones		0.3	0.2	0.06	Aceptable	Aplicar controles	-Tener perfil definido de usuarios que pueden acceder a la información compartida(Preventivo) -Limitar y definir el acceso temporal a los usuarios que necesiten información del proyecto(Correctiva)
		Jefe de proyectos	R30	No existe contrato de confidencialidad	Gerente de Proyecto	0.5	0.4	0.2	Moderado	Aplicar controles	-Establecer un contrato de confidencialidad(Preventivo) -En las reuniones quincenales mencionar el aspecto de confidencialidad(Correctivo)
			R31	Acceso lógico sin restricciones		0.3	0.2	0.06	Aceptable	Aplicar controles	-Tener perfil definido de usuarios que pueden acceder a la información compartida(Preventivo) -Limitar y definir el acceso temporal a los usuarios que necesiten información del proyecto(Correctiva)
		Gerente de Proyectos	R32	No existe contrato de confidencialidad	Gerente de Proyecto	0.5	0.4	0.2	Moderado	Aplicar controles	-Establecer un contrato de confidencialidad(Preventivo) -En las reuniones quincenales mencionar el aspecto de confidencialidad(Correctivo)
			R33	Acceso lógico sin restricciones		0.3	0.3	0.09	Aceptable	Aplicar controles	-Tener perfil definido de usuarios que pueden acceder a la información compartida(Preventivo) -Limitar y definir el acceso temporal a los usuarios que necesiten información del proyecto(Correctiva)

SERVICIO											
FÍSICO	Internet	R34	Falta de mantenimiento de equipos	Jefe de Proyecto	0.3	0.2	0.06	Aceptable	Aplicar controles	-Revisión física y lógica mensual del modem router(Preventivo) -Realizar un test de conectividad hacia internet (Correctivo)	
		R35	Carencia de equipos alternativo		0.5	0.4	0.2	Moderado	Aplicar controles	-Contar con un equipo modem router de contingencia(Preventivo) -Usar conexión temporal como de uso de datos de celular. (Correctivo)	
		R36	Corte programado por el proveedor del servicio		0.5	0.2	0.1	Aceptable	Aplicar controles	-Contratar un servicio de internet alternativo (Preventivo) -Usar conexión temporal de internet de otro proveedor (Correctivo)	
		R37	Incumplimiento en pago de servicio		0.7	0.4	0.28	Moderado	Aplicar controles	-Realizar un cronograma de pagos y un recordatorio (Preventivo) -Realizar el pago y conversar con el proveedor para agilizar la reconexión (Correctivo)	
	Telefonía	R38	Falta de mantenimiento de equipos	Jefe de Proyecto	0.3	0.2	0.06	Aceptable	Aplicar controles	-Revisión física y lógica mensual del celular(Preventivo) -Realizar temporalmente un celular prestado(Correctivo)	
		R39	Carencia de equipos alternativo		0.5	0.4	0.2	Moderado	Aplicar controles	-Contar con un equipo celular de contingencia(Preventivo) -Usar equipo celular prestado. (Correctivo)	
		R40	Corte programado por el proveedor del servicio		0.5	0.2	0.1	Aceptable	Aplicar controles	-Contratar un servicio de internet alternativo (Preventivo) -Usar conexión temporal de internet de otro proveedor (Correctivo)	
		R41	Incumplimiento en pago de servicio		0.7	0.4	0.28	Moderado	Aplicar controles	-Realizar un cronograma de pagos y un recordatorio (Preventivo) -Realizar el pago y conversar con el proveedor para agilizar la reconexión (Correctivo)	
	Electricidad	R42	Indisponibilidad del servicio por Falla en las instalaciones del servicio	Jefe de Proyecto	0.5	0.4	0.2	Moderado	Aplicar controles	-Se aplica Política de seguridad física y del entorno de la empresa el cual se tiene como respaldo las instalaciones de la sede en Ecuador	
		R43	Indisponibilidad del servicio por corte de servicio		0.5	0.4	0.2	Moderado	Aplicar controles	-Se aplica Política de continuidad de negocio de la empresa el cual se tiene como respaldo las instalaciones de la sede en Ecuador	
	FÍSICO	Servidor Prox y Duo 2FA	R44	Fallas de sistema servidor virtual	Jefe de Proyecto	0.5	0.4	0.2	Moderado	Aplicar controles	-De forma quincenal se realiza un snapshot al entorno virtual del servidor virtual
			R45	Nuevas Vulnerabilidades tecnológicas		0.3	0.2	0.06	Aceptable	Aplicar controles	-Realizar el parchado correspondiente del sistema operativo del servidor
R46			Perdida de Información de configuración	0.5		0.4	0.2	Moderado	Aplicar controles	-De forma quincenal se realiza un snapshot al entorno virtual del servidor virtual	
Fire wall Palo Alto		R47	Fallas de Hardware	Jefe de Proyecto	0.5	0.4	0.2	Moderado	Aplicar controles	-Se tiene como contingencia VPN SSL con el equipo FW Check Point , esta solución no tiene 2FA pero permite continuar con la operatividad	
		R48	Nuevas Vulnerabilidades tecnológicas		0.3	0.2	0.06	Aceptable	Aplicar controles	-Realizar el parchado correspondiente del sistema operativo del Firewall	
		R49	Perdida de Información de configuración		0.7	0.4	0.28	Moderado	Aplicar controles	-Se tiene planificado realizar el backup Inter diario.	

Fuente: Elaboración Propia,2021

3.2.8 Plan de Gestión de Interesados (Stakeholders):

En el presente plan se identifica y describe a los principales interesados del proyecto implementado, además se detalla sus roles, influencia y participación durante todo el proyecto.

3.2.8.1 Registro de Interesados Preliminar

A continuación, se describe los principales interesados en el proyecto a realizar, así como su nivel de participación e influencia.

Tabla 20. Registro de Interesados Preliminar

Cargo	Ubicación	Influencia / poder	Nivel de participación
Gerente Comercial	Área comercial	Fuerte	Baja
Gerente Financiero	Área administrativa	Fuerte	Baja
Gerente de Proyecto	Área de Ingeniería	Media	Media
Jefe de Proyecto	Área de Ingeniería	Fuerte	Alta
Ingeniero Implementador	Área de Ingeniería	Fuerte	Alta
Ingeniero de Soporte	Área de Ingeniería	Baja	Media

Fuente: Elaboración Propia,2021

3.2.8.2 Registro de Interesados

A continuación, se identifican los interesados en el proyecto, detallando su rol en el proyecto, influencia, participación, entre otros.

Tabla 21. Registro de Interesados

N°	Interesado	Cargo en la organización	Ubicación	Rol en el Proyecto	Tipo de Interesado	Influencia en el Proyecto	Fase en el proyecto de mayor participación	Principales Requerimientos
1	Ismael N.	Gerente Comercial	Área comercial	Usuario Indirecto	Interno	Fuerte	Inicial, Planificación y cierre	<ul style="list-style-type: none"> • Apoyar en la cotización del licenciamiento de las tecnologías Palo Alto y Cisco. • Realizar la compra del licenciamiento de las tecnologías Palo Alto y Cisco.
2	Francisco S.	Gerente Financiero	Área administrativa	Patrocinador	Interno	Fuerte	Inicial, Planificación y cierre	<ul style="list-style-type: none"> • Indicadores de rentabilidad • Disponer y controlar el presupuesto asignado a Ingeniería. • Cumplimiento de las políticas financieras de la empresa. • Indicadores comerciales de rentabilidad por el proyecto.
3	Percy S.	Gerente de Proyecto	Área de Ingeniería	Gerente de Proyecto	Interno	Media	Inicial, Planificación, Ejecución, Seguimiento y control y Cierre	<ul style="list-style-type: none"> • Organizar el funcionamiento adecuado del proyecto y asegurar el cumplimiento de los objetivos del proyecto
4	Ever Pastor	Jefe de Proyecto	Área de Ingeniería	Jefe de Proyecto	Interno	Fuerte	Inicial, Planificación, Ejecución, Seguimiento y control y Cierre	<ul style="list-style-type: none"> • Realizar seguimiento y cumplimiento de cada fase del proyecto, así como validar el cumplimiento de los objetivos.
5	Ever Pastor	Ingeniero Implementador	Área de Ingeniería	Ingeniero Implementador	Interno	Fuerte	Inicial, Planificación, Ejecución, Seguimiento y control y Cierre	<ul style="list-style-type: none"> • Responsable de cumplir con todas las actividades programadas del proyecto • Cumplir correctamente con las configuraciones correctas para el desarrollo de la nueva solución tecnológica que se está implementando.
6	Carlos C.	Ingeniero de Soporte	Área de Ingeniería	Usuario de Pruebas	Interno	Baja	Ejecución y Seguimiento y Control	<ul style="list-style-type: none"> • Realizar pruebas de funcionamiento de la nueva solución implementada.

Fuente: Elaboración Propia,2021

3.2.8.3 Matriz de Análisis de los Interesados

Tabla 22. Matriz de Análisis de los Interesados

N°	Interesado	Nivel de Participación	Evaluación del impacto de no cumplir con sus requerimientos	Nivel de accesibilidad a los interesados
1	Ismael Navarro	Media	Medio	Medio
2	Francisco Saavedra	Media	Alto	Medio
3	Percy Sotelo	Media	Medio	Alto
4	Ever Pastor	Alta	Alto	Alto
5	Carlos Chacchi	Media	Bajo	Bajo

Fuente: Elaboración Propia,2021

3.2.8.4 Estrategia de gestión de Interesados

Tabla 23. Estrategia de gestión de Interesados

Interesado	Interés en el proyecto	Impacto	Estrategia para obtener apoyo y reducir conflictos
Ismael Navarro (Gerente Comercial)	Disponibilidad de Información oportuna y exacta para la toma de decisiones comerciales.	Alto	<ul style="list-style-type: none"> •Las reuniones con el interesado deben ser previamente planeados con el patrocinador. •En las reuniones el patrocinador debe estar presente.
Francisco Saavedra (Gerente Financiero/Patrocinador)	Integridad de la información. Cumplimiento de políticas financieras de empresa.	Alto	<ul style="list-style-type: none"> •Cualquier aviso de conflicto en el proyecto que presente alto riesgo debe ser previamente discutido con el patrocinador. •Correos dirigidos con copia a Gerencia deben ser copiados también al gerente financiero.
Percy Sotelo (Gerente de Proyectos)	Mayor fluidez de información entre el área Comercial, Financiero y de Ingeniería.	Medio	<ul style="list-style-type: none"> •Mostrarle los beneficios que se obtendrá con el uso de la nueva solución implementada.
Ever Pastor (Ingeniero Implementador/Jefe de Proyecto)	Evidenciar e informar sobre los avances en cada fase de la implementación de la nueva solución.	Media	<ul style="list-style-type: none"> •Las reuniones con el interesado deben ser previamente planeados con el Jefe y Gerente de Proyecto.

Fuente: Elaboración Propia,2021

3.3 Fase de Implementación

3.3.1 Actividades Realizadas

3.3.1.1 Implementación de componentes de la nueva solución tecnológica

La nueva solución se trata de implementar y establecer una conexión de acceso remoto seguro usando el protocolo de seguridad SSL(Secure Sockets Layer) que es un protocolo de capa sesión de OSI que permite autenticar, cifrar y descifrar toda la información enviada a través del internet a la cual se complementa o agrega el protocolo TLS(Transport Layer Security) versión 1.2 la cual se suma y brinda una conexión remota más segura es decir técnicamente hablo de una VPN(Virtual Private Network) SSL/TLS una vez implementada la VPN a la cual agrego un certificado auto firmado para establecer parámetros y criterios de cifrado robusto para este caso usaré el cifrado SHA512 que brinda una longitud amplia y robusta para que en caso algún atacante intente descifrar la contraseña este demore demasiados años a diferencia de cifrados más bajos que un atacante puede lograr vulnerarlo, este cifrado que pertenece al algoritmo RSA(Rivest, Shamir y Adleman) la cual es uno de los sistemas de cifrado asimétricos más exitosos y robustos de la actualidad debido a que usa dos claves diferentes: una pública y una privada de la cual ambos operan de forma complementaria entre sí, lo que significa que una data cifrada con uno de ellos sólo puede ser descifrado por su contraparte, la nueva solución tiene varios componentes principales que trabajan entre sí una vez culminada la implementación y son los siguientes:

1.-Firewall Palo Alto: Es un componente principal que integra la solución remota VPN SSL con el doble factor de autenticación y el control de acceso de dispositivo, este equipo contiene las configuraciones de redes tanto segmentos internos y externos en sus interfaces de red y rutas estáticas configuradas, adicional para mayor detalle en las especificaciones técnicas de hardware, red y seguridad del Firewall 3050 ver Anexo 1, Anexo 3 y Anexo 4.

2.-Agente VPN SSL Global Protect: Debe estar instalado y configurado en los dispositivos de cada colaborador para poder establecer la conexión remota segura, en el agente Global Protect se configura la ip pública de la VPN es decir la interfaz WAN del Firewall Palo Alto a donde todos los usuarios apuntarán para habilitar la sesión remota segura, también es el componente la cual el colaborador ingresar su usuario y password para la autenticación.

3.-Portal VPN SSL Global Protect: Es un componente que a nivel de configuración permite asociar el perfil de autenticación radius, además de brindar la página de inicio que mostrará el agente VPN SSL que permite brindar la opción de usuario y password para la autenticación de cada usuario.

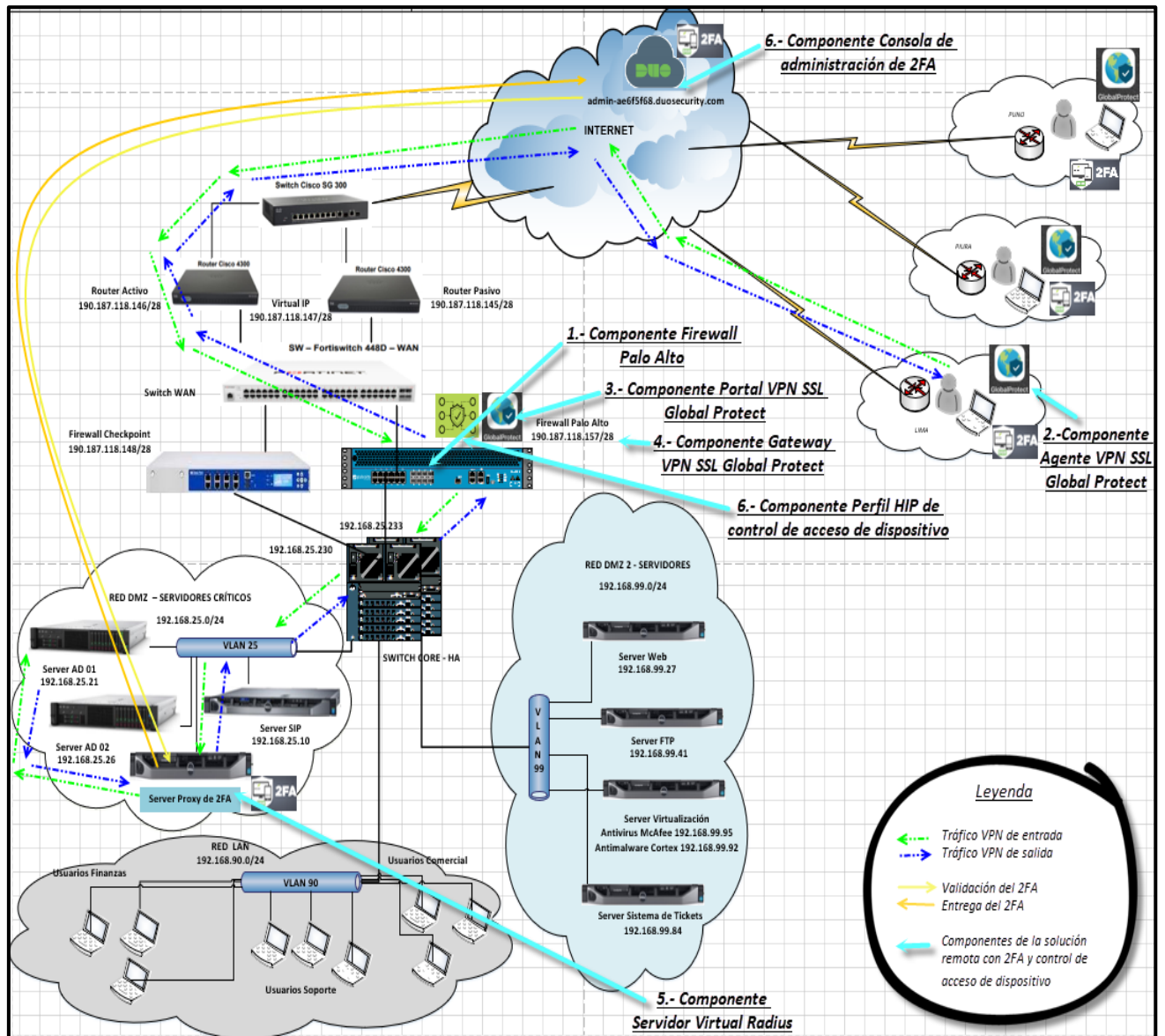
4.-Gateway VPN SSL Global Protect: Es el componente que proporciona seguridad para el tráfico de aplicaciones de la VPN SSL, tener en cuenta que todos los agentes Global Protect necesitan apuntar a un Gateway para que pueda aplicar la validación de autenticación y mecanismos de acceso de los usuarios a los recursos internos de la empresa privada, maneja el Access list de acceso donde se coloca la red remota asignada(172.31.1.0/24) a la VPN y el destino la cual son las redes privadas internas (192.168.25.0/24, 192.168.90.0/24, 192.168.99.0/24) de la empresa privada, el Gateway de la VPN es la IP 190.187.118.157.

5.-Servidor Virtual Radius: Es el componente que se utiliza como intermediario entre el servidor de directorio activo 192.68.25.21 y el firewall Palo Alto a la cual se integra este servidor Proxy usando el método de autenticación Radius que es uno de los protocolos de autenticación muy seguro además este componente protege y sirve como proxy evitando un contacto directo hacia el directorio activo, adicional se instala el servicio de doble factor y mediante API(Application Programming Interface) se comunica hacia la consola de administración de doble factor de autenticación la cual es la siguiente: <https://admin-ae6f5f68.duosecurity.com/admins/profile>.

6.-Consola de administración doble factor de autenticación: El presente complemento una vez implementado se encarga de realizar el mecanismo del doble factor de autenticación a los usuarios registrados que intentan autenticarse por el acceso remoto a través de la VPN SSL Global Protect otorgándole una capa de seguridad adicional en el proceso de autenticación, en el presente componente se configura los dispositivos(smartphone) y se sincronizan los usuarios autorizados para poder brindarles acceso mediante el mecanismo del doble factor de autenticación.

7.-Perfil HIP Profile de control de acceso de dispositivo: El componente llamado perfil de identificación de host el cual permite el control de acceso de dispositivo se logra implementar las características activas y de ejecución de varios software permitidos y recomendados a nivel de seguridad informática de acuerdo a la experiencia técnica, dentro de los perfiles se ha configurado considerando la experiencia técnica y profesional el cual es permitir que el dispositivo tenga instalado y activo un antivirus y un antimalware por lo menos con 1 día de escaneo realizado, también se considera dentro de los criterios que debe tener activa la función de cifrado de disco duro, el software que también debe tener instalado y activo en el dispositivo es la función DLP (Data Loss Prevention) para evitar la fuga de datos, también deben tener instalados y activos los parches de Windows a nivel de sistema operativo y el firewall de Windows activo y habilitado, otro criterio técnico a considerar es el sistema operativo versión Windows 10 Enterprise , debe estar dentro del dominio de la empresa privada y utilizar la versión 5 del agente Global Protect.

Figura 43. Diagrama de Red con la nueva solución y sus componentes principales.

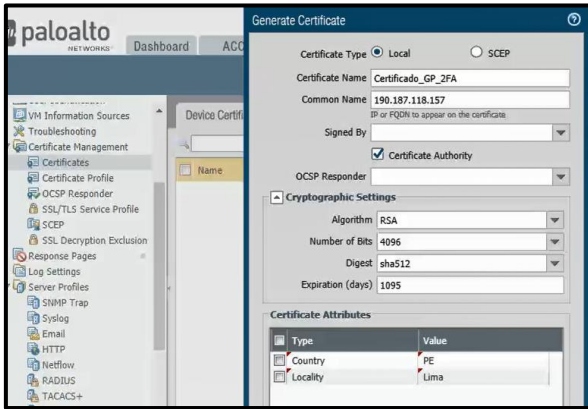


Fuente: Elaboración Propia,2021

Ejecución de la implementación de la VPN SSL Global Protect en el Firewall Palo Alto:

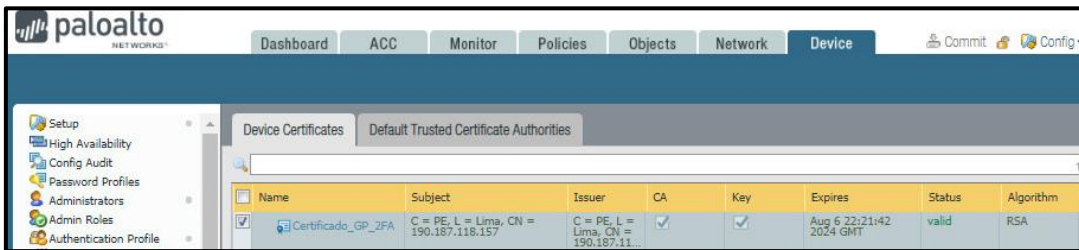
1.-Procedo con la creación y configuración del certificado auto firmado del Firewall Palo Alto para el uso de la VPN SSL Global Protect, se configura el cifrado sha512 el más alto para tener un cifrado bien robusto de acuerdo con la experiencia y conocimiento técnico el algoritmo configurado permite cifrar la data con una longitud muy amplia la cual permite la transmisión de data segura.

Figura 44. Creación de certificado para VPN SSL.



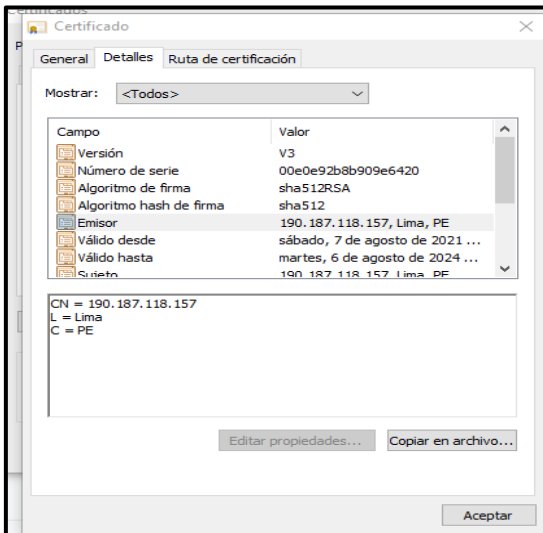
Fuente: Elaboración Propia,2021

Figura 45. Validación de certificado para VPN SSL



Fuente: Elaboración Propia,2021

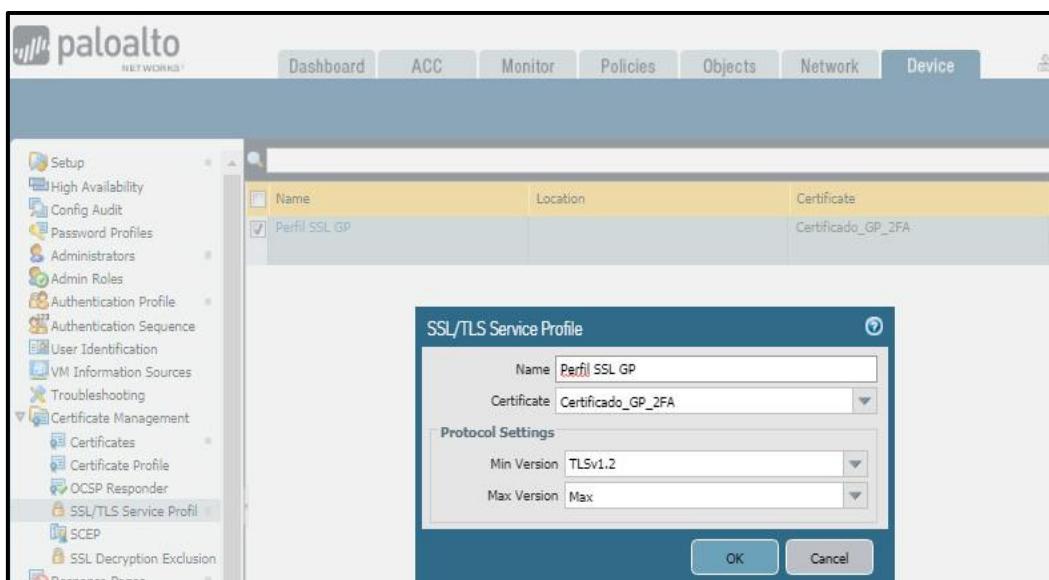
Figura 46. Detalle de certificado para VPN SSL



Fuente: Elaboración Propia,2021

2.-Procedí a crear el perfil de seguridad SSL/TLS que estará asociado al portal y Gateway de la VPN SSL Global Protect y también es el perfil donde se asocia el certificado auto firmado (Figura 31) creado inicialmente, se considera que para la interacción entre componentes de la VPN SSL Global Protect como son el Portal, Agente Global Protect y Gateway se debe realizar a través de una conexión SSL/TLS y en cada componente se debe utilizar el certificado auto firmado creado inicialmente para finalmente agregar en el firewall Palo Alto mediante un perfil SSL/TLS, adicional se considera que el certificado debe instalarse localmente en cada dispositivo donde se tiene el componente de Agente Global Protect de esta forma todos los componentes usan un medio de conexión conocida entre ellos evitando que exista alguna alteración o interceptación, en la configuración del perfil empleo como mínimo el TLS V1.2 debido a que optar por versiones anteriores no sería lo recomendable por las diversas vulnerabilidades que manejan y ya son protocolos muy antiguos, esta versión de protocolo TLS V1.2 nos permite autenticar y trasportar datos en internet de forma muy segura.

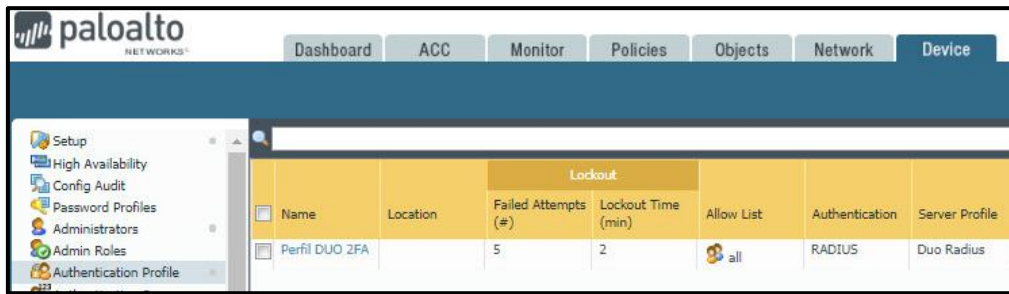
Figura 47. Perfil de seguridad SSL/TLS



Fuente: Elaboración Propia,2021

3.-Creación del perfil de autenticación que contiene el tipo de autenticación Radius que se encuentra integrado el Servidor Proxy 2FA que tiene la comunicación con el server AD, el perfil será utilizado para la autenticación de usuarios en los compontes de la VPN SSL Global Protect como son el portal y el Gateway del Global Protect, el tipo de autenticación que utilizo es el Radius la cual es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP, este tipo de autenticación permite el acceso de todos los usuarios legítimos a los recursos conectados a la red e impide el acceso no autorizado.

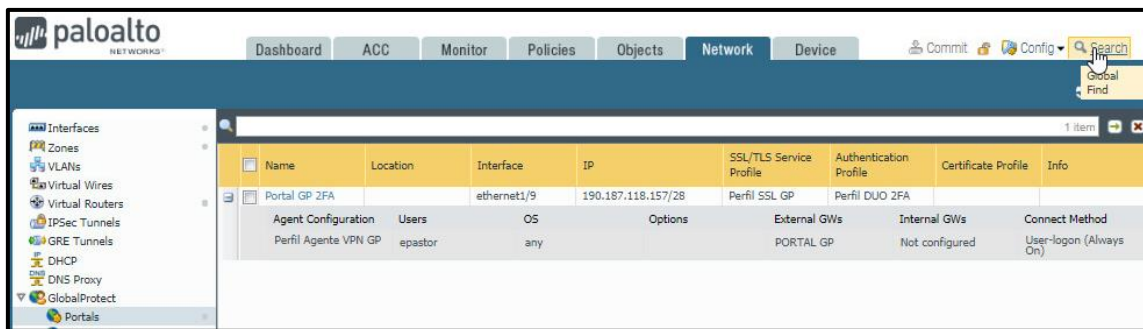
Figura 48. Perfil de autenticación para la VPN SSL



Fuente: Elaboración Propia,2021

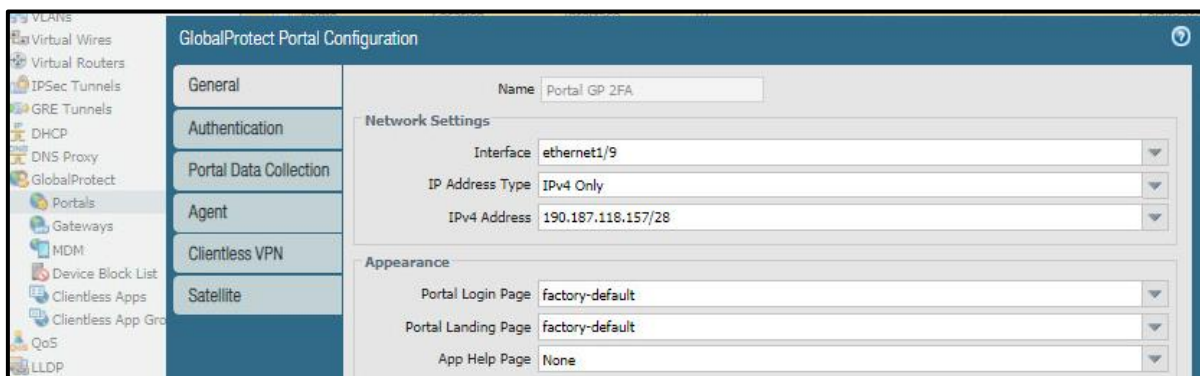
4.-Realizo la creación y configuración del portal Global Protect de la VPN SSL, la cual es uno de los componentes de la VPN SSL Global Protect este portal permite brindar la página de inicio que permite brindar la opción de usuario y Password para la autenticación de cada usuario, para configurarlo se utiliza la interface WAN que en el firewall es la interfaces 1/9 , también se agrega la ip pública 190.187.118.157 a la cual todos los usuarios apuntarán a para la autenticación de acceso remoto, también se asocia el perfil TLS de certificado para cifrar la comunicación y el perfil de autenticación donde está configurado el protocolo de autenticación Radius.

Figura 49. Portal Global Protect para la VPN SSL.



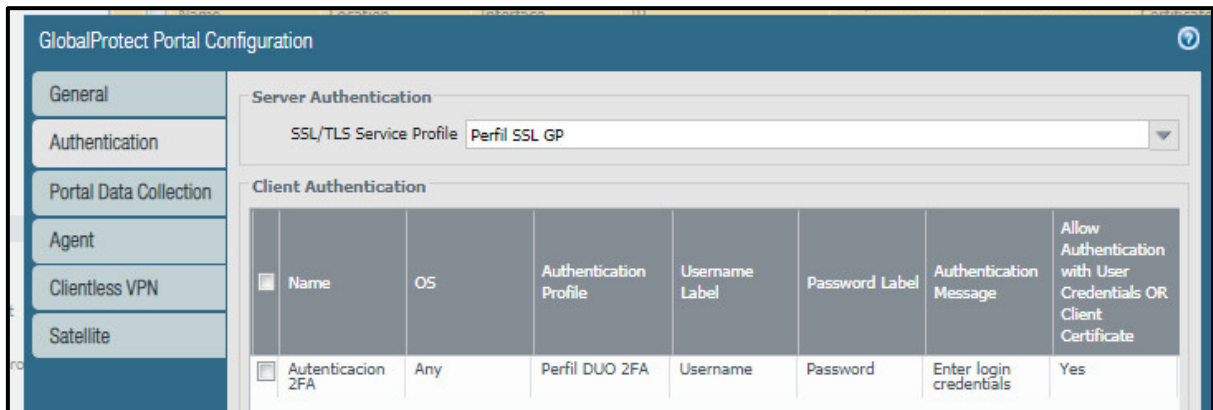
Fuente: Elaboración Propia,2021

Figura 50. Detalle general de configuración del portal Global Protect.



Fuente: Elaboración Propia,2021

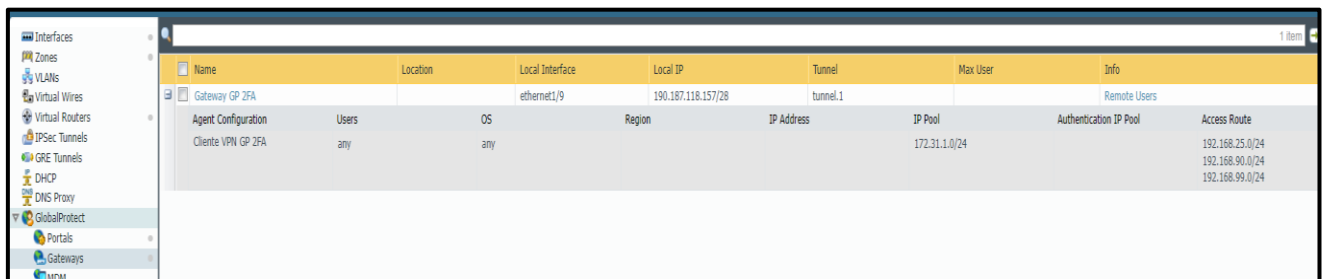
Figura 51. Detalle de autenticación del portal Global Protect.



Fuente: Elaboración Propia,2021

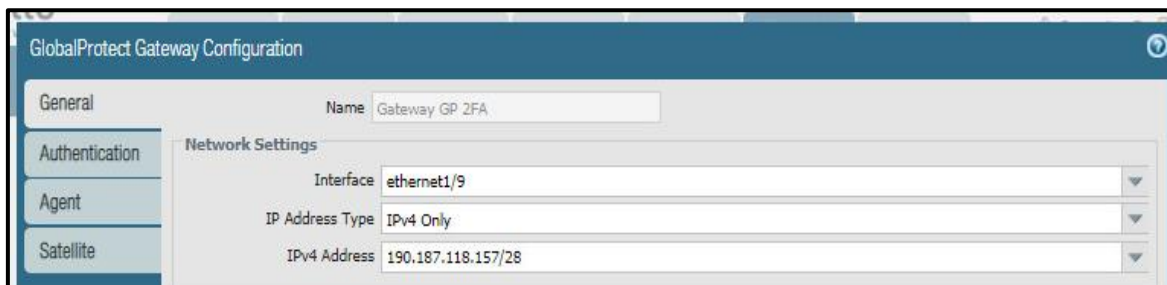
5.- Procedo con la creación y configuración del Gateway de la VPN SSL Global Protect, este componente es el que proporciona seguridad para el tráfico de aplicaciones de la VPN SSL, todos los agentes Global Protect necesitan apuntar a un gateway para que pueda aplicar la validación de autenticación y acceso de los usuarios a los recursos internos de la empresa privada, tener en cuenta que se configuró el Gateway asociado a la interface Ethernet 1/9 asociada a la interface WAN, se asigna la Ip pública 190.187.118.157 hacia donde apuntarán los usuarios, el segmento de red asignado a los usuarios que se conecten remotamente y también se configura las rutas de acceso es decir las redes internas de la empresa privada donde se encuentran los recursos disponibles de la empresa.

Figura 52. Gateway de Global Protect para la VPN SSL.



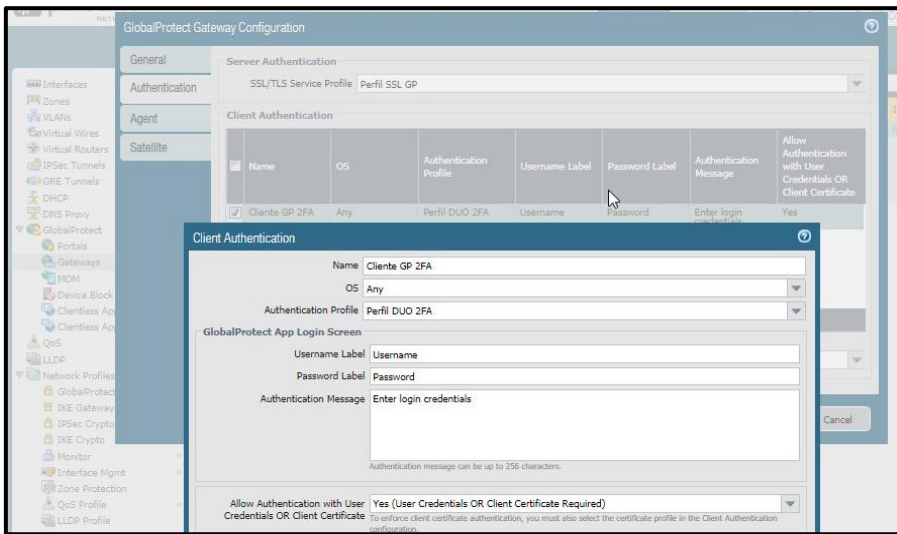
Fuente: Elaboración Propia,2021

Figura 53. Detalle general de configuración de Gateway de Global Protect.



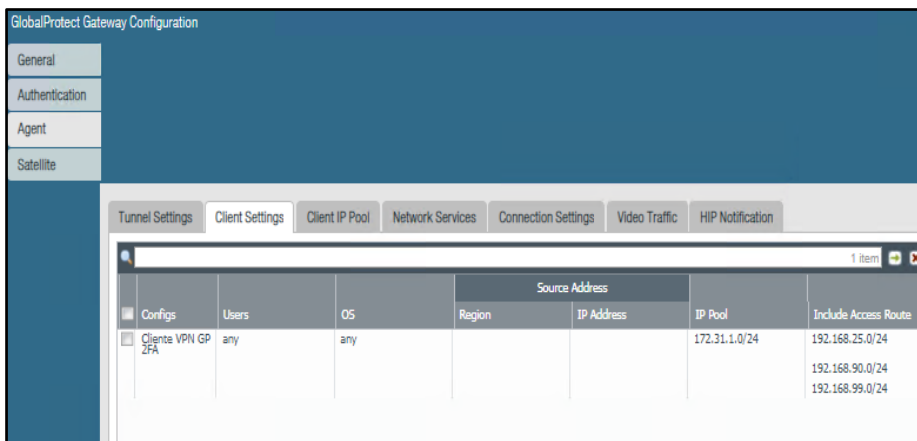
Fuente: Elaboración Propia,2021

Figura 54. Detalle de autenticación de cliente de Gateway de Global Protect.



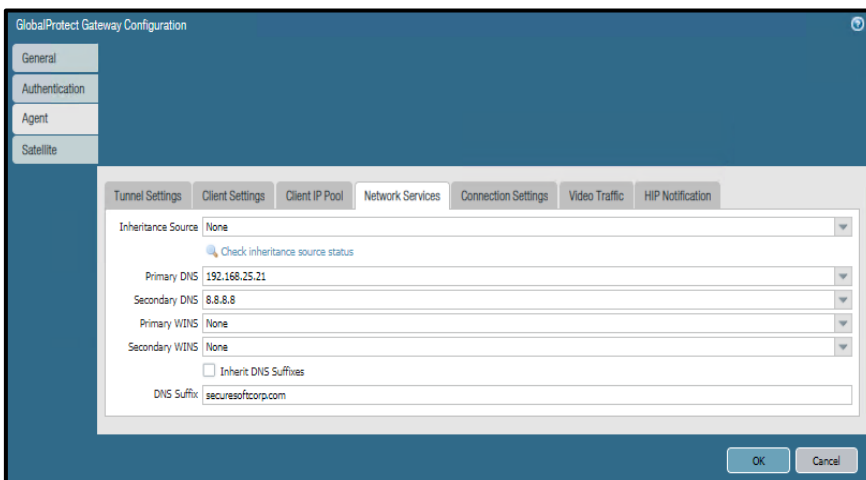
Fuente: Elaboración Propia,2021

Figura 55. Detalle de configuración de agente de Gateway de Global Protect.



Fuente: Elaboración Propia,2021

Figura 56. Detalle de configuración de servicios de red del Gateway de Global Protect.



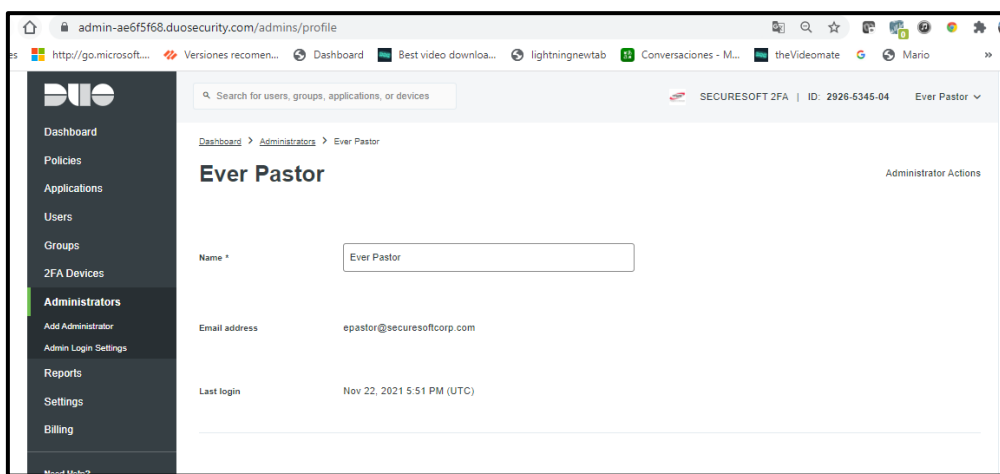
Fuente: Elaboración Propia,2021

Con lo realizado hasta el presente punto tenemos completado la implementación de la VPN SSL Global Protect, la cual llega a ser una parte de la implementación general de la nueva solución de acceso remoto.

El siguiente paso es realizar la implementación de la consola de administración del doble factor de autenticación Cisco DUO Security en el portal web administrador, así como la implementación y configuración del componente servidor Duo Proxy (IP 192.168.25.19) que es el intermediario en la comunicación entre el Servidor de AD (IP 192.168.25.21) con la consola nube de Administración de doble factor de autenticación.

1.-Se creó el usuario ‘epastor’ de acceso administrador para el usuario implementador Ever Pastor en la consola de administración y la URL de acceso a la consola de administración es la siguiente <https://admin-ae6f5f68.duosecurity.com/admins/profile>.

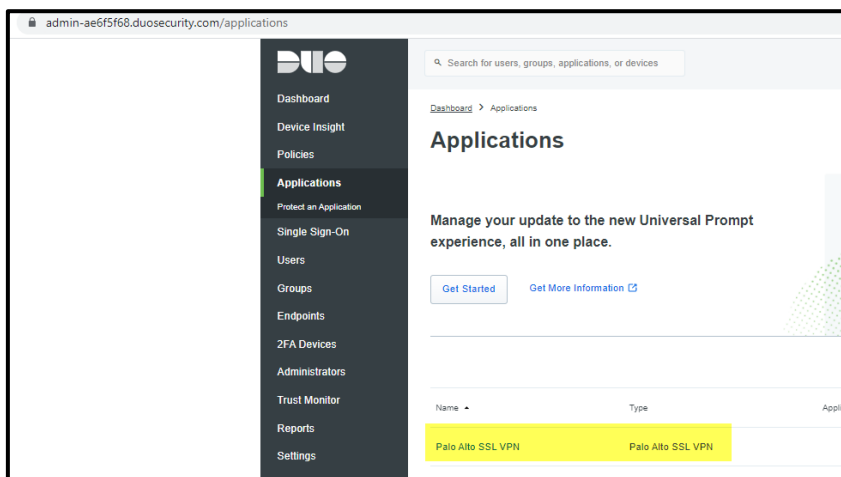
Figura 57. Detalle de cuenta administrador de la solución Cisco Duo Security.



Fuente: Elaboración Propia,2021

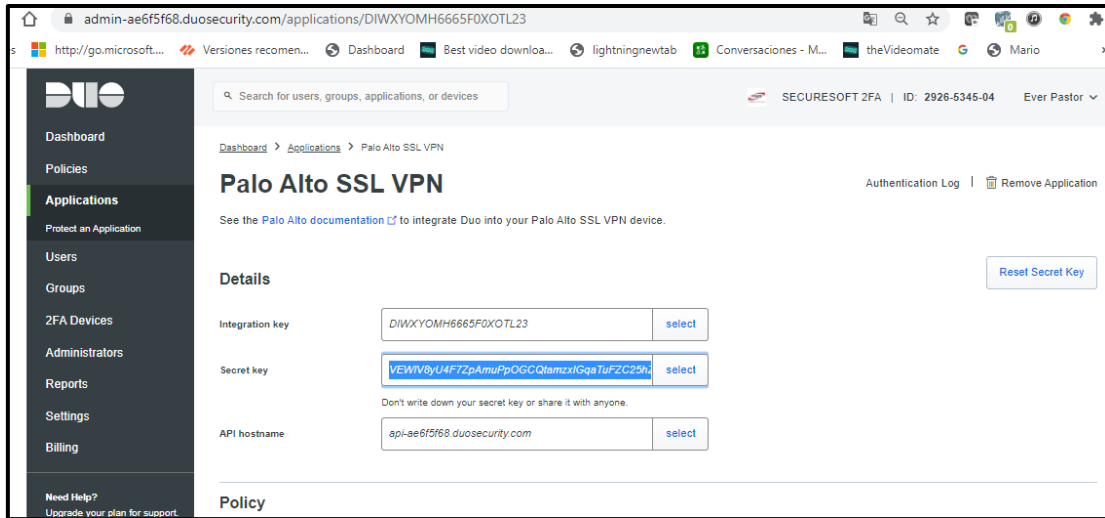
2.-Configuré y activé la aplicación “VPN SSL de Palo Alto” y se creó claves de integración que se empleará en la implementación del componente Servidor Proxy 2FA, la aplicación se conectará mediante una API (Interfaz de programación de aplicaciones) hacia el servidor Proxy 2FA.

Figura 58. Configuración de la aplicación “VPN SSL de Palo Alto” en Cisco Duo.



Fuente: Elaboración Propia,2021

Figura 59. Detalle de Configuración de “VPN SSL de Palo Alto” en Cisco Duo.



Fuente: Elaboración Propia,2021

3.-Configuré la política personalizada con criterios seguros para la autenticación del 2FA (Doble Factor de Autenticación) aplicado a la política de la aplicación Palo Alto SSL VPN, estos criterios seguros son requerir la inscripción de usuarios no inscritos, otro criterio seguro es aplicar en la política una validación de autenticación de dos factores siempre, el método de autenticación es el duo push mediante autorización de acceso por la aplicación Duo Móbil.

Figura 60. Configuración de política de acceso global en Cisco Duo.

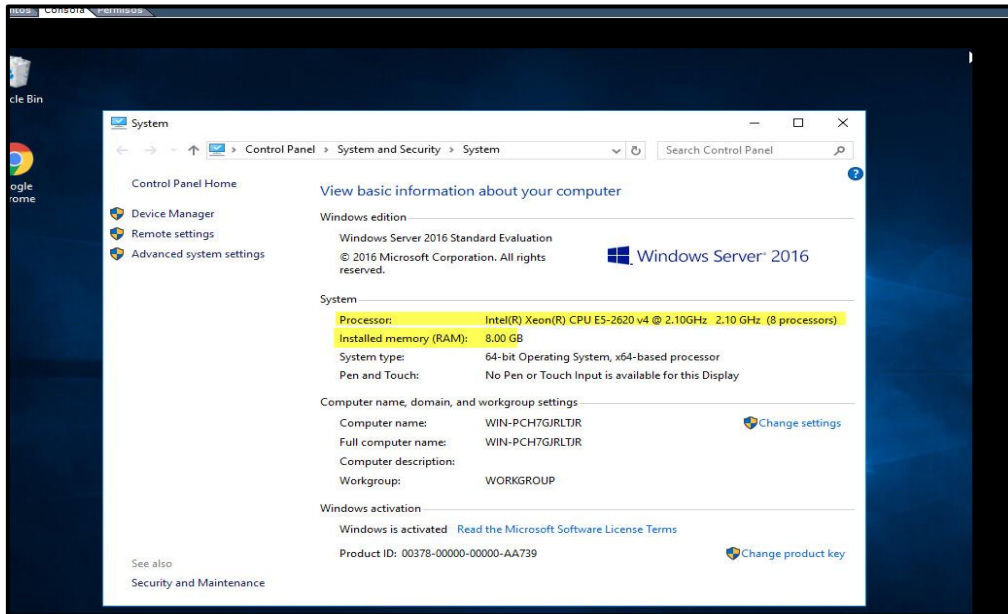


Fuente: Elaboración Propia,2021

Continuando con las actividades de implementación de la nueva solución, procedo con la implementación del servidor de Autenticación Proxy la cual es un componente importante del acceso remoto seguro.

1.-Validación que el servidor se encuentre con los requisitos mínimos de recursos instalados, es decir disponibilidad de recursos CPU, Memoria y Disco.

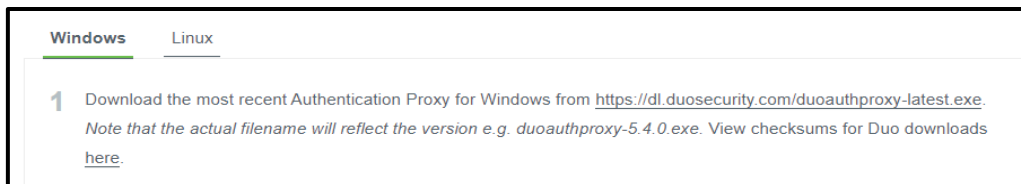
Figura 61. Validación de recursos disponibles en el servidor Autenticación Proxy.



Fuente: Elaboración Propia,2021

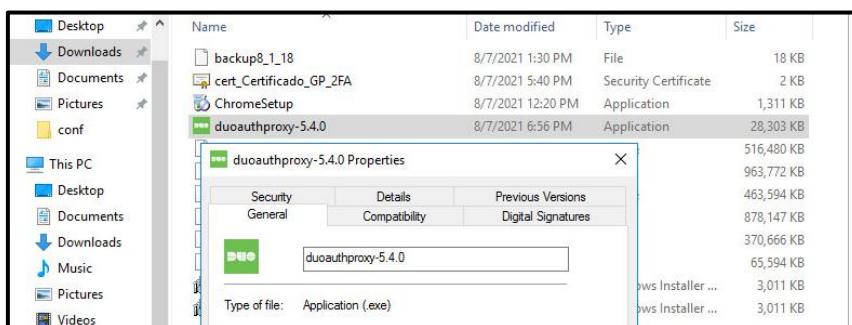
2.- Procedo a descargar, instalar y configurar la aplicación Autenticación Duo en el Servidor Proxy.

Figura 62. Ruta de descarga de aplicación Autenticación Proxy.



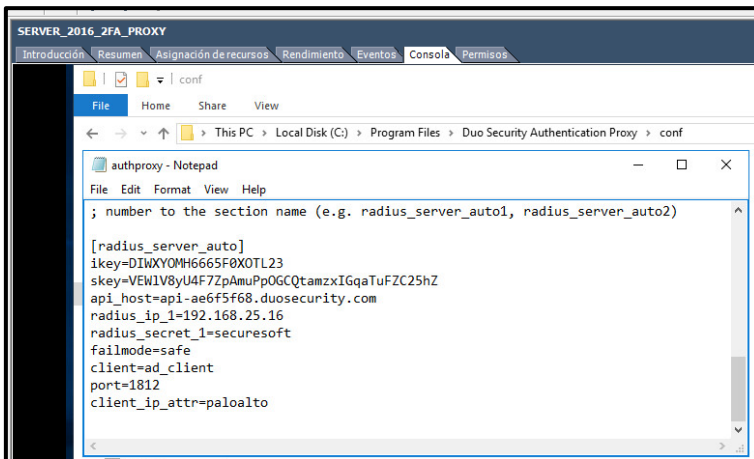
Fuente: Elaboración Propia,2021

Figura 63. Aplicación Autenticación Proxy.



Fuente: Elaboración Propia,2021

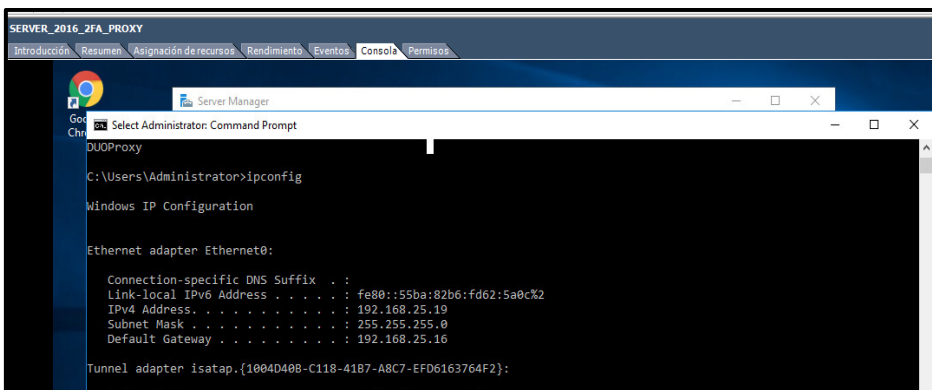
Figura 64. Configuración de aplicación Autenticación Proxy.



Fuente: Elaboración Propia,2021

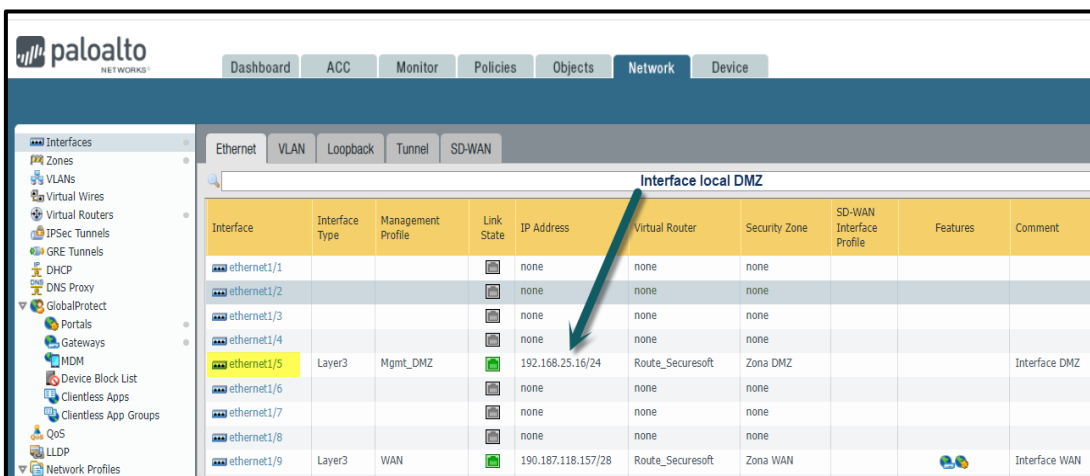
La ip del servidor Proxy 2FA es 192.168.25.19 y la ip de la interfaz del puerto DMZ del firewall Palo Alto es la 192.168.25.16 son valores importantes para la configuración e integración de componentes de la solución, el puerto utilizado es el 1812.

Figura 65. Configuración de red de servidor Duo Proxy.



Fuente: Elaboración Propia,2021

Figura 66. Interfaz local de red DMZ en el firewall Palo Alto.



Fuente: Elaboración Propia,2021

Validación de comunicación satisfactoria desde el Firewall Palo Alto en donde se encuentra implementada la VPN SSL hacia el servidor Duo Proxy la cual se conectarán mediante el protocolo Radius para validación de autenticación de los usuarios remotos.

Figura 67. Prueba de conectividad desde el Firewall hacia el servidor Duo Proxy.

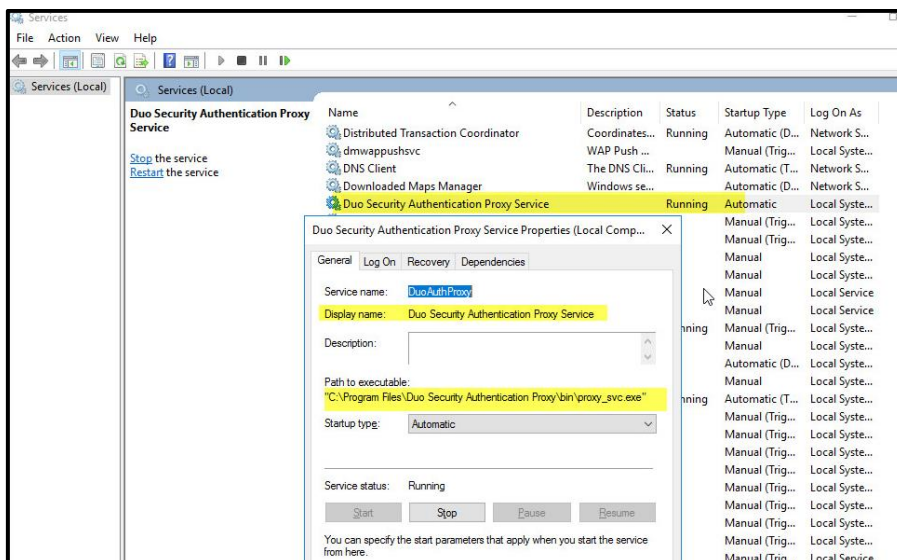
```
securesoft@PA-3050-Securesoft> ping source
<value> Source address of echo request

securesoft@PA-3050-Securesoft> ping source 192.168.25.16 host 192.168.25.19
PING 192.168.25.19 (192.168.25.19) from 192.168.25.16 : 56(84) bytes of data.
64 bytes from 192.168.25.19: icmp_seq=1 ttl=128 time=0.699 ms
64 bytes from 192.168.25.19: icmp_seq=2 ttl=128 time=0.690 ms
64 bytes from 192.168.25.19: icmp_seq=3 ttl=128 time=0.698 ms
64 bytes from 192.168.25.19: icmp_seq=4 ttl=128 time=0.735 ms
64 bytes from 192.168.25.19: icmp_seq=5 ttl=128 time=0.703 ms
64 bytes from 192.168.25.19: icmp_seq=6 ttl=128 time=0.677 ms
64 bytes from 192.168.25.19: icmp_seq=7 ttl=128 time=0.688 ms
64 bytes from 192.168.25.19: icmp_seq=8 ttl=128 time=0.661 ms
64 bytes from 192.168.25.19: icmp_seq=9 ttl=128 time=0.705 ms
64 bytes from 192.168.25.19: icmp_seq=10 ttl=128 time=0.670 ms
64 bytes from 192.168.25.19: icmp_seq=11 ttl=128 time=0.703 ms
64 bytes from 192.168.25.19: icmp_seq=12 ttl=128 time=0.677 ms
64 bytes from 192.168.25.19: icmp_seq=13 ttl=128 time=0.685 ms
64 bytes from 192.168.25.19: icmp_seq=14 ttl=128 time=0.671 ms
64 bytes from 192.168.25.19: icmp_seq=15 ttl=128 time=0.686 ms
64 bytes from 192.168.25.19: icmp_seq=16 ttl=128 time=0.718 ms
64 bytes from 192.168.25.19: icmp_seq=17 ttl=128 time=0.675 ms
64 bytes from 192.168.25.19: icmp_seq=18 ttl=128 time=0.712 ms
64 bytes from 192.168.25.19: icmp_seq=19 ttl=128 time=0.681 ms
^C
--- 192.168.25.19 ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 17997ms
rtt min/avg/max/mdev = 0.661/0.691/0.735/0.026 ms
securesoft@PA-3050-Securesoft> ping source 192.168.25.16 host 192.168.25.21
PING 192.168.25.21 (192.168.25.21) from 192.168.25.16 : 56(84) bytes of data.
64 bytes from 192.168.25.21: icmp_seq=1 ttl=128 time=0.691 ms
64 bytes from 192.168.25.21: icmp_seq=2 ttl=128 time=0.671 ms
64 bytes from 192.168.25.21: icmp_seq=3 ttl=128 time=0.716 ms
64 bytes from 192.168.25.21: icmp_seq=4 ttl=128 time=0.681 ms
64 bytes from 192.168.25.21: icmp_seq=5 ttl=128 time=0.713 ms
64 bytes from 192.168.25.21: icmp_seq=6 ttl=128 time=0.712 ms
64 bytes from 192.168.25.21: icmp_seq=7 ttl=128 time=0.661 ms
64 bytes from 192.168.25.21: icmp_seq=8 ttl=128 time=0.690 ms
64 bytes from 192.168.25.21: icmp_seq=9 ttl=128 time=0.709 ms
^C
--- 192.168.25.21 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 7996ms
rtt min/avg/max/mdev = 0.661/0.693/0.716/0.037 ms
securesoft@PA-3050-Securesoft>
```

Fuente: Elaboración Propia,2021

3.- Se inicia el servicio instalado de Duo Security, el servicio es indispensable para establecer la comunicación mediante la API entre el servidor Proxy 2FA y la consola de administración en nube del doble factor de autenticación.

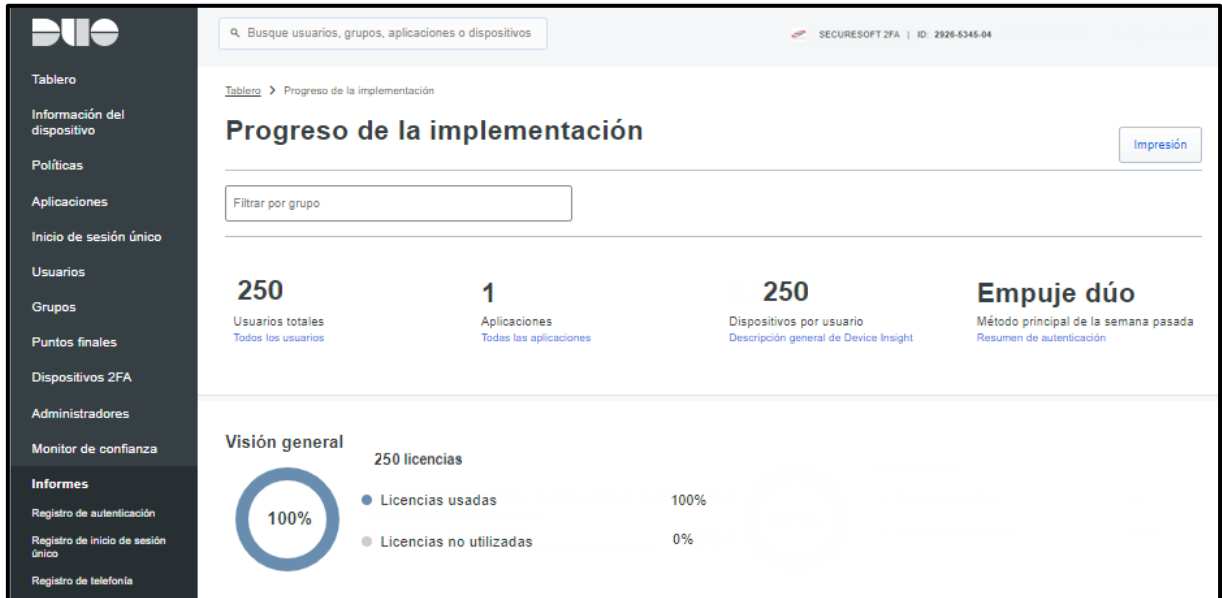
Figura 68. Servicio de Autenticación Proxy.



Fuente: Elaboración Propia,2021

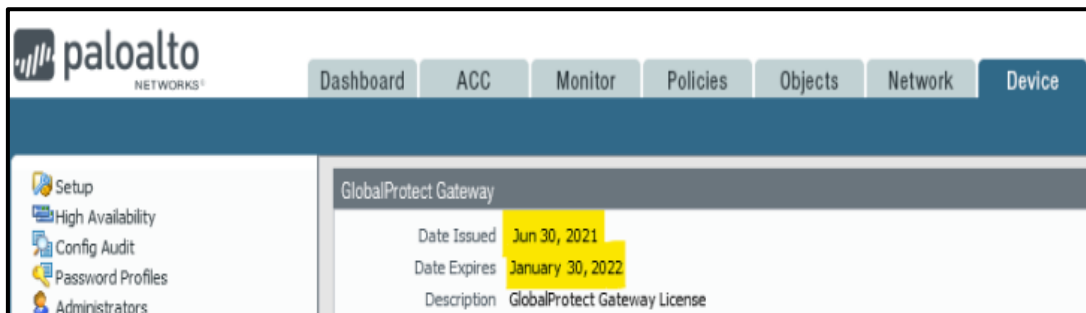
Se realiza instalación de licencia del 2FA en el portal administrador Cloud de la solución doble factor de autenticación y licencia del Global Protect para la función de HIP Profile.

Figura 69. Licencia de la plataforma Cisco Duo Security para el doble factor de autenticación.



Fuente: Elaboración Propia,2021

Figura 70. Licencia Global Protect para el HIPs Profile, para el control de acceso de dispositivo.

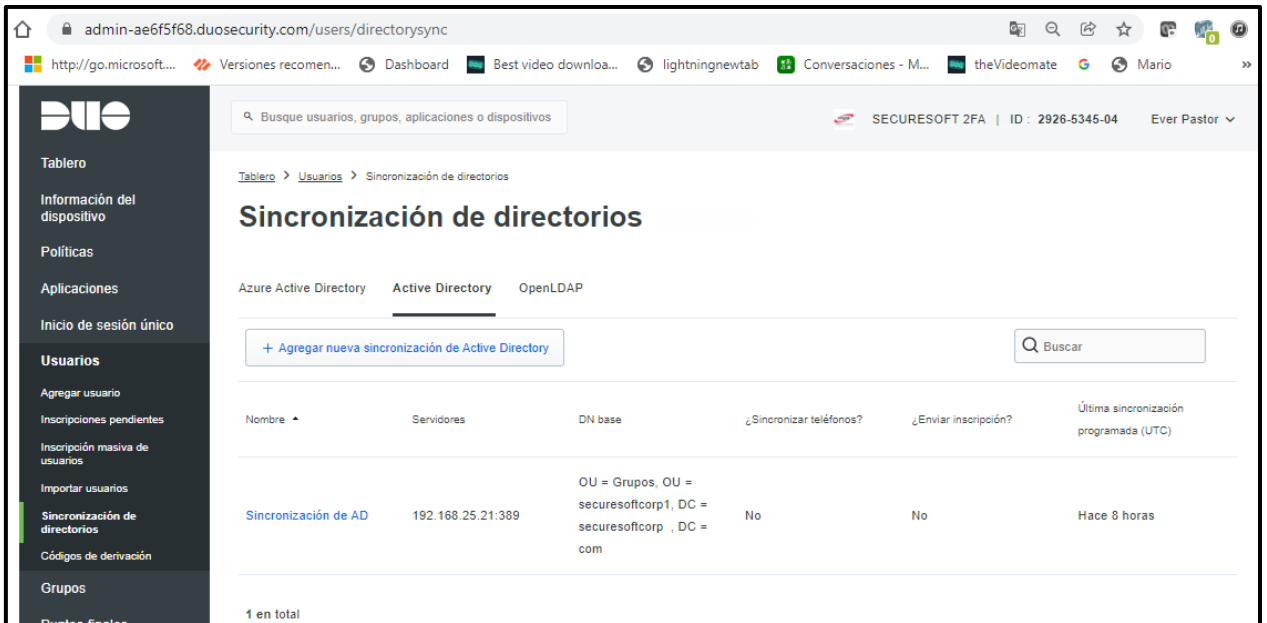


Fuente: Elaboración Propia,2021

4.-Desde el portal de doble factor de autenticación procedo con la configuración y registro del servidor AD (ip 192.168.25.21) en el portal de administración del 2FA y valido su comunicación correctamente para la lectura del grupo donde se encuentran los usuarios de la empresa a la cual se le brindará el cada requerimiento de autenticación el mecanismo de doble factor.

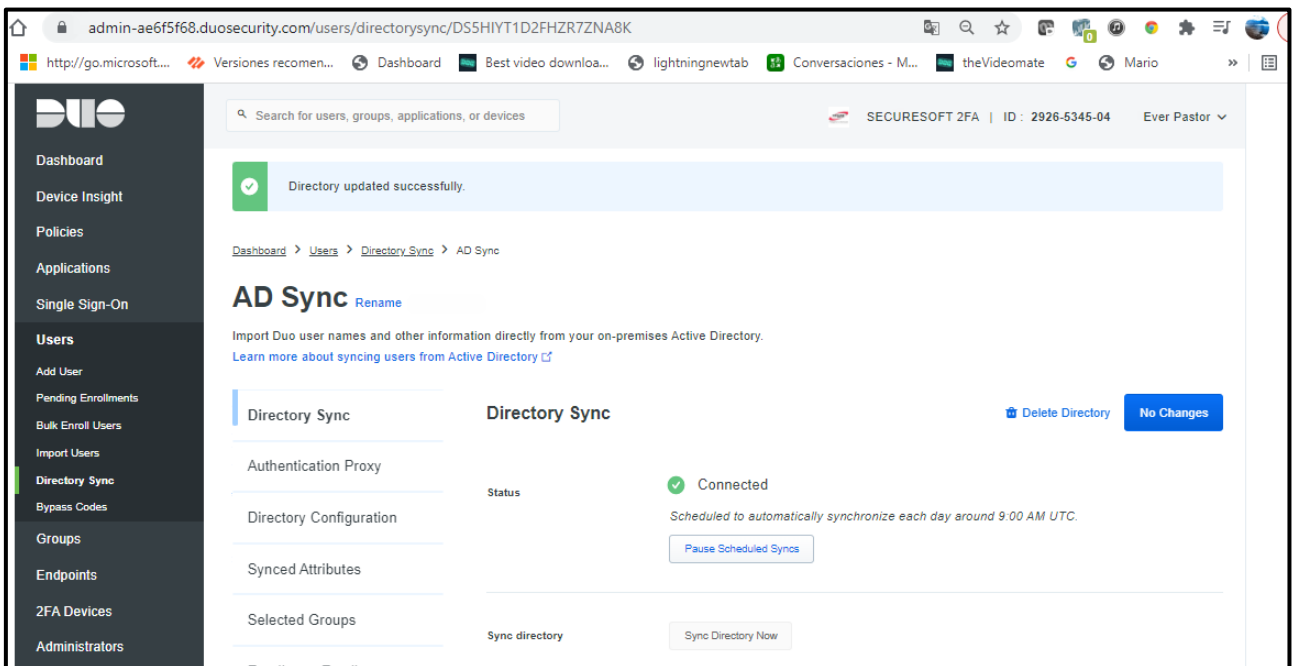
El puerto usado es el 389 el servidor registrado es el 192.168.25.21 y el DN Base registrada es el OU=Grupos, OU=seuresoft1, DC=seuresoft, DC=com

Figura 71. Registro del server AD en el portal de 2FA.



Fuente: Elaboración Propia,2021

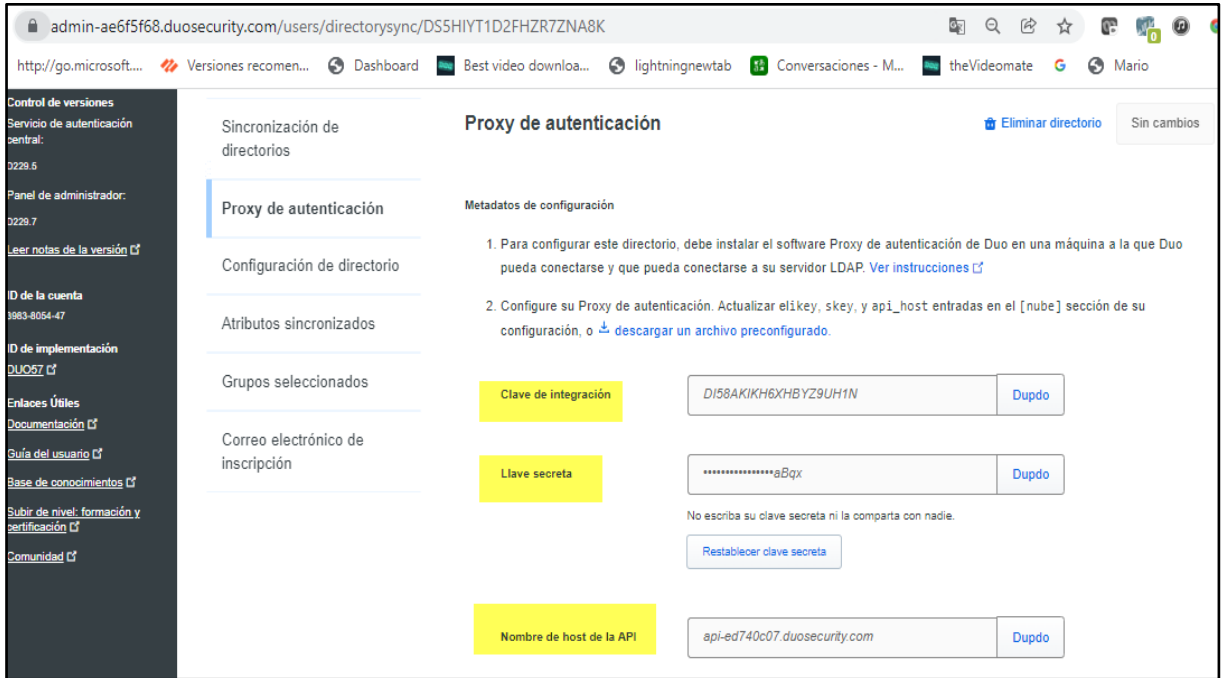
Figura 72. Conexión y sincronización del server AD en el portal de 2FA.



Fuente: Elaboración Propia,2021

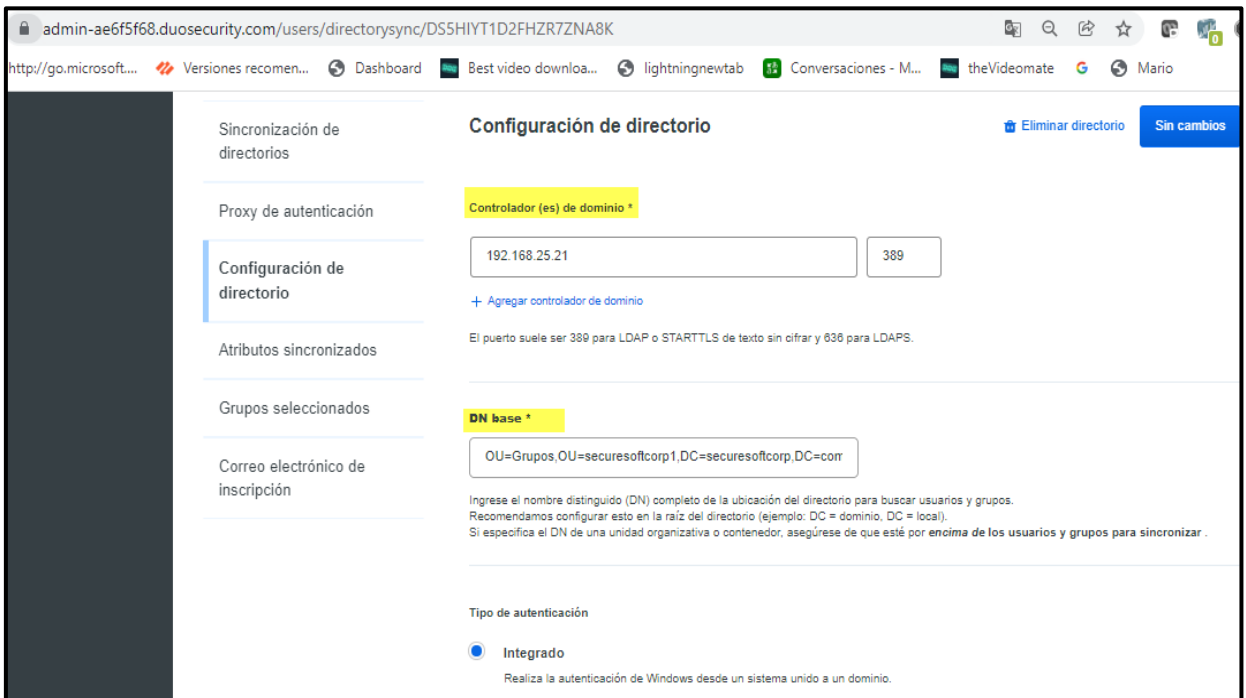
Configuración de atributos de API que se emplean en el Servidor Proxy Duo para la sincronización, detalle de configuración de Active Directory para la correcta lectura de los usuarios que se autentican para facilitarle el doble factor de autenticación.

Figura 73. Metadatos de API de configuración del Proxy de Autenticación.



Fuente: Elaboración Propia,2021

Figura 74. Parámetros configurados del servidor AD (IP server) y el DN Base.



Fuente: Elaboración Propia,2021

Figura 75. Atributos de perfil de usuario sincronizados y el grupo GlobalProtect2FA

The screenshot displays the 'Atributos sincronizados' (Synchronized Attributes) configuration page. On the left, a navigation menu includes 'Sincronización de directorios', 'Proxy de autenticación', 'Configuración de directorio', 'Atributos sincronizados', 'Grupos seleccionados', and 'Correo electrónico de inscripción'. The main content area is titled 'Atributos sincronizados' and includes a 'Eliminar directorio' link and a 'Sin cambios' button. The 'Nombre de usuario' field is set to 'samaccountname'. Below it, a note states 'Este atributo está en uso y no se puede cambiar.' The 'Alias de nombre de usuario' section includes a '+ Agregar un atributo de alias de nombre de usuario' link and explanatory text. The 'Nombre completo' field is set to 'displayname' with a 'Predeterminado: displayname' label. The 'Correo electrónico' field is set to 'mail' with a 'Predeterminado: correo' label. There are two unchecked checkboxes for 'Importar notas' and 'Importar teléfonos'. At the bottom, the 'Grupos seleccionados' section shows a dropdown menu with 'GlobalProtect2FA' selected.

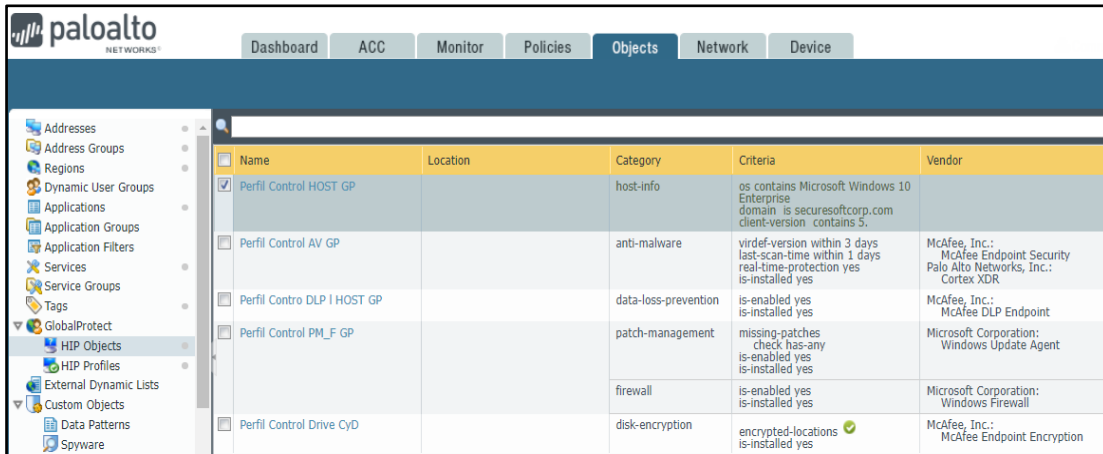
Fuente: Elaboración Propia,2021

A continuación, se realiza la configuración de los perfiles con los criterios de seguridad de control de acceso de dispositivo en el firewall Palo Alto como tercer medio de control de seguridad para el acceso remoto, es decir establecemos criterios seguros en la implementación para que algún dispositivo que no se encuentre autorizado es decir no cumpla con requisitos mínimos como tener un antivirus actualizado estos dispositivos no puedan conectarse a la red interna de la empresa privada.

Primero se implementa los objetos:

Configuro los atributos sobre las funciones de seguridad que debe tener los dispositivos que se conectan de forma remota a la red interna de la empresa, atributos son condiciones tales como el dispositivo deben estar registrado al dominio, debe tener el antimalware instalado y ofrecer en tiempo real la protección, debe tener el DLP instalado y activo, entre otros como muestra la imagen figura 76.

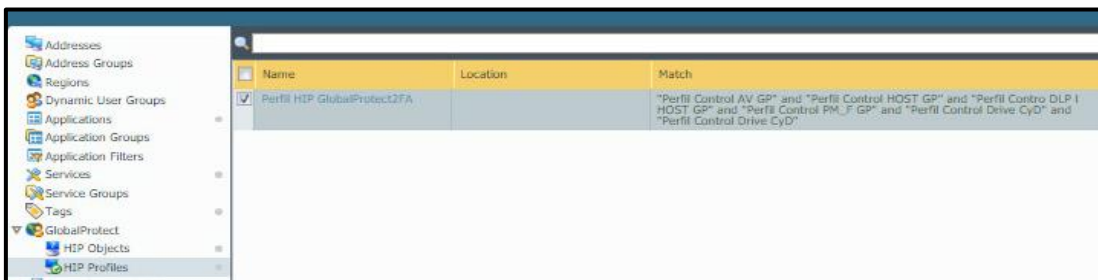
Figura 76. Configuración de objeto HIP Profile



Fuente: Elaboración Propia,2021

Segundo procedo a crear el perfil de objetos donde están las condiciones a cumplir y se agrupan los objetos creados en la imagen Figura 76.

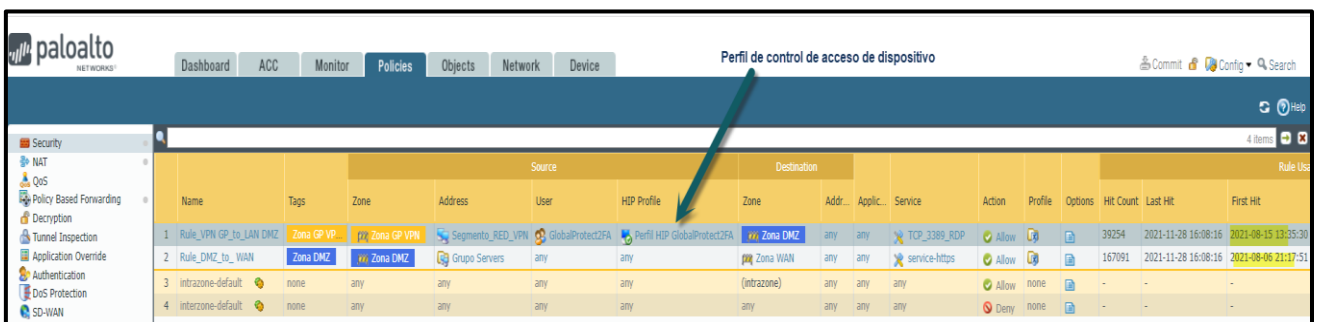
Figura 77. Configuración de perfil HIP Profile.



Fuente: Elaboración Propia,2021

Implementación del perfil HIPs profile es decir el control de acceso de dispositivo en las política de seguridad del firewall Palo Alto permite el acceso a los recursos internos de la empresa privada una vez que haya aprobado el acceso por el doble factor de autenticación y el control de acceso de dispositivo caso contrario se denegará el acceso a los recursos internos, se define Zona como LAN, DMZ, GP(relacionada a la VPN SSL), origen, destino, grupo de usuarios, perfil HIP Profile (control de acceso de dispositivo), puertos 3389 relacionado a RDP y la acción de permitir.

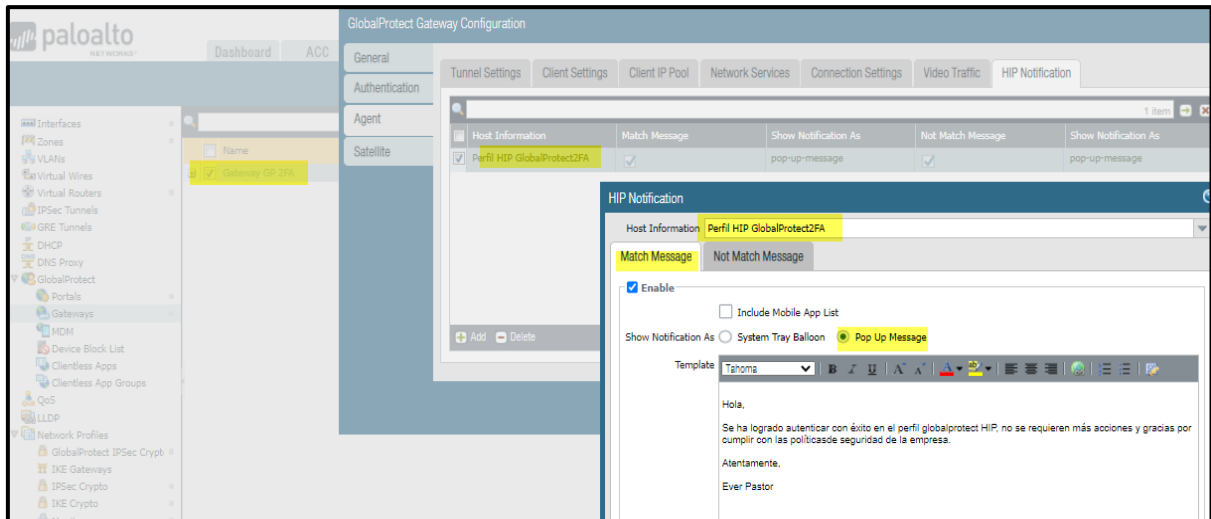
Figura 78. Configuración de perfil HIP Profile en la política de seguridad del Firewall



Fuente: Elaboración Propia,2021

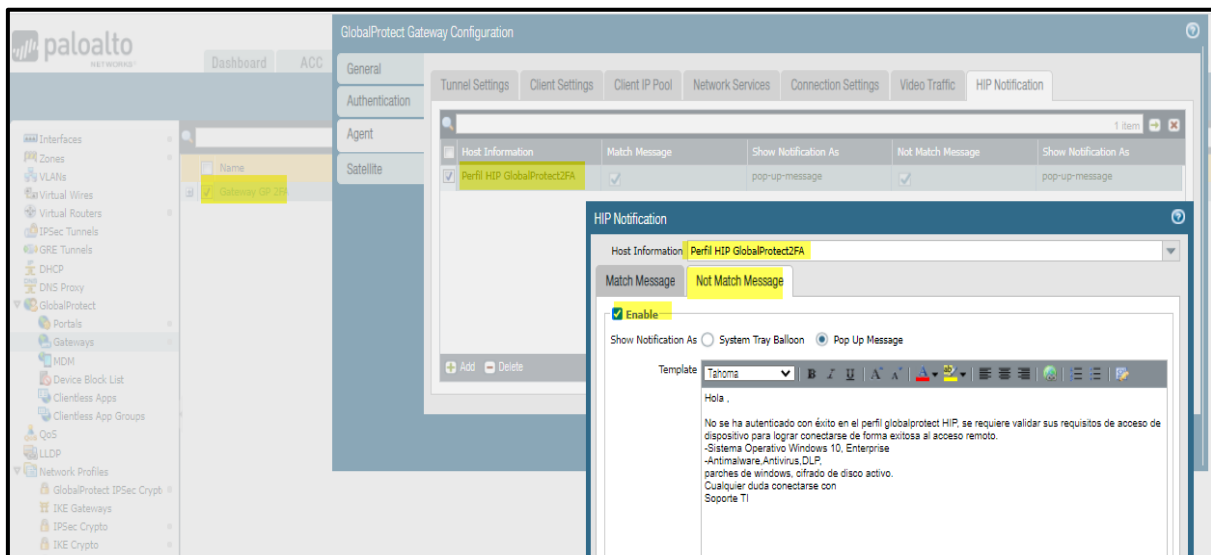
Implementación de las notificaciones del control de acceso de dispositivo en la VPN SSL es decir una vez lograda la conexión recibirá el usuario una notificación de acceso permitido y de no lograr la autenticación usando la nueva solución implementada recibirá un mensaje de autenticación fallida, esto nos permite establecer un control del usuario para que pueda conectarse correctamente o tener conocimiento de dónde pedir ayuda.

Figura 79. Configuración notificación aceptado de control de acceso de dispositivo



Fuente: Elaboración Propia,2021

Figura 80. Configuración notificación denegado de control de acceso de dispositivo

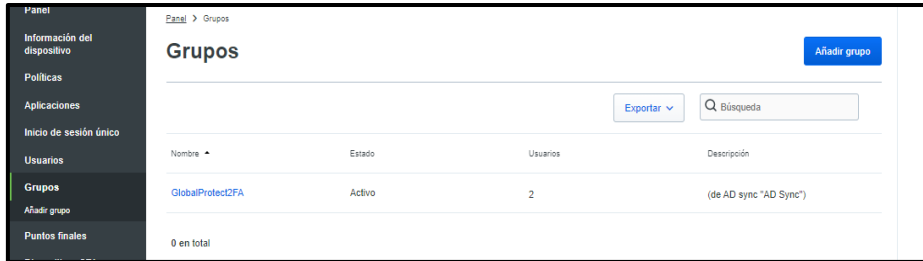


Fuente: Elaboración Propia,2021

Integración de grupo GlobalProtect2FA con AD:

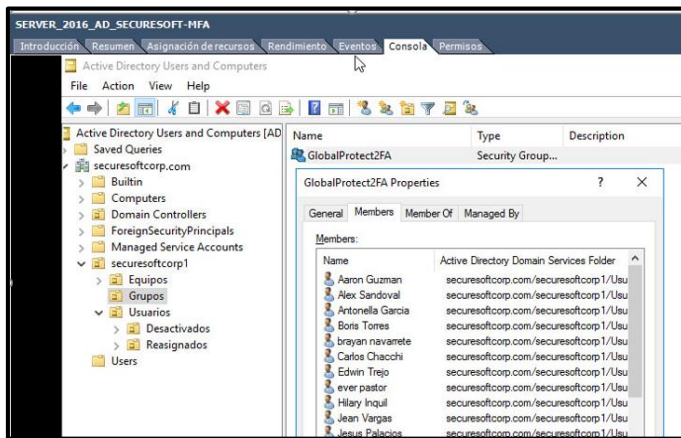
1.- Asigno el grupo de usuarios de AD en la consola de administración del 2FA Cisco DUO Security para que puedan sincronizarse los usuarios en su grupo permitido.

Figura 81. Grupo de usuarios de AD en la consola de administración Cisco DUO Security



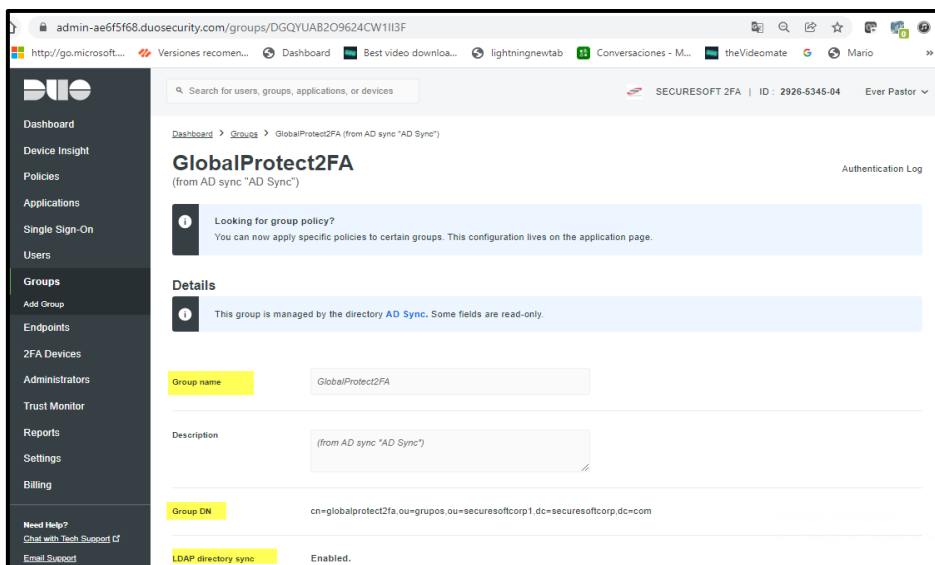
Fuente: Elaboración Propia,2021

Figura 82. Grupo “GlobalProtect2FA” que tiene los usuarios de la empresa desde el AD.



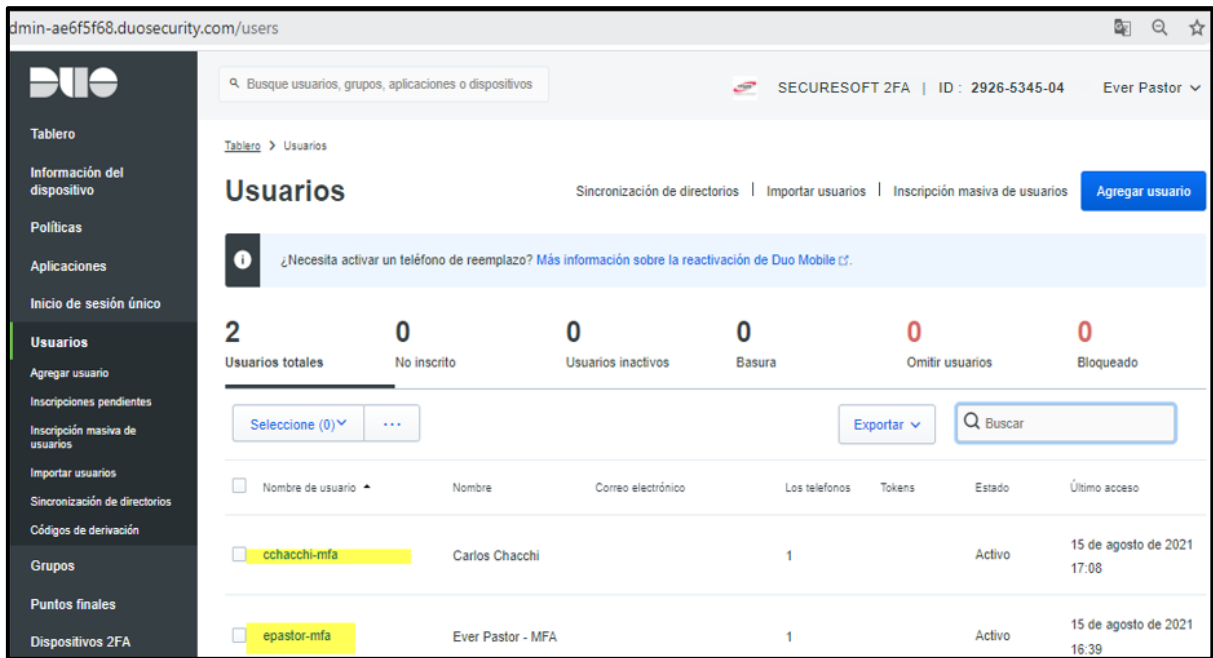
Fuente: Elaboración Propia,2021

Figura 83. Detalle del grupo de AD “GlobalProtect2FA” desde la consola de administración Cisco DUO Security.



Fuente: Elaboración Propia,2021

Figura 84. Usuarios iniciales sincronizados del grupo “GlobalProtect2FA”

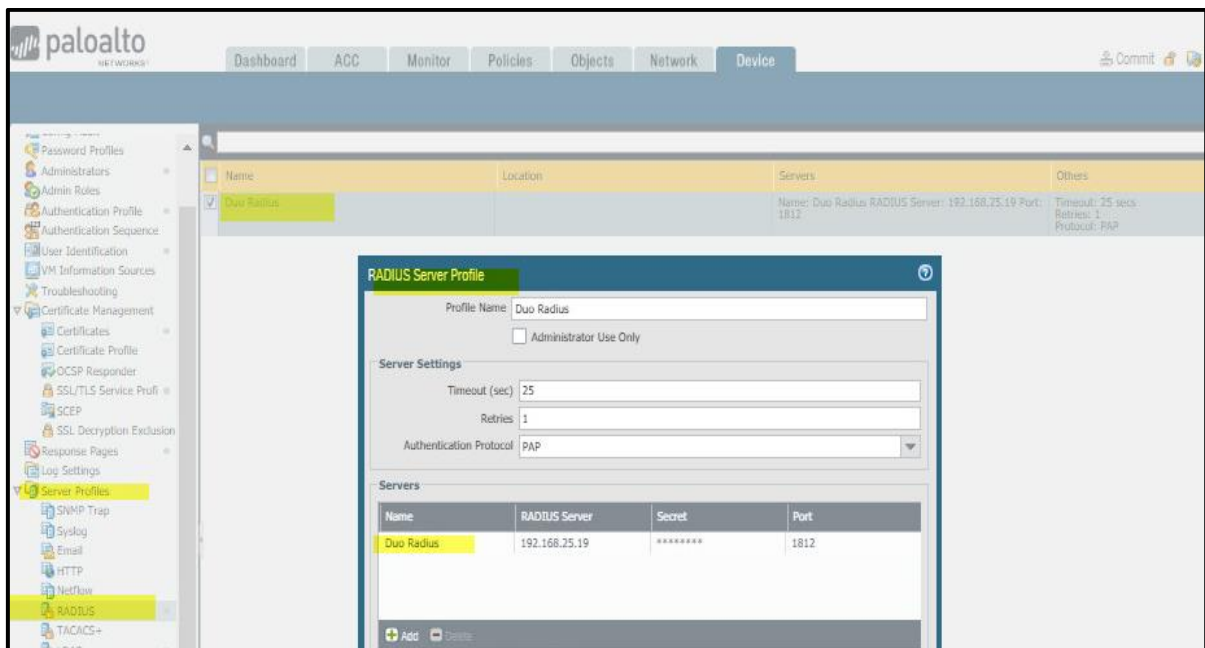


Fuente: Elaboración Propia,2021

2.-Configuro y sincronizo el servidor Duo Proxy (192.168.25.19) en el firewall Palo usando el protocolo de autenticación Radius con su perfil el cual procedo a configurar, detalle del servidor y puerto 1812 que utilizaré para la comunicación entre el Firewall y el server Duo Proxy.

En este punto se configura el perfil radius con sus parámetros de red principales del servidor radius el cual integra y sincroniza el server Proxy 2FA con el firewall Palo Alto.

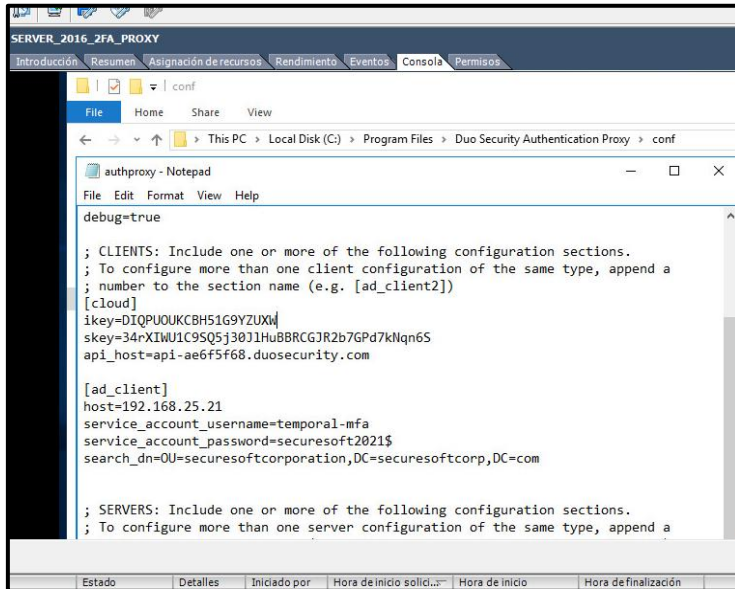
Figura 85. Configuración del servidor radius en el firewall Palo Alto



Fuente: Elaboración Propia,2021

3.-Configuración de los atributos y parámetros de red del servidor AD (IP 192.68.25.21) en el Server Proxy 2FA para la comunicación entre en servidor Duo Proxy y el Active Directory.

Figura 86. Configuración de los atributos y parámetros de red del servidor AD en el Server Proxy 2FA.



Fuente: Elaboración Propia,2021

Configuración y pruebas de usuarios iniciales.

1.-Configuración de método de autenticación en el Portal Duo Security para los usuarios iniciales.

Figura 87. Configuración del método de autenticación en el portal Duo Security.

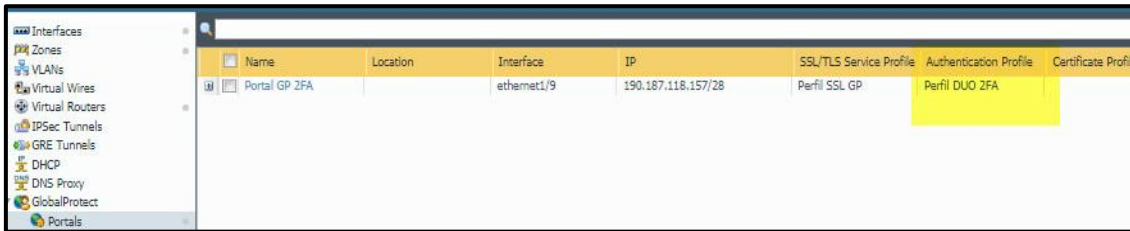


Fuente: Elaboración Propia,2021

2.- Configuración del perfil de autenticación en la configuración Global Protect VPN SSL en el firewall Palo Alto, este perfil está asociado a la autenticación radius, en donde los usuarios se enganchan al Gateway 190.187.11.8.157 y al tener el perfil Radius configurada en la VPN permite la validación y acceso de los usuarios autenticados reconocidos por el perfil de autenticación radius.

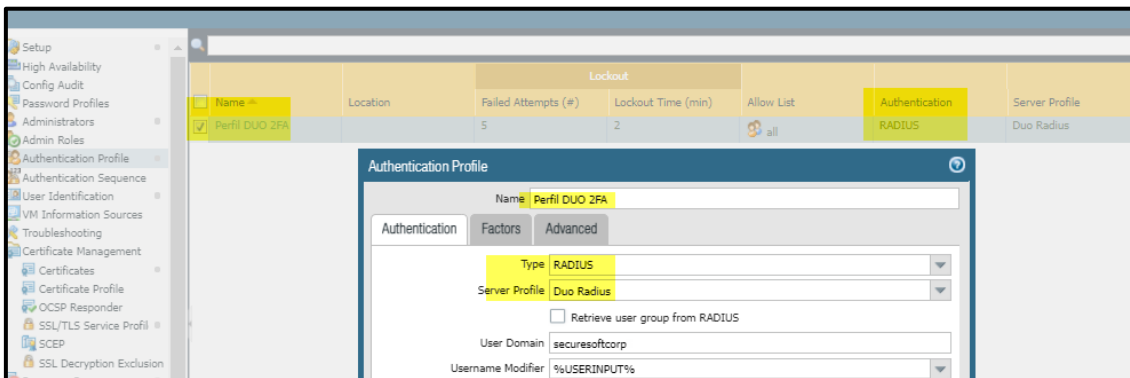
En el portal y Gateway:

Figura 88. Configuración del perfil de autenticación en el Portal Global Protect.



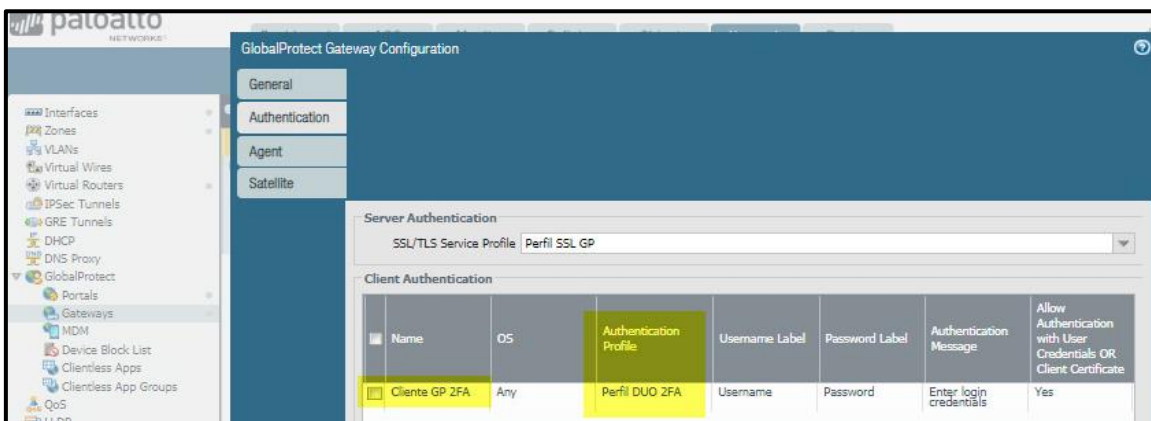
Fuente: Elaboración Propia,2021

Figura 89. Configuración del perfil de autenticación en el Portal Global Protect.



Fuente: Elaboración Propia,2021

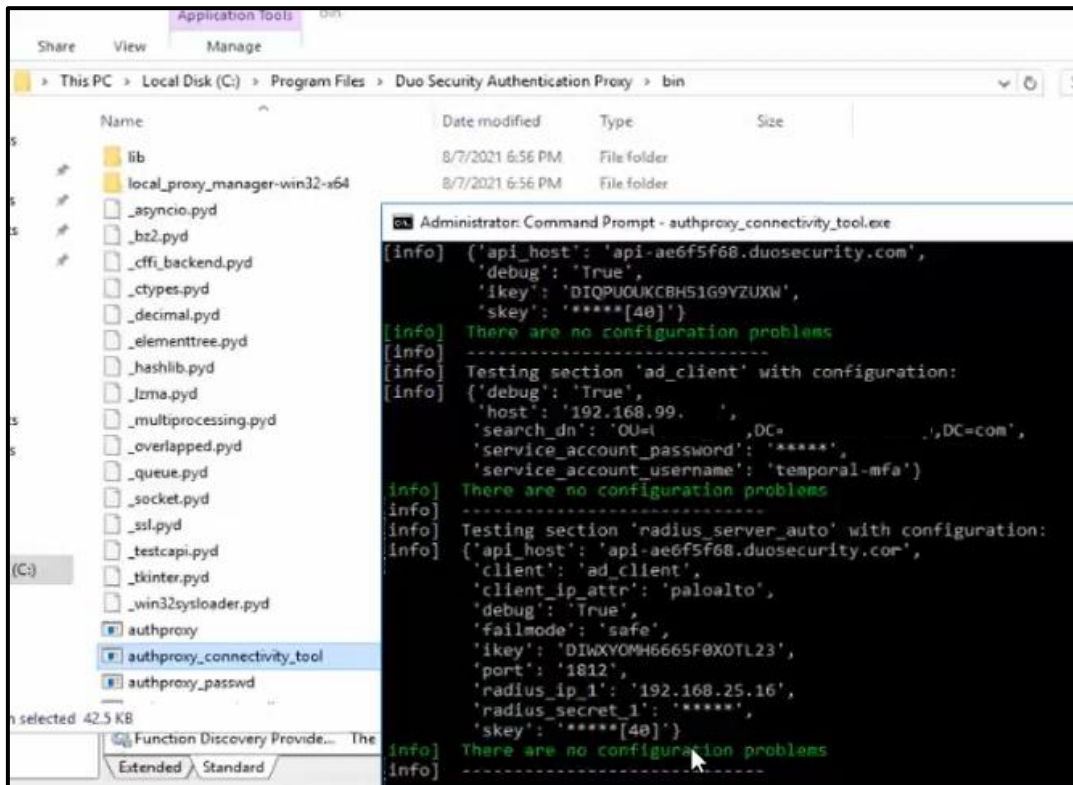
Figura 90. Configuración del perfil de autenticación “Perfil Duo 2FA” en el Gateway



Fuente: Elaboración Propia,2021

3.- Validación configuración de la API y parámetros de red y seguridad en el Duo Proxy Server, para la lectura correcta de los usuarios de la empresa privada.

Figura 91. Configuración de API y parámetros de red y seguridad del Duo proxy Server.



Fuente: Elaboración Propia,2021

4.- Prueba con usuarios iniciales: Se realiza el registro e importación de usuarios, descarga de token en los usuarios, prueba de funcionamiento del doble factor de autenticación de usuarios.

Figura 92. Sincronización de usuario 1



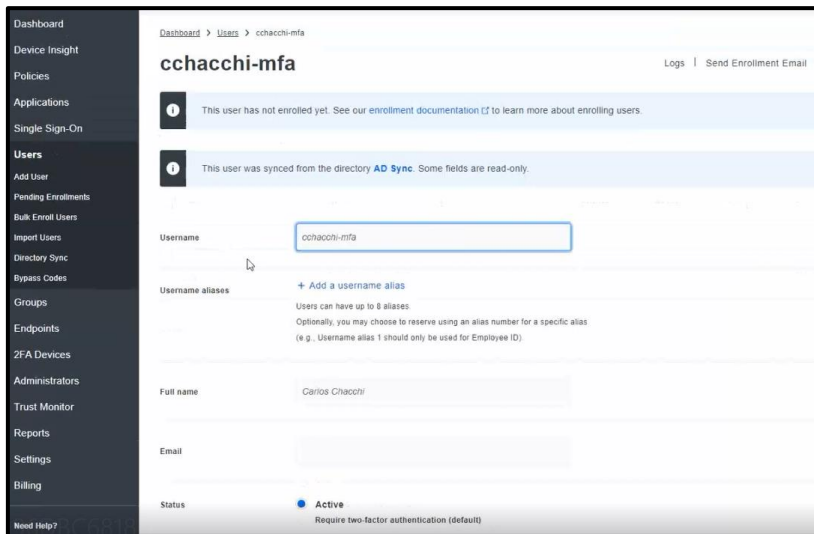
Fuente: Elaboración Propia,2021

Figura 93. Sincronización de usuario 2



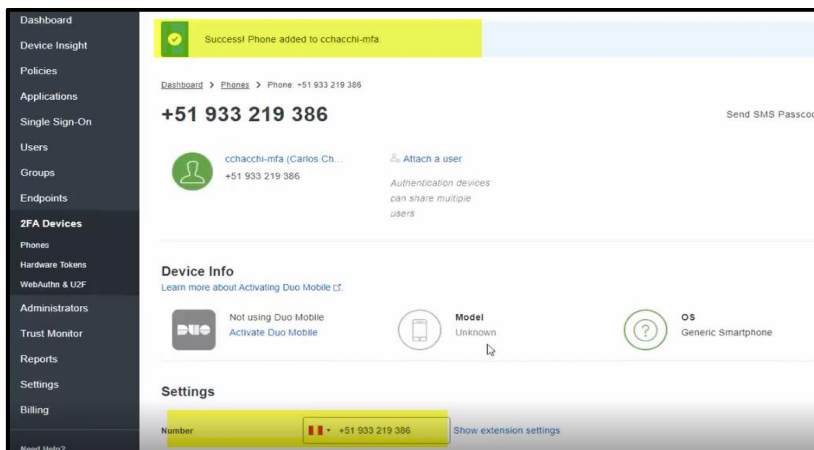
Fuente: Elaboración Propia,2021

Figura 94. Perfil de usuario de prueba como estado activo



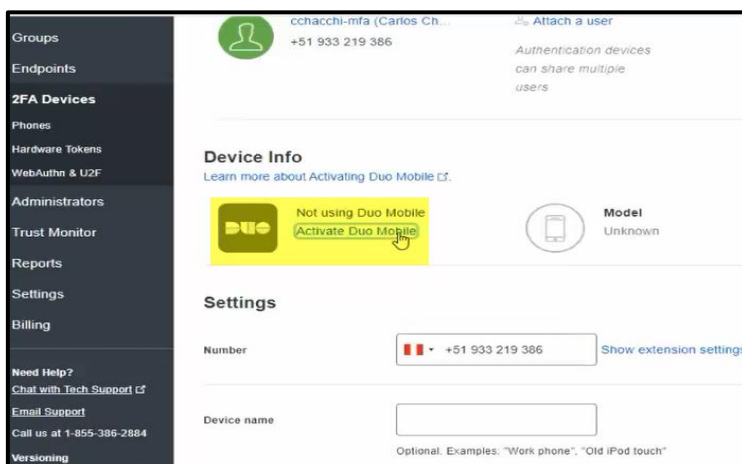
Fuente: Elaboración Propia,2021

Figura 95. Asignación de dispositivo para usuario de prueba



Fuente: Elaboración Propia,2021

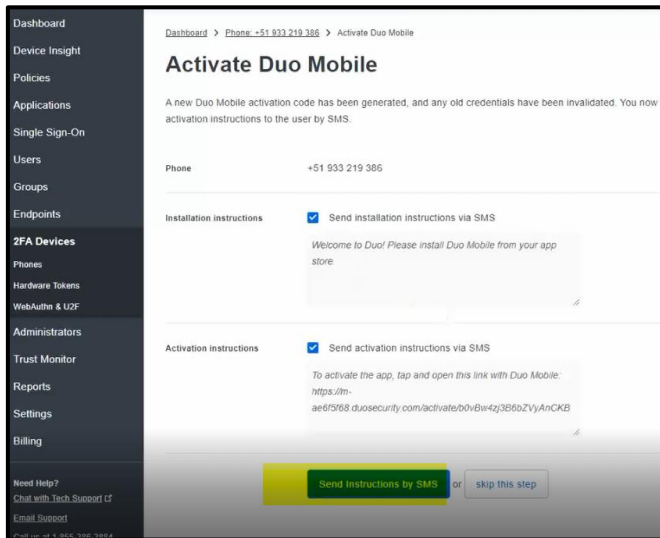
Figura 96. Activación del Duo Mobile



Fuente: Elaboración Propia,2021

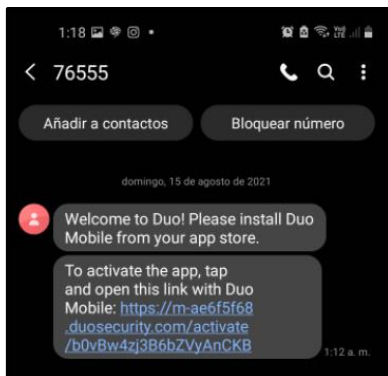
Se envía el enrolamiento del usuario con el dispositivo smartphone.

Figura 97. Envío de invitación de enrolamiento de usuario con la aplicación 2FA.



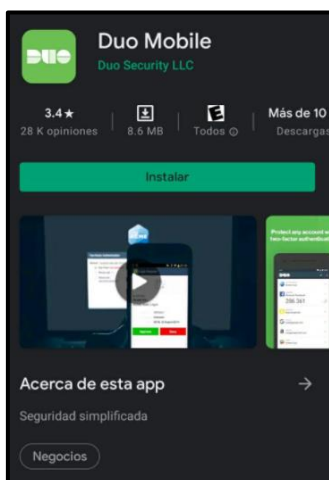
Fuente: Elaboración Propia,2021

Figura 98. Validación de notificación para activar la aplicación Duo Mobile.



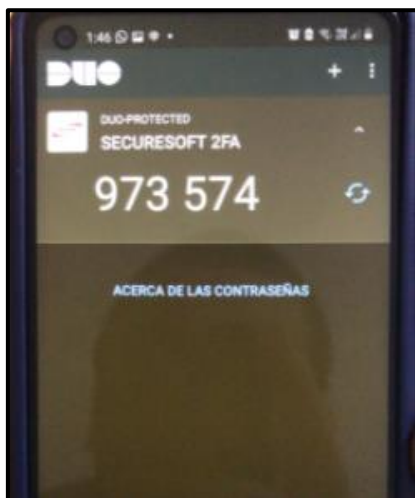
Fuente: Elaboración Propia,2021

Figura 99. Aplicación Duo Mobile.



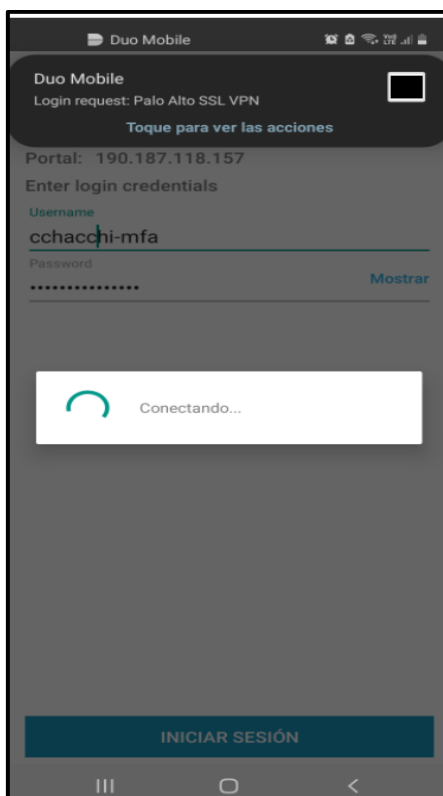
Fuente: Elaboración Propia,2021

Figura 100. Cuenta asociada de la empresa privada a la aplicación Duo Mobile.



Fuente: Elaboración Propia,2021

Figura 101. Inicio de sesión de usuario en la Aplicación Duo Mobile.



Fuente: Elaboración Propia,2021

Se evidencia el push de autenticación de sesión del proceso de la implementación del doble factor de autenticación para que el usuario valide aceptando la sesión o rechazándola si no es válida su conexión.

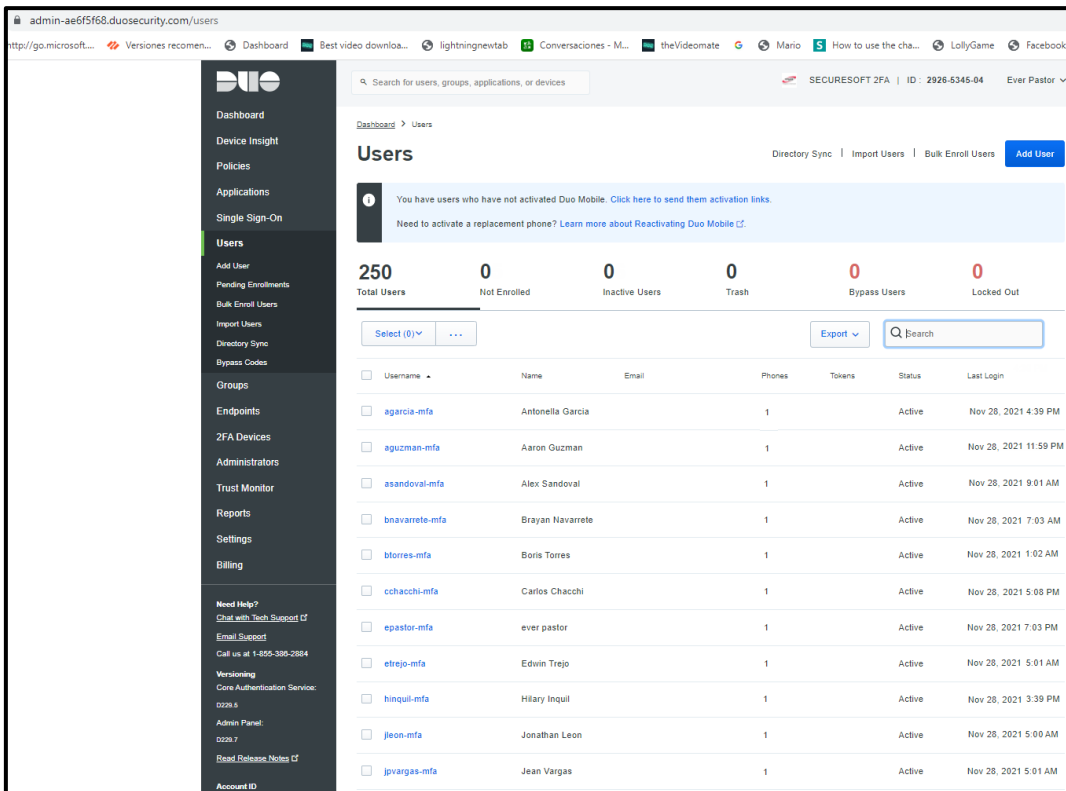
Figura 102. Push de validación de sesión del proceso de doble factor.



Fuente: Elaboración Propia,2021

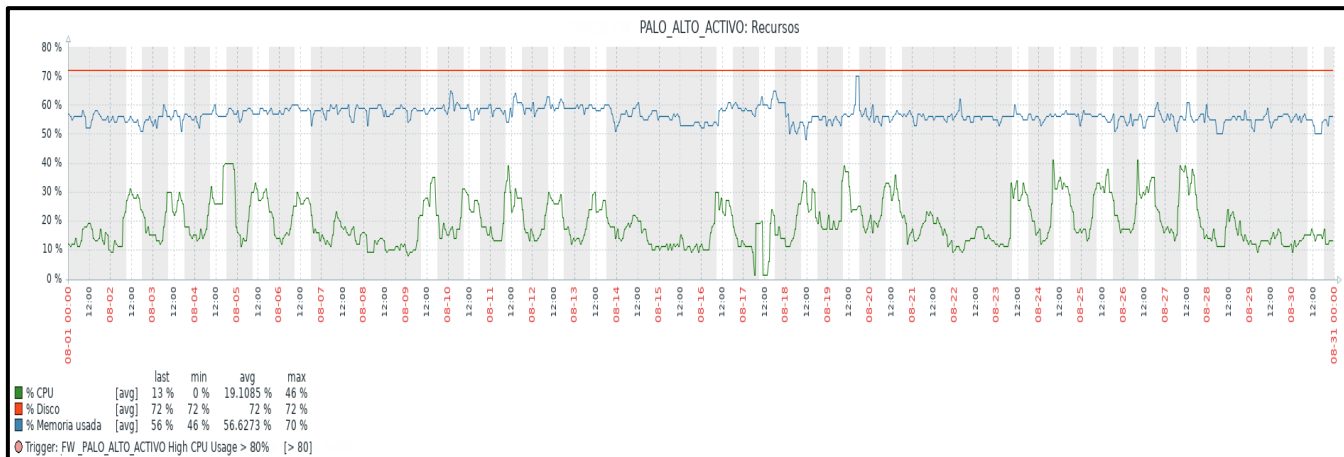
El despliegue y autorización de token fue bajo el mismo procedimiento mostrado con el usuario cchacchi-mfa, con este último punto completamos las actividades de implementación.

Figura 103. Usuarios registrados en la consola de administración de doble factor de autenticación al finalizar la implementación.



Fuente: Elaboración Propia,2021

Figura 106. Detalle del consumo de recursos Firewall Palo Alto.



Fuente: Herramienta de monitoreo Zabbix, 2021

Definición y detalle de Indicadores empleados:

Umbral con indicador de consumo de CPU: Para el seguimiento adecuado del consumo de recurso de CPU del equipamiento firewall el cual está en operación el proyecto implementado se define que dicho umbral no debe pasar al 80% de su uso de consumo tanto de management CPU y data plane de CPU este indicador ayuda a que la implementación no muestre afectada ante alguna falla del procesamiento del equipo que integra la solución implementada, durante el monitoreo no se observó algún consumo elevado o superación del umbral definido de consumo de CPU el cual es 80% de uso.

Umbral con indicador de cantidad de sesiones de red procesadas: Se define un umbral máximo de 367000 sesiones de red procesadas que equivalen a un 70% en relación con un total de sesiones soportadas de 524286, en caso supere dicho umbral será considerado que la plataforma no se encuentra estable para la operación de la solución implementada, durante el monitoreo de la operación de la nueva solución no se identificó que hubiese superado el umbral durante la fase de monitoreo y control de la solución implementada.

Figura 107. Detalle del consumo de Disco del Firewall Palo Alto

```
securesoft@PA-3050-Securesoft> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        3.8G  3.2G  440M  89% /
none            1.9G   64K  1.9G   1% /dev
/dev/sda5        7.6G  1.5G  5.7G  21% /opt/pancfg
/dev/sda6        3.8G  2.8G  892M  76% /opt/panrepo
tmpfs            1.9G  251M  1.6G  14% /dev/shm
/dev/sda8        90G   2.4G   83G   3% /opt/panlogs
```

Fuente: Elaboración Propia,2021

Figura 108. Detalle del consumo de Memoria del Firewall Palo Alto.

```

192.168.25.16 - PuTTY
top - 03:28:54 up 8 days, 11:43, 1 user, load average: 0.06, 0.04, 0.05
Tasks: 125 total, 3 running, 122 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.6 us, 0.6 sy, 0.1 ni, 98.6 id, 0.0 wa, 0.0 hi, 0.1 si, 0.0 st
KiB Mem : 3849884 total, 768996 free, 2189956 used, 890932 buff/cache
KiB Swap: 3056660 total, 2899400 free, 157260 used. 1272138 avail Mem

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM     TIME+ COMMAND
 6126   root    20   0 43884   3464 1828  R   6.2   0.1   0:00.01 top
    1   root    20   0  4324    200   172  S   0.0   0.0   0:04.93 init
    2   root    20   0     0     0     0  S   0.0   0.0   0:00.00 kthreadd
    3   root    20   0     0     0     0  S   0.0   0.0   0:22.86 ksoftirqd/0
    5    0 -20    0     0     0  S   0.0   0.0   0:00.00 kworker/0:+
    7   root    rt   0     0     0     0  S   0.0   0.0   0:04.74 migration/0
    8   root    20   0     0     0     0  S   0.0   0.0   0:00.00 rcu_bh
    9   root    20   0     0     0     0  S   0.0   0.0   1:52.32 rcu_sched
   10   root    20   0     0     0     0  R   0.0   0.0   0:00.00 watchdog/0
   11   root    20   0     0     0     0  R   0.0   0.0   0:00.00 watchdog/1
   12   root    rt   0     0     0     0  S   0.0   0.0   0:04.83 migration/1
   13   root    20   0     0     0     0  S   0.0   0.0   0:23.27 ksoftirqd/1
   14   root    20   0     0     0     0  S   0.0   0.0   0:00.00 kworker/1:0

```

Fuente: Elaboración Propia,2021

Usuarios enrolados y conectados:

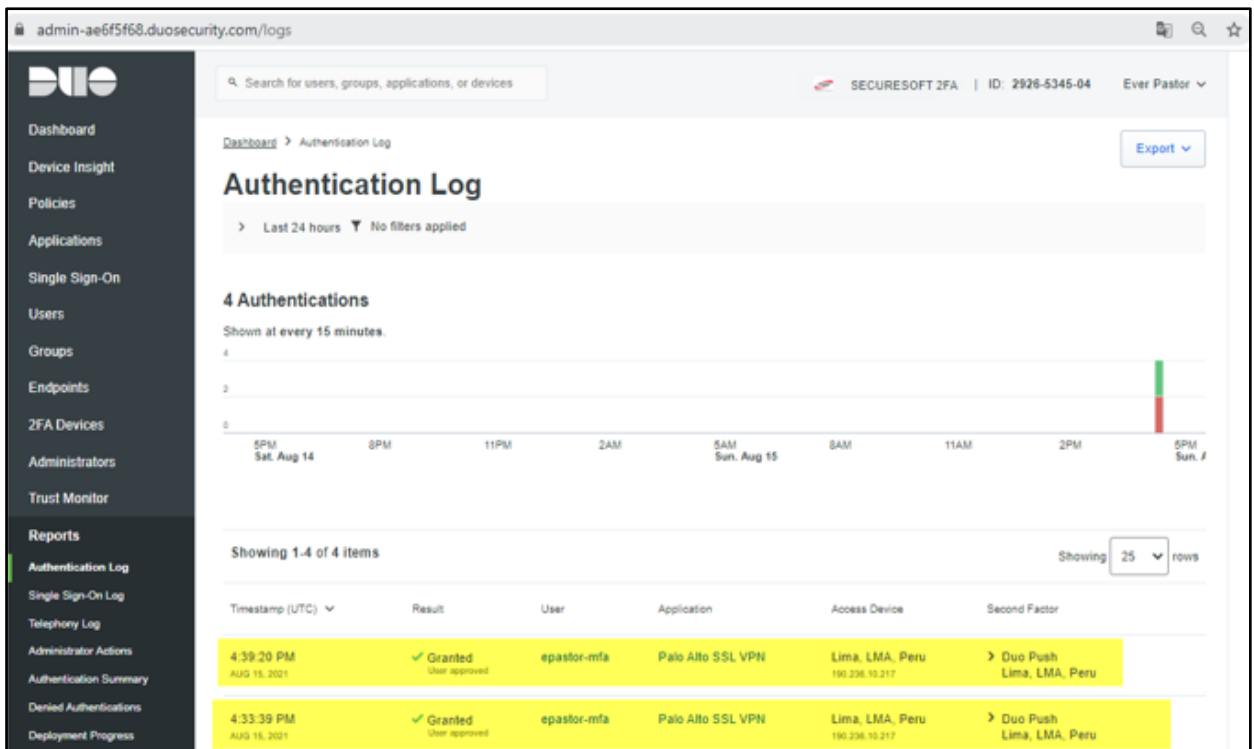
Figura 109. Registro 1 de usuarios enrolados y conectado.

Authentication Log Last 6 attempts					
Full authentication log					
Timestamp (UTC)	Result	User	Application	Access Device	Second Factor
5:08:08 PM AUG 15, 2021	✔ Granted User approved	cchacchi-mfa	Palo Alto SSL VPN	Lima, LMA, Peru 190.236.10.217	▼ Duo Push +51 933 219 386 Lima, LMA, Peru 190.236.10.217
5:07:51 PM AUG 15, 2021	✔ Granted User approved	cchacchi-mfa	Palo Alto SSL VPN	Lima, LMA, Peru 190.236.10.217	▼ Duo Push +51 933 219 386 Lima, LMA, Peru

Fuente: Elaboración Propia,2021

Indicador de registro satisfactorio por usuario: Se define que si se tiene durante el monitoreo de la solución implementada varios registros de autenticación satisfactoria es decir más de 15 registros de autenticación satisfactoria de un solo usuario por día es un indicador de alarma para validar con el usuario si las autenticaciones realizadas son las correctos o tiene algún problema con su internet o con la autenticación de su password e incluso con uso del doble factor de autenticación, además en la consola de administración de la solución implementada del doble factor de autenticación existe la forma de como validar si un usuario intentó autenticarse más de 15 veces por día.

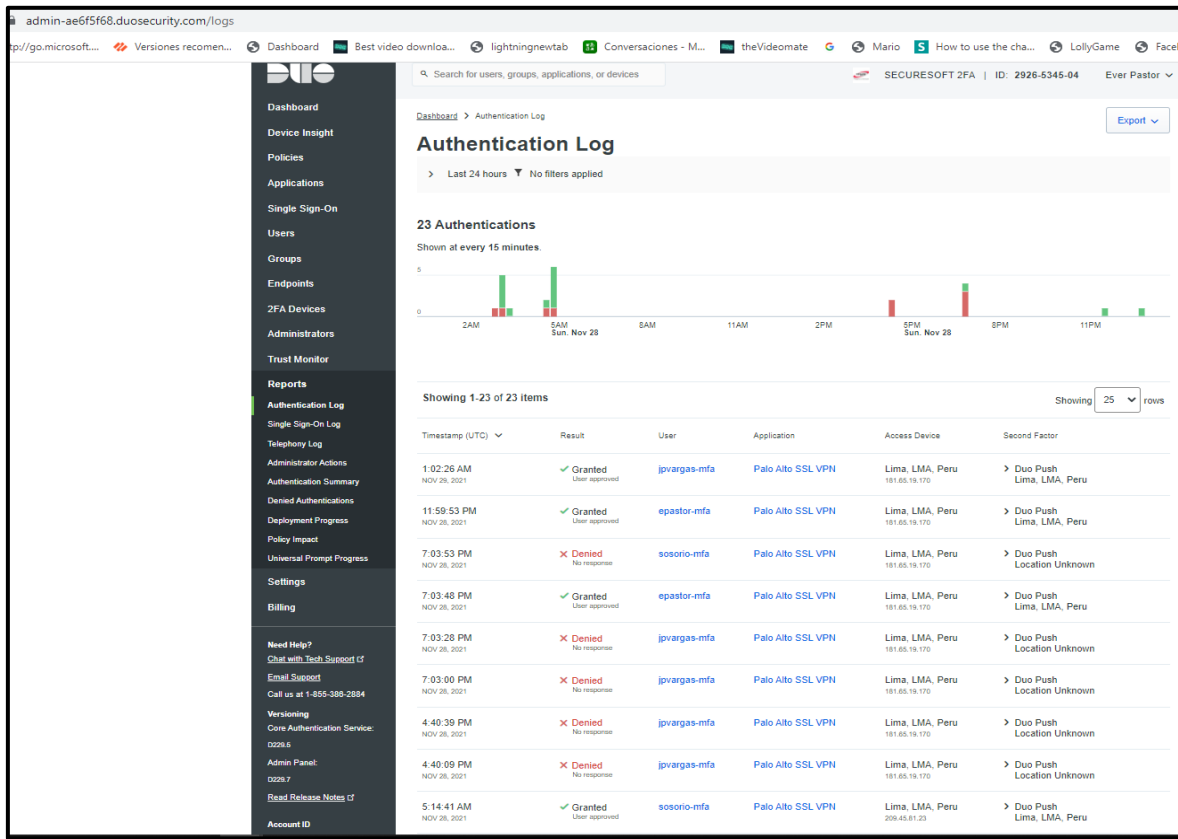
Figura 110. Registro 2 de usuarios enrolados y conectado.



Fuente: Elaboración Propia, 2021

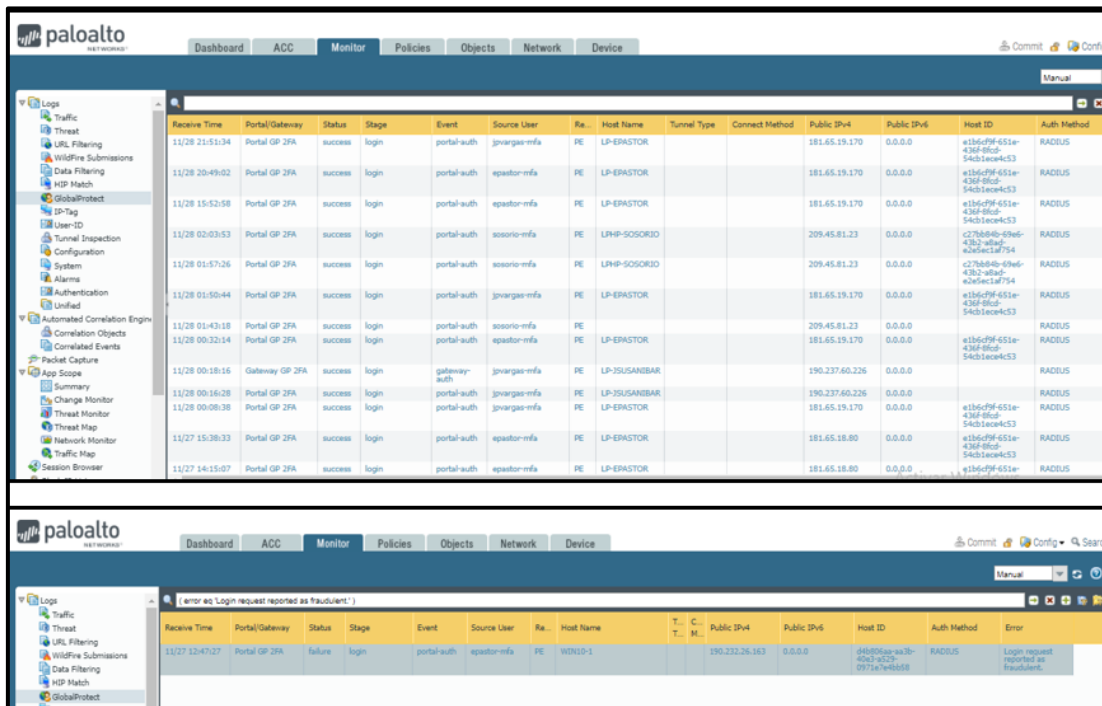
Indicador de registro denegado por usuario: Se define que si se tiene durante el monitoreo de la solución implementada existen varios registros de autenticación denegada es decir más de 5 registros de autenticación de un solo usuario por día es un indicador de alerta para validar con el usuario si tiene algún problema con el ingreso de su password o uso del doble factor de autenticación o también si no intentó las 5 veces del registro para identificar si se trata de algún intento de ataque de suplantación de identidad, en la consola de administración de la solución implementada del doble factor de autenticación existe la forma de como validar si un usuario intentó autenticarse fallidamente más 5 veces por día e incluso brinda detalle de la ip pública, ubicación geográfica y otros detalles para un análisis amplio de lo ocurrido.

Figura 111. Registro de otros usuarios con sus respectivas conexiones por doble factor de autenticación



Fuente: Elaboración Propia, 2021

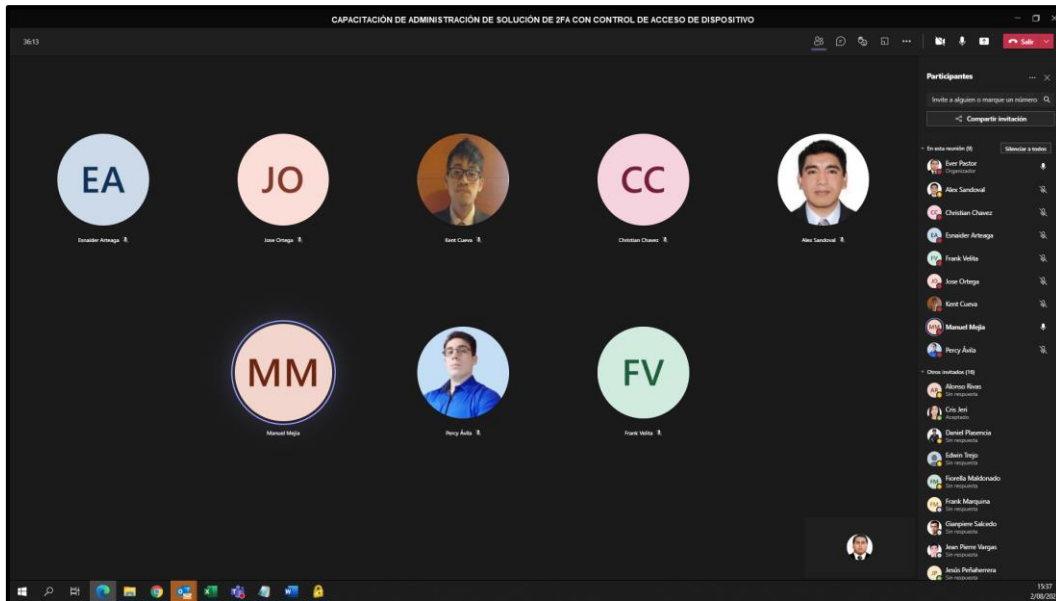
Figura 112. Registros del control de acceso de dispositivo



Fuente: Elaboración Propia, 2021

Reunión de capacitación programada sobre la explicación de la solución implementada.

Figura 113. Capacitación de la solución implementada.



Fuente: Elaboración Propia,2021

3.4 Fase de Cierre

Luego de validar el correcto funcionamiento y estabilidad de la nueva solución implementada durante 5 días se elabora la documentación de la implementación en donde se registra las instalaciones, configuraciones aplicadas las cuales evidencian el correcto funcionamiento de la solución también elaborar los entregables del proyecto. El Jefe del proyecto valida la documentación de los entregables del proyecto y envía los documentos en formato PDF adjunto, adicional se entrega la documentación del proyecto con los siguientes nombres de documentos:

- Diagrama de red final de la solución implementada. (Ver Anexo 2)
- Cronograma del Proyecto. (Ver Figura 35)
- Estado final de la solución. (Ver Actividades realizadas en la Fase de Implementación del Desarrollo de la solución)
- Alcance del proyecto. (Ver punto 3.2.1 de la fase de planificación de proyecto)
- Licenciamiento Adquirido. (Ver Figura 69 y Figura 70)

CAPITULO 4

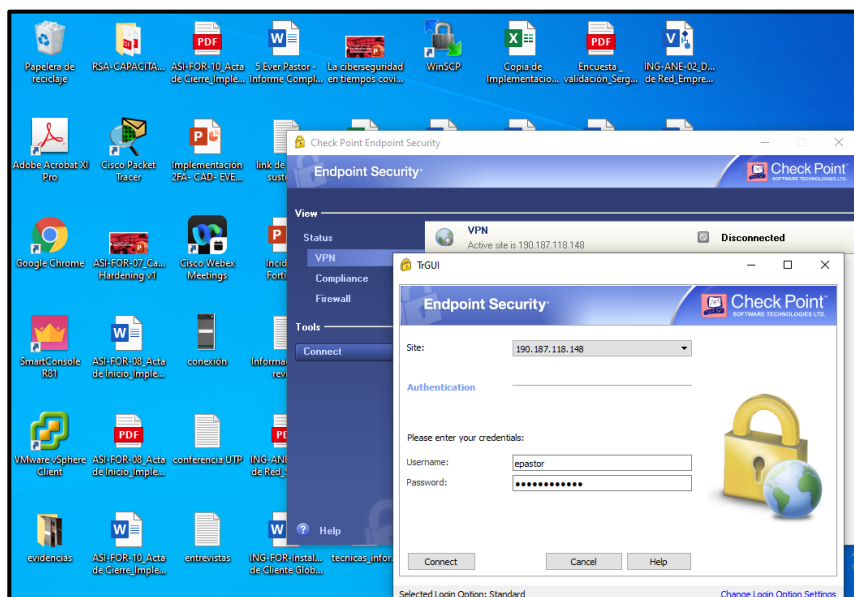
RESULTADOS

4.1.Resultados

En el presente capítulo menciono y brindo los resultados obtenidos luego de la implementación realizada y previamente muestro la solución antes de la implementación para evidenciar las mejoras realizadas luego de la implementación finalizada con los resultados exitosos, una vez que ya hemos finalizado la implementación de la nueva solución y encontrarse en producción fue posible obtener la solución al problema que presentaba la empresa privada, la implementación fue culminada satisfactoriamente brindando mejoras a nivel de seguridad informática, beneficios económicos en ahorrar algún gasto de uso de las instalaciones físicas (consumo de luz, agua) por parte de los trabajadores, ahorro también con el reinvento y reutilización de activo de la empresa para lograr la implementación deseada como es el caso de firewall Palo Alto debido a que no fue necesario incurrir a un gasto de equipamiento adicional permitiendo ahorro económico y de beneficio de salud debido a que todos los colaboradores trabajarían de forma remota logrando evitar algún riesgo de contagio de Covid-19, a continuación mostraré los resultados.

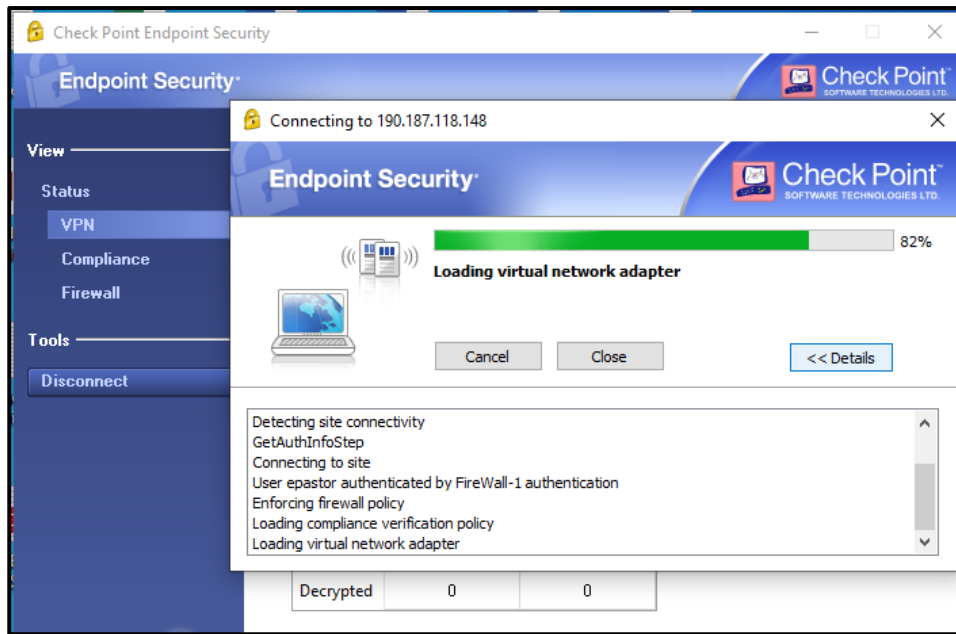
- 4.1.1.** Muestro la evidencia de conexión remota con básico acceso (usuario y contraseña) mediante el agente Check Point Endpoint Security la cual muestra sólo un mecanismo de seguridad con sólo un acceso por contraseña la cual puede ser vulnerado en cualquier momento, también se muestra y evidencia que el dispositivo del usuario no es el correcto para efectuar una conexión de acceso remoto debido a que no tiene ningún antivirus o antimalware activo la cual muestra una carencia a nivel de seguridad y tecnología, esta evidencia es antes de la implementación:

Figura 114. Autenticación de acceso remoto básico para VPN SSL Check Point.



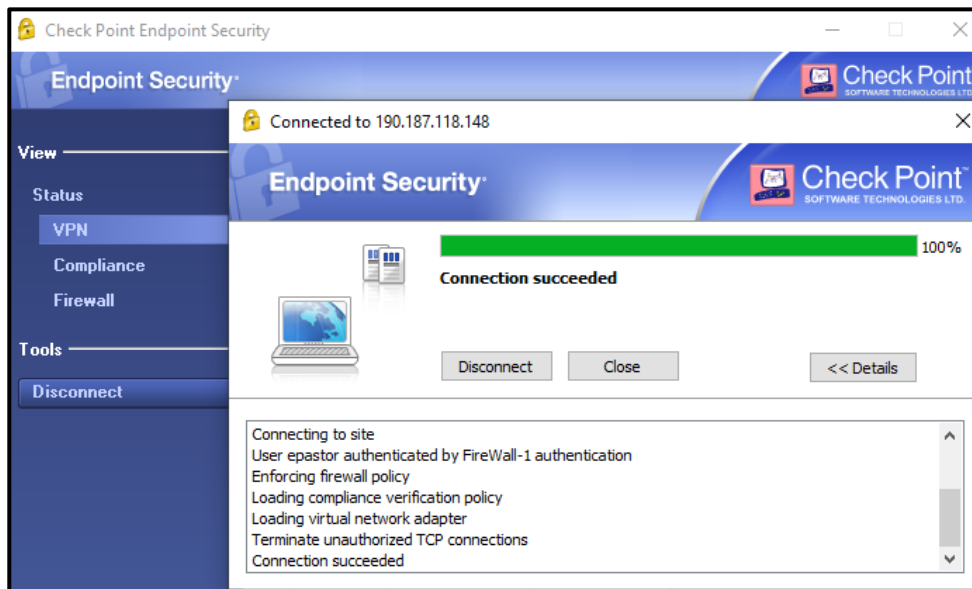
Fuente: Elaboración Propia,2021

Figura 115. Conexión de acceso remoto básico para VPN SSL Check Point



Fuente: Elaboración Propia,2021

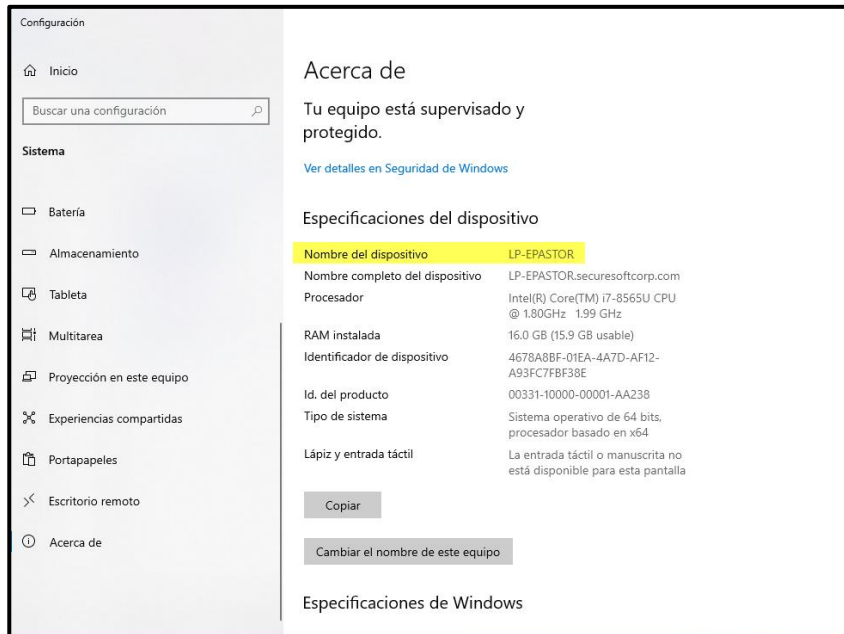
Figura 116. Conexión satisfactoria del acceso remoto básico para VPN SSL Check Point.



Fuente: Elaboración Propia,2021

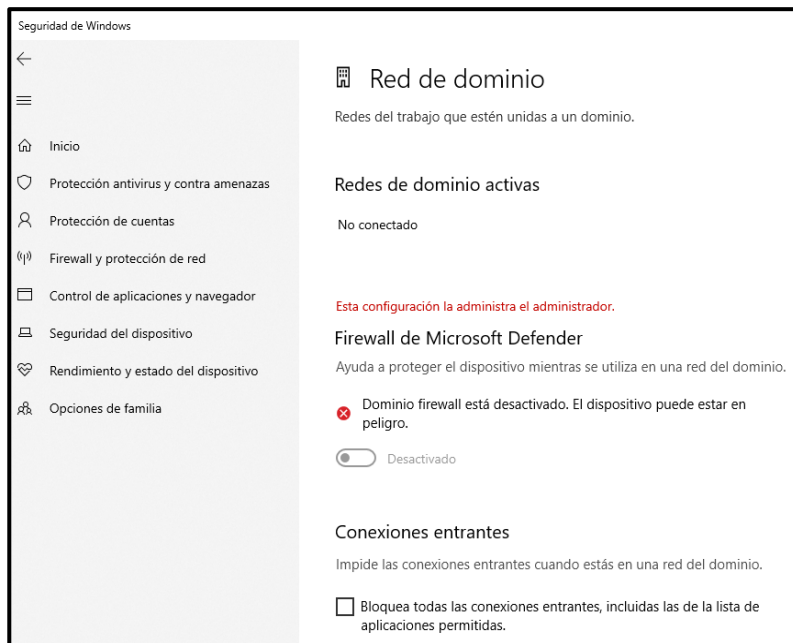
4.1.2. También muestro y evidencio que la laptop con hostname LP-PASTOR el mismo usuario que utiliza la conexión de acceso remoto mediante el agente Check Point no tiene control de acceso de dispositivo debido a que no tiene antivirus, antimalware, no pertenece al dominio y su disco no está cifrado sin embargo permite su conexión remota y acceso a recursos internos de la empresa privada originando una total falta de control de acceso a nivel seguridad informática, esta evidencia es antes de la implementación:

Figura 117. Información de equipo utilizado LP-EPASTOR para el acceso remoto.



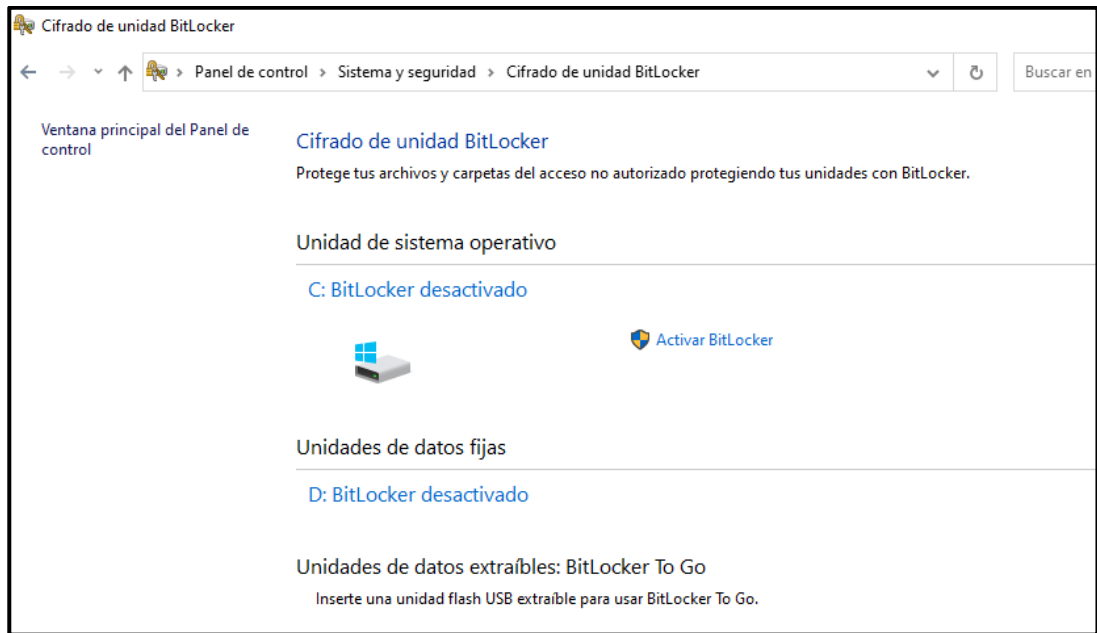
Fuente: Elaboración Propia,2021

Figura 118. Equipo utilizado LP-EPASTOR no tiene funciones de seguridad activas.



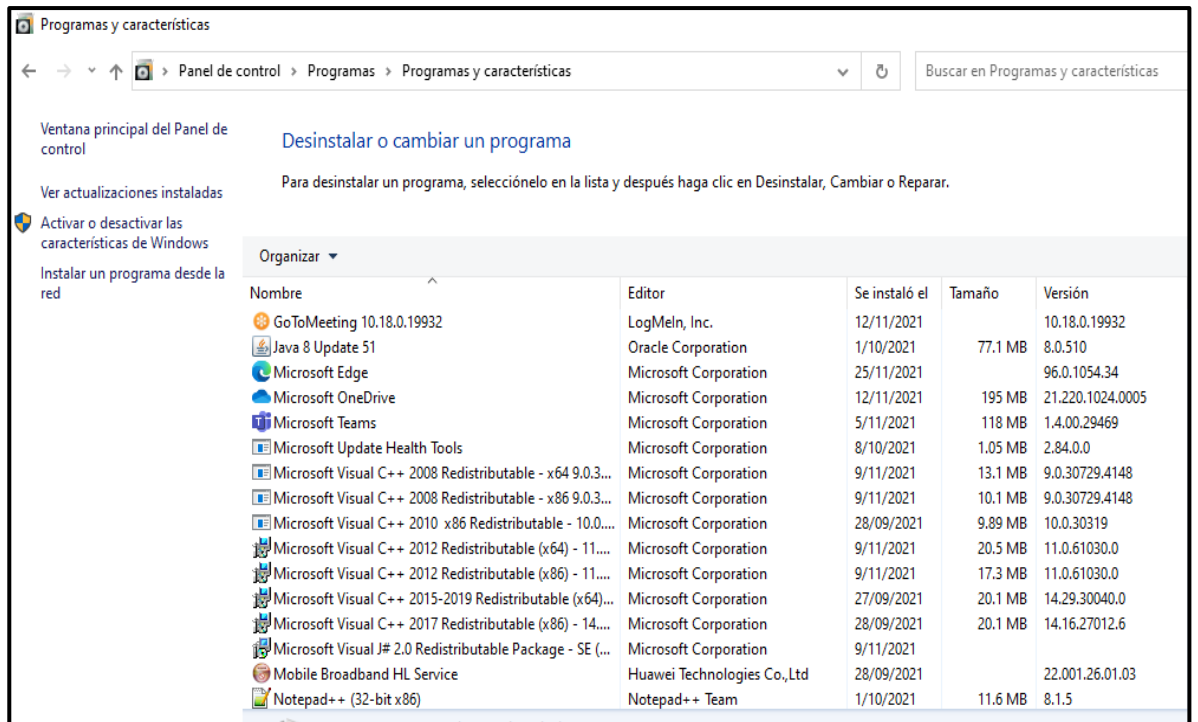
Fuente: Elaboración Propia,2021

Figura 119. Equipo utilizado LP-EPASTOR no tiene cifrado de disco activado.



Fuente: Elaboración Propia,2021

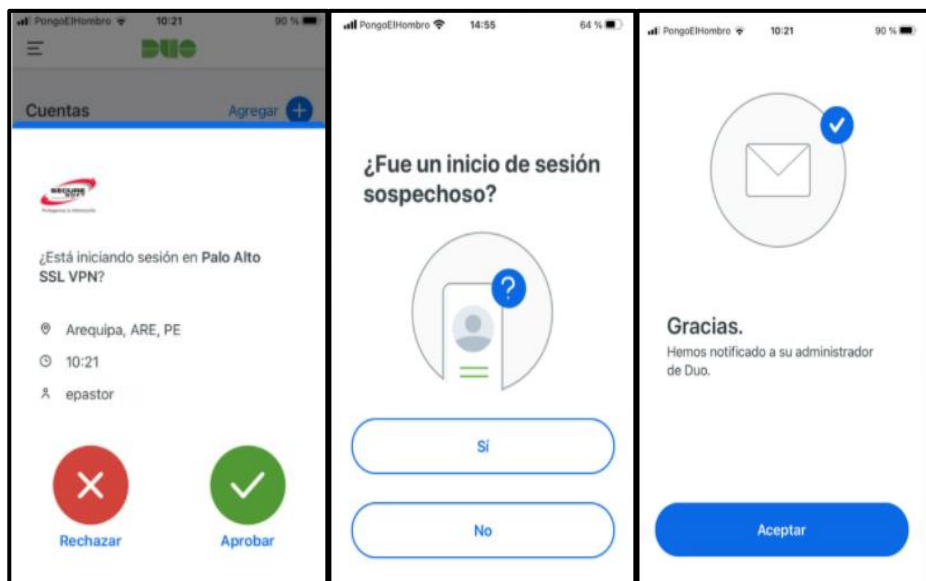
Figura 120. Equipo utilizado LP-EPASTOR no tiene antivirus o antimalware instalado.



Fuente: Elaboración Propia,2021

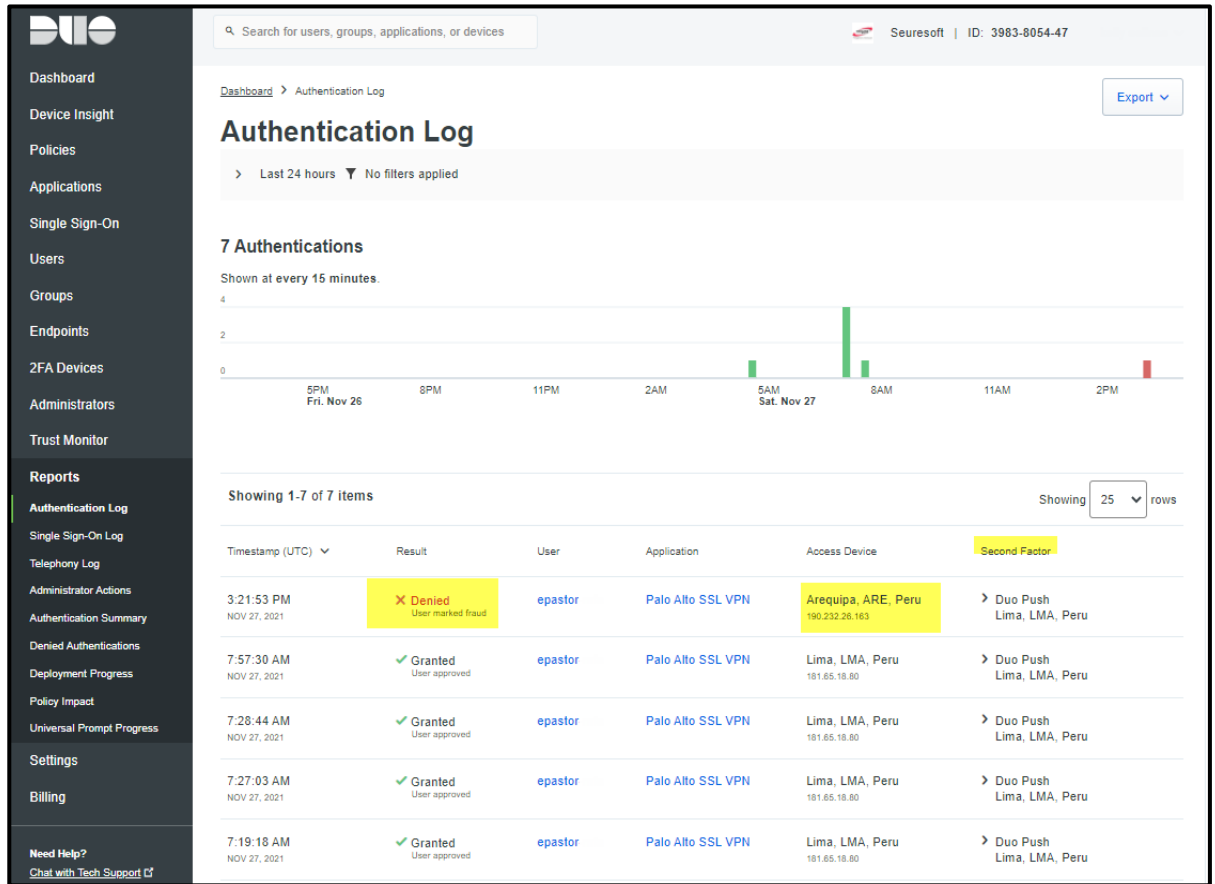
4.1.3. A continuación como primer resultado muestro y evidencio la mejora realizada con la implementación ya en operación donde el usuario ‘epastor’ con el dispositivo LP-EPASTOR que no cuenta con las medidas de seguridad informática activas como se muestra en los puntos 4.1.1 y 4.1.2, presento el resultado del acceso remoto denegado por una atacante que se encontraba en la localidad de Arequipa según el registro de la solución implementada, el atacante contaba con la contraseña del usuario epastor pero debido que ya se encontraba en operación la implementación de doble factor de autenticación y el usuario Ever Pastor (epastor) reconoce que no es su conexión la que intenta conectarse a la VPN remota debido a que se encuentra en la ciudad de Lima y no en Arequipa otra localidad, el usuario procede a rechazar la conexión y notifica al administrador para iniciar el proceso interno de la empresa para realizar el cambio de contraseña a nivel de Active Directory, con el presente resultado se evidencia que la solución implementada permite incrementar la seguridad informática del acceso remoto y adicional permitiendo realizar una mejora tecnológica a una solución que se adapta a las necesidades de las empresas privadas actuales.

Figura 121. Resultado de aplicación y notificación de rechazo conexión remota.



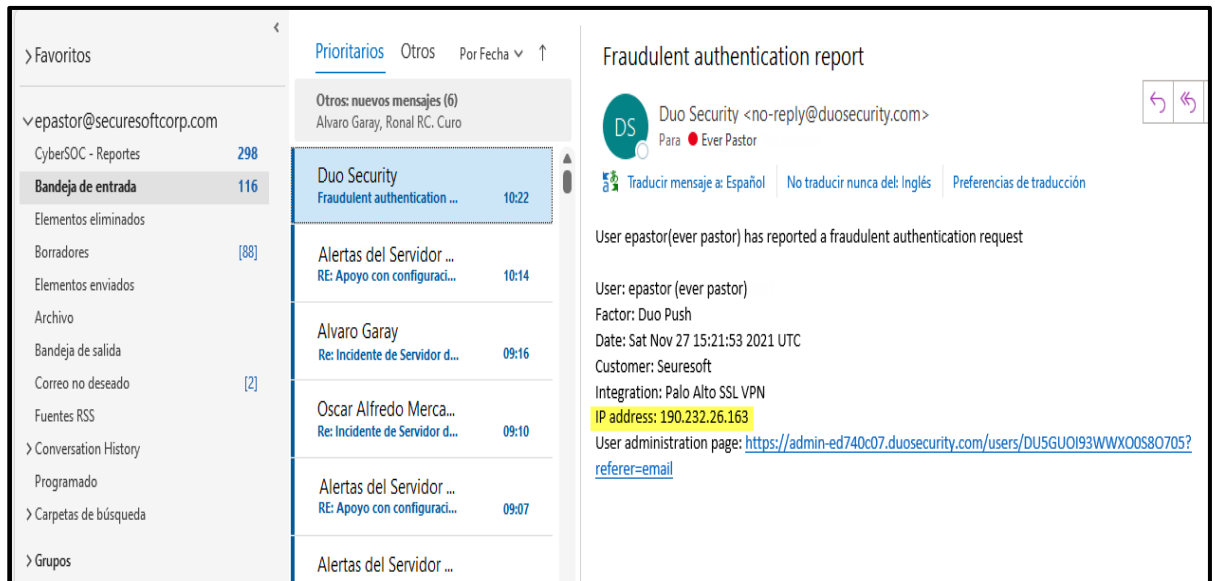
Fuente: Elaboración Propia,2021

Figura 122. Registros de rechazo conexión remota el cual no fue autorizado por el usuario real, desde la plataforma Doble Factor de Autenticación.



Fuente: Elaboración Propia,2021

Figura 123. Notificación de rechazo conexión remota el cual no fue autorizado por el usuario real, desde el correo corporativo.



Fuente: Elaboración Propia,2021

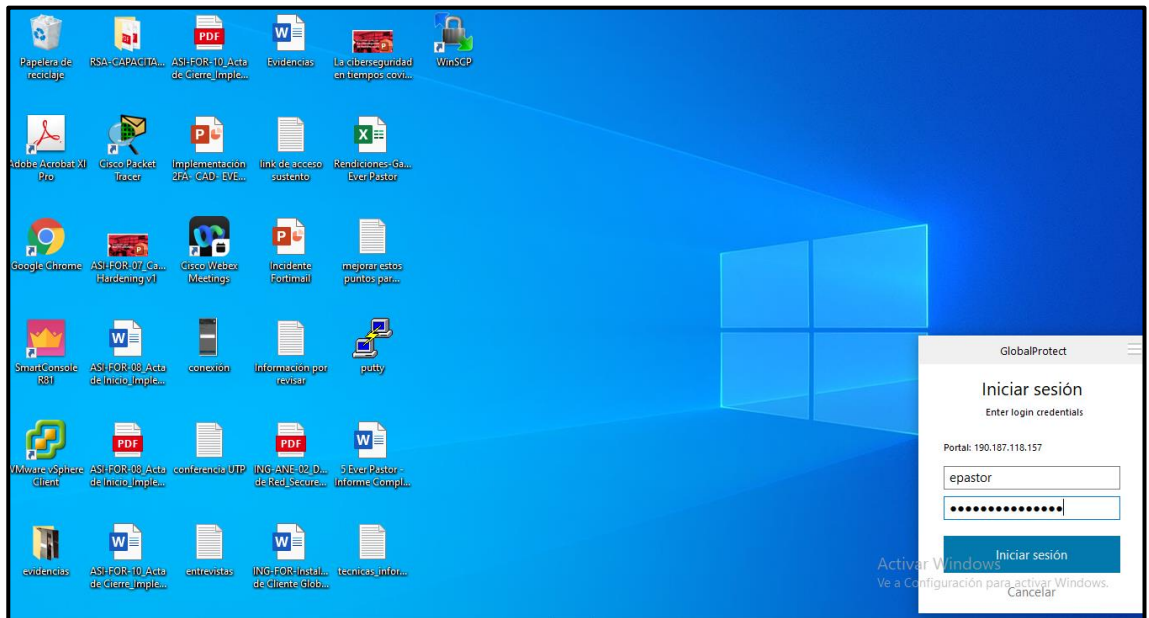
Figura 124. Registro de rechazo conexión remota el cual no fue autorizado por el usuario real, desde el Firewall Palo Alto donde está implementada la VPN SSL.

Portal/Gateway	Status	Stage	Event	Source User	Re...	Host Name	Tunnel Type	Connect Method	Public IPv4	Public IPv6	Host ID	Auth Method	Error
Portal GP ZFA	failure	login	portal-auth	epastor	PE	WIN10-1			190.232.26.163	0.0.0.0	d4b806aa-aa3b-40e3-a529-0971e7e4bb58	RADIUS	Login request reported as fraudulent.
Portal GP ZFA	success	before-login	portal-prelogin		PE				190.232.26.163	0.0.0.0	d4b806aa-aa3b-40e3-a529-0971e7e4bb58		

Fuente: Elaboración Propia,2021

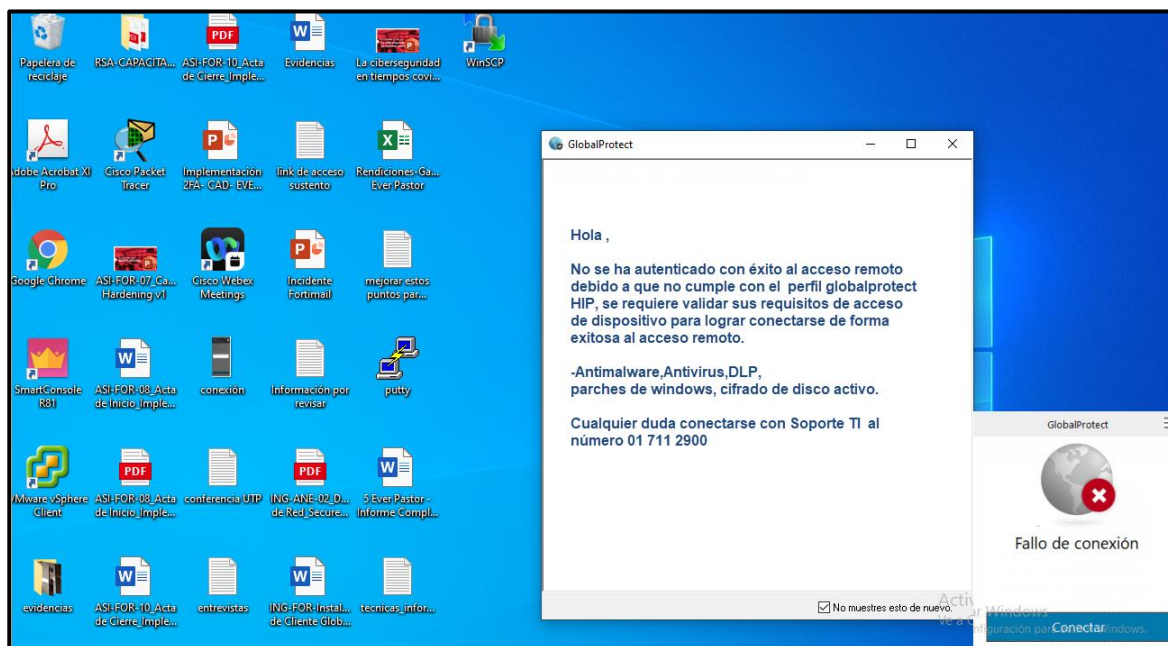
4.1.4. A continuación, muestro y evidencio el resultado del acceso remoto denegado por el control de acceso de dispositivo debido a que el dispositivo no cumple con los criterios mínimos de seguridad informática, se evidencia como resultado que el usuario Ever Pastor (epastor) se intenta conectarse con su equipo(Laptop) que no tiene activo un antivirus y antimalware, pero la solución implementada tiene ya un control de acceso de dispositivo en operación el cual rechaza la conexión y el acceso remoto, procede a notificarle e informarle que debe cumplir con ciertos criterios mínimos de seguridad informática como ejemplo tener un cifrado de disco activo, instalado algún antivirus y antimalware para que recién el control de acceso de dispositivo le permita ingresar a los recursos internos de la empresa privada.

Figura 125. Inicio de sesión de usuario epastor por el agente de conexión remota (Global Protect).



Fuente: Elaboración Propia,2021

Figura 126. Notificación de rechazo de la conexión remota por el control de acceso de dispositivo debido a que no tiene las funciones de seguridad activas.



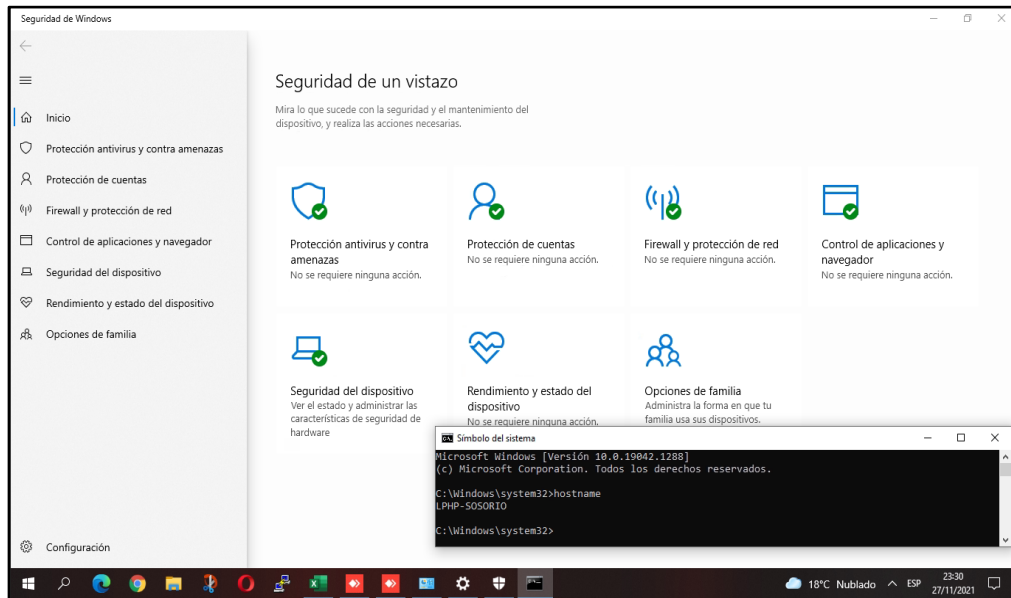
Fuente: Elaboración Propia,2021

4.1.5. A continuación muestro y evidencio como resultado exitoso de acceso remoto en donde la nueva implementación hace cumplir el doble factor de autenticación y control de acceso de dispositivo exitosamente debido a que identifica que el usuario Sergio Osorio identifica que se conecta desde su ubicación de Lima y es consciente que está realizando la conexión para brindar la autorización correspondiente aplicando el doble factor de autenticación y también su dispositivo(Laptop) cumple con requisitos mínimo de seguridad informática la cual tiene el antivirus y antimalware instalado y 1 día como máximo de último día de escaneo, cifrado de disco correctamente aplicado y una vez que el firewall Palo Alto identifica que el usuario Sergio Osorio pasó satisfactoriamente ambos procesos de doble factor de autenticación y control de acceso del dispositivo, el firewall permite la conexión y acceso a recursos internos de la empresa todo este proceso es una evidencia del incremento de seguridad informática que brinda la nueva solución implementada.

Se valida que el dispositivo tiene instalado software requerido a nivel de seguridad informática de acuerdo con el perfil (Figura 76 y 77) de seguridad informática definido en conjunto con el cliente para que la nueva implementación le pueda brindar el acceso remoto usando un mecanismo seguro de doble factor de autenticación y otro mecanismo de control de acceso de dispositivo.

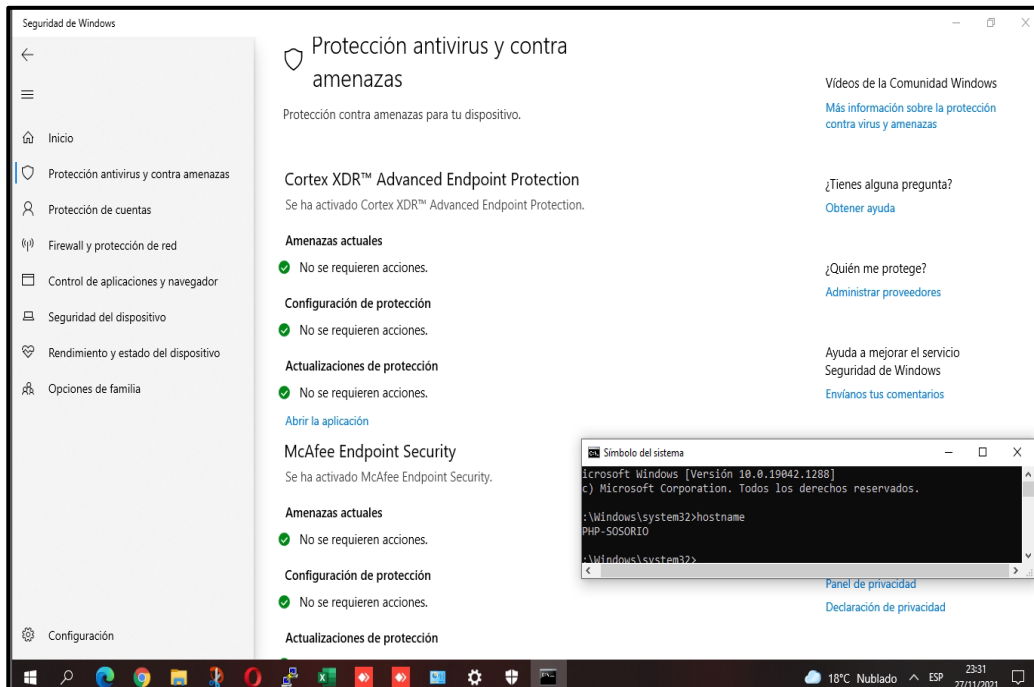
A continuación, se evidencia que el dispositivo (Laptop) tiene los componentes de seguridad informática el cual permite establecer una conexión remota exitosa, se valida activa la protección de amenazas, firewall activo, antivirus, antimalware, cifrado de disco duro, DLP en funcionamiento, a continuación, se detalla gráficamente el proceso.

Figura 127. Validación de funciones de seguridad activas del dispositivo LPHP-SOSORIO



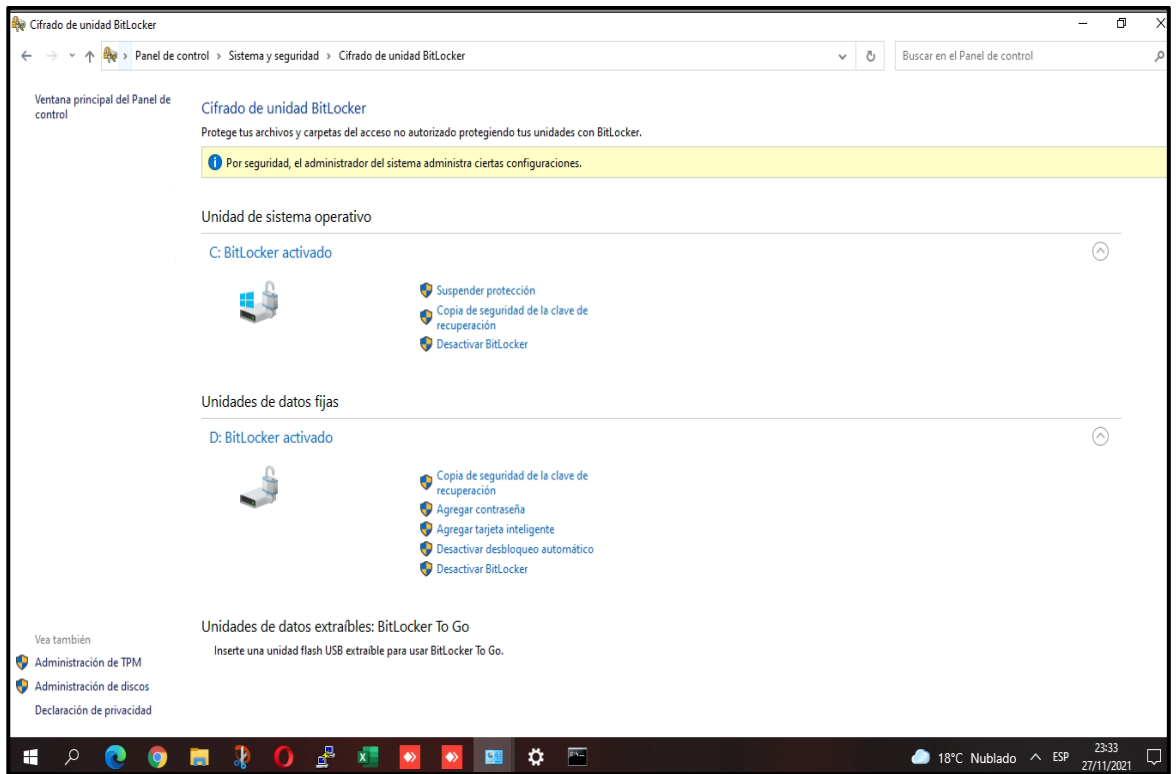
Fuente: Elaboración Propia,2021

Figura 128. Validación de funciones activas de Protección de Antivirus y Antimalware en dispositivo LPHP-SOSORIO



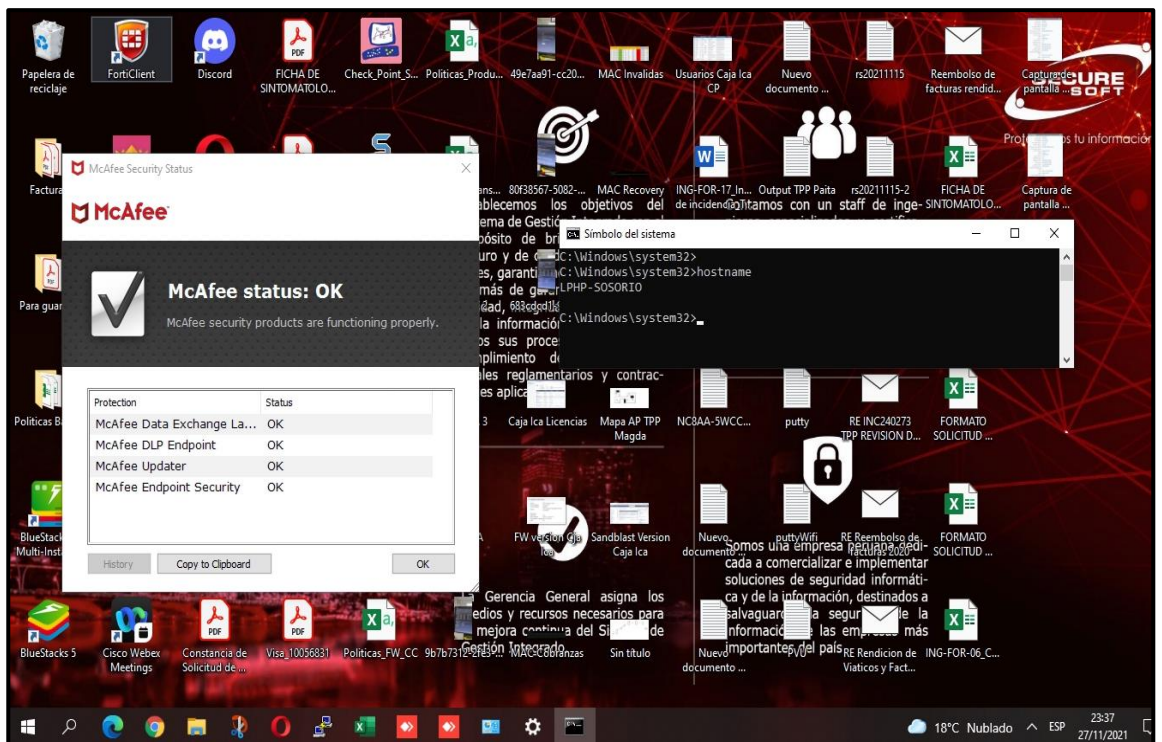
Fuente: Elaboración Propia,2021

Figura 129. Validación de cifrado de disco activo en dispositivo LPHP-SOSORIO



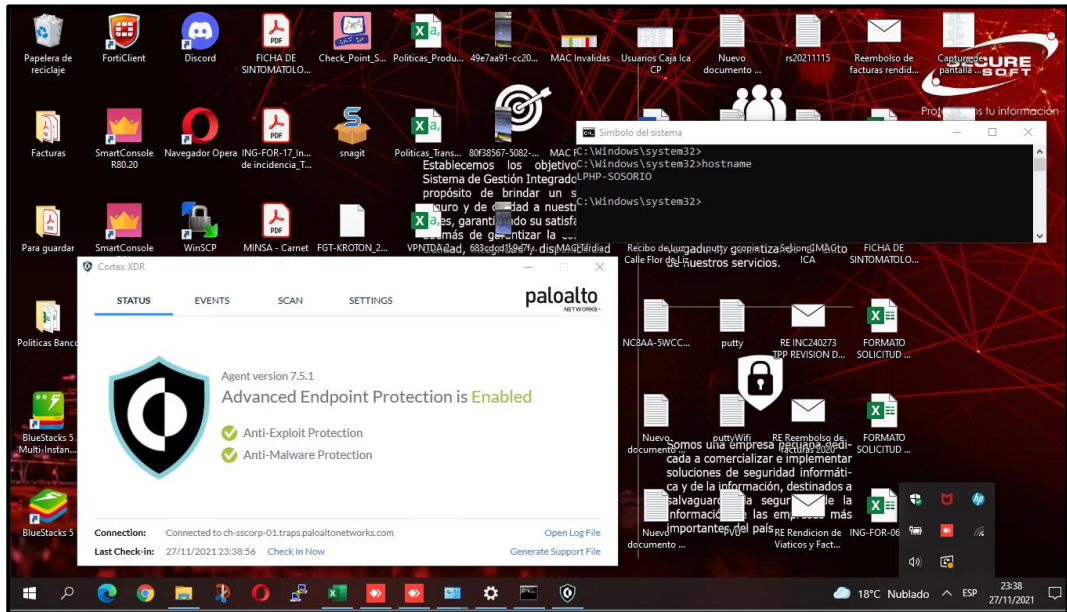
Fuente: Elaboración Propia,2021

Figura 130. Antivirus y DLP instalado correctamente en el dispositivo que utilizará el dispositivo LPHP-SOSORIO



Fuente: Elaboración Propia,2021

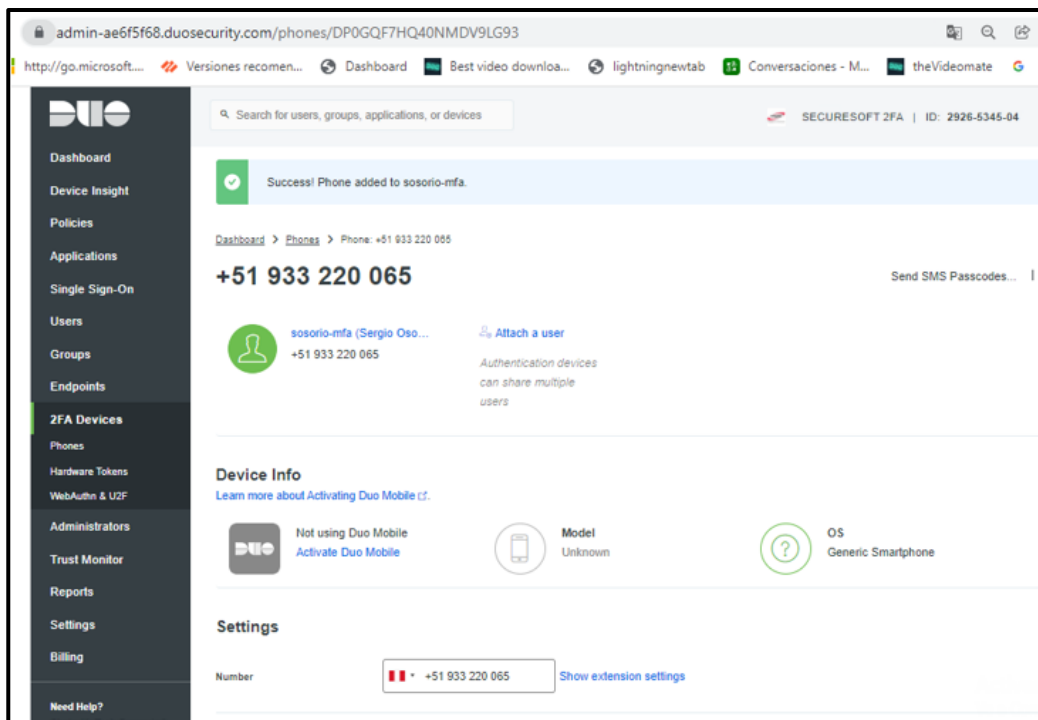
Figura 131. Antimalware instalado correctamente en el dispositivo LPHP-SOSORIO



Fuente: Elaboración Propia,2021

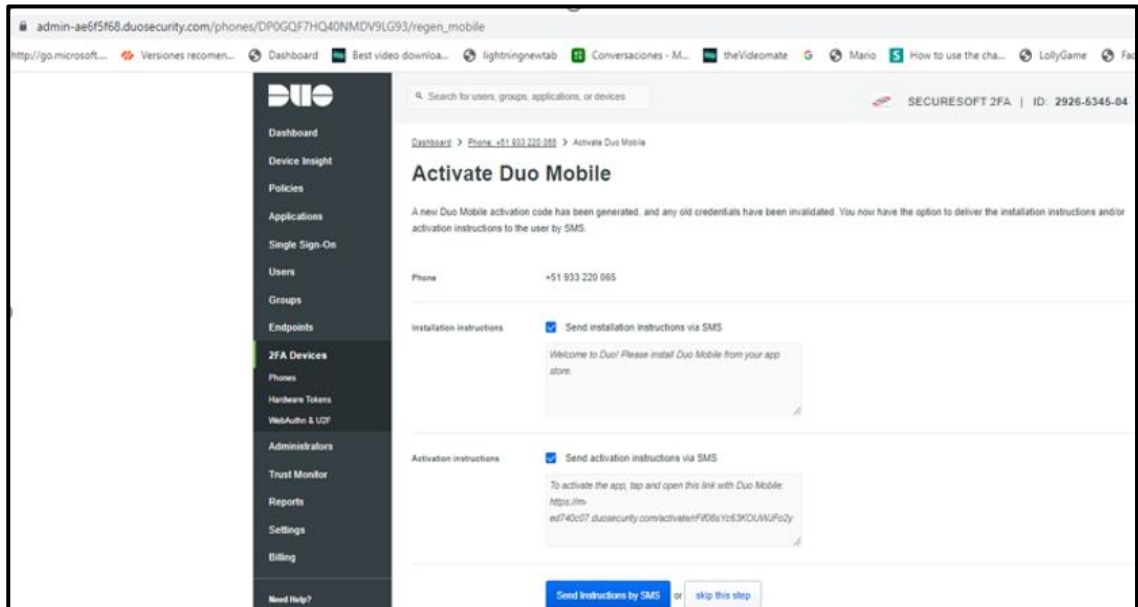
Se evidencia el registro y vinculación del dispositivo móvil con la cuenta de usuario de Active Directory en la plataforma de administración de la solución doble factor de autenticación.

Figura 132. Vinculación de cuenta de usuario en la aplicación Duo Mobile con su dispositivo móvil desde la consola de administración de 2FA.



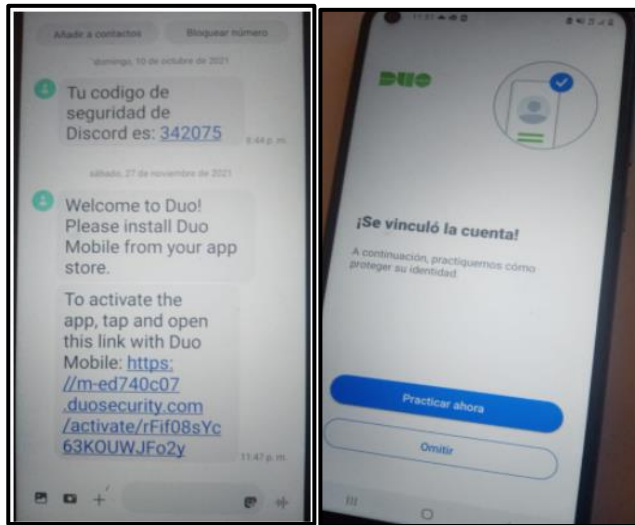
Fuente: Elaboración Propia,2021

Figura 133. Activación desde la consola Duo Doble factor de autenticación hacia el dispositivo móvil a vincular



Fuente: Elaboración Propia,2021

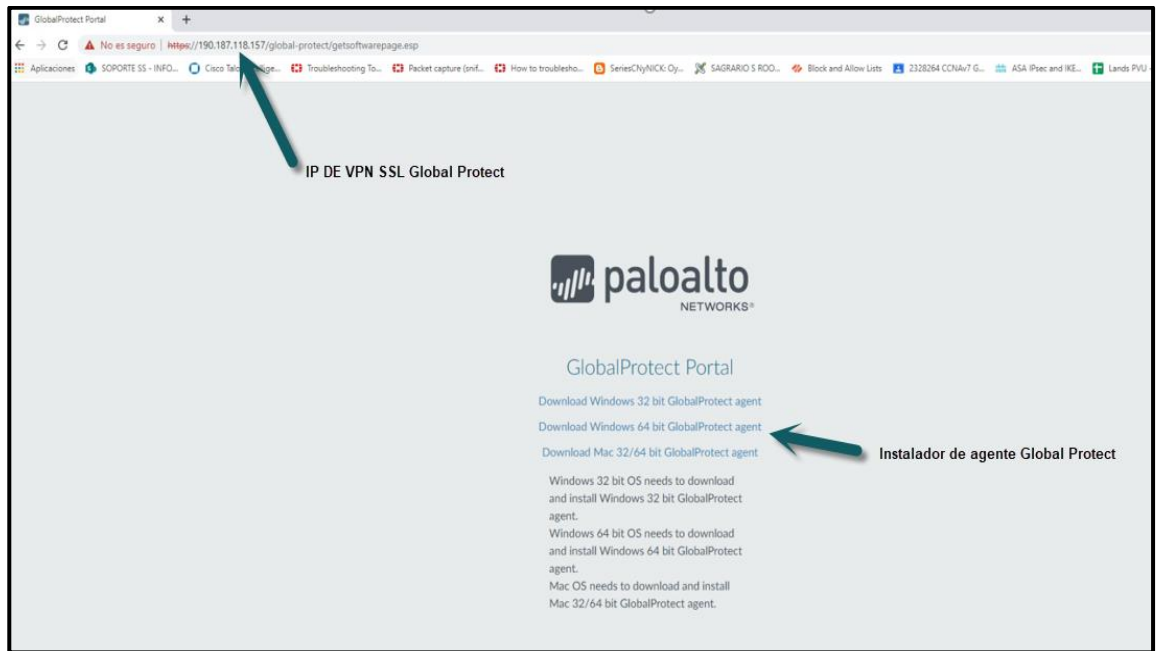
Figura 134. Mensaje validado desde el celular del usuario para su enrolamiento a la consola de administración desde la aplicación Duo Mobile.



Fuente: Elaboración Propia,2021

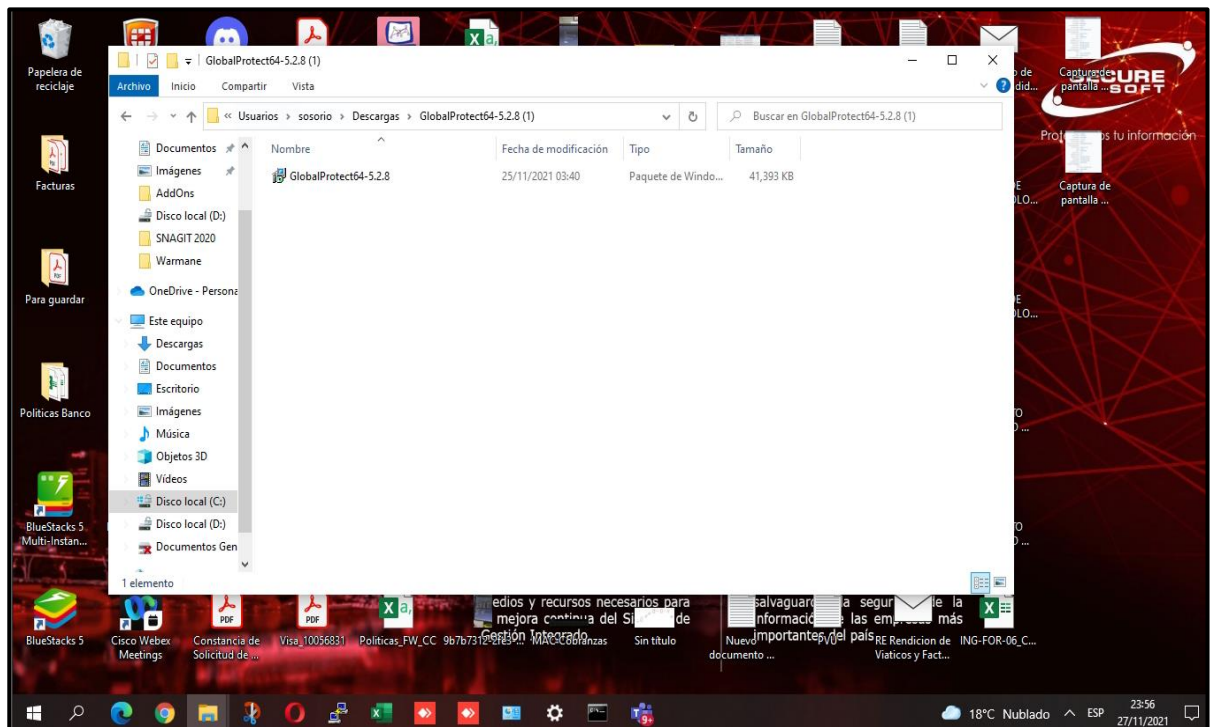
El proceso inicia cuando el usuario Sergio Osorio en su Laptop se conecta vía web a la IP pública 190.187.118.157 la cual es el gateway de la conexión de acceso remoto es gateway resuelve un portal la cual es otro componente del acceso remoto en donde te solicita usuario y contraseña para autenticarte una vez que permite la autenticación se debe descargar la aplicación Global protect de Palo Alto con la cual se instala el agente Global Protect para finalmente autenticarse y se evidencia el mecanismo de doble factor de autenticación y en paralelo se evidencia el acceso con el control de acceso de dispositivo para finalmente establecer exitosamente la conexión remota segura usando una solución nueva implementada con capas de seguridad adicionales que permiten aumentar la seguridad informática.

Figura 135. Instalación de agente Global Protect parte 1



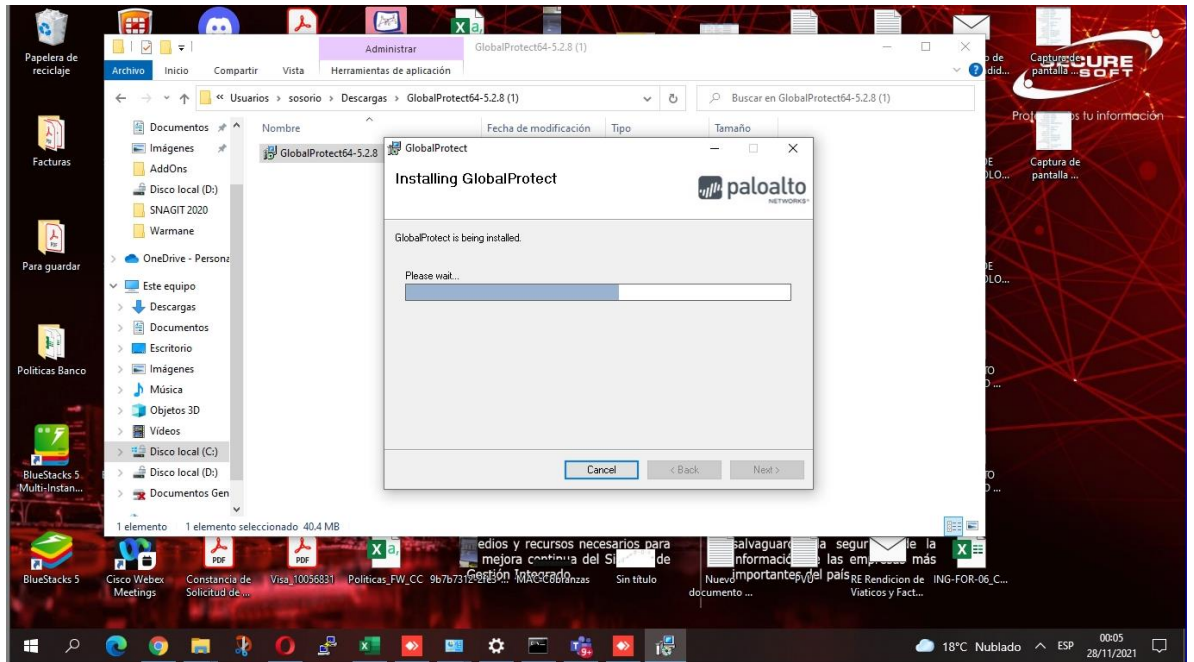
Fuente: Elaboración Propia,2021

Figura 136. Instalación de agente Global Protect parte 2



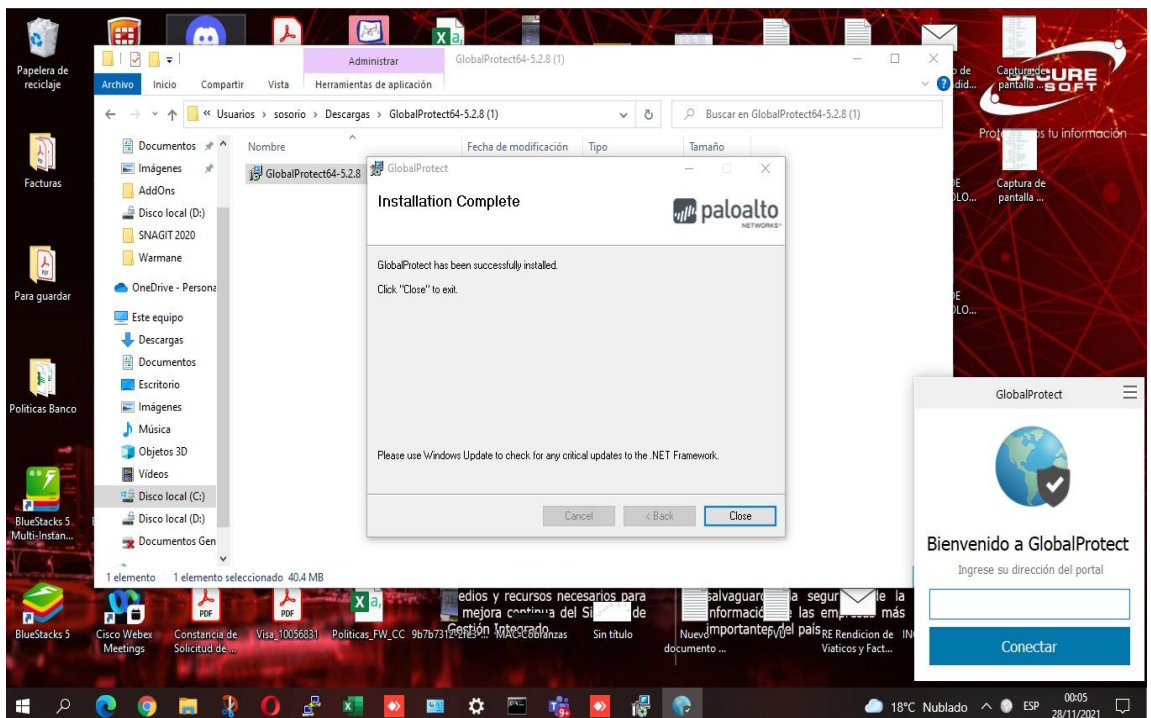
Fuente: Elaboración Propia,2021

Figura 137. Instalación de agente Global Protect parte 3



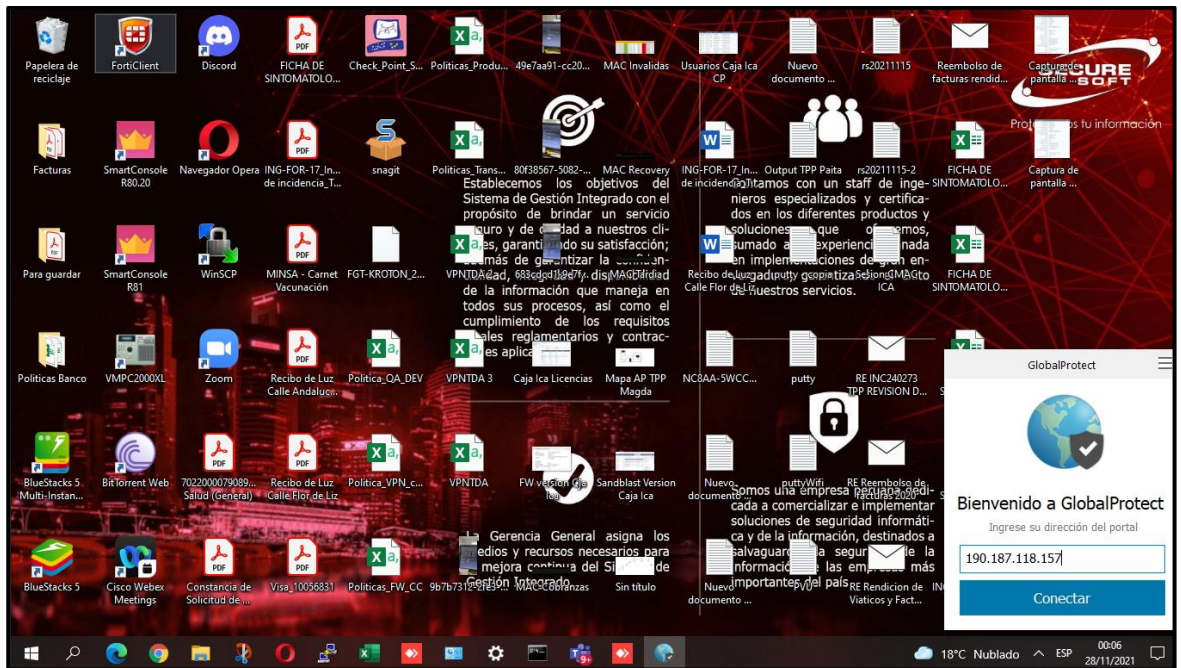
Fuente: Elaboración Propia,2021

Figura 138. Instalación de agente Global Protect VPN SSL finalizada.



Fuente: Elaboración Propia,2021

Figura 139. Configuración de la ip pública VPN SSL para el acceso remoto.



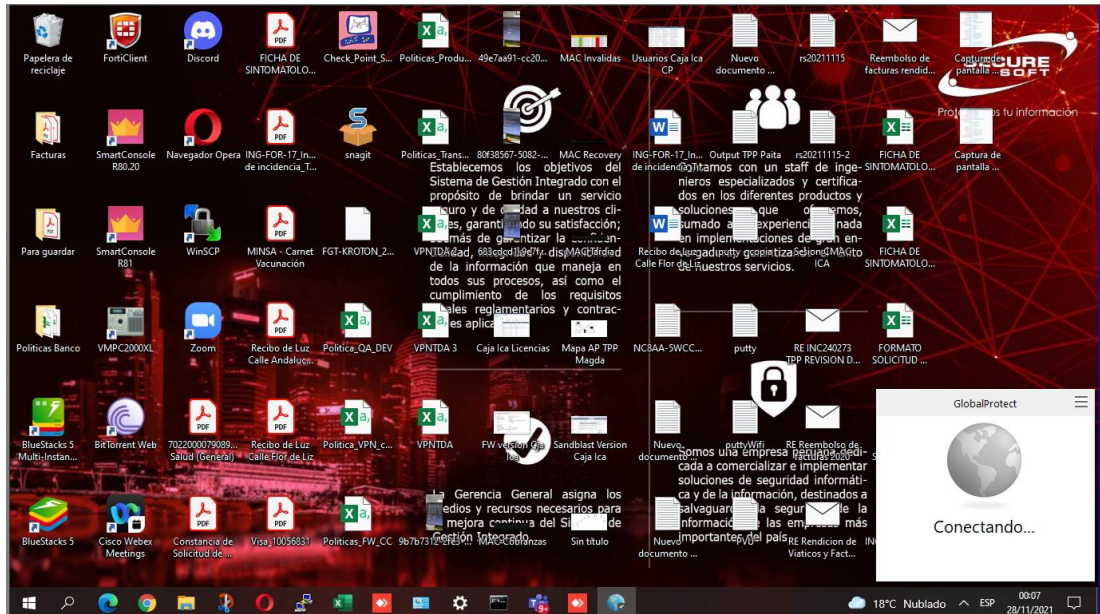
Fuente: Elaboración Propia,2021

Figura 140. Inicio de Sesión de usuario con la conexión remota segura.



Fuente: Elaboración Propia,2021

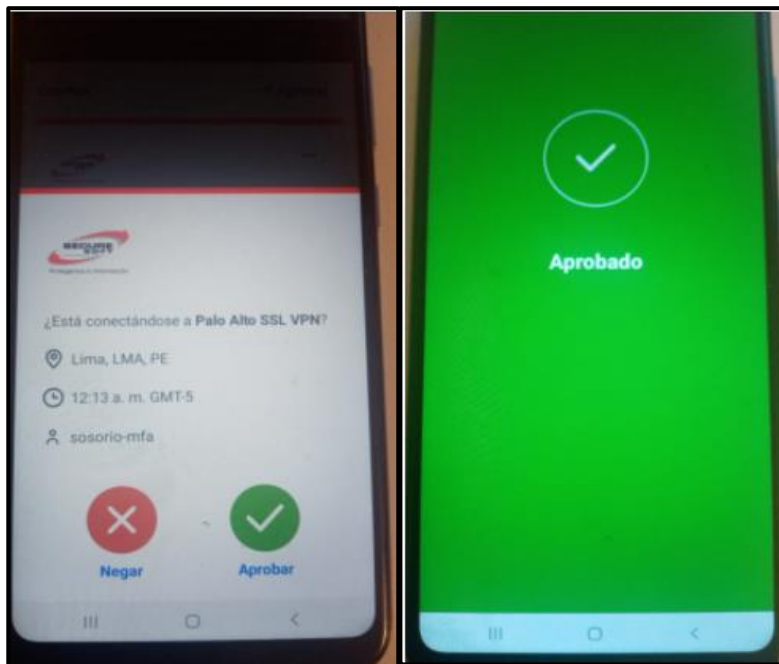
Figura 141. Proceso en curso de la conexión remota segura mediante el agente Global Protect.



Fuente: Elaboración Propia,2021

La evidencia mostrada es el resultado del proceso de doble factor de autenticación al momento de autenticarse con su usuario y password de directorio activo y rápidamente le envía el segundo mecanismo de seguridad el cual es el push del doble factor de autenticación para validación correspondiente de identificación correcta del usuario, se muestra que el usuario responde aceptar la conexión debido a que tiene conocimiento de su propia conexión la cual real y válida.

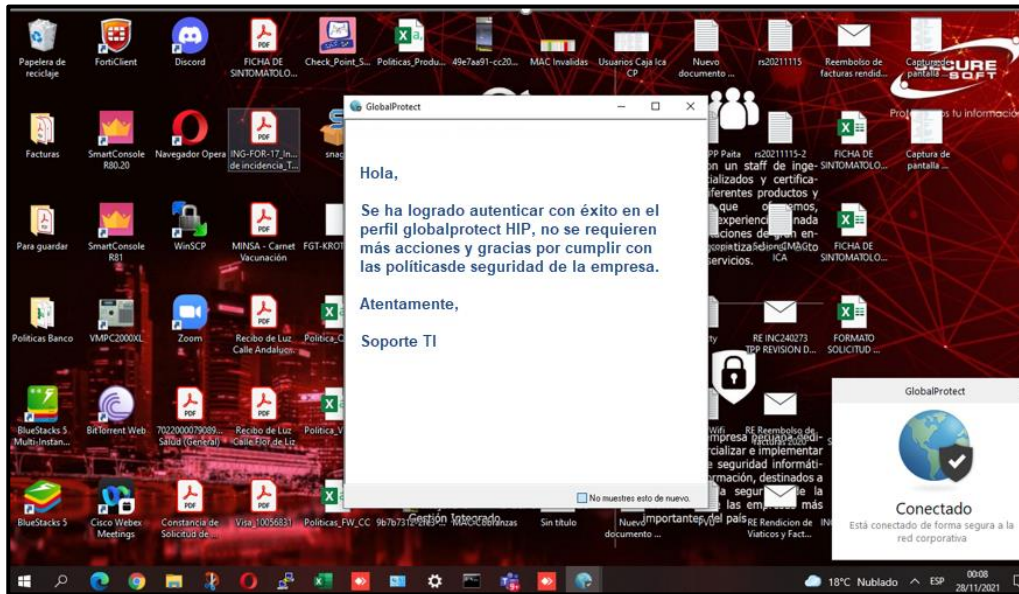
Figura 142. Notificación de autorización de acceso utilizando el 2FA, en donde se valida que es realmente el usuario real el que se conectará.



Fuente: Elaboración Propia,2021

4.1.6. Continuando con el mismo usuario Sergio Osorio (sosorio) muestro el resultado de permitir el acceso utilizando la implementación de control de acceso de dispositivo, debido a que el dispositivo del usuario Sergio Osorio (sosorio-mfa) cumple con los software activos de seguridad informática en un perfil ya definido en conjunto con el cliente la cual es tener instalados y activos el antivirus, antimalware, DLP, cifrado de disco para lograr pasar el control de la solución de control de acceso de dispositivo en donde se le notifica al usuario que la conexión fue exitosa.

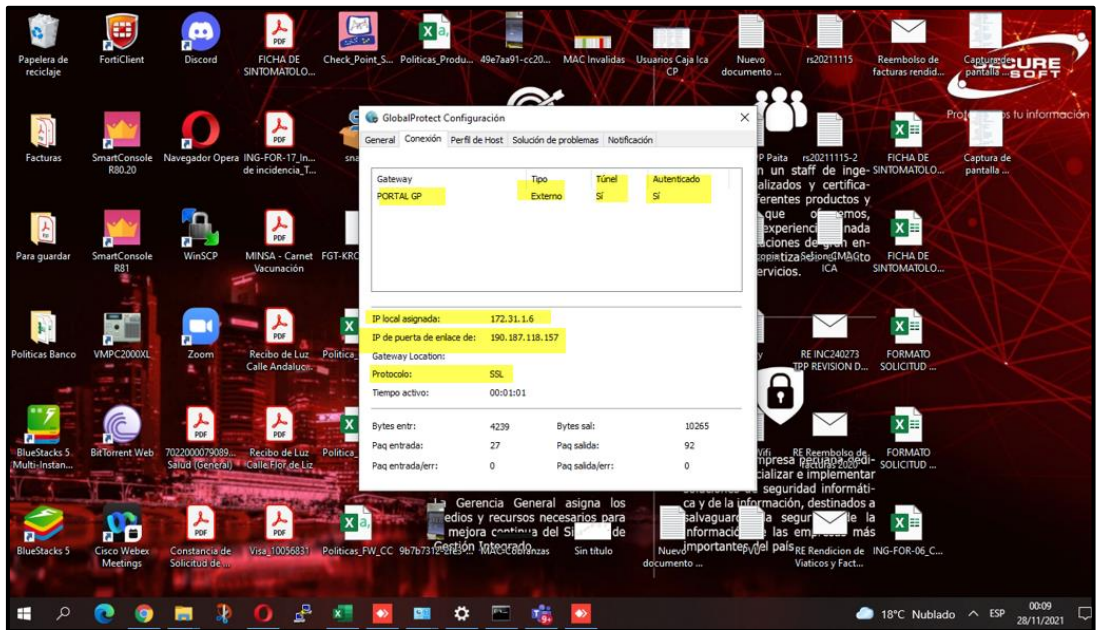
Figura 143. Notificación satisfactoria de control de acceso de dispositivo.



Fuente: Elaboración Propia,2021

A continuación se muestra detalle técnicos adicionales como la ip asignada 172.31.1.6 la cual corresponde al segmento de red asignada para la conexión de acceso remoto, una vez establecida la conexión de acceso remoto usando los controles de la nueva solución implementada, también muestra el gateway 190.187.118.157 a cual está conectado, muestra el protocolo SSL la cual se usa de forma muy segura para la transferencia de hipertexto(web sites), además es un protocolo que te asegura el cifrado de la data la cual garantiza que la información transmitida por la red pública sea muy segura, además muestra el tiempo de actividad del usuario, también los bytes y paquetes enviados/recibidos que te permite saber si está trasladando información muy pesada o ligera.

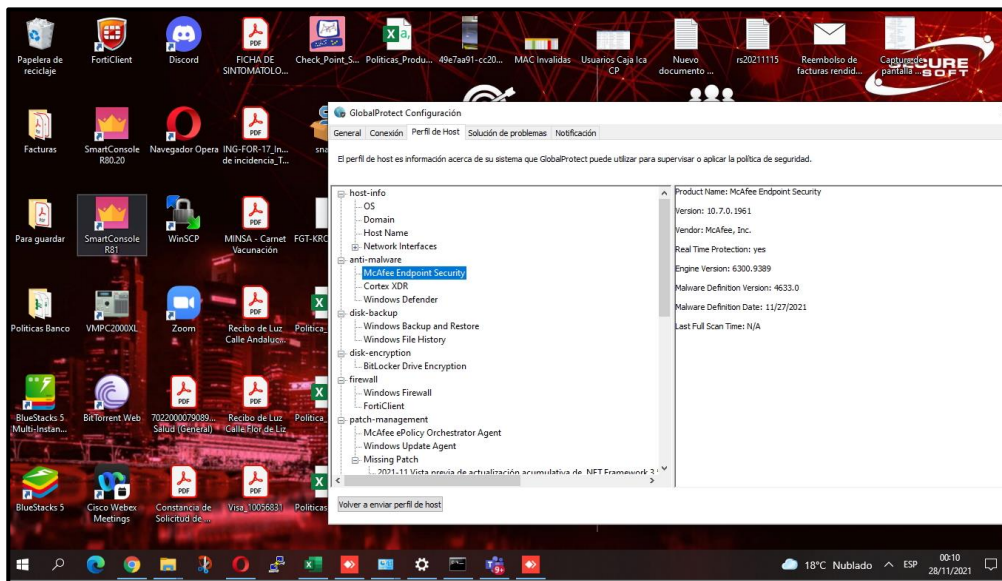
Figura 144. Validación de conexión segura como parámetros de red, Gateway de la solución de acceso remoto, protocolo usando, tiempo de actividad, entre otros.



Fuente: Elaboración Propia,2021

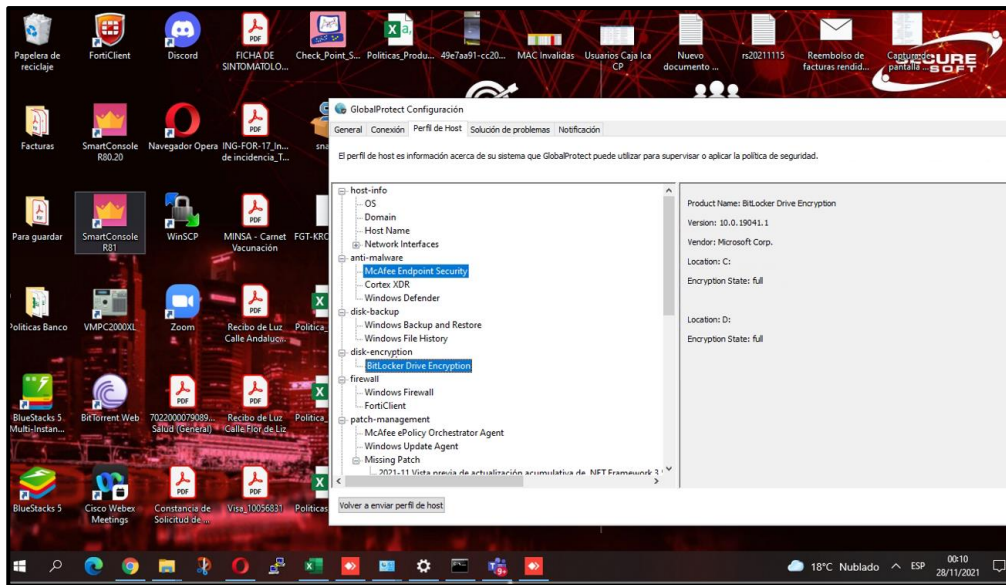
El agente Global Protect el cual es un componente de la conexión remota segura nos permite evidenciar que se logra identificar las características o funciones de protección activas del dispositivo remoto como tener el antimalware activo, saber si se está ejecutando en tiempo real, conocer su versión en ejecución del producto antimalware, saber que fabricante está instalado y también lo mismo para los demás componentes de seguridad activos en los dispositivos remotos.

Figura 145. Antivirus detectado por el agente Global Protect



Fuente: Elaboración Propia,2021

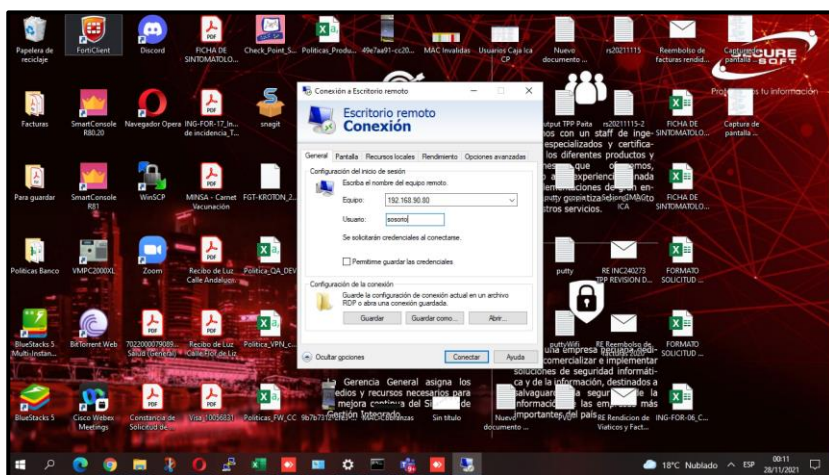
Figura 146. Cifrado de disco detectado por el agente Global Protect



Fuente: Elaboración Propia,2021

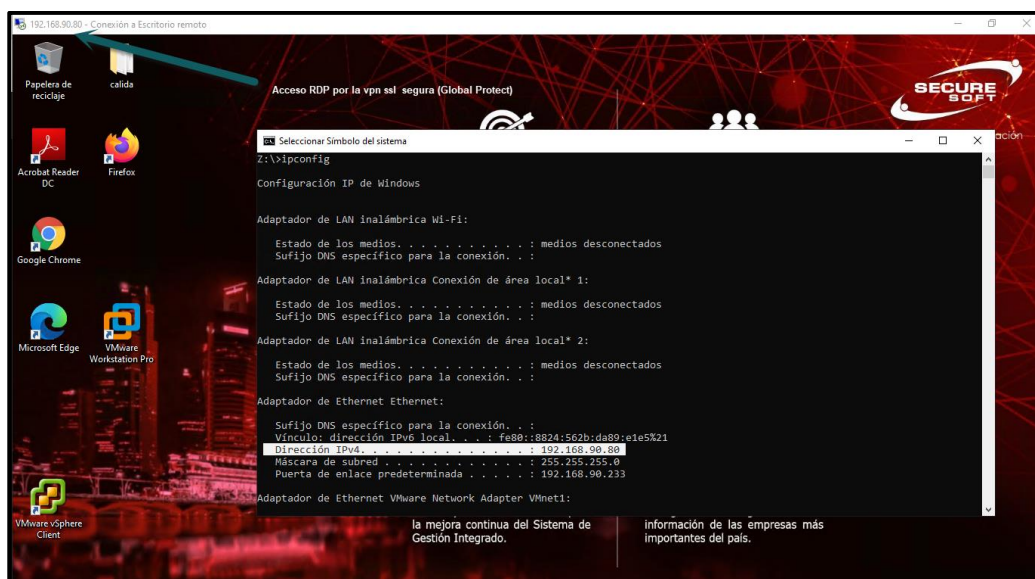
Finalmente, el usuario Sergio Osorio establece conexión de acceso seguro por escritorio remoto usando el puerto TCP 389 hacia una desktop con ip 192.168.90.80 que se encuentra físicamente en la empresa privada la cual es un activo de la empresa privada este acceso está permitido mediante una política del firewall Palo Alto donde se encuentra integrada la nueva solución implementada considerando que previamente tiene que pasar los controles de seguridad de la nueva solución implementada como son el doble factor de autenticación y el control de acceso de dispositivo, los resultados mostrados evidencian un mejoramiento a nivel técnico de los mecanismos de autenticación ya no usando un mecanismo de 1 factor como usuario y contraseña, actualmente se evidencia el uso de dos mecanismo adicionales que usan protocolos de autenticación y cifrado muy robustos que permite estar totalmente tranquilos al usar el acceso remoto.

Figura 147. El acceso remoto seguro hacia el destino 192.168.90.80 (activo local) usando el doble factor de autenticación y el control de acceso de dispositivo.



Fuente: Elaboración Propia,2021

Figura 148. Conectado remotamente al destino 192.168.90.80 (activo local) con acceso remoto seguro



Fuente: Elaboración Propia,2021

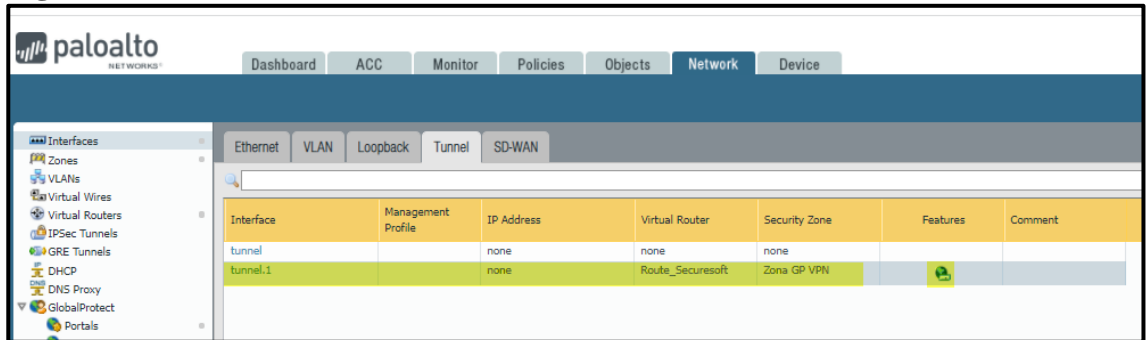
4.1.7. Evidencia de Red y detalles adicionales del Firewall Palo Alto, la cual es el equipo en donde se tiene configurada la VPN SLL (Global Protect) que es un componente de la nueva solución implementada, este componente se integra con el mecanismo de doble factor de autenticación y control de acceso de dispositivo logrando aumentar la seguridad informática, a continuación evidenciamos la interfaz WAN la cual es ethernet 1/9 y tiene configurada la ip 190.187.118.157 y corresponde a la puerta de enlace donde apuntan los usuarios remotos y la interfaz DMZ la cual es ethernet 1/5 con ip 192.168.25.16 correspondiente a la red interna de la empresa privada.

Figura 149. Interfaz Wan (Pública) y Dmz (Interna) en el firewall Palo Alto.

Interface	Interface Type	Management Profile	Link State	IP Address	MAC Address	Virtual Router	Security Zone	Features	Comment
ethernet1/1			none			none	none		
ethernet1/2			none			none	none		
ethernet1/3			none			none	none		
ethernet1/4			none			none	none		
ethernet1/5	Layer3	Mgmt_DMZ	up	192.168.25.16/24	d4:1d:71:8b:3f:14	Route_Securesoft	Zona DMZ		Interface DMZ
ethernet1/6			none			none	none		
ethernet1/7			none			none	none		
ethernet1/8			none			none	none		
ethernet1/9	Layer3	WAN	up	190.187.118.157/28	d4:1d:71:8b:3f:18	Route_Securesoft	Zona WAN		Interface WAN
ethernet1/10			none			none	none		

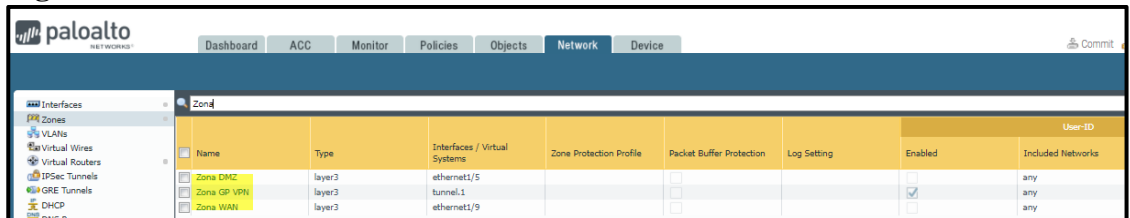
Fuente: Elaboración Propia,2021

Figura 150. Interfaz Túnel de la VPN SSL en el firewall Palo Alto.



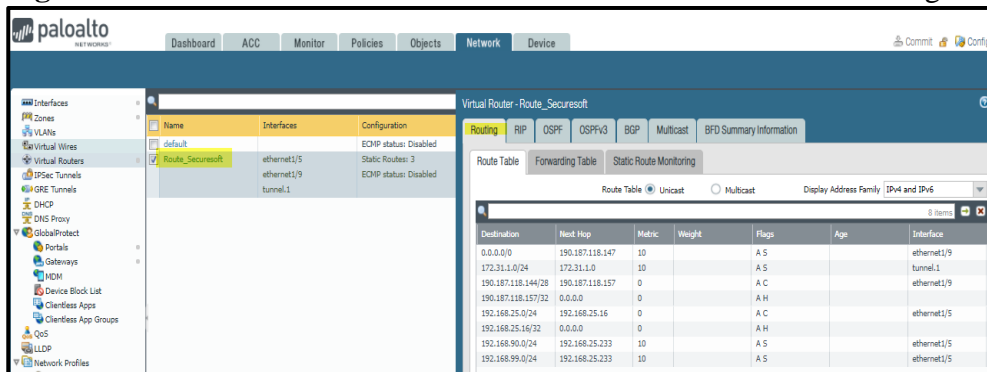
Fuente: Elaboración Propia,2021

Figura 151. Zonas asociadas a las interfaces del firewall Palo Alto.



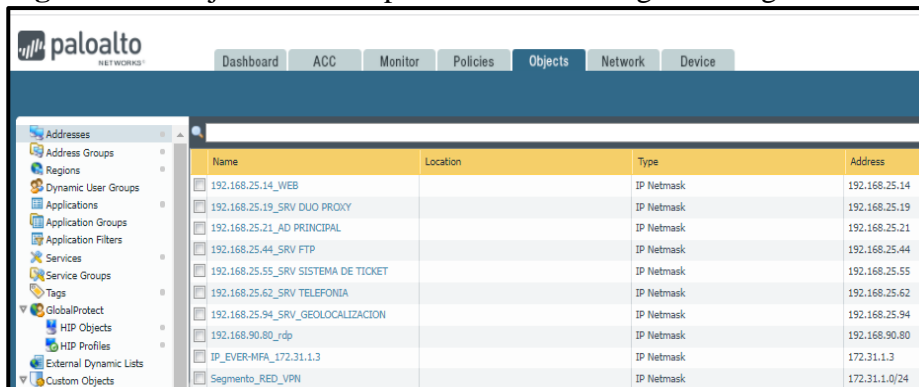
Fuente: Elaboración Propia,2021

Figura 152. Tabla de rutas donde se encuentran las rutas estáticas configuradas.



Fuente: Elaboración Propia,2021

Figura 153. Objetos creados para el uso de las reglas de seguridad.



Fuente: Elaboración Propia,2021

4.1.8. Encuesta de tres usuarios que utilizan la nueva solución implementada para validar conformidad sobre su uso.

Figura 154. Resultado de encuesta usuario1 (Carlos Chacchi)

Encuesta sobre Implementación de una solución remota con doble factor de autenticación y control de acceso de dispositivo para incrementar la seguridad informática en la empresa privada.

1 ¿Ha presentado en la actualidad algún problema de conexión con el acceso remoto con la nueva implementación realizada con el agente Global Protect?
Hasta el momento la nueva solución implementada está funcionando correctamente


2 ¿Considera que actualmente aumentó el nivel de seguridad en su acceso remoto con la implementación de la nueva solución en donde se agregaron dos capas de seguridad una de autorización de doble factor desde la aplicación móvil y la otra usar las funciones de seguridad operativas como por ejemplo antivirus?
Agregar dos capas adicionales al acceso remoto considero que nos permite aumentar el nivel de seguridad informática en la empresa.

3 ¿Considera que es importante aumentar la protección a nivel de seguridad informática para salvaguardar la información tanto de la compañía y personal?
Son sumamente importante para evitar grandes pérdidas ya sea de activos o de información

4 ¿Cuántos controles de seguridad tiene actualmente para la autenticación remota?
Son 2 controles , ingresando contraseña y autorizando por la aplicación duo móvil

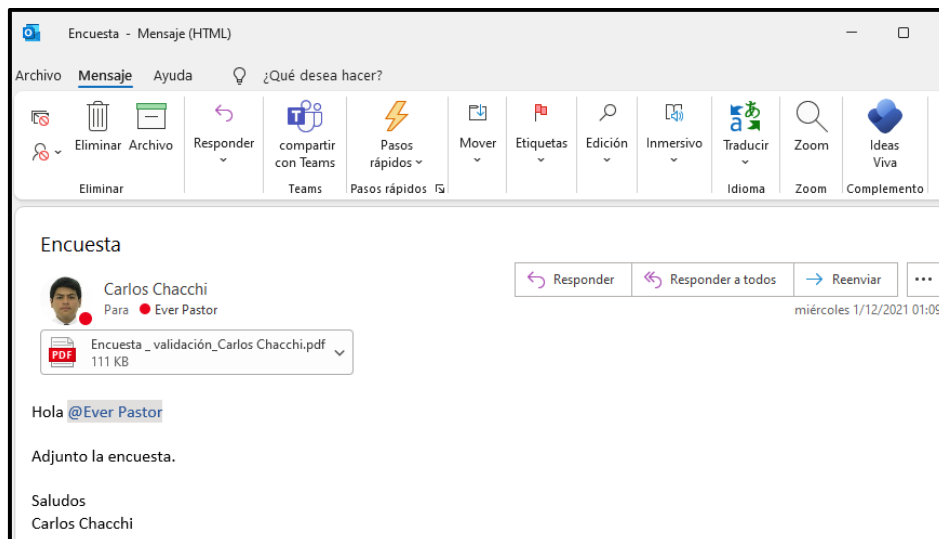
5 ¿En la actualidad cree usted que es necesaria tener su antivirus y antimalware activo y actualizado?
Considero que si es necesaria en la actualidad con tantas variantes de malware existentes es necesario tener antivirus y antimalware.

6 ¿Se siente más protegido con la nueva solución implementada de conexión remota segura?
Si ya que me permite asegurarme que realmente sea mi persona quien realiza la conexión remota.


Nombre Completo: Carlos Arturo Chacchi Niño
DNI: 71732894

Fuente: Elaboración Propia,2021

Figura 155. Evidencia de encuesta usuario1 (Carlos Chacchi)



Fuente: Elaboración Propia,2021

Figura 156. Resultado de encuesta usuario2 (Jean Vargas)

Encuesta sobre Implementación de una solución remota con doble factor de autenticación y control de acceso de dispositivo para incrementar la seguridad informática en la empresa privada.

1 ¿Ha presentado en la actualidad algún problema de conexión con el acceso remoto con la nueva implementación realizada con el agente Global Protect?
No he tenido ningún problema en utilizarla

2 ¿Considera que actualmente aumentó el nivel de seguridad en su acceso remoto con la implementación de la nueva solución en donde se agregaron dos capas de seguridad una de autorización de doble factor desde la aplicación móvil y la otra usar las funciones de seguridad operativas como por ejemplo antivirus?
Con los nuevos mecanismos de acceso implementado considero que actualmente la empresa si aumentó su nivel de seguridad.


3 ¿Considera que es importante aumentar la protección a nivel de seguridad informática para salvaguardar la información tanto de la compañía y personal?
Siempre agregar más controles a nivel de seguridad es muy importante ya que nos permite estar más tranquilos al momento de trabajar remotamente.

4 ¿Cuántos controles de seguridad tiene actualmente para la autenticación remota?
Para la autenticación tenemos 2 controles y considero que son muy importantes.

5 ¿En la actualidad cree usted que es necesaria tener su antivirus y antimalware activo y actualizado?
Si es necesaria para protección de nuestros dispositivos.

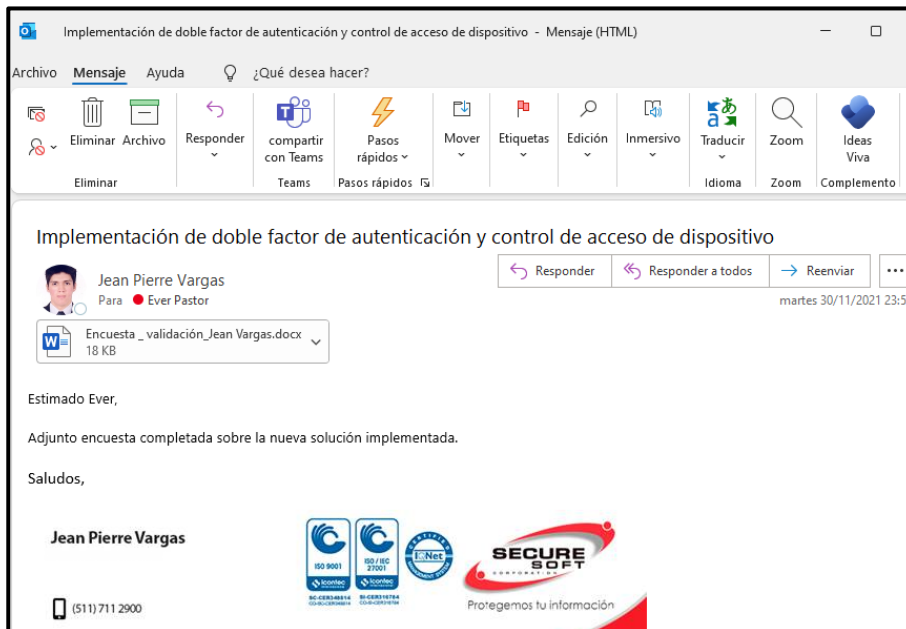
6 ¿Se siente más protegido con la nueva solución implementada de conexión remota segura?
Definitivamente si debido a que estos controles que implementaron me ayudan a estar protegidos cuando me encuentre trabajando.

Nombre colaborador: Jean Vargas
Área al que pertenece: Soporte

Firma: 

Fuente: Elaboración Propia,2021

Figura 157. Evidencia de encuesta usuario2 (Jean Vargas)



Fuente: Elaboración Propia,2021

Figura 158. Resultado de encuesta usuario3 (Sergio Osorio)

Encuesta sobre Implementación de una solución remota con doble factor de autenticación y control de acceso de dispositivo para incrementar la seguridad informática en la empresa privada.

1 ¿Ha presentado en la actualidad algún problema de conexión con el acceso remoto con la nueva implementación realizada con el agente Global Protect?
No por el momento no he tenido problemas, la nueva solución está funcionando correctamente.

2 ¿Considera que actualmente aumentó el nivel de seguridad en su acceso remoto con la implementación de la nueva solución en donde se agregaron dos capas de seguridad una de autorización de doble factor desde la aplicación móvil y la otra usar las funciones de seguridad operativas como por ejemplo antivirus?
Si me parece importante que se tenga más control debido a que hay muchas amenazas en la red con ello considero que si aumentó el nivel de seguridad


3 ¿Considera que es importante aumentar la protección a nivel de seguridad informática para salvaguardar la información tanto de la compañía y personal?
Si es muy importante proteger nuestra información y de la empresa para evitar que nos roben mi información sensible.

4 ¿Cuántos controles de seguridad tiene actualmente para la autenticación remota?
Hasta donde me he percatado son 2 el acceso de contraseña, luego el push del doble factor.

5 ¿En la actualidad cree usted que es necesaria tener su antivirus y antimalware activo y actualizado?
Si considero que es muy importante para proteger nuestra información.

6 ¿Se siente más protegido con la nueva solución implementada de conexión remota segura?
Pienso que sí debido a que mientras tenga más controles de seguridad siento que estaré bien protegido.

Nombre colaborador: __Sergio Osorio__
Área al que pertenece: __Contabilidad__



Firma: _____

Fuente: Elaboración Propia,2021

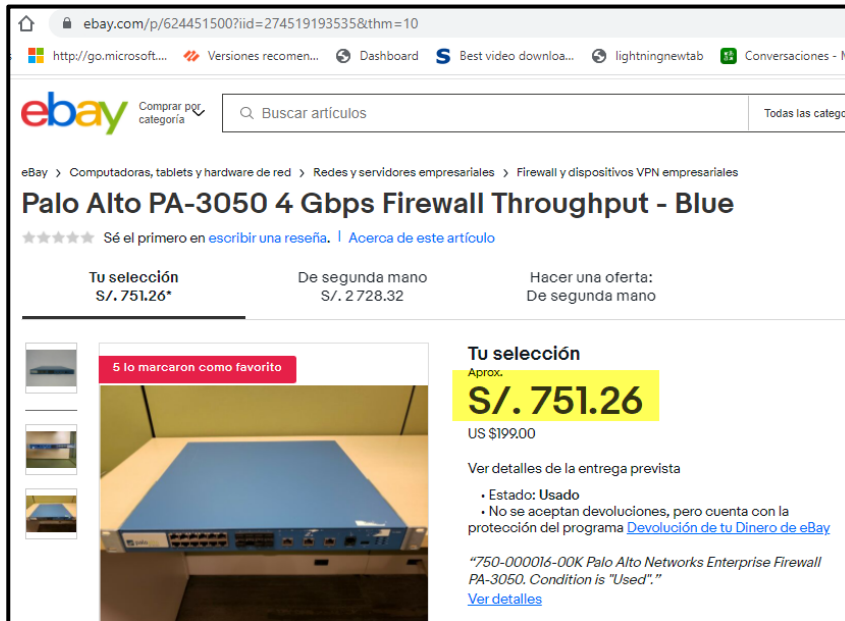
Figura 159. Evidencia de encuesta usuario3 (Sergio Osorio)



Fuente: Elaboración Propia,2021

4.1.9. Se evidencia que la reutilización de un firewall Palo Alto el cual se encontraba en el almacén de la empresa Privada ayudó con un ahorro en compra de equipamiento debido a la fuente EBay se valida que el precio del equipo usado es de 751.26 nuevos soles, pero debemos considerar que es el precio de un equipo usado y con este dato se estima un precio de 1500 nuevos soles un equipamiento nuevo la cual ayuda en ahorrar en gastos por compra de equipos de seguridad.

Figura 160. Precio de equipo Firewall Palo Alto 3050.



Fuente: Ebay,2021

Figura 161. Equipo Firewall Palo Alto 3050 en almacén.



Fuente: Elaboración Propia,2021

Figura 162. Equipo Firewall Palo Alto 3050 en instalado, implementado y en operación



Fuente: Elaboración Propia,2021

4.1.10. En el aspecto económico la nueva implementación de la solución de doble factor de autenticación y control de acceso de dispositivo aportó en mantener los proyectos existentes y nuevos proyectos que se tiene con cada cliente debido a que la nueva solución implementada brinda estabilidad en la conexión y acceso la cual brinda aumento en la seguridad informática para la protección de la información de los clientes y colaboradores esto permite brindar a la empresa privada estabilidad y seguridad y sobre todo mantener y aumentar el crecimiento económico de la empresa privada así como también mantener su buena reputación sobre el mercado tecnológico.

Figura 163. Proyectos tecnológicos de renovación con clientes

Nombre	Tipo
[PRO-R-20-087-2017]- Renovación tecnológica IPS - MACFEE	Carpeta de archivos
[PRO-R-20-219-2159]- Miqración servicio Forcepoint Web a Nube	Carpeta de archivos
[PRO-R-21-004-2221] Renovación licenciamiento antispam	Carpeta de archivos
[PRO-R-21-007-2219] Renovación de soporte de firewall CheckPoint	Carpeta de archivos
[PRO-R-21-009-2224] Renovaciones de Licencias y tecnológico	Carpeta de archivos
[PRO-R-21-011-2232]Renovación de licenciamiento Forcepoint web security	Carpeta de archivos
[PRO-R-21-017-2235] Renovación de soporte CES & AMP	Carpeta de archivos
[PRO-R-21-040-2256] Renovación soporte de Disk Encryption - McAfee	Carpeta de archivos
[PRO-R-21-047-2267] Renovación de Soporte DLP	Carpeta de archivos
[PRO-R-21-078-2301] Renovación de 125 Softtokens	Carpeta de archivos
[PRO-R-21-102-2323]]Renovacion de 40 softtokens	Carpeta de archivos
[PRO-R-21-168-2397] Renovación Hardware SecureID - 5to año	Carpeta de archivos
[PRO-R-21-202-2431]-Renovación de 50 licencias Pulse Secure	Carpeta de archivos

Fuente: Elaboración Propia,2021

Figura 164. Proyectos tecnológicos de ampliación de servicio de clientes.

Nombre	Tipo
[PRO-A-21-002-2217] Ampliación de servicio Cybersoc	Carpeta de archivos
[PRO-A-21-025-2242] Toma de gestión de solución antivirus - ePo	Carpeta de archivos
[PRO-A-21-079-2302] Adquisicion 50 semillas y softtokens RSA	Carpeta de archivos
[PRO-A-21-134-2362] Ampliación de servicio Cybersoc	Carpeta de archivos
[PRO-A-21-197-2423] Adquisición de 700 licenciamiento de Patch Management - Qualys	Carpeta de archivos

Fuente: Elaboración Propia,2021

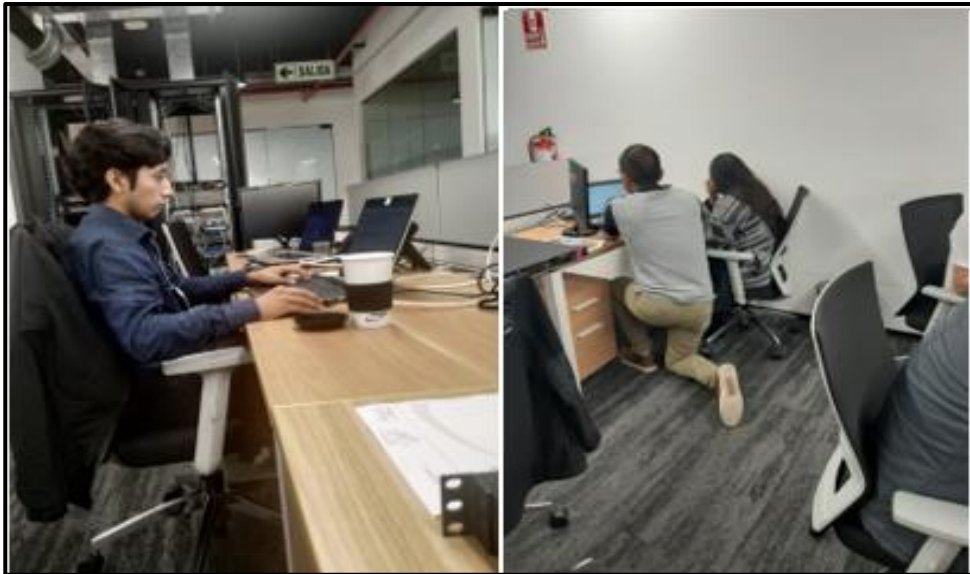
Figura 165. Nuevos proyectos tecnológicos de nuevos clientes.

Nombre	Fecha de modificac
[GTD CHILE][PRO-N-21-055-2274] Implementación de solución de Gestión de Accesos Privilegiados (PAM) CyberArk]	26/08/2021 10:04
[PRO-N-19-210-1912-1913]]Implementación de MFA - RSA	29/05/2021 09:28
[PRO-N-20-204-2149]Implementación VPN SSL	29/05/2021 05:15
[PRO-N-20-267-2198] Implementación AntiDDoS Onpremise	25/08/2021 15:01
[PRO-N-21-008-2223]Servicios Plataformas de Seguridad	29/05/2021 05:09
[PRO-N-21-042-2261] Adquisición de 3000 tokens	24/08/2021 09:31
[PRO-N-21-073-2293]]Upgrade de la solución Mvision protect Standard y DLP	24/08/2021 08:24

Fuente: Elaboración Propia,2021

4.1.11. Se evidencia un ahorro en el uso de la infraestructura (gasto en agua, luz, internet, sanitarios, entre otros) de parte de los colaboradores debido a que la nueva solución implementada permite brindar estabilidad de la operación al remoto y mejora la seguridad de acceso remoto de todos los colaboradores para que puedan emplear el teletrabajo durante toda la pandemia la cual ayuda a cada colaborador a disminuir el riesgo de contagio y permite un ahorro económico tanto para la empresa privada y el colaborador como por ejemplo el transporte, alimentación.

Figura 166. Trabajo antes de pandemia covid-19



Fuente: Elaboración Propia,2021

Figura 167. La infraestructura sin deteriorarse, sin personal en sitio.



Fuente: Elaboración Propia,2021

Figura 168. Trabajo al remoto usando la nueva implementación de forma segura



Fuente: Elaboración Propia,2021

4.1.12. El beneficio del método usado por la nueva implementación del doble factor de autenticación es evidenciado y garantizado por el mismo Google la cual menciona que en Octubre del 2021 activó el doble factor de autenticación de forma automática a 150 millones de cuentas cuyo objetivo fue minimizar el éxito de los ataques que tienen como finalidad comprometer cuentas, luego obtiene como resultado y aseguró que se redujo a 50% el compromiso de cuentas en comparación a las cuentas que no tienen el mecanismo mencionado, con lo mencionado se evidencia que la implementación aumenta la seguridad informática para cualquier empresa privada debido a que es un mecanismo de seguridad totalmente comprobado.

Figura 169. Noticia sobre la activación automática del doble factor a cuentas de Google.



Con la verificación en dos pasos, Google asegura haber asestado un gran golpe contra la ciberdelincuencia que afecta a sus usuarios. (Foto: Google)

Fuente: El comercio,2021

4.1.13. A continuación, muestro la velocidad de gestión de la información utilizando la conexión de acceso remoto, también la latencia, antes y después de la implementación realizada como resultado muestra un mejoramiento en la velocidad de transmisión de la información disminución de la latencia después de la implementación.

Velocidad de gestión de información antes de la ejecución del Proyecto:

Interfaz WAN por donde se negociaban las conexiones VPN SSL.

Figura 170. Detalle 01 de interfaz WAN de firewall Check Point

```
eth7      Link encap:Ethernet  HWaddr 00:0A:F7:9B:8F:CF
          inet addr:190.187.118.148  Bcast:190.187.118.159  Mask:255.255.255.240
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7058106595  errors:1598  dropped:0  overruns:0  frame:0
          TX packets:4878857883  errors:1575  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:1000
          RX bytes:486426317170 (453.0 GiB)  TX bytes:83629396955 (77.8 GiB)
          Interrupt:64
```

Fuente: Elaboración Propia,2021

Figura 171. Detalle 02 de interfaz WAN de firewall Check Point

Name	Type	IPv4 Address	Subnet Mask	Link Speed	IPv6 Address	IPv6 Mask Length	Link Status
eth7	Ethernet	190.187.118.148	255.255.255.240	1000 Mbps	-	-	Up
lo	Loopback	127.0.0.1	255.0.0.0	N/A	-	-	Up

Fuente: Elaboración Propia,2021

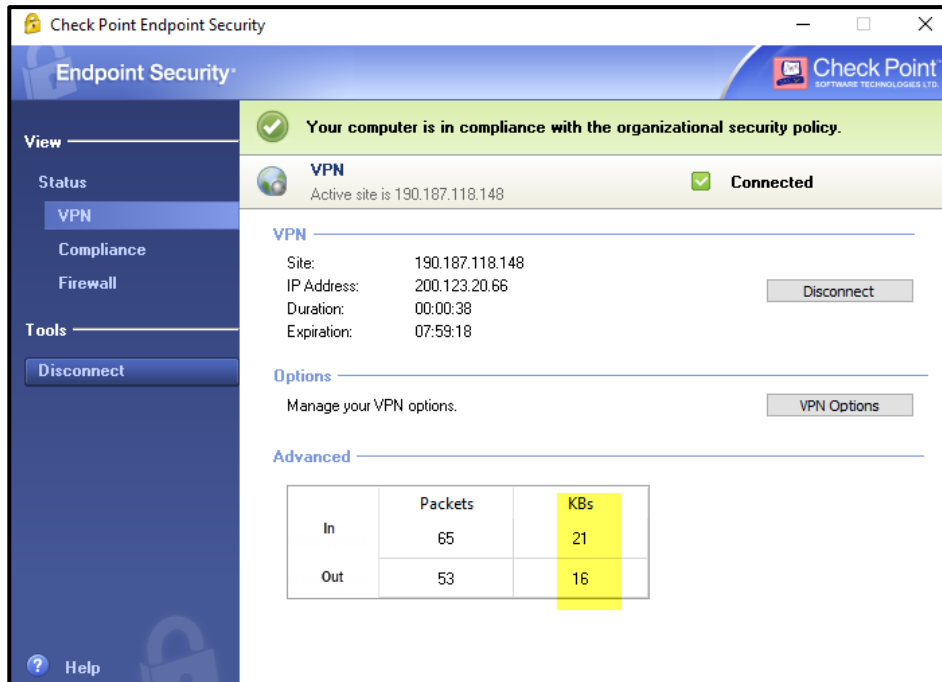
Figura 172. Detalle de velocidad de negociación de la interfaz WAN de firewall Check Point

```
[Expert@SS:0]# ethtool eth7
Settings for eth7:
    Supported ports: [ TP ]
    Supported link modes:   10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Half 1000baseT/Full
    Supported pause frame use: No
    Supports auto-negotiation: Yes
    Supported FEC modes: Not reported
    Advertised link modes:  10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Half 1000baseT/Full
    Advertised pause frame use: No
    Advertised auto-negotiation: Yes
    Advertised FEC modes: Not reported
    Link partner advertised link modes:  10baseT/Half 10baseT/Full
                                         100baseT/Half 100baseT/Full
                                         1000baseT/Full
    Link partner advertised pause frame use: No
    Link partner advertised auto-negotiation: Yes
    Link partner advertised FEC modes: Not reported
    Speed: 1000Mb/s
    Duplex: Full
    Port: Twisted Pair
    PHYAD: 4
    Transceiver: internal
    Auto-negotiation: on
    MDI-X: on
    Supports Wake-on: g
    Wake-on: d
    Current message level: 0x000000ff (255)
                           drv probe link timer ifdown ifup rx_err tx_err
    Link detected: yes
```

Fuente: Elaboración Propia,2021

Velocidad de gestión de información, de entrada 21 KBs y de salida 16 KBs

Figura 173. Detalle de velocidad de gestión de información antes del proyecto



Fuente: Elaboración Propia,2021

Velocidad de gestión de información después de la ejecución del Proyecto:

Interfaz WAN por donde se negociaban las conexiones VPN SSL.

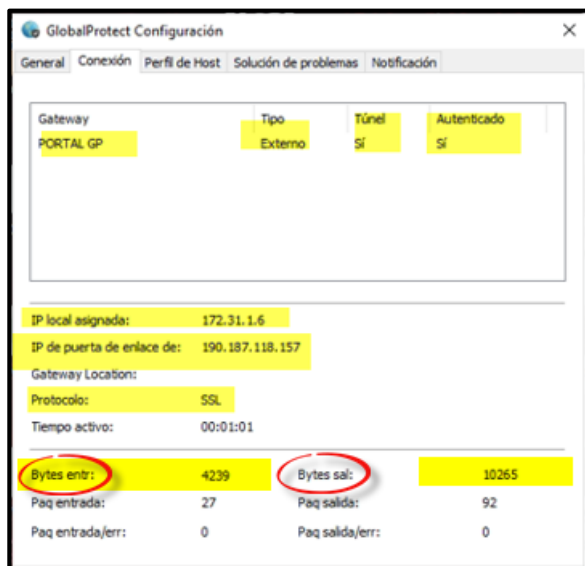
Figura 174. Detalle de velocidad de negociación de la interfaz WAN de firewall Palo Alto

```
Name: ethernet1/9, ID: 132, 802.lq tag: 200
Operation mode: layer3
Virtual router R1
Interface MTU 1500
Interface IP address: 190.187.118.157/28
Interface management profile: PING
  ping: yes telnet: no ssh: no http: no https: no
  snmp: no response-pages: no userid-service: no
Service configured: IKE SSL-VPN
Link status:
  Runtime link speed/duplex/state: 1000/full/up
  Configured link speed/duplex/state: auto/auto/auto
-----
Logical interface counters read from CPU:
-----
bytes received          5452381541463
bytes transmitted      5422336337
packets received       2969714205
packets transmitted    14118106
receive errors         0
packets dropped        8555151
packets dropped by flow state check 1112
forwarding errors      0
no route               0
arp not found          781436
neighbor not found     0
neighbor info pending  0
mac not found          0
packets routed to different zone 3823
land attacks           0
ping-of-death attacks  0
teardrop attacks       2
ip spoof attacks       0
mac spoof attacks      0
ICMP fragment         0
layer2 encapsulated packets 0
layer2 decapsulated packets 0
tcp cps                0
udp cps                0
sctp cps               0
other cps              0
```

Fuente: Elaboración Propia,2021

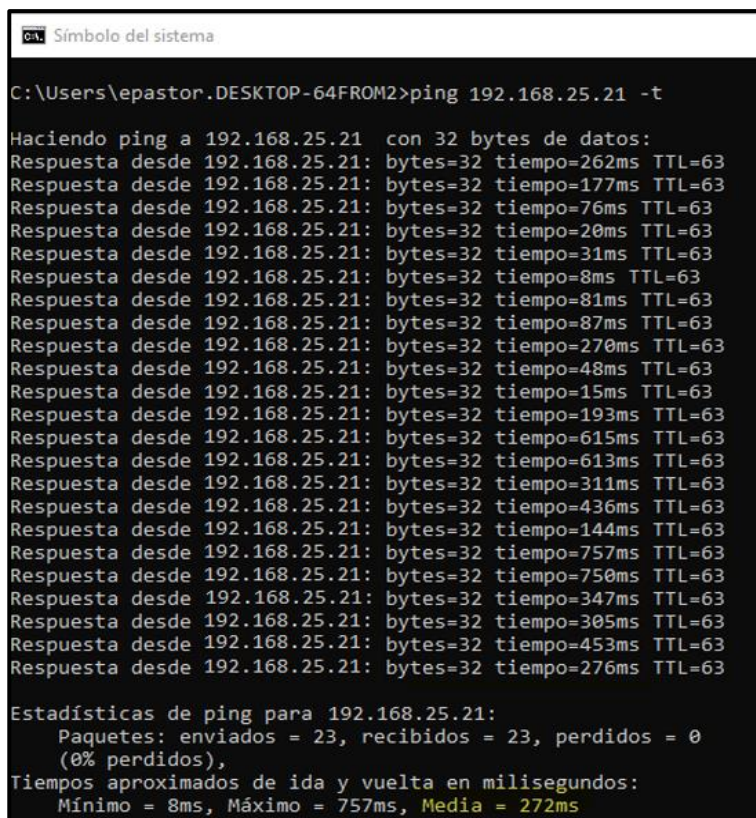
Velocidad de gestión de información, de entrada 4239 Bytes equivalentes a 4.14 KBs y de salida 10265 Bytes equivalentes a 10 KBs donde se muestra una mejora en la velocidad de transmisión.

Figura 175. Detalle de velocidad de gestión de información después del proyecto.



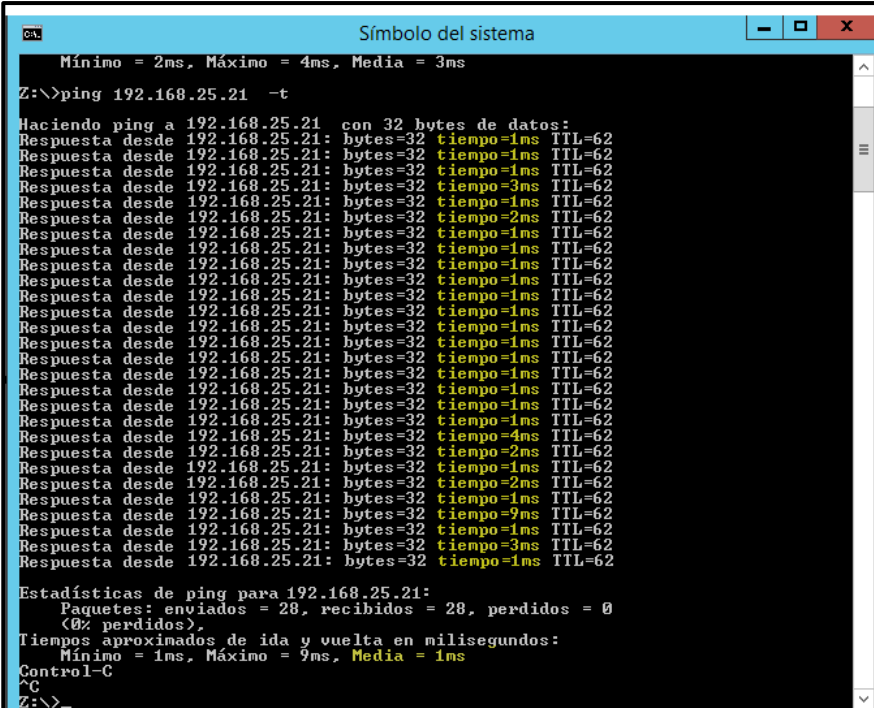
Fuente: Elaboración Propia,2021

Figura 176. Detalle de latencia de sistema antes de la ejecución del Proyecto:



Fuente: Elaboración Propia,2021

Figura 177. Detalle de latencia de sistema después de la ejecución del Proyecto:



```

C:\>
Mínimo = 2ms, Máximo = 4ms, Media = 3ms
Z:\>ping 192.168.25.21 -t
Haciendo ping a 192.168.25.21 con 32 bytes de datos:
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=3ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=2ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=4ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=2ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=2ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=9ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=3ms TTL=62
Respuesta desde 192.168.25.21: bytes=32 tiempo=1ms TTL=62
Estadísticas de ping para 192.168.25.21:
Paquetes: enviados = 28, recibidos = 28, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 1ms, Máximo = 9ms, Media = 1ms
Control-C
^C
Z:\>
```

Fuente: Elaboración Propia,2021

Compatibilidad de los equipos Instalados:

-Firewall Palo Alto 3050:

1.-Compatible con puertos físicos de red ethernet 10/100/1000 Base-T RJ45 ports con la cual funciona la solución para la interfaz física Wan donde se tiene implementada la red privada virtual site to client llamado Global Protect, adicional es compatible con 8 puertos SPF (small form-factor pluggable) disponibles para conexión de fibra óptica en un futuro cuando el cliente pueda contratar un enlace de mayor capacidad de ancho de banda cuando incremente el tamaño de su red.

-(12) puertos 10/100/1000, (8) puertos SFP ópticos Gigabit

2.-Compatible con el modo de funcionamiento de sus interfaces en capa 3 la cual se usa para la presente implementación.

El modo de uso de la interfaz de red en capa 3 permiten crear en el firewall múltiples redes de nivel 3 y encaminar los paquetes realizando Funciones de routing.

-Modo de operación de interfaces: L2, L3(capa 3), Tap, Virtual Wire (modo transparente)

3.-Compatibilidad de enrutamiento estático el cual se utiliza en la presente implementación para enrutar el acceso a los servicios de redes internas (LAN y DMZ) y el enrutar el acceso hacia internet por la interfaz WAN, también es compatible con otros tipos de enrutamiento como RIP, OSPF y BGP.

-Modos de routing compatibles: OSPF, RIP, BGP, estático

4.-Compatible con IPV6 para futuras migraciones a nivel de red.

En IPV6 soporta L2(capa2), L3(capa3), Tap, Virtual Wire (modo transparente) y funciones App-ID, User-ID, Content-ID, WildFire y descifrado SSL.

5.-Compatibilidad de red privada virtual tipo acceso remoto SSL llamado Global Protect el cual se utiliza en la presente implementación.

-Soporta Gateway GlobalProtect

-Soporta Portal GlobalProtect

-Compatibilidad de Transporte: IPSec con SSL fall-back

-Compatible con Autenticación: LDAP, Radius, SecurID, SAML o base de datos local

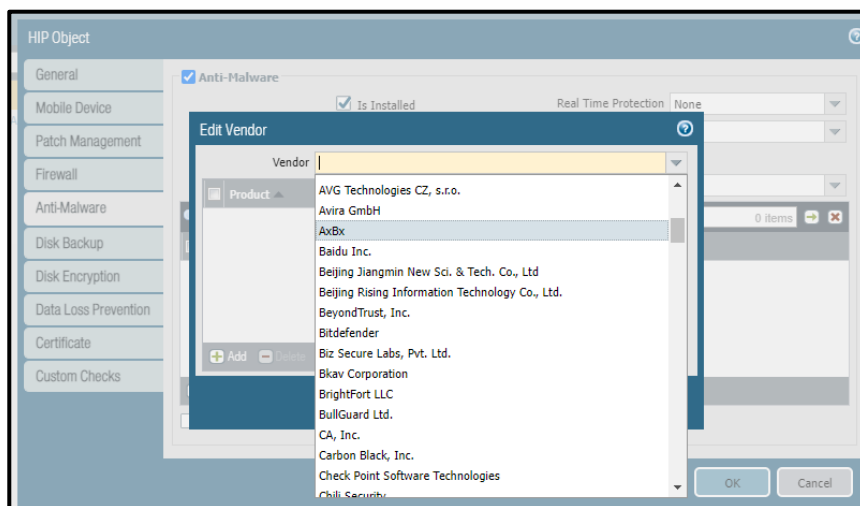
-Compatible con Sistemas operativos cliente: Mac OS X 10.6, 10.7 (32/64 bits), 10.8 (32/64 bits), Windows XP, Windows Vista (32/64 bits), Windows 7 (32/64 bits), Windows 10 (32/64 bits).

-Compatibilidad y Soporte de cliente de terceros: Apple iOS, Android 4.0 y posterior, VPNC IPSec para Linux

-HIP (host identification profile):

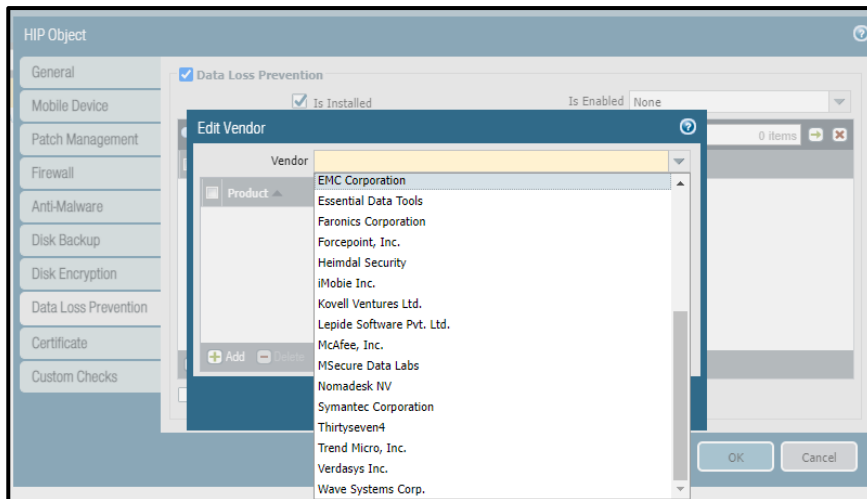
1.-Compatibilidad para recopilar información sobre el estado de seguridad de agentes endpoint de cualquier fabricante, por ejemplo, si tienen instalados los últimos parches de seguridad de cualquier fabricante, definiciones de antivirus, cifrado de disco, data loss prevention entre otros de cualquier fabricante.

Figura 178. Detalle 01 de compatibilidad de HIP profile con otros fabricantes.



Fuente: Elaboración Propia,2021

Figura 179. Detalle 02 de compatibilidad de HIP profile con otros fabricantes.



Fuente: Elaboración Propia,2021

Cisco Duo Security:

1.-Su aplicación duo mobile es compatible tanto para iPhone como para Android, así como para dispositivos portátiles como el Apple Watch.

Android: la versión actual de Duo Mobile es compatible con Android 7.0 y superior

iPhone: la versión actual de Duo Mobile es compatible con iOS 11.0 y superior.

2.-Compatible con varios tipos de métodos de doble factor, soporta los siguientes:

-SMS 2FA

-TOTP 2FA(The Time-Based One Time Password), es decir método 2FA de contraseña de un solo uso basada en el tiempo, TOTP es parte de la arquitectura de seguridad de autenticación abierta (OAUTH), La clave de seguridad es generalmente un código QR que el usuario escanea con su dispositivo móvil para generar una serie de números

-2FA basado en push, basado en push mejora el SMS y TOTP 2FA al agregar capas adicionales de seguridad, al tiempo que mejora la facilidad de uso para los usuarios finales.

-WebAuthn, WebAuthn (API de autenticación web) permite a terceros como Duo aprovechar las capacidades integradas en computadoras portátiles, teléfonos inteligentes y navegadores, lo que permite a los usuarios autenticarse rápidamente y con las herramientas que ya tienen a su alcance.

3.-Compatible con varios servicios para integrar el 2FA.

Duo es una solución ágil y flexible para el crecimiento de cualquier empresa, accesos a sistemas ERP, aplicaciones Office 365, también la flexibilidad de poder activar doble factor de autenticación para diversos servicios como VPN Netscaler Citrix, VPN SSL Global Protect entre otros de diferentes fabricantes.

4.-Para la integración de autenticación con el servidor AD es compatible con protocolos de autenticación LDAP y RADIUS.

5.-El servidor DUO Proxy para alojar la instalación del Proxy de autenticación Duo. El proxy es compatible con estos sistemas operativos:

- ✓ Windows Server 2012 o posterior (se recomienda Server 2016+)
- ✓ CentOS 7 o posterior (se recomienda CentOS 8+)
- ✓ Red Hat Enterprise Linux 7 o posterior (se recomienda RHEL 8+)
- ✓ Ubuntu 16.04 o posterior (se recomienda Ubuntu 18.04+)
- ✓ Debian 7 o posterior (se recomienda Debian 9+)

4.1.14. A continuación, muestro detalle de Protecciones eléctricas y disposición de energía eléctrica de soporte en caso de emergencias donde se encuentra instalado el equipo principal Firewall Palo Alto y el servidor Proxy Virtual en el ambiente de la data center de la empresa Privada.

Disposición de Protección de Energía Eléctrica e iluminación:

El data center y la infraestructura en general de la empresa privada recibe suministro de energía eléctrica de la empresa Luz del Sur.

Como sistema de energía alterno, en caso de interrupción de alimentación principal, el edificio cuenta con grupo electrógeno que permite la cobertura de energía del centro de datos (donde se encuentra los equipos de la solución implementada) y de iluminación de áreas comunes.

En los demás ambientes internos cuentan con circuito interno de iluminación de emergencia con sistema de carga independiente, cuya activación es automática en caso de ausencia de fluido eléctrico o una caída de tensión, a fin de posibilitar la evacuación de las áreas comunes del edificio cuentan con equipos de iluminación de emergencia (hall, escaleras y corredores).

Detalle de suministro eléctrico donde se encuentra la implementación:

El suministro eléctrico para el funcionamiento del proyecto se efectúa desde el banco de medidores en baja tensión 380 V, 3Ø, 60 Hz, el proyecto consta de un medidor para el tablero de distribución general y otro para el tablero general de bomba contra incendio.

Demanda Máxima: Los suministros eléctricos para la oficina 1401, desde la subestación hacia la distribución interna del piso 14, es un sistema 380V+N+T trifásico y de 60 Hz.

La potencia contratada para la oficina 1401, este suministro es de 111kW.

La acometida principal para la oficina 1401 es de 3-1x240mm² N2XOH + 1-1X240mm²(N) +1x50mm²(T), el cual llega al interior del centro de datos de la oficina.

Tableros Eléctricos:

El tablero de data center, está provisto de interruptores automáticos termomagnéticos del tipo de caja moldeada y del tipo de riel Din, son para montaje adosado, lleva una barra neutra y una barra de puesta a tierra, este tablero se ubica en el cuarto de data y deriva circuito de alumbrado, alimenta al tablero sub-tablero de energía ininterrumpida.

El sub-tablero de energía ininterrumpida (TSI), está provisto de interruptores termomagnéticos del tipo riel din. Cuenta con enclavamiento mecánico, lleva una barra neutra y una barra de puesta a tierra, este tablero deriva circuitos para gabinete de servidores, gabinete de cómputo 01, gabinete de computo02, central de alarma, panel de agente limpio, toma de control de acceso, y CCTV.

Alimentadores: Están constituidos por conductores con aislamiento de compuesto termoplástico no halogenado, instalados en tuberías de Conduit rígido del tipo EMT, para instalación adosada. El alimentador principal tiene aislamiento compuesto termoplástico no halogenado HFFR del tipo N2XOH,90°C.

Los alimentadores están calculados considerando:

-Demanda máxima continua.

-Máxima caída de tensión permisible < 4% (Caída de tensión en todo el circuito, que va desde la alimentación eléctrica hasta el punto final de la carga).

Distribución Eléctrica: De acuerdo con los requerimientos de la empresa privada se tiene lo siguiente:

Circuitos derivados de alumbrado y tomacorrientes: Circuito de alumbrado unipolares de 1x20A, conformados por conductores de 1-1x4mm² NH-80+1-1X4mm²(N)+1x25mm²(T), en tuberías del tipo EMT, para la instalación adosada y empotrada.

Circuitos de tomacorrientes unipolares de 1x20A, conformados por conductores de 1-1x4mm² NH-80+1-1X4mm²(N)+1x25mm²(T), en tuberías del tipo EMT, para la instalación adosada y empotrada los tomacorrientes son dobles con toma a tierra.

Circuitos derivados de alumbrado de emergencia: Circuito de alumbrado unipolares de 1x20A, conformados por conductores de 1-1x4mm² NH-80+1-1X4mm²(N)+1x25mm²(T), en tuberías del tipo EMT, para la instalación adosada y empotrada.

Circuitos derivados de tomacorrientes con suministro eléctrico de computadoras (estabilizado): circuitos de tomas estabilizadas unipolares de 1x20A, conformados por conductores de 1-1x4mm² NH-80+1-1X4mm²(N)+1x25mm²(T), en tuberías del tipo EMT, para la instalación adosada y empotrada los tomacorrientes son dobles con toma a tierra. Los tomacorrientes son del tipo dado y dobles, con salidas planas y conexión a tierra, capacidad 16 A , 250 V.

Figura 180. Detalle de pruebas eléctricas.

1.7. PRUEBAS ELECTRICAS

Se efectuaron pruebas de aislamiento de toda la instalación. También se realizaron pruebas de continuidad.

Prueba de Red Eléctrica

Antes de aplicar tensión al sistema se realizó la medición de resistencia de aislamiento de cada circuito, según se describe a continuación.

Cableado

Se realizó la medición de resistencia de fase a fase y de fase a tierra; esto requiere tres lecturas para circuito monofásicos, de acuerdo a lo siguiente:

A. La resistencia mínima de aislamiento de los tramos de la instalación eléctrica ubicados entre dos dispositivos de protección contra sobrecorriente; o a partir del último dispositivo de protección, los valores obtenidos fueron de no menor de 1000 Ohmios/voltio.

B. Las pruebas se realizaron con una tensión directa de 500V.

Resistencias de Aislamiento

Los valores mínimos permisibles para las resistencias de aislamiento entre cada 2 fases y entre cada fase y tierra, se muestran en la siguiente tabla:

Mínima resistencia de aislamiento para instalaciones

CODIGO NACIONAL DE ELECTRICIDAD - UTILIZACION TABLAS

Tabla 24
(Ver Regla 200-130)
Mínima resistencia de aislamiento para instalaciones

Tensión nominal de la instalación [V]	Tensión de ensayo en corriente continua [V]	Resistencia de aislamiento [MΩ]
Muy baja tensión de seguridad		
Muy baja tensión de protección	250	≥ 0,25
inferior o igual a 500 V, excepto las casas inteligentes	500	≥ 0,5
Superior a 500 V	1 000	≥ 1,0

Nota 1: Esta Tabla está cada para una instalación en la cual el conjunto de canalizaciones y cualquier sea el número de conductores que los componen, no excede de 100 m. Cuando no es posible el aislamiento de óhmico a 500 V a la tensión de ensayo se el valor de la resistencia de aislamiento de toda la instalación sea, que muestra el método que la comparación, inversamente proporcional a la longitud total de las canalizaciones.

Nota 2: Cuando los puntalones, interruptores, reláctores de abate u otros electrodomésticos se conectan a la instalación, o donde están, siempre han de tener un sistema de aislamiento.

Nota 3: Se debe tener como referencia las Normas Técnicas Peruanas correspondientes.

Excepción 1: Para instalaciones estantes se puede considerar la resistencia de aislamiento mínima de 1 000 Ω / V (por ejemplo: 220 kΩ a 220 V) si toda la corriente de fuga no deberá ser mayor de 1 mA a la tensión de 220 V. Si estos tramos tienen una longitud mayor a 100 m, la corriente de fuga se puede incrementar en 1 mA por cada 100 m de longitud o tramo adicional.

Excepción 2: Para instalaciones estantes en áreas que posean dispositivos y equipo a prueba de falla apropiados, se se requiere cumplir con la Excepción 1, pero la resistencia de aislamiento no debe ser menor de 500 Ω / V.

Fuente: Dossier de calidad Eléctrica de la empresa privada,2021

Figura 181. Certificado de Aterramiento.

CERTIFICADO DE ATERRAMIENTO EQUIPOS ELECTRÓNICOS

Por intermedio de la presente el Ing. Pedro Huarcaya Carhuas, con registro del Colegio de Ingenieros del Perú N° 151612, con registro de habilidad vigente y habilitado para ejercer la profesión, luego de ejecutar la conexión de la línea a tierra a la masa de los EQUIPOS ELECTRÓNICOS tales como Gabinetes de Comunicación, Servidores, Central de Alarma, Central de Control de acceso, instalados en el local donde está como locatario SECURESOFT CORPORATION S.A.C., con cable LSOH-80 calibre 2.5mm2, conector tipo Ojal de Cu 2.5mm2 y cumpliendo con lo exigido en las secciones 060-002 del CNE – Utilización así como también en lo descrito en las secciones 3.6.14.5 y 4.1.1.8 del CNE – Tomo V, garantizo mediante el protocolo correspondiente, su funcionalidad para lo cual ha sido diseñado el sistema de puesta a tierra, las cuales se encuentran instaladas en el LOCAL SECURESOFT (OFICINA SECURESFT – PLUS OLGUIN – 14° PISO – OFICINA 1401), ubicado en Av. Manuel Olguin 327, piso 14, oficina 1401, distrito de Santiago de Surco.

Fuente: Certificado de aterramiento de la empresa privada,2021

Figura 182. Disposición 01 de energía eléctrica de soporte en caso de emergencias

PLAN DE SEGURIDAD

ANEXO N° 10.

PROCEDIMIENTOS PARA CORTE INESPERADO DE ENERGIA ELÉCTRICA

Los cortes de energía eléctrica producto de la actividad de la propia naturaleza (sismos, inundaciones, etc.), acciones tendenciosas, causas de fuerza mayor (para realizar obras de mantenimiento), descuidos (desperfectos, caídas de cable y/o torres) o negligencia de la empresa que suministra este tipo de servicio público, originan cuantiosas pérdidas en comercios, industrias, servicios, negocios, etc.; de igual forma, causan zozobra e inseguridad en las personas y también son circunstancias propicias para la comisión de delitos de diversa índole en el interior de las instalaciones, como en la vía pública.

Miles de empresas tienen que suspender sus actividades durante unas horas al día, con el consiguiente impacto sobre la economía del país.

Bajo este panorama la suspensión del suministro de energía, es un riesgo que debe preocuparnos para adoptar las medidas más convenientes a fin de minimizar las consecuencias expresadas.

Para casos de corte, el edificio cuenta con apoyo de un grupo electrógeno de reserva de capacidad de abastecer energía a las áreas necesarias, producción e interiores de las oficinas.

CONCEPTOS BASICOS:

- **Conexión a Tierra:** Sistema que se utiliza para enviar una descarga eléctrica hacia el suelo y así esta no pueda dañar elementos conectados a un sistema de abastecimiento de corriente, se utiliza en caso de rayos y descargas de estática por movimiento.
- **Corto Circuito:** Corto que se produce accidentalmente por el contacto directo entre dos polos de energía opuesta y que suele generar una descarga brusca.
- **Conectores:** Elementos usados en sistemas eléctricos y sirven para conectar y conformar un sistema de suministro de energía.
- **Conductores eléctricos:** elementos por donde transita la corriente eléctrica en diferentes polaridades y cargas electrónicas.
- **Transformador:** Elemento que sirve para cambiar un tipo de corriente, elevándola o disminuyéndola de potencia. Elevación o disminución de voltaje.

Fuente: Plan de Seguridad de la empresa privada,2021

Figura 183. Disposición 02 de energía eléctrica de soporte en caso de emergencias

<p>Procedimientos:</p> <p>ANTES</p> <p>Aunque los cortes generalmente provienen del exterior, es probable que internamente las podamos producir, aunque sea momentáneamente. A continuación se describen unas recomendaciones preventivas.</p> <ul style="list-style-type: none">▪ Dar cumplimiento al programa de mantenimiento del circuito de electrificación de las instalaciones (revisión de tableros, cajas, conductores, tomacorrientes, interruptores y conectores).▪ El área de Mantenimiento, periódicamente debe:<ul style="list-style-type: none">➢ Verificar la instalación, operatividad y mantenimiento del pozo tierra y/o solicitar los protocolos de operatividad.➢ Determinar la capacidad de operatividad de los cables eléctricos a fin de establecer la continuidad del trabajo de estos con relación a los equipos y maquinarias instaladas.➢ Utilizar conductores específicos para el tipo y cantidad de energía.➢ Utilizar material para sistemas eléctricos normados por el Código Nacional de Electricidad.➢ Verificar que no se sobrecarguen los tomacorrientes. No se debe conectar varios enchufes en un solo tomacorriente.➢ Verificar que no existan conductores eléctricos en malas condiciones o sin la protección adecuada (pelados y expuestos)➢ Verificar el funcionamiento de las luces de emergencia.➢ Constatar que no existan conexiones no autorizadas▪ Tener a la mano el directorio telefónico de emergencia.▪ Dictar una charla al personal sobre los riesgos eléctricos y medidas a adoptar. <p>DURANTE</p> <ul style="list-style-type: none">▪ No desesperarse, si hay corte se encenderán las luces de emergencia y unos instantes después el grupo electrógeno.▪ Permanecer en el lugar▪ Cuidar los efectos personales y el patrimonio de la empresa, sobre todo los más valiosos.▪ En el caso de las PC o laptop proceder de acuerdo a indicaciones del proveedor, descritas en el manual de operaciones del fabricante.▪ Desconectar aquellos artefactos o equipos energizados que sean pertinentes.▪ Comunicar a la Gerencia, en caso el corte sea parcial.▪ Los brigadistas estarán atentos a propiciar que se mantenga la calma en los ambientes. Prestarán auxilio que corresponda.

Fuente: Plan de Seguridad de la empresa privada,2021

Figura 184. Disposición 03 de energía eléctrica de soporte en caso de emergencias

<ul style="list-style-type: none">▪ En caso de accidente:<ul style="list-style-type: none">➢ Separar a la víctima del punto de contacto con la electricidad, desconectando la energía eléctrica. Por ningún motivo tocar al accidentado mientras se encuentre en contacto con la corriente.➢ Proporcionarle respiración pulmonar o reanimación cardiopulmonar, si el caso lo amerita.➢ Trasladarlo o llamar a emergencias del hospital o clínica más cercana, e indicar que se trata de un herido por descarga eléctrica. <p>DESPUÉS</p> <ul style="list-style-type: none">▪ Inmediatamente después del corte de energía el área de mantenimiento tomará acciones para tratar de volver a la situación de normalidad.▪ Una vez que ha retomado la energía encender artefactos que fueron desconectados.▪ Verificar el estado normal de los recursos bajo su responsabilidad.▪ El área de Mantenimiento elaborará un informe al respecto de las causas y procedimientos efectuados.▪ El servicio de seguridad debe registrar el incidente para el histórico de antecedentes.
--

Fuente: Plan de Seguridad de la empresa privada,2021

4.1.Presupuesto

En la presente etapa se evalúa todos los costos empleados para el desarrollo del presente proyecto las cuales fueron necesarios para culminar la implementación satisfactoriamente, los flujos de costos serán presentados en tablas de precios, considerar que esta información se encuentra también disponible en la fase de planificación en el Plan de Gestión Financiera.

Detalle de Egresos

Tabla 24. Planilla mensual del personal

PUESTO DE TRABAJO	PLANILLA MENSUAL \$
Gerente de Proyecto	1,800
Jefe del Proyecto	1,500
Implementador	1,200
Analista de Soporte	500
Gerente Comercial	1,800
Gerente Financiero	1,800

Fuente: Elaboración Propia,2021

Figura 185. Costo de Personal por asignación de trabajo

% DE ASIGNACION PERSONAL DE PROYECTO Implementación de 2FA y control de acceso de dispositivo							
Fecha de ultima actualización:		16/08/2021					
Moneda:		Dolares		Utilización Mensual de Personal por %			
Total Costo Personal:		1,826.43		TC:			
						1	2
DETALLE	Nro	PUESTOS DE TRABAJO	COSTO	ESTUDIOS	TOTAL	Julio-21	Agosto-21
PERSONAL	1	Gerente de Proyecto	673.32		40.40	2%	2%
PERSONAL	2	Jefe del Proyecto	561.10		392.77	30%	30%
PERSONAL	3	Implementador	503.74		957.11	80%	80%
PERSONAL	4	Analista de Soporte	187.03		355.36	80%	80%
PERSONAL	5	Gerente Comercial	673.32		40.40	2%	2%
PERSONAL	6	Gerente Financiero	673.32		40.40	2%	2%

Fuente: Elaboración Propia,2021

Figura 186. Costos de Servicios y Consumibles del proyecto

COSTOS VALOR AGREGADO DEL PROYECTO Implementación de 2FA y control de acceso de dispositivo												
Fecha de ultima actualización:		16/08/2021		INSERTAR FILAS								
Moneda:		Dolares										
Costo Bienes y Servicios:		12,771.80		4.01								
Descripción	PROVEEDOR	#TI	TIPO DE ITEM	CONDICIÓN DE CUOT	CANTIDAD ITEM	CANTIDAD de CUOTA	Moneda	Costo U	COSTO MENSU	MES INICIC	#MESES PAG	TOTAL
HABILITACION DEL PERSONAL									0.00			
Prueba Covid	Rimac	D	SERVICIO	UNICO	4	1	Dolares	40.00	160.00	1	0	160.00
SCTR - SALUD (Mediano Riesgo)	Rimac	D	SERVICIO	UNICO	2	1	Dolares	30.00	60.00	1	0	60.00
SCTR - PENSION (Mediano Riesgo)	Rimac	D	SERVICIO	UNICO	2	1	Dolares	30.80	61.80	1	0	61.80
EQUIPOS DE PROTECCION PERSONAL # UNIFORMES									0.00			
Mascarilla,guantes,protector facial	Sodimac	D	CONSUMIBLE	UNICO	16	1	Dolares	40.00	640.00	1	0	640.00
Maletin de herramienta Soporte Microinformatico	Sodimac	D	BIEN	UNICO	2	1	Dolares	80.00	160.00	1	0	160.00
Utiles de oficina	Sodimac	D	CONSUMIBLE	UNICO	1	1	Dolares	50.00	50.00	1	0	50.00
TELEFONÍA-INTERNET									0.00			
Servicio Datos « 2 meses	Servicios	D	SERVICIO	UNICO	2	1	Dolares	300.00	600.00	1	0	600.00
OTROS									0.00			
Insumos / Consumibles / Refrigerios	Servicios	D	CONSUMIBLE	UNICO	2	1	Dolares	80.00	160.00	1	0	160.00
EPP	Servicios	D	CONSUMIBLE	UNICO	2	1	Dolares	40.00	80.00	1	0	80.00
Movilidad	Servicios	D	SERVICIO	UNICO	1	1	Dolares	300.00	300.00	1	0	300.00
Licenciamiento Palo Alto y Cisco por 12 meses	Servicios	D	SERVICIO	UNICO	1	1	Dolares	10,000.00	10,000.00	1	0	10,000.00
Caja chica # Contingencia	Servicios	D	SERVICIO	UNICO	1	1	Dolares	500.00	500.00	1	0	500.00

Fuente: Elaboración Propia,2021

3.2.3.2 Detalle de Ingresos

Tabla 25. Detalle de ingresos del proyecto

Descripción	Tipo	Marca	Precio (\$)
Standard Cisco Duo 2FA edition	Licencia	CISCO	3,800.00
GlobalProtect subscription for device in an HA pair year 1, PA-850 - Fecha de inicio 01/06/21	Licencia	Palo Alto	4,800.00
Servicio de implementación de la solución.	IMPLEMENTACION	Servicios	7,000.00
Soporte de la solución por 3 meses	SOPORTE	Servicios	2,000.00
Capacitación remota de la solución - 04 horas	CAPACITACIÓN	Servicios	300.00
Gestión del proyecto	PROYECTOS	Servicios	3,100.00
Precio Total (\$)			21,000.00

Fuente: Elaboración Propia,2021

3.2.3.3 Flujo de Caja de Proyecto

A continuación, se presenta el flujo de caja:

Figura 187. Flujo de Caja del Proyecto

Concepto	Totales Dolares	VPN Dolares	%	1	2
				Jul-21	Ago-21
Ingresos	21,000.00	20,934.84	100.00%	15,000	6,000
Fijos	21,000.00	20,707.50		15000	6000
Variables	-	0.00			
Egresos	14,162.08	13,997.28	67.44%	13,357	585
Personal sueldo	1,390.28	1,364.18	9.82%	584.79	584.79
Personal bono	-	0.00	0.00%	-	-
Personal movilidad	-	0.00	0.00%	-	-
Bienes	160.00	158.26	1.13%	160.00	-
Servicios	11,681.80	11,554.94	82.49%	11,681.80	-
Arrendamiento	-	0.00	0.00%	-	-
Capex	-	0.00	0.00%	-	-
Consumibles	930.00	919.90	6.57%	930.00	-
Valor agregado	-	0.00	0.00%	-	-
Costo financiero	-	0.00	0.00%	-	-
Utilidad de Proyecto	6,837.92	6,937.56	32.56%	1,643	5,415
Contingencia	-	-	0.00%	-	-
Gestión del Servicio	-	-	0.00%	-	-
Utilidad bruta	6,837.92	6,937.56	32.56%	1,643	5,415
Utilidad bruta acumulada				1,643	7,059
% Utilidad Bruta Acumulada				11.0%	33.6%

Fuente: Elaboración Propia,2021

CONCLUSIONES

Con la implementación realizada permitió mejorar el proceso de autenticación de acceso remoto de todos los colaboradores, debido a que se evidencia que anteriormente contaba con el uso un simple mecanismo de autenticación de usuario y contraseña y en la actualidad con la nueva implementación en operación ya cuenta con un mecanismo adicional de validación de identificación de conexión de usuario el cual es un mecanismo de doble factor de autenticación implementado, gracias a la implementación los colaboradores ya no sufrirán suplantación de identidad debido a que existe una doble validación de identidad de usuario logrando cumplir el objetivo en mejorar el proceso de autenticación de los usuarios.

Gracias a la implementación realizada permitió mejorar el proceso de control de acceso de los diferentes dispositivos que se conectan de forma remota debido a que anteriormente los usuarios podían conectarse desde cualquier dispositivo incluso dispositivos que no tienen ningún control de protección como un antimalware o antivirus instalado y activo, una vez en operación la implementación de la nueva solución logró asegurar que sólo los dispositivos autorizados y que tienen y cumplen un control de protección con un alto nivel de seguridad informática cumpliendo con el perfil técnico de acceso lograrán ingresar al acceso remoto y a los recursos de la empresa privada de forma muy segura.

La presente implementación permitió robustecer los mecanismos de acceso remoto la cual consistió en agregar dos controles adicionales de acceso remoto el cual es el doble factor de autenticación y el control de acceso de dispositivo usando protocolos de autenticación muy seguros como SSL , TLS y un cifrado de información de un alto nivel como el SHA 512 la cual permite estar mucho más seguros al momento de autenticarnos, conectarnos y transmitir la información de forma remota muy segura a los recursos internos de la empresa logrando mitigar cualquier tipo de incidente de seguridad que se presenta diariamente como también disminuir a gran escala el riesgo de alguna suplantación de identidad y otros riesgos de seguridad informática.

RECOMENDACIONES

En relación a la implementación realizada sobre la nueva solución de acceso remoto con doble factor de autenticación y control de acceso de dispositivo se recomienda validar y realizar la actualización de sistema operativo de forma trimestral del firewall Palo Alto la cual es el equipo donde se encuentra la nueva solución implementada, la actualización de sistema operativo PAN-OS debe ejecutarse en una ventana de trabajo programa con finalidad de no afectar el acceso y conexión de acceso remoto a los usuarios durante el horario productivo considerando que es necesaria debido a las vulnerabilidades que usualmente registran y son notificados por varios fabricantes tecnológicos.

Se recomienda evaluar la adquisición de un enlace de internet adicional de otro proveedor para contar con un enlace secundario como contingencia y poder replicar la configuración de la VPN en otro Gateway con otro proveedor de internet esto nos serviría para que en caso alguna caída de servicio del proveedor de internet el servicio pueda mantenerse operativo mediante la VPN con el Gateway de contingencia usando otro proveedor de internet, considerar que la ip pública debe configurarse en otra de las interfaces disponibles del firewall Palo Alto debido a que si existe disponibilidad de interfaz de red y es viable su implementación.

Se recomienda que la solución implementada de acceso remoto con doble factor de autenticación y control de acceso de dispositivo debe mantenerse de forma dedicada en el Firewall Palo Alto 3050, considerar no incluir otro servicio en el Firewall Palo Alto la cual es un equipo dedicado para el servicio de acceso remoto, considerar que para otros servicios se encuentra el firewall Principal Checkpoint en donde se tienen publicaciones WEB, servicios FTP, navegación de internet entre otros servicios, no se recomienda agregar otros servicios al Firewall Palo Alto dedicado a la nueva implementación debido a que puede generar un incremento elevado de recursos como CPU, memoria y disco duro con la cual podría saturar la performance del equipo permitiendo generar indisponibilidad en el acceso remoto.

Se recomienda configurar el envío de eventos de seguridad desde el Firewall Palo Alto a un SIEM (Security Information and Event Management) para que un equipo especializado como un SOC (Centro de operaciones de seguridad) revise algún evento de salud del Firewall o algún tráfico o evento anómalo de las conexiones de la nueva solución implementada a la cual se pueda realizar algún análisis más amplio y poder determinar algún tratamiento, el firewall Palo Alto tienen la capacidad de soportar la configuración de reenvíos de eventos de sistema y seguridad a un SIEM utilizando el protocolo syslog.

BIBLIOGRAFÍAS

Palo Alto Networks. (2021). *Guía de Administración PAN-OS Palo Alto Networks*.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin.html>

Cisco Netacad. (2021). *CCNAv7: Switching, Routing, and Wireless Essentials*. <https://www.netacad.com/es>

Cisco Netacad. (2021). *CCNAv7: Introduction to Networks*. <https://www.netacad.com/es>

Cisco Duo Security. (2021). *Guía para la autenticación de dos factores*. <https://guide.duo.com/>

Cisco Duo Security. (2021). *Authentication Proxy – Reference*. <https://duo.com/docs/authproxy-reference>

Palo Alto Networks. (2021). *Configure MFA Between Duo and the Firewall*.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/configure-multi-factor-authentication/configure-mfa-between-duo-and-the-firewall.html>

Gil, M. (2014). Redes Privadas Virtuales, tipos y características. *TELDAT Blog*.

<https://www.teldat.com/blog/es/virtual-private-networks-types-and-characteristics/>

ARIEL, M. (2020). La historia de la VPN. *Infosertec*.

<https://infosertecla.com/2020/01/29/la-historia-de-la-vpn/>

Gillis, A. S. (2021). Red privada virtual o VPN. *TechTarget*.

<https://searchdatacenter.techtarget.com/es/definicion/Red-privada-virtual-VPN>

A3sides. (2020). *Qué es el doble factor de autenticación y para qué sirve*.


<https://www.a3sides.es/blog/que-es-doble-factor-autenticacion/>

Palo Alto Networks. (2019). *Para empezar: VPN*.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CISYCA0&lang=es%E2%80%A9>

ANEXOS

ANEXO 1: Datasheet Firewall Palo Alto 3050



PA-3000 SERIES

Los cortafuegos de nueva generación de la serie PA-3000 Series de Palo Alto Networks, que incluye los modelos PA-3060, PA-3050 y PA-3020, están concebidos para implementaciones de puertas de enlace a Internet de alta velocidad. Los dispositivos de la serie PA-3000 Series controlan los flujos de tráfico en la red mediante procesamiento y memoria dedicados para redes, seguridad, gestión y prevención de amenazas.

Principales funciones de seguridad

Clasifica todas las aplicaciones, en todos los puertos, en todo momento


- Identifica la aplicación, independientemente del puerto, el cifrado SSL/SSH o la técnica evasiva empleada.
- Utiliza la aplicación, no el puerto, como base para todas las decisiones de habilitación segura de políticas: permitir, denegar, programar, inspeccionar y aplicar la catalogación del tráfico.
- Organiza en categorías las aplicaciones no identificadas para el control de políticas, la investigación forense de amenazas o el desarrollo de la tecnología App-ID™.

Aplica políticas de seguridad para cualquier usuario y en cualquier ubicación

- Implementa políticas coherentes a usuarios locales y remotos que trabajan en plataformas de Windows®, macOS®, Linux, Android® o Apple iOS.
- Permite la integración sin agentes de Microsoft Active Directory® y Terminal Services, LDAP, Novell eDirectory™ y Citrix
- Integra de forma fácil sus políticas de cortafuegos con el estándar 802.1X para redes inalámbricas, los proxies, el control de acceso a la red y cualquier otra fuente de información sobre la identidad del usuario.

Previene contra las amenazas conocidas y desconocidas

- Bloquea una serie de amenazas conocidas (como exploits, malware y spyware) en todos los puertos, independientemente de las tácticas habituales de evasión de amenazas utilizadas.
- Limita la transferencia no autorizada de archivos y datos confidenciales y permite la navegación segura por sitios web no relacionados con el trabajo.
- Identifica el malware desconocido, lo analiza basándose en cientos de comportamientos maliciosos y, a continuación, crea y aplica automáticamente la protección.



El elemento de control de la serie PA-3000 Series es PAN-OS®, que clasifica de forma nativa todo el tráfico (incluido el tráfico de aplicaciones, amenazas y contenido) y lo vincula al usuario, independientemente de su ubicación o del tipo de dispositivo que utilice. La aplicación, el contenido y el usuario —o, lo que es lo mismo, los elementos que hacen funcionar su empresa— sirven como base para sus políticas de seguridad, lo que se traduce en una mejora de la estrategia de seguridad y una reducción del tiempo de respuesta ante incidentes.

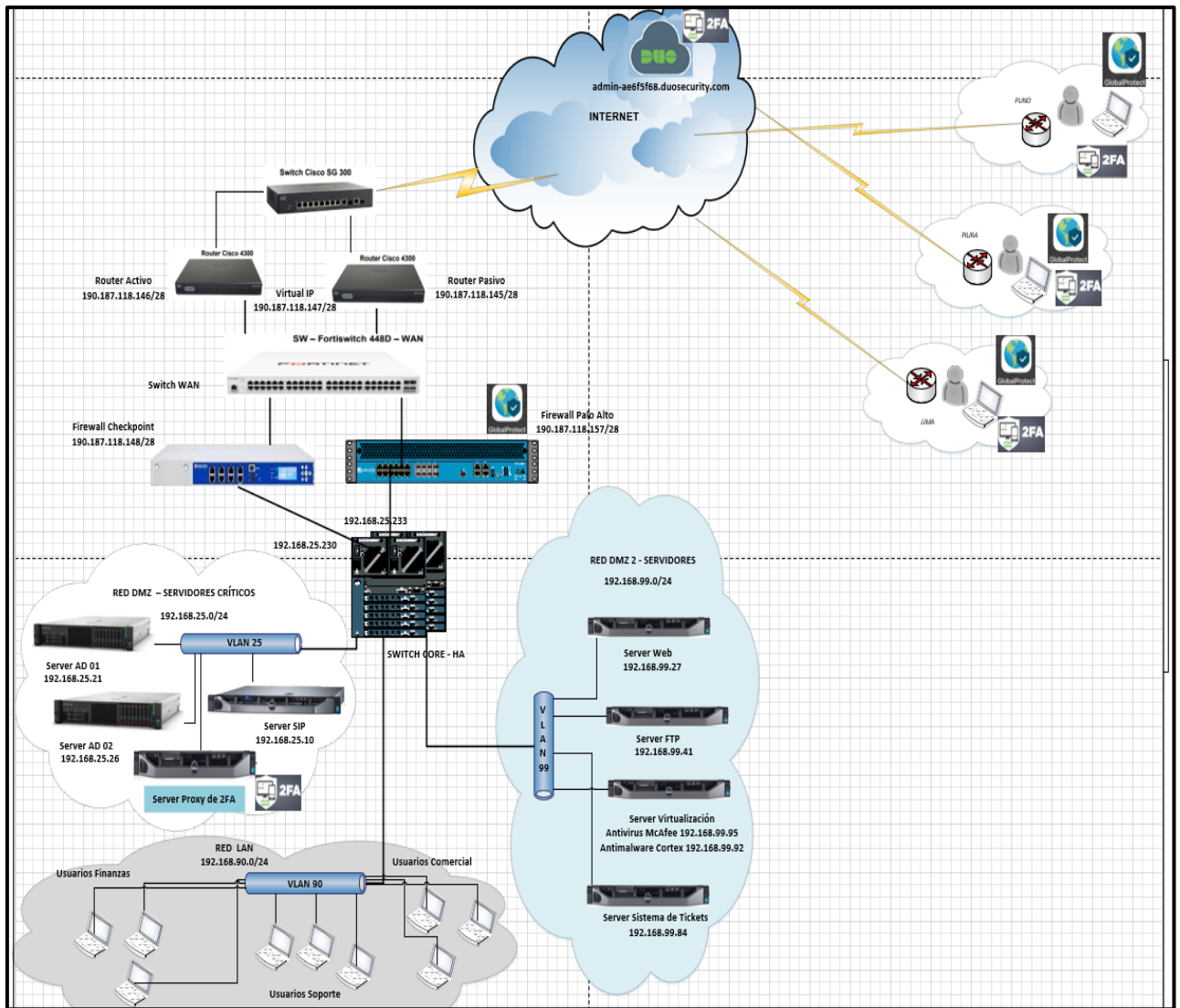
Rendimiento y capacidad	PA-3050	PA-3060	PA-3020
Rendimiento del cortafuegos ¹	4 Gbps	4 Gbps	2 Gbps
Rendimiento de Threat Prevention ²	2 Gbps	2 Gbps	1 Gbps
Rendimiento de VPN IPsec ³	500 Mbps	500 Mbps	500 Mbps
Nuevas sesiones por Segundo ⁴	50 000	50 000	50 000
Número máximo de sesiones	500 000	500 000	250 000
Sistemas virtuales (base/máx.) ⁵	1/6	1/6	1/6

1. El rendimiento del cortafuegos se calcula con App-ID y la creación de logs activados usando transacciones HTTP/combinación de aplicaciones de 64 kB.
 2. El rendimiento de Threat Prevention se calcula con App-ID, IPS, antivirus, antispymware, WildFire y la creación de logs activados usando transacciones HTTP/combinación de aplicaciones de 64 kB.
 3. El rendimiento de VPN IPsec se calcula con transacciones HTTP de 64 kB.
 4. El cálculo de las nuevas sesiones por segundo se realiza con cancelación de aplicaciones usando transacciones HTTP de 1 byte.
 5. Para añadir sistemas virtuales a la cantidad base, es preciso adquirir una licencia por separado.

Palo Alto Networks | PA-3000 Series | Datasheet
1

Fuente : Palo Alto Networks , 2021

ANEXO 2: Diagrama de red final de la nueva solución.



Fuente : Elaboración Propia , 2021

ANEXO 3: Especificaciones técnicas de Hardware y Red del Firewall Palo Alto 3050

<p>ESPECIFICACIONES DEL HARDWARE</p> <p>E/S</p> <ul style="list-style-type: none">• (12) 10/100/1000, (8) puertos SFP ópticos Gigabit <p>GESTIÓN DE E/S</p> <ul style="list-style-type: none">• (1) puerto de administración fuera de banda 10/100/1000, (2) alta disponibilidad 10/100/1000, (1) puerto de consola RJ-45 <p>CAPACIDAD DE ALMACENAMIENTO</p> <ul style="list-style-type: none">• Unidad de estado sólido (SSD) de 120 GB <p>FUENTE DE ALIMENTACIÓN (CONSUMO ELÉCTRICO MEDIO/MÁXIMO)</p> <ul style="list-style-type: none">• 250 W (150 / 200) <p>BTU/H MÁXIMO</p> <ul style="list-style-type: none">• 683 <p>VOLTAJE DE ENTRADA (FRECUENCIA DE ENTRADA)</p> <ul style="list-style-type: none">• 100-240 VAC (50-60 Hz) <p>CONSUMO MÁXIMO DE CORRIENTE</p> <ul style="list-style-type: none">• 2A a 100 VAC	<p>PREPARADO PARA MONTAJE EN BASTIDOR (DIMENSIONES)</p> <ul style="list-style-type: none">• 1U, bastidor estándar de 19" (4,45 x 43,18 x 43,18 cm – 1,75 x 17 x 16.75 pulgadas) <p>DIMENSIONES (SOLO DISPOSITIVO/DISPOSITIVO PREPARADO PARA ENVÍO)</p> <ul style="list-style-type: none">• 6,8 Kg / 9,07 Kg <p>SEGURIDAD</p> <ul style="list-style-type: none">• UL, CUL, CB <p>INTERFERENCIA ELECTROMAGNÉTICA</p> <ul style="list-style-type: none">• Clase A de FCC, Clase A de CE, Clase A de VCCI, TUV <p>CERTIFICACIONES</p> <ul style="list-style-type: none">• ICSA <p>ENTORNO</p> <ul style="list-style-type: none">• Temperatura de funcionamiento: De 0 a 50 °C (de 32 a 122 °F)• Temperatura de almacenamiento: De -20 a 70 °C (de -4 a 158 °F)
<p>CONEXIÓN A RED</p> <p>MODOS DE LOS INTERFACES</p> <ul style="list-style-type: none">• L2, L3, Tap, Virtual Wire (modo transparente) <p>ENRUTAMIENTO</p> <ul style="list-style-type: none">• Modos: OSPF, RIP, BGP, estático• Tamaño de la tabla de reenvío (entradas por dispositivo/por VR): 5.000/2.500 (PA-3050), 2.500/2.500 (PA-3020)• Reenvío basado en políticas• Protocolo punto a punto sobre Ethernet (PPPoE)• Tramas Jumbo: tamaño máximo de trama de 9.210 bytes• Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, y v3 <p>ALTA DISPONIBILIDAD</p> <ul style="list-style-type: none">• Modos: Activo/Activo, Activo/Pasivo• Detección de fallos: monitorización de ruta, monitorización de interfaz <p>ASIGNACIÓN DE DIRECCIONES</p> <ul style="list-style-type: none">• Asignación de direcciones por dispositivo: cliente DHCP/PPPoE/Estática• Asignación de direcciones por usuarios: servidor DHCP/Relay DHCP/Estática <p>IPV6</p> <ul style="list-style-type: none">• L2, L3, Tap, Virtual Wire (modo transparente)• Funciones: App-ID, User-ID, Content-ID, WildFire y descifrado SSL	<p>VLAN</p> <ul style="list-style-type: none">• Etiquetas VLAN 802.1q por dispositivo / por interfaz: 4,094/4,094• Número máximo de interfaces: 2.048 (PA-3050), 1.024 (PA-3020)• Interfaces de agregado (802.3ad) <p>NAT/PAT</p> <ul style="list-style-type: none">• Número máximo de reglas NAT: 1.000• Número máximo de reglas NAT (DIPP): 200• Intervalo de direcciones IP y puertos dinámicos: 254• Intervalo de direcciones IP dinámicas: 16,234• Modos NAT: NAT 1:1, NAT n:n, NAT m:n• Sobresuscripción DIPP (direcciones IP de destino único por dirección IP y puerto de origen): 2• NAT64 <p>VIRTUAL WIRE</p> <ul style="list-style-type: none">• Número máximo de Virtual Wires: 10• Tipos de interfaz asignados a Virtual Wires: físicos y subinterfaces <p>REENVÍO DE NIVEL 2</p> <ul style="list-style-type: none">• Tamaño de tabla ARP por dispositivo: 2.500 (PA-3050), 1500 (PA-3020)• Tamaño de tabla MAC por dispositivo: 2.500 (PA-3050), 1500 (PA-3020)• Tamaño de tabla de vecino de IPV6: 2.500 (PA-3050), 1500 (PA-3020)

Fuente : Palo Alto Networks , 2021

ANEXO 4: Especificaciones técnicas de seguridad del Firewall Palo Alto 3050

<p>SEGURIDAD</p> <p>FIREWALL</p> <ul style="list-style-type: none">• Control de las aplicaciones, los usuarios y los contenidos basado en políticas• Protección de paquetes fragmentados• Protección de escaneos de reconocimiento• Protección frente a denegación de servicio (DoS) y denegación de servicio distribuido (DDoS)• Descifrado: SSL (entrante y saliente), SSH <p>WILDFIRE</p> <ul style="list-style-type: none">• Identifica y analiza archivos específicos y desconocidos pudiendo reconocer más de 100 conductas maliciosas.• Genera y ofrece una protección automática contra malware recién descubierto a través de actualizaciones de firmas.• Distribución de actualizaciones de firmas en menos de 1 hora. Logging y generación de informes integrado. Acceso a la API de WildFire para el envío programado de hasta 100 muestras al día y de hasta 250 consultas al día de informes por archivo hash (se requiere suscripción). <p>FILTRADO DE ARCHIVOS Y DATOS</p> <ul style="list-style-type: none">• Transferencia de archivos: control bidireccional sobre más de 60 tipos de archivo únicos• Transferencia de datos: control bidireccional sobre la transferencia no autorizada de números de tarjetas de crédito y seguridad social• Protección contra descargas "drive-by download" <p>INTEGRACIÓN DE USUARIOS (USER-ID)</p> <ul style="list-style-type: none">• Microsoft Active Directory, Novell eDirectory, Sun One y otros directorios basados en LDAP• Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010• Microsoft Terminal Services, Citrix XenApp• API XML para facilitar la integración con repositorios de usuario no estándar <p>VPN IPSEC (SITE-TO-SITE)</p> <ul style="list-style-type: none">• Intercambio de claves: clave manual, IKE v1• Cifrado: 3DES, AES (128 bits, 192 bits, 256 bits)• Autenticación: MD5, SHA-1, SHA-256, SHA-384, SHA-512• Creación de túneles VPN dinámicos (GlobalProtect)	<p>PREVENCIÓN DE AMENAZAS (SE REQUIERE SUSCRIPCIÓN)</p> <ul style="list-style-type: none">• Protección contra exploits de vulnerabilidades del sistema operativo y de aplicaciones• Protección basada en flujos contra virus, spyware y gusanos (incluidos los incrustados en HTML, Javascript, archivos PDF y archivos comprimidos) <p>FILTRADO DE URL (SE REQUIERE SUSCRIPCIÓN)</p> <ul style="list-style-type: none">• Categorías de URL predefinidas y personalizadas• Memoria caché para las URL a las que se ha accedido recientemente• Categorías de URL como parte del criterio de coincidencia de las políticas de seguridad• Información del tiempo de navegación <p>CALIDAD DEL SERVICIO (QOS)</p> <ul style="list-style-type: none">• Control del tráfico basado en políticas por aplicación, usuario, origen, destino, interfaz, túnel de VPN IPsec, etc.• 8 clases de tráfico con parámetros de ancho de banda garantizado, máximo y prioritario• Supervisión de ancho de banda en tiempo real• Por marcado de Diffserv de política• Interfaces físicas compatibles con QoS: 6 <p>VPN/ACCESO REMOTO SSL (GLOBALPROTECT)</p> <ul style="list-style-type: none">• Gateway GlobalProtect• Portal GlobalProtect• Transporte: IPsec con SSL fall-back• Autenticación: LDAP, SecurID o base de datos local• Sistema operativo cliente: Mac OS X 10.6, 10.7 (32/64 bits), 10.8 (32/64 bits), Windows XP, Windows Vista (32/64 bits), Windows 7 (32/64 bits)• Soporte de cliente de terceros: Apple iOS, Android 4.0 y posterior, VPNC IPsec para Linux <p>ADMINISTRACIÓN, GENERACIÓN DE INFORMES, HERRAMIENTAS DE VISIBILIDAD</p> <ul style="list-style-type: none">• Interfaz web integrada, CLI o administración central (Panorama)• Interfaz de usuario en varios idiomas• Syslog, Netflow v9 y SNMP v2/v3• REST API basada en XML• Resumen gráfico de aplicaciones, categorías de URL, amenazas y datos (ACC)• Visualizar, filtrar y exportar tráfico, amenazas, WildFire, URL y registros de filtrado de datos• Generación de informes totalmente personalizable
---	--

Fuente : Palo Alto Networks , 2021